ON THE INVERSE PROBLEM OF GALOIS THEORY

BY

J. KOVACIC⁽¹⁾

ABSTRACT. Let k be a field, F a finite subfield and G a connected solvable algebraic matrix group defined over F . Conditions on G and k are given which ensure the existence of a Galois extension of k with group isomorphic to the F -rational points of G .

Introduction. A natural question in Galois theory is the question of the existence of a Galois extension of a given field whose Galois group is isomorphic to a given group. Shafarevich [10] has solved this so-called inverse problem for solvable groups over an algebraic number field. Here we consider solvable groups over fields of characteristic $p > 0$.

Let k be a given field and F a finite field contained in k . Then, for any algebraic group G defined over F , G_F is a finite group and we may ask for a (separable) Galois extension K of k whose Galois group is isomorphic to G_F . We call the set of such extensions $E_k(G_F)$. If G is a connected solvable matrix group satisfying certain rationality conditions we can describe $E_k(G_F)$ in terms of k (see Theorems 1 and 2 in §5). We do this by using the Frobenius automorphism (see §1) in a way quite analogous to the way we used a derivation in [3] and [4]. Our method is, in some sense, a generalization of "Kummer theory" (see §2).

Notation. Throughout this paper Ω denotes a fixed universal field of characteristic $p > 0$. By a field we shall always mean a subfield of Ω over which Ω is universal, thus Ω is algebraically closed and has infinite transcendence degree over any field discussed. A field k and a finite subfield F of k will be fixed throughout. The cardinality of F will be denoted by q . The prime field will be denoted by $\mathbb{F}_p$.

By an F -set we shall mean an algebraic set with respect to the universe Ω which is defined over F . By an F -mapping we shall mean a rational mapping defined over F .

Received by the editors March 7, 1974.

AMS (MOS) subject classifications (1970). Primary 12F10.

Key words and phrases. Galois theory, inverse problem in Galois theory, Kummer theory, Frobenius automorphism.

⁽¹⁾Supported in part by NSF Grant GP-28242A #2.

If K is a Galois extension of k we denote by $G(K/k)$ the Galois group of automorphisms of K over k .

1. The Frobenius automorphism. Most of the material in this section is well known and may be found in Lang [5] or Serre [9, pp. 115–119].

Let A be an F -set. The mapping $f: \Omega \rightarrow \Omega, x \mapsto x^q$, leaves F fixed and therefore defines a mapping $A \rightarrow A$, also denoted by f , as follows. If $x \in A$ and $\phi: U \rightarrow \Omega^n$ is an affine open set which contains x , then $f(x) = \phi^{-1}((\phi x)_1^q, \dots, (\phi x)_n^q)$. Evidently $\rho \circ f = f \circ \rho$ for every F -mapping $\rho: A \rightarrow B$. If G is an F -group then $f: G \rightarrow G$ is an F -homomorphism. We now define an F -mapping $\mathfrak{f}: G \rightarrow G$ by the formula $\mathfrak{f}(x) = f(x) \cdot x^{-1}$.

PROPOSITION 1. *Let G and G' be F -groups and $\phi: G \rightarrow G'$ be an F -homomorphism. Then, for $x \in G$, $\mathfrak{f}(\phi x) = \phi(\mathfrak{f} x)$.*

If $x \in G$ we denote the conjugation $y \mapsto xyx^{-1}$ by $\tau_x: G \rightarrow G$.

PROPOSITION 2. *Let G be an F -group and $x, y \in G$. Then $\mathfrak{f}(xy) = \mathfrak{f}(x) \cdot \tau_x \mathfrak{f}(y)$.*

PROPOSITION 3. *Let G be an F -group and $x, y \in G$. $\mathfrak{f}(x) = \mathfrak{f}(y)$ if and only if $x^{-1}y \in G_F$.*

PROOF. $\mathfrak{f}(x) = \mathfrak{f}(y)$ if and only if $f(x^{-1}y) = x^{-1}y$.

PROPOSITION 4. *Let G be an F -group and $x \in G$. Then $k(x)$ is a finite separably algebraic extension of $k(\mathfrak{f} x)$.*

PROOF. Since $k(x) = k(x, \mathfrak{f} x) = k(x, fx, \mathfrak{f} x) = k(fx) \cdot k(\mathfrak{f} x) = k(x)^q \cdot k(\mathfrak{f} x)$, the proposition follows from Lang [6, p. 266].

PROPOSITION 5. *Let G be a connected F -group. Then the mapping $\mathfrak{f}: G \rightarrow G$ is surjective.*

PROOF (LANG [5, p. 557]). Let $y \in G$. Set $E = F(y)$ and let x be generic for G over E . Then, by Proposition 4, $\mathfrak{f}(x)$ is also generic for G over E . In addition, $E(x) = E(x, f(x)yx^{-1}) = E(f(x), f(x)yx^{-1}) = E(x)^q \cdot E(f(x)yx^{-1})$. Thus, by Lang [6, p. 266], $f(x)yx^{-1}$ is also generic for G over E . The generic specialization $\mathfrak{f}(x) \rightarrow f(x)yx^{-1}$ over E induces an isomorphism $E(\mathfrak{f} x) \rightarrow E(f(x)yx^{-1})$ which we extend to an isomorphism σ of $E(x)$. Since σ leaves F fixed there is a unique element of G , denoted by αx , such that this isomorphism is induced by the specialization $x \rightarrow \alpha x$. Thus

$$\begin{aligned} \mathfrak{f}(x^{-1}\alpha x) &= \mathfrak{f}(x^{-1})\tau_{x^{-1}}\mathfrak{f}(\alpha x) \\ &= f(x)^{-1} \cdot x \cdot x^{-1} \sigma(\mathfrak{f} x)x = f(x)^{-1}(f(x)yx^{-1})x = y. \end{aligned}$$

This proves the proposition.

PROPOSITION 6. *Let G be a connected F -group and H be a nonempty homogeneous F -space for G . Then $H_F \neq \emptyset$.*

PROOF. Choose any $x \in H$. Then $f(x) \in H$ so there exists $g \in G$ with $xg = f(x)$. By Proposition 5, there exists $\alpha \in G$ such that $\mathfrak{f}\alpha = g^{-1}$. Thus $f(x\alpha) = f(x)f(\alpha) = xg\mathfrak{f}(\alpha)\alpha = x\alpha$, whence $x\alpha \in H_F$.

COROLLARY. *Let $1 \rightarrow H \rightarrow G \rightarrow G' \rightarrow 1$ be an exact sequence of F -groups with H connected. Then $1 \rightarrow H_F \rightarrow G_F \rightarrow G'_F \rightarrow 1$ is exact.*

PROOF. This is obvious except perhaps for the surjectivity of $G_F \rightarrow G'_F$. Let $\alpha' \in G'_F$ and define $V = \{x \in G \mid x \mapsto \alpha'\}$. Note that V is a nonempty homogeneous F -space for H and hence $V_F \neq \emptyset$. This proves the corollary.

2. G -primitives.

DEFINITION. Let G be an F -group. By a G -extension of k we mean a Galois extension K of k such that there is an injective homomorphism $G(K/k) \rightarrow G_F$.

PROPOSITION 7. *Let G be an F -group. Let $\alpha \in G$ be such that $\mathfrak{f}(\alpha) \in G_k$. Then $K = k(\alpha)$ is a Galois extension of k , and the formula $\sigma \mapsto \alpha^{-1}\sigma\alpha$ defines an injective homomorphism $c: G(K/k) \rightarrow G_F$. Thus K is a G -extension of k .*

PROOF. By Proposition 4, K is separably algebraic over k . Let σ be an isomorphism of K over k . Then

$$\mathfrak{f}(\alpha^{-1}\sigma\alpha) = \mathfrak{f}(\alpha^{-1})\tau_{\alpha^{-1}}\mathfrak{f}(\sigma\alpha) = \tau_{\alpha^{-1}}(\mathfrak{f}(\alpha)^{-1}\sigma\mathfrak{f}(\alpha)) = 1,$$

so $c(\sigma) = \alpha^{-1}\sigma\alpha \in G_F$. Since $F \subset k$, σ is an automorphism of K . Therefore K is a Galois extension of k . In addition, for $\sigma, \tau \in G(K/k)$,

$$c(\sigma\tau) = \alpha^{-1}\sigma\tau\alpha = \alpha^{-1}\sigma\alpha \cdot \sigma(\alpha^{-1}\tau\alpha) = c(\sigma)\sigma(c(\tau)) = c(\sigma)c(\tau),$$

because $c(\tau) \in G_F$. Finally, $c(\sigma) = 1$ implies that $\sigma\alpha = \alpha$ and hence that $\sigma = \text{id}_K$. This proves the proposition.

DEFINITION. Let G be an F -group. By a G -primitive over k we mean an element α of G such that $\mathfrak{f}(\alpha) \in G_k$. A Galois extension K of k such that there is a G -primitive α over k with $K = k(\alpha)$ is called a G -primitive extension.

By Proposition 7 every G -primitive extension is a G -extension. Under certain conditions every G -extension is a G -primitive extension. It is these conditions that we now investigate.

Let k_s denote the separably algebraic closure of k . We recall that k_s is a Galois extension of k and that its Galois group, $G(k_s/k)$, is a topological group

with respect to the Krull topology in which the sets $G(k_s/E)$, where E is a finite Galois extension of k , are open neighborhoods of the identity.

Let G be an F -group. We recall that a (one-) cocycle of $G(k_s/k)$ into G is a map $c: G(k_s/k) \rightarrow G_{k_s}$ which is continuous with respect to the Krull and discrete topologies and which satisfies $c(\sigma\sigma') = c(\sigma)\sigma c(\sigma')$ ($\sigma, \sigma' \in G(k_s/k)$). Two cocycles c, c' are cohomologous if there exists $\alpha \in G_{k_s}$ with $c'(\sigma) = \alpha^{-1}c(\sigma)\alpha$ ($\sigma \in G(k_s/k)$) and the set of cohomology classes is denoted by $H^1(k, G)$. The cohomology class of the constant map $\sigma \mapsto 1$ ($\sigma \in G(k_s/k)$) is denoted by 1.

PROPOSITION 8. *Let G be an F -group. Let K be a Galois extension of k and $c: G(K/k) \rightarrow G_F$ be an injective homomorphism. If $H^1(k, G) = 1$ then there is a G -primitive α over k with $K = k(\alpha)$ and $c(\sigma) = \alpha^{-1}\sigma\alpha$ ($\sigma \in G(K/k)$). In particular if $H^1(k, G) = 1$ then every G -extension of k is a G -primitive extension.*

PROOF. Let $\rho: G(k_s/k) \rightarrow G(K/k)$ be defined by the formula $\rho(\sigma) = \sigma|_K$. ρ is continuous in the Krull and discrete topologies. Let $c' = c \circ \rho$. Then $c': G(k_s/k) \rightarrow G_{k_s}$ is continuous and for $\sigma, \tau \in G(k_s/k)$, $c'(\sigma\tau) = c'(\sigma)c'(\tau) = c'(\sigma)\sigma(c'(\tau))$ because $c'(\tau) \in G_F$. By assumption there exists $\alpha \in G_{k_s}$ such that $c'(\sigma) = \alpha^{-1}\sigma\alpha$ ($\sigma \in G(k_s/k)$). But for $\sigma \in G(k_s/K)$, $\alpha^{-1}\sigma\alpha = c'(\sigma) = 1$, whence $\alpha \in G_K$. Evidently $c(\sigma) = \alpha^{-1}\sigma\alpha$ for $\sigma \in G(K/k)$. If $\sigma \in G(K/k(\alpha))$ then $1 = \alpha^{-1}\sigma\alpha = c(\sigma)$ so $\sigma = \text{id}_K$, thus $K = k(\alpha)$. Finally $\sigma f(\alpha) = f(\sigma\alpha) = f(\alpha c(\sigma)) = f(\alpha)$ for every $\sigma \in G(K/k)$ so that $f(\alpha) \in G_k$. This proves the proposition.

Propositions 7 and 8 may be rephrased in the following way.

COROLLARY. *Let G be an F -group and assume that $H^1(k, G) = 1$. Let G' denote the set of $\alpha \in G$ with $f\alpha \in G_k$ and let $k' = k((\alpha)_{\alpha \in G'})$. Then there is a surjective mapping $\phi: G' \rightarrow \text{Hom}(G(k'/k), G_F)$ given by $\phi(\alpha)(\sigma) = \alpha^{-1}\sigma\alpha$.*

If G is commutative, then ϕ is a group homomorphism with kernel G_k .

It is known that $H^1(k, G) = 1$ if $G = \text{GL}(n), \text{SL}(n), G_a, G_m$ (the additive and multiplicative one dimensional groups) or if G is k -solvable (generalizations of "Hilbert's Theorem 90"; see, for example, Kolchin and Lang [2]), or if $G = W_n$ is the group of Witt vectors of length n (Witt [12, Satz 11, p. 134]).

In various special cases Propositions 7 and 8 reduce to well-known forms of Kummer theory.

1. Let $G = G_m$. Then G_F is the group of $(q-1)$ st roots of unity and, for $\alpha \in G$, $f\alpha = \alpha^{q-1}$. A G -primitive extension is thus one generated by a $(q-1)$ st root. Propositions 7 and 8 reduce, in this case, to multiplicative Kummer theory for cyclic extensions of degree dividing $q-1$ (see, for example, Lang [6, Chapter 8, §8]).

2. Let $G = G_a$ and F be the prime field. Then $G_F = \mathbb{Z}/(p)$ and, for $\alpha \in G$,

$f\alpha = \alpha^p - \alpha$. Thus we obtain (elementary) additive Kummer theory (Lang [6, loc. cit.]).

3. Let $G = W_n$ and F be the prime field. We obtain Witt's generalized additive Kummer theory (Witt [12]).

In the three cases above $\text{Hom}(G(k'/k), G_F)$ turns out to be the character group of $G(k'/k)$.

4. Let $G = \text{GL}(n)$. If K is any Galois extension of k of degree n , then there is an injective homomorphism $G(K/k) \rightarrow \text{GL}(n)_F$. Proposition 8 implies that K is a $\text{GL}(n)$ -primitive extension of k .

This fact can be proven directly and the details are somewhat amusing, so we state the results below with their straightforward proofs omitted.

PROPOSITION 9. *Let K be an extension of k and $\eta_1, \dots, \eta_n \in K$. Then $\eta_1, \dots, \eta_n$ are linearly independent over F if and only if*

$$\det W(\eta_1, \dots, \eta_n) = \det(\eta_j^{q^{i-1}})_{1 \leq i, j \leq n} \neq 0.$$

$W(\eta_1, \dots, \eta_n)$ has many properties analogous to those of the Wronskian matrix.

PROPOSITION 10. *Let K be a Galois extension of k of degree n . Choose $\eta_1, \dots, \eta_n$, linearly independent over F , such that $K = k(\eta_1, \dots, \eta_n)$ and such that $G(K/k)$ carries $\{\eta_1, \dots, \eta_n\}$ into itself. Let $\alpha = W(\eta_1, \dots, \eta_n)$. Then $K = k(\alpha)$.*

Let $(\det \alpha)^{-1} \det W(\eta_1, \dots, \eta_n, X) = X^{q^n} - \sum_{i=1}^n a_i X^{q^{i-1}} = P$. Then $P \in k[X]$, $a_1 \neq 0$, and

$$f(\alpha) = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ a_1 & \dots & a_n & \end{pmatrix} \in \text{GL}(n)_k$$

3. Classes of extensions. Throughout this section G is an F -group.

DEFINITION. Let $E(G) = E_k(G_F)$ denote the set of Galois extensions K of k such that $G(K/k)$ is isomorphic to G_F .

Our goal is to describe $E(G)$ entirely in terms of G , F , and k . For this purpose we define an equivalence relation, called similarity, on a set closely related to $E(G)$.

DEFINITION. Consider pairs (K, c) where $K \in E(G)$ and c is an isomorphism of $G(K/k)$ onto G_F . Two such pairs (K, c) and (K', c') are *similar* if $K' = K$ and there exists $a \in G_F$ with $c' = \tau_a \circ c$. The set of similarity classes is denoted by

$S(G) = S_k(G_F)$. Evidently if $G_F \cong G_{F'}$, where F' is another finite subfield of k and G' is an F' -group, then $S_k(G_F) \cong S_k(G_{F'})$.

PROPOSITION 11. *There is a (noncanonical) bijection $S(G) \rightarrow E(G) \times (\text{Aut } G_F)/(\text{Inn } G_F)$, where $\text{Inn } G_F$ is the group of inner automorphisms of G_F . In particular, if $S(G)$ is infinite, then $\text{card } E(G) = \text{card } S(G)$.*

Choose an isomorphism $c_K: G(K/k) \rightarrow G_F$ for each $K \in E(G)$. An element of $S(G)$ with representative (K, c) is sent to the pair whose first coordinate is K and whose second is the residue class of $c \circ c_K^{-1}$.

Unfortunately $S(G)$ is no easier to compute than $E(G)$. Thus we single out a subset of $S(G)$ for further study.

DEFINITION. Let $PS(G) = PS_k(G_F)$ be the set of similarity classes $s \in S(G)$ for which there is a representative (K, c) with the following property. There is a G -primitive α over k with $K = k(\alpha)$ and $c(\sigma) = \alpha^{-1}\sigma\alpha$ for every $\sigma \in G(K/k)$. Evidently if one representative of s has this property, then every representative does also.

By Proposition 8, $PS(G) = S(G)$ whenever $H^1(k, G) = 1$.

DEFINITION. Two elements a, a' of G_k are said to be *similar* if there exists $b \in G_k$ such that $a' = \mathfrak{f}(b)\tau_b a$.

PROPOSITION 12. *There is an injective mapping μ of $PS(G)$ into the set of similarity classes of elements of G_k with the following property. If $s \in PS(G)$ and $(K, c) \in s$ and α is a G -primitive over k with $K = k(\alpha)$ and $c(\sigma) = \alpha^{-1}\sigma\alpha$ for every $\sigma \in G(K/k)$, then $\mathfrak{f}(\alpha) \in \mu(s)$.*

PROOF. Let $s \in PS(G)$ and $(K, c), (K, c') \in s$. Let α, α' be G -primitives as above. By definition of similarity of pairs there exists an element a of G_F such that $c' = \tau_a \circ c$. Thus, for every $\sigma \in G(K/k)$,

$$\alpha'^{-1}\sigma\alpha' = c'(\sigma) = ac(\sigma)a^{-1} = a \cdot \alpha^{-1}\sigma\alpha \cdot a^{-1} = (\alpha a^{-1})^{-1}\sigma(\alpha a^{-1}).$$

Whence $b = \alpha'a\alpha^{-1} \in G_k$. But $\mathfrak{f}(\alpha') = \mathfrak{f}(\alpha'a) = \mathfrak{f}(b\alpha) = \mathfrak{f}(b)\tau_b\mathfrak{f}(\alpha)$, so that $\mathfrak{f}(\alpha')$ and $\mathfrak{f}(\alpha)$ are similar in G_k . This proves that there is a mapping μ with the stated property.

Suppose that $s, s' \in PS(G)$ are such that $\mu(s) = \mu(s')$. Choose $(K, c) \in s$, $(K', c') \in s'$ and G -primitives α and α' as above. By supposition there exists $b \in G_k$ such that $\mathfrak{f}(\alpha') = \mathfrak{f}(b)\tau_b\mathfrak{f}(\alpha) = \mathfrak{f}(b\alpha)$. Hence there exists $a \in G_F$ with $\alpha' = b\alpha a$. In particular $K' = k(\alpha') = k(\alpha) = K$. But also

$$\begin{aligned} c'(\sigma) &= \alpha'^{-1}\sigma\alpha' = a^{-1}\alpha^{-1}b^{-1}\sigma(b\alpha a) \\ &= a^{-1} \cdot \alpha^{-1}\sigma\alpha \cdot a = (\tau_{a^{-1}} \circ c)(\sigma) \quad (\sigma \in G(K/k)). \end{aligned}$$

Thus $s = s'$ which proves that μ is injective.

DEFINITION. $L(G) = L_k(G_F) = \mu(PS(G))$.

REMARK. If $a \in G_k$ is a representative of an element of $L(G)$, and $\alpha \in G$ is such that $\mathfrak{f}(\alpha) = a$, then $G(k(\alpha)/k) \cong G_F$. Indeed, by definition, there exist $\alpha' \in G$ and $b \in G_k$ such that $G(k(\alpha')/k) \cong G_F$ and $a = \mathfrak{f}(b)\tau_b \mathfrak{f}(\alpha') = \mathfrak{f}(b\alpha')$. Since $k(\alpha) = k(\alpha')$, the assertion is clear.

4. Reductions of the inverse problem.

PROPOSITION 13. *Let $\rho: G \rightarrow G'$ be a surjective F -homomorphism of F -groups and assume that $\ker \rho$ is connected. Then the mapping $\rho_k: G_k \rightarrow G'_k$ induces a mapping $\rho^\#$ of $L(G)$ into $L(G')$.*

PROOF. By Proposition 1, ρ_k induces a mapping of the set of similarity classes in G_k to the set of similarity classes of G'_k .

Let $a \in G_k$ be a representative of an element of $L(G)$. Then there exists a G -primitive α over k such that $a = \mathfrak{f}(\alpha)$. $k(\alpha)$ is a Galois extension of k and the formula $\sigma \mapsto \alpha^{-1}\sigma\alpha$ defines an isomorphism $c: G(k(\alpha)/k) \rightarrow G_F$. Let $K' = k(\rho\alpha)$. Then $\mathfrak{f}(\rho\alpha) = \rho(\mathfrak{f}(\alpha)) = \rho_k a$ so $\rho\alpha$ is a G' -primitive over k and the formula $\sigma' \mapsto \rho\alpha^{-1}\sigma'\rho\alpha$ defines an injective homomorphism $c': G(K'/k) \rightarrow G'_F$. But $K' \subset k(\alpha)$ and $c'(\sigma') = \rho(\alpha^{-1}\sigma\alpha) = (\rho \circ c)(\sigma)$, where $\sigma \in G(k(\alpha)/k)$ is such that $\sigma|K' = \sigma'$. But $\rho \circ c: G(k(\alpha)/k) \rightarrow G'_F$ is surjective (by the corollary to Proposition 6) so $(K', c') \in S(G')$. This proves the proposition.

Let $\rho: G \rightarrow G'$ be a surjective F -homomorphism of F -groups. Recall that a k -cross section for ρ is a rational mapping σ (not necessarily a homomorphism), defined over k , of G' into G such that $\rho \circ \sigma = \text{id}_{G'}$. A k -cross section exists, for example, if $\ker \rho$ is affine, connected and k -solvable. (See, for example, Rosenlicht [7].)

PROPOSITION 14. *Let $\rho: G \rightarrow G'$ be a surjective F -homomorphism of connected F -groups with connected kernel. Assume that there is a k -cross section for ρ . Assume further that the only subgroup H of G_F with $\rho H = G'_F$ is G_F . Then $\rho^\#: L(G) \rightarrow L(G')$ is surjective.*

PROOF. Let $\phi: G' \rightarrow G$ be a k -cross section for ρ .

If $a' \in G'_k$ is a representative for an element of $L(G')$ then there is a G' -primitive α' over k such that $a' = \mathfrak{f}(\alpha')$ and such that $c': G(k(\alpha')/k) \rightarrow G'_F$ with $c'(\sigma') = \alpha'^{-1}\sigma'\alpha'$ is an isomorphism. Let $a = \phi(a') \in G_k$ and choose an element α of G with $\mathfrak{f}(\alpha) = a$ (Proposition 5). Then $K = k(\alpha)$ is a Galois extension of k and the formula $\sigma \mapsto \alpha^{-1}\sigma\alpha$ defines an injective homomorphism $c: G(K/k) \rightarrow G_F$ (Proposition 7). Set $H = \text{im } c$.

Because $\mathfrak{f}(\rho\alpha) = \rho \mathfrak{f}(\alpha) = \rho a = a' = \mathfrak{f}(\alpha')$, there exists $b \in G_F$ with $\rho\alpha = \alpha'b$. For every $\sigma \in G(K/k)$,

$$\begin{aligned}\rho \circ c(\sigma) &= \rho(\alpha^{-1}\sigma\alpha) = \rho\alpha^{-1}\sigma\rho\alpha = b^{-1}\alpha'^{-1}\sigma(\alpha'b) \\ &= b^{-1} \cdot \alpha'^{-1}\sigma\alpha' \cdot b = b^{-1}c'(\sigma')b,\end{aligned}$$

where $\sigma' = \sigma|k(\alpha')$. Thus $\rho(H) = \text{im } \rho \circ c = \text{im } \tau_{b^{-1}} \circ c' = G'_F$. By hypothesis $H = G_F$ and c is surjective. Evidently $\rho^\#$ applied to the similarity class of a is the similarity class of a' , which proves the proposition.

COROLLARY. *Let $\rho: G \rightarrow G'$ be an F -isomorphism of connected F -groups. Then $\rho^\#: L(G) \rightarrow L(G')$ is bijective.*

We now develop an example of the use of this proposition.

Let G be an abstract group. We denote by G^* the subgroup generated by elements of the form $xyx^{-1}y^{p-1}$ ($x, y \in G$). G^* is normal and is the smallest normal subgroup such that the quotient is commutative of exponent p .

LEMMA. *Let G be an abstract group and N a normal nilpotent subgroup of finite exponent a power of p . If H is a subgroup of G such that $H \cdot N^* = G$, then $H = G$.*

PROOF. Let $G_1 = G/[N, N]$ and denote by N_1, H_1 the images of N, H in G_1 . Note that N_1 is commutative and that the image of N^* in G_1 is $(N_1)^* = N_1^p$.

Let $H' = H_1 \cap N_1$. Since $H_1 \cdot N_1^p = G_1$, for each $n \in N_1$ there exist $h \in H_1$ and $n' \in N_1$ such that $n = h(n')^p$. Evidently $h \in H'$ and thus $N_1 = H'N_1^p$. Using the commutativity of N_1 , we find that $N_1^p = H'^pN_1^{p^2}$, and hence that $N_1 = H'N_1^{p^2}$. Continuing by induction and using the fact that N_1 has finite exponent a power of p , we find that $N_1 = H'$. Whence $H_1 \supset N_1$ and $H_1 = H_1N_1^p = G_1$. Therefore $H \cdot [N, N] = G$.

Let $H'' = H \cap N$. As above $N = H'' \cdot [N, N]$. By Hall [1, Corollary 10.3.3, p. 155], $H'' = N$. Thus $H \supset N$ and $H = H \cdot [N, N] = G$.

PROPOSITION 15. *Let G be a connected matrix F -group and N a normal connected nilpotent F -subgroup of finite exponent a power of p . Suppose that $(N^*)_F = (N_F)^*$. If $\rho: G \rightarrow G/N^*$ is the quotient homomorphism, then $\rho^\#: L(G) \rightarrow L(G/N^*)$ is surjective.*

Since $(G/N^*)_F = G_F/N_F^*$ (corollary to Proposition 6), this proposition follows immediately from Proposition 14 and the lemma.

We note that, in general, $(N^*)_F \neq (N_F)^*$. Indeed, let

$$N = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^q - a \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \Omega \right\},$$

and assume that $p \neq 2$. Then $x^p = 1$ for every $x \in N$ and $N^* = [N, N]$. Since N is not commutative whereas N_F is, $[N_F, N_F] \neq [N, N]_F$. It is interesting to note that $L_F(N_F) = \emptyset$, because N_F is not cyclic, but that, if F is the prime field, $L_F((N/[N, N])_F) \neq \emptyset$, since $(N/[N, N])_F$ is isomorphic to the additive group of F .

As another example, consider

$$N = \left\{ \left(\begin{array}{ccc|cc} 1 & a^q - a & b & & \\ 0 & 1 & a^q - a & 0 & \\ 0 & 0 & 1 & & \\ \hline & & & 1 & a \\ & & 0 & 0 & 1 \end{array} \right) : a, b \in \Omega \right\},$$

and assume that $p = 2$. Since N is commutative, $N^* = N^2$ and $(N^2)_F \neq (N_F)^2$. Again in this example, $L_F(N_F) = \emptyset$ but, if F is the prime field, $L_F((N/N^2)_F) \neq \emptyset$.

PROPOSITION 16. *Let G_1 and G_2 be connected F -groups. Assume that the only normal subgroup H_1 of G_{1F} with the property that there is a surjective homomorphism of G_{2F} onto G_{1F}/H_1 is G_{1F} . Then there is a bijection between $L(G_1 \times G_2)$ and $L(G_1) \times L(G_2)$.*

PROOF. Let $\phi: L(G_1 \times G_2) \rightarrow L(G_1) \times L(G_2)$ be the map induced by the projections $\rho_i: G_1 \times G_2 \rightarrow G_i$ ($i = 1, 2$). We shall show first that ϕ is injective.

Let a and a' be representatives of elements of $L(G_1 \times G_2)$ which have the same image under ϕ . Then $\rho_i a = \{ (b_i) \tau_{b_i} \rho_i a' \}$ for some $b_i \in G_{iF}$ ($i = 1, 2$). Let $b = (b_1, b_2) \in (G_1 \times G_2)_F$. Clearly $a = \{ (b) \tau_b a' \}$, which proves that ϕ is injective.

For each $i = 1, 2$, let a_i be a representative of an element of $L(G_i)$. Then there exist $\alpha_i \in G_i$ such that $k(\alpha_i)$ is Galois over k , the formula $\sigma_i \mapsto \alpha_i^{-1} \sigma_i \alpha_i$ defines an isomorphism c_i of $G(k(\alpha_i)/k)$ onto G_{iF} and $a_i = \{ (\alpha_i) \}$. Set $K = k(\alpha_1, \alpha_2)$. Then $\{ (\alpha_1, \alpha_2) = (a_1, a_2) \in (G_1 \times G_2)_k$ so K is a Galois extension of k and the formula $\sigma \mapsto (\alpha_1^{-1} \sigma \alpha_1, \alpha_2^{-1} \sigma \alpha_2)$ defines an injective homomorphism $c: G(K/k) \rightarrow (G_1 \times G_2)_F$. We must show that c is surjective.

Set $H = \text{im } c$. By definition of K , $\rho_i(H) = G_{iF}$ for $i = 1, 2$. Let $H_1 \times \{1\} = \ker \rho_2|_H$, then $H_1 = \rho_1(\ker \rho_2|_H)$ is a normal subgroup of $\rho_1(H) = G_{1F}$. Denote by $\pi: G_{1F} \rightarrow G_{1F}/H_1$ the quotient homomorphism. Because $\ker \rho_2|_H \subset \ker(\pi \circ \rho_1|_H)$, there is a homomorphism $\lambda: G_{2F} \rightarrow G_{1F}/H_1$ such that $\lambda \circ \rho_2|_H = \pi \circ \rho_1|_H$; evidently λ is surjective. By hypothesis $H_1 = G_{1F}$ and therefore $\ker \rho_2|_H = G_{1F} \times \{1\}$. But

$$\begin{aligned} \text{ord } H &= (\text{ord } \ker \rho_2|_H) (\text{ord } \text{im } \rho_2|_H) \\ &= (\text{ord } G_{1F}) (\text{ord } G_{2F}) = \text{ord}(G_1 \times G_2)_F. \end{aligned}$$

Therefore $H = (G_1 \times G_2)_F$ and c is surjective. This proves the proposition.

For semidirect products we obtain a much weaker result.

Let $G = G_1 \cdot G_2$ be the semidirect product of the connected F -groups G_1 and G_2 with G_1 normal in G . Let $b \in G_{2k}$. Then there exists $\beta \in G_2$ such that $\mathfrak{f}(\beta) = b$ and if β' is another element of G_2 with $\mathfrak{f}(\beta') = b$ then there exists $d \in G_{2F}$ with $\beta' = \beta d$. For any $\alpha \in G_1$,

$$\tau_{f(\beta')} \mathfrak{f}(\tau_{\beta'}^{-1} \alpha) = \tau_{f(\beta d)} \mathfrak{f}(\tau_{\beta d}^{-1} \alpha) = \tau_{f(\beta)} \tau_d \mathfrak{f}(\tau_d^{-1} \tau_{\beta}^{-1} \alpha) = \tau_{f(\beta)} \mathfrak{f}(\tau_{\beta}^{-1} \alpha),$$

because $f(d) = d \in G_{2F}$ and therefore τ_d is an F -homomorphism of G_1 . Because of this we may denote $\tau_{f(\beta)} \mathfrak{f}(\tau_{\beta}^{-1} \alpha)$ by $\mathfrak{f}_b(\alpha)$, where $\beta \in G_2$ is such that $\mathfrak{f}(\beta) = b$.

Let $b \in G_{2k}$ and $\beta \in G_2$ be such that $\mathfrak{f}(\beta) = b$. Let $\alpha \in G_1$ be such that $\mathfrak{f}_b(\alpha) \in G_{1k}$. Let σ be any isomorphism of $k(\alpha, \beta)$ over $k(\beta)$. Then $\mathfrak{f}(\tau_{\beta}^{-1}(\sigma\alpha)) = \tau_{f(\beta)}^{-1} \sigma(\mathfrak{f}_b(\alpha)) = \mathfrak{f}(\tau_{\beta}^{-1} \alpha)$, so there exists $d \in G_{1F}$ such that $\tau_{\beta}^{-1}(\sigma\alpha) = (\tau_{\beta}^{-1} \alpha)d$, so $\alpha^{-1} \sigma\alpha = \tau_{\beta} d \in G_{1k(\beta)}$. It follows that $k(\alpha\beta) = k(\alpha, \beta)$ is a Galois extension of $k(\beta)$ and the formula $\sigma \mapsto \tau_{\beta}^{-1}(\alpha^{-1} \sigma\alpha)$ defines a homomorphism of $G(k(\alpha\beta)/k(\beta))$ into G_{1F} , which is evidently injective. Moreover, it is straightforward to verify that the condition that this homomorphism be surjective depends only on b and $\mathfrak{f}_b(\alpha)$ and not on the choice of α and β .

DEFINITION. Let $G = G_1 \cdot G_2$ be the semidirect product of the connected F -groups G_1 and G_2 with G_1 normal in G . Let $b \in G_{2k}$. Denote by $l(G_1, b) = l_k(G_{1F}, b)$ the set of elements a of G_{1k} which satisfy the following condition. If $\beta \in G_2$ is such that $\mathfrak{f}(\beta) = b$ and $\alpha \in G_1$ is such that $\mathfrak{f}_b(\alpha) = a$, then the injective homomorphism of $G(k(\alpha\beta)/k(\beta))$ into G_{1F} , defined by $\sigma \mapsto \tau_{\beta}^{-1}(\alpha^{-1} \sigma\alpha)$, is surjective.

If β as above has the property that $\tau_{\beta}|_{G_1} = \text{id}_{G_1}$, then $l(G_1, b)$ is merely the set of elements of G_{1k} which are representatives of elements of $L_{k(\beta)}(G_{1F})$.

PROPOSITION 17. Let $G = G_1 \cdot G_2$ be the semidirect product of the

connected F -groups G_1 and G_2 with G_1 normal in G . Let $\rho: G \rightarrow G_2$ be the canonical homomorphism. Then the image of $\rho^\#: L(G) \rightarrow L(G_2)$ is the set of those classes for which there is a representative b with $l(G_1, b) \neq \emptyset$:

PROOF. Let $y \in L(G_2)$ be in the image of $\rho^\#$, say $\rho^\#x = y$. Let $ab \in G_{1k} \cdot G_{2k} = G_k$ be a representative of x . Let $\beta \in G_2$ be such that $f(\beta) = b$, let $\alpha \in G_1$ be such that $f_b(\alpha) = a$. Because $x \in L(G)$, $G(k(\alpha\beta)/k) \cong G_F$, thus $[k(\alpha\beta): k] = \text{ord } G_F$. Moreover the formula $\sigma \mapsto \beta^{-1}\sigma\beta$ defines an injective homomorphism of $G(k(\beta)/k)$ into G_{2F} and the formula $\sigma \mapsto \tau_\beta^{-1}(\alpha^{-1}\sigma\alpha)$ defines an injective homomorphism of $G(k(\alpha\beta)/k(\beta))$ into G_{1F} . Because $\text{ord } G_F = (\text{ord } G_{1F})(\text{ord } G_{2F})$, these homomorphisms must be surjective.

Let $y \in L(G_2)$ and $b \in y$ be such that the formula $\sigma \mapsto \tau_\beta^{-1}(\alpha^{-1}\sigma\alpha)$ defines an isomorphism of $G(k(\alpha\beta)/k(\beta))$ onto G_{1F} , where $\beta \in G_2$ is such that $f(\beta) = b$ and $\alpha \in G_1$ is such that $f_b(\alpha) = a$. Note that

$$f(\alpha\beta) = f(\beta \cdot \tau_\beta^{-1}\alpha) = f(\beta)\tau_\beta f(\tau_\beta^{-1}\alpha) = \tau_{f(\beta)} f(\tau_\beta^{-1}\alpha) \cdot f(\beta) = f_b(\alpha) f(\beta) = ab.$$

Thus the formula $\sigma \mapsto (\alpha\beta)^{-1}\sigma(\alpha\beta)$ defines an injective homomorphism of $G(k(\alpha\beta)/k)$ into G_F . But $G(k(\beta)/k) \cong G_{2F}$ and $G(k(\alpha\beta)/k(\beta)) \cong G_{1F}$ and therefore $[k(\alpha\beta): k] = (\text{ord } G_{1F})(\text{ord } G_{2F}) = \text{ord } G_F$ so that the homomorphism must be surjective. But then ab is a representative of an element of $L(G)$, which proves the proposition.

PROPOSITION 18. Let $G = G_1G_2$ be a semidirect product of subgroups with G_1 normal in G and commutative. Assume that $G_1 = A \times B$ is the direct product of groups which are invariant under the action of G_2 . Assume also that the only subgroup H of B_F , invariant under the action of G_2 , such that there is a surjective homomorphism which commutes with the action of G_2 of A_F onto B_F/H is B_F . Let d be a representative of an element of $L(G_2)$. If $l(A, d) \neq \emptyset$ and $l(B, d) \neq \emptyset$ then $l(G_1, d) \neq \emptyset$.

PROOF. Let $\delta \in G_2$ be such that $f(\delta) = d$. Then the formula $\sigma \mapsto \delta^{-1}\sigma\delta$ defines an isomorphism $G(k(\delta)/k) \rightarrow G_{2F}$. Choose $a \in l(A, d)$, $b \in l(B, d)$ and $\alpha \in A$, $\beta \in B$ such that $f_a(\alpha) = a$, $f_d(\beta) = b$. Then $\gamma = \alpha\beta \in G_1$ and $f_d(\gamma) = ab$. The formula $\sigma \mapsto \tau_\delta^{-1}(\gamma^{-1}\sigma\gamma)$ defines an injective homomorphism $c: G(k(\gamma\delta)/k(\delta)) \rightarrow G_{1F}$. Let $C = \text{im } c$. We shall first show that C is invariant under the action of G_{2F} .

Let $x \in C$ and $y \in G_{2F}$. Then there exists $\sigma \in G(k(\gamma\delta)/k(\delta))$ such that $x = \tau_\delta^{-1}(\gamma^{-1}\sigma\gamma)$ and $\phi \in G(k(\delta)/k)$ such that $y = \delta^{-1}\phi\delta$. Then $c(\phi)yc(\phi^{-1})y^{-1} = c(\phi)yc(\phi^{-1})y^{-1} = 1$, so that, by the commutativity of G_1 ,

$$\begin{aligned}
\tau_y(x) &= yxy^{-1} = c(\phi) yxc(\phi^{-1}) y^{-1} = c(\phi) y \cdot x \cdot c(\phi^{-1}) \phi^{-1} y^{-1} \\
&= ((\gamma\delta)^{-1} \phi(\gamma\delta)) ((\gamma\delta)^{-1} \sigma(\gamma\delta)) ((\gamma\delta)^{-1} \phi^{-1}(\gamma\delta)) \\
&= ((\gamma\delta)^{-1} \phi(\gamma\delta)) \phi((\gamma\delta)^{-1} \sigma(\gamma\delta)) \phi\sigma((\gamma\delta)^{-1} \phi^{-1}(\gamma\delta)) \\
&= (\gamma\delta)^{-1} \phi\sigma\phi^{-1}(\gamma\delta) = c(\phi\sigma\phi^{-1}) \in C.
\end{aligned}$$

Therefore C is invariant under the action of G_{2F} .

Denote by $\pi_A: C \rightarrow A_F$ and $\pi_B: C \rightarrow B_F$ the canonical projections. By construction π_A and π_B are surjective. Let $1 \times H = \ker \pi_A$. Then H is a subgroup of B_F which is invariant under G_{2F} . If $\rho: B_F \rightarrow B_F/H$ is the quotient homomorphism then there is a homomorphism $\phi: A_F \rightarrow B_F/H$ such that $\phi \circ \pi_A = \rho \circ \pi_B$. ϕ is evidently surjective and commutes with the action of G_{2F} . By hypothesis $H = B_F$. Thus

$$\text{ord } C = (\text{ord im } \pi_A)(\text{ord ker } \pi_A) = (\text{ord } A_F)(\text{ord } B_F) = \text{ord } G_{1F},$$

whence $C = G_{1F}$ which proves the proposition.

5. The inverse problem for connected solvable algebraic matrix groups. We first consider nilpotent groups.

Let G be a connected nilpotent matrix F -group. Then $G = U \times T$, where U is the unipotent part of G and T is the unique maximal torus. Because F is perfect, U and T are F -groups (Rosenlicht [8, p. 37]). Note that U is a p -group of finite exponent (Tits [11, p. 118]). Assume that $(U_F)^* = (U^*)_F$. Then, by Proposition 15, there is a surjection $L(G) \rightarrow L(G/U^*)$. This reduces the inverse problem for G to that for $G_1 = U_1 \times T$, where $U_1 = U/U^*$ is commutative of exponent p .

We claim that if H is a normal subgroup of U_{1F} such that there is a surjective homomorphism $\phi: T_F \rightarrow U_{1F}/H$, then $H = U_{1F}$. Indeed $\phi(\alpha^p) = \phi(\alpha)^p = 1$ for every $\alpha \in T_F$. But the p th power mapping of T is surjective and therefore the p th power mapping of T_F is surjective (corollary to Proposition 6) and so $\phi(T_F) = 1$, which proves our claim.

Because of Proposition 16 there is a bijection $L(G_1) \rightarrow L(U_1) \times L(T)$. We consider $L(U_1)$ first. Let $\text{card } F = q = p^r$.

PROPOSITION 19. *Let U be a commutative connected unipotent F -group with exponent p and dimension u . Then $L_k(U_F)$ is in bijective correspondence with the set of ru -tuples of elements of the F_p -vector space $k/\mu(k)$ which are linearly independent, where $\mu: k \rightarrow k$ is defined by $\mu(\kappa) = \kappa^p - \kappa$.*

PROOF. By Tits [11, p. 130], U is an F -vector group, i.e. U is F -isomorphic to G_a^u . By Proposition 8 there is a bijection $L_k(U_F) \cong PS_k(U_F) \cong S_k(U_F)$. Since $U_F = F^u \cong F_p^u = (G_a^u)_{F_p}$, $S_k(U_F) \cong S_k((G_a^u)_{F_p}) \cong L_k((G_a^u)_{F_p})$. Thus we may assume that $U = G_a^u$ and $F = F_p$. The proposition now follows by additive Kummer theory.

PROPOSITION 20. *Let T be an F -split torus of dimension t . Then $L(T)$ is in bijective correspondence with the set of t -tuples of elements of the $\mathbb{Z}/(q-1)\mathbb{Z}$ -module $k^*/\nu(k^*)$ which are linearly independent, where $\nu: k^* \rightarrow k^*$ is defined by $\nu(\kappa) = \kappa^{q-1}$ and the action of $\mathbb{Z}/(q-1)\mathbb{Z}$ on $k^*/\nu(k^*)$ is given by $(e, x) \mapsto x^e$.*

PROOF. By hypothesis T is F -isomorphic to G_m^t . The proposition follows by multiplicative Kummer theory.

We may collect the results of this discussion in the following theorem.

THEOREM 1. *Let G be a connected nilpotent matrix F -group with unipotent part U and maximal torus T . Assume that $(U_F)^* = (U^*)_F$ and that T is F -split. Set $u = \dim U/U^*$ and $t = \dim T$. Define $\mu: k \rightarrow k$ by $\kappa \mapsto \kappa^p - \kappa$ and consider $k/\mu k$ as an F_p -vector space. Define $\nu: k^* \rightarrow k^*$ by $\kappa \mapsto \kappa^{q-1}$ and consider $k^*/\nu k^*$ as a $\mathbb{Z}/(q-1)\mathbb{Z}$ -module by exponentiation. Then there is a surjection of $L_k(G_F)$ onto the set of elements $(a_1, \dots, a_{ru}, b_1, \dots, b_t)$ of $(k/\mu k)^{ru} \times (k^*/\nu k^*)^t$ such that $a_1, \dots, a_{ru}$ are linearly independent over F_p and $b_1, \dots, b_t$ are linearly independent over $\mathbb{Z}/(q-1)\mathbb{Z}$.*

If $k = k'(x)$ where x is transcendental over the field k' , then $\dim k/\mu k = \aleph_0 \cdot \text{card } k'$ and $\text{rk } k^*/\nu k^* = \aleph_0 \cdot \text{card } k'$. It follows from Proposition 11 that $\text{card } E_k(G_F) = \aleph_0 \cdot \text{card } k'$ (if $G \neq 1$). However if $k = k'((x))$ is the field of formal power series and k' is closed under the taking of $(q-1)$ st roots, then $\dim k/\mu k = \aleph_0 \cdot \text{card } k'$ but $\text{rk } k^*/\nu k^* = 1$. Thus $E_k(G_F)$ is empty unless $\dim T \leq 1$, and if this is the case, then $\text{card } E_k(G_F) \geq \aleph_0 \cdot \text{card } k'$ (if $G \neq 1$).

For solvable groups we obtain a somewhat weaker result. In particular we assume that $F = F_p$.

Now let G be a connected solvable matrix F -group. Then $G = U \cdot T$ (semi-direct) where U is the unipotent part of G and T is a maximal F -torus. Since F is perfect, U is defined over F . Assume that $(U_F)^* = (U^*)_F$. Then, by Proposition 15, there is a surjection $L(G) \rightarrow L(G/U^*)$. Let $G_1 = G/U^* = V \cdot T$, where $V = U/U^*$. V is an F -vector group which we write additively.

Tits [11, p. 146] describes G by means of the action of the torus T on the vector group V and defines weights of the action for this purpose. Unfortunately two distinct weights may become identical when restricted to T_F acting on V_F . In the following paragraph we essentially replace V by another vector

group so that this difficulty does not arise.

A weight of T_F in V_F is a character χ , i.e. a homomorphism $\chi: T_F \rightarrow F^*$, such that $V_{F\chi} = \{v \in V_F \mid \tau_\beta v = \chi(\beta)v \text{ for all } \beta \in T_F\}$ is nontrivial. $V_{F\chi}$ is called the weight space associated to χ . Assume now that T is F -split, then we may suppose that $T = G_m^t$, where $t = \dim T$. For any weight χ there exist unique integers $e_1, \dots, e_t$ with $0 \leq e_i < p-1$ such that $\chi(\beta_1, \dots, \beta_t) = \prod_{i=1}^t \beta_i^{e_i}$ ($\beta = (\beta_1, \dots, \beta_t) \in T_F$). Let $\chi_1, \dots, \chi_m$ be the weights of T_F in V_F and $V_{F1}, \dots, V_{Fm}$ the weight spaces. Then V_F is the direct sum of the V_{Fi} ($i = 1, \dots, m$). Set $v_i = \dim V_{Fi}$ (as an F -vector space). Let $e_{ij} \in \{0, 1, \dots, p-1\}$ be such that $\chi_i(\beta) = \prod_{j=1}^t \beta_j^{e_{ij}}$. Define $V_i = G_a^{v_i}$. We let T act on V_i by the formula $\beta \cdot v = \prod_j \beta_j^{e_{ij}} v$ where $\beta = (\beta_1, \dots, \beta_t) \in T$, and consider the semidirect product $(\bigoplus V_i) \cdot T$ with respect to this action. We call this group G_2 . Then $G_{2F} = G_{1F}$. By Proposition 8 there is a bijection

$$L(G_1) \cong PS(G_1) \cong S(G_1) = S(G_2) \cong PS(G_2) \cong L(G_2).$$

We claim that the only subgroup H of $(V_m)_F = V_{Fm}$ with the property that there is a surjective homomorphism ϕ which commutes with the action of T_F of $(\bigoplus_{i=1}^{m-1} V_i)_F$ onto V_{Fm}/H is V_{Fm} . Indeed, if $v_i \in V_{Fi}$ and $\beta = (\beta_1, \dots, \beta_t) \in T_F$ then $\chi_m(\beta)\phi(v_i) = \phi(\chi_i(\beta)v_i) = \chi_i(\beta)\phi(v_i)$ because ϕ is a group homomorphism and $F = F_p$. If $\phi(v_i) \neq 0$ then $\chi_m(\beta) = \chi_i(\beta)$ for every $\beta \in T_F$ and therefore for every $\beta \in T$. Therefore $\phi(v_i) = 0$ for every $v_i \in V_{Fi}$ and every $i = 1, \dots, m-1$. This proves our claim.

By Propositions 17 and 18, the image of $L(G_2) \rightarrow L(T)$ is the set of $x \in L(T)$ for which there is a representative $b \in x$ with $l(V_p, b) \neq \emptyset$ for each $i = 1, \dots, m$.

We now shall describe $l(V_p, b)$; we drop the subscript in what follows. Letting $v = \dim V$, $V \cong G_a^v$ and we may assume equality and write V additively. For any $\beta = (\beta_1, \dots, \beta_t) \in T = G_m^t$ and $\alpha \in V$, $\tau_\beta \alpha = \chi(\beta)\alpha = (\prod_{j=1}^t \beta_j^{e_j})\alpha$ where $0 \leq e_j < p-1$. Choosing $\beta \in T$ such that $\mathfrak{f}(\beta) = b$ we find that, for any $\alpha = (\alpha_1, \dots, \alpha_v) \in V$,

$$\mathfrak{f}_b(\alpha) = \tau_{f(\beta)} \mathfrak{f}(\tau_\beta^{-1} \alpha) = \chi(f(\beta))(\chi(\beta^{-1})^p \alpha^p - \chi(\beta^{-1}) \alpha)$$

$$= \alpha^p - \chi(b)\alpha = (\alpha_1^p - \chi(b)\alpha_1, \dots, \alpha_v^p - \chi(b)\alpha_v).$$

Let $L: \Omega \rightarrow \Omega$ be defined by $L(x) = x^p - \chi(b)x$. Note that L is an F -vector space homomorphism and denote by $\pi: k \rightarrow k/L(k)$ the quotient homomorphism of F -vector spaces.

LEMMA. $l(V, b)$ is the set of v -tuples $(a_1, \dots, a_v) \in k^v$ such that $\pi(a_1), \dots, \pi(a_n)$ are linearly independent over F .

PROOF. Let $a = (a_1, \dots, a_v) \in k^v$ and suppose first that $c_1\pi(a_1) + \dots + c_v\pi(a_v) = 0$ for $c_1, \dots, c_v$ in F , not all zero. Let $\alpha \in V$ be such that $f_b(\alpha) = a$. Then there exists $\kappa \in k$ such that $L(\kappa) = \sum_{i=1}^v c_i a_i = L(\sum c_i \alpha_i)$. Setting $A = \kappa - \sum c_i \alpha_i$ we see that

$$0 = L(A) = \chi(\beta^{-1})^p L(A) = (\chi(\beta^{-1})A)^p - \chi(\beta^{-1})A,$$

thus there exists $d \in F$ such that $\chi(\beta)d = A = \kappa - \sum c_i \alpha_i$. In particular $\sum c_i \alpha_i \in k(\beta)$ so that $[k(\alpha, \beta): k(\beta)] < v$ and $G(k(\alpha, \beta)/k(\beta))$ is not isomorphic to V_F . Therefore $a \notin I(V, b)$.

Now suppose that $\pi(a_1), \dots, \pi(a_v)$ are linearly independent over F . The formula $\sigma \mapsto \tau_\beta^{-1}(\sigma\alpha - \alpha) = \chi(\beta^{-1})(\sigma\alpha - \alpha)$ defines an injective homomorphism of $G(k(\alpha, \beta)/k(\beta))$ into V_F . Let H denote the image; we shall assume that $H \neq V_F$ and force a contradiction. H is then a proper F -vector subspace of $V_F = F^v$ so there exist $c_1, \dots, c_v \in F$, not all zero, such that $\sum_{i=1}^v c_i \chi(\beta^{-1})(\sigma\alpha_i - \alpha_i) = 0$ for every $\sigma \in G(k(\alpha, \beta)/k(\beta))$. Whence $g = \sum c_i \alpha_i \in k(\beta)$. In addition $g^p - \chi(\beta)g = L(g) = \sum c_i \alpha_i \in k$. For $\sigma \in G(k(\beta)/k)$ define $d(\sigma) = \chi(\beta^{-1})(\sigma g - g)$. Then

$$\begin{aligned} d(\sigma)^p &= \chi(f(\beta^{-1}))\sigma(g^p - \chi(\beta)g) + \chi(\beta^{-1})\sigma g - \chi(f(\beta^{-1}))g^p \\ &= \chi(f(\beta^{-1}))(g^p - \chi(\beta)g) + \chi(\beta^{-1})\sigma g - \chi(f(\beta^{-1}))g^p \\ &= d(\sigma), \end{aligned}$$

hence $d(\sigma) \in F$. For $\sigma, \sigma' \in G(k(\beta)/k)$,

$$\begin{aligned} d(\sigma\sigma') &= \chi(\beta^{-1})(\sigma\sigma'g - g) = \chi(\beta^{-1})\sigma(\sigma'g - g) + \chi(\beta^{-1})(\sigma g - g) \\ &= d(\sigma) + \chi(\beta^{-1})\sigma\chi(\beta)d(\sigma') = d(\sigma) + \chi(\beta^{-1}\sigma\beta)d(\sigma'). \end{aligned}$$

Thus $d: G(k(\beta)/k) \rightarrow F$ is a crossed homomorphism. Since p does not divide the order of $G(k(\beta)/k)$, this crossed homomorphism splits. Let $\gamma \in F$ be such that

$$d(\sigma) = \chi(\beta^{-1}\sigma\beta)\gamma - \gamma = \chi(\beta^{-1})(\sigma\chi(\beta)\gamma) - \chi(\beta)\gamma.$$

It follows that $\kappa = g - \chi(\beta)\gamma \in k$. Since

$$L(\chi(\beta)\gamma) = \chi(\beta)^p \gamma^p - \chi(\beta)\chi(\beta)\gamma = \chi(f(\beta))(\gamma^p - \gamma) = 0,$$

$L(\kappa) = \sum c_i \alpha_i$ and $\sum c_i \pi \alpha_i = 0$. This contradicts the linear independence of $\pi \alpha_1, \dots, \pi \alpha_v$ and proves the lemma.

The above remarks prove the following theorem.

THEOREM 2. *Let G be a connected solvable matrix F -group with unipotent part U and maximal F -torus T . Assume that $F = F_p$, that $(U_F)^* = (U^*)_F$, and*

that T is F -split. Let $\chi_1, \dots, \chi_m$ be the weights of T_F in $(U/U^*)_F$, and let $u_1, \dots, u_m$ be the dimensions of the associated weight spaces. For each $b \in T_k$ let $L_{ib}: k \rightarrow k$ be defined by $L_{ib}(\kappa) = \kappa^p - \chi_i(b)\kappa$.

Let $x \in L(T)$. Then x is in the image of the mapping $L(G) \rightarrow L(T)$ if and only if there is a representative $b \in T_k$ of x such that for each $i = 1, \dots, m$ there is a u_i -tuple of elements of k whose residue classes modulo $L_{ib}(k)$ are linearly independent over F .

If $k = k'(x)$, where x is transcendental over the field k' , then, for each $b \in T_k$, $\dim k/L_{ib}(k) = \aleph_0 \cdot \text{card } k'$. Since $\text{card } L(T) = \aleph_0 \cdot \text{card } k'$ (see the remarks following Theorem 1), $\text{card } E_k(G_F) = \aleph_0 \cdot \text{card } k'$ (if $G \neq 1$).

However if $k = k'((x))$ is the field of formal power series and k' is closed under the taking of $(p-1)$ st roots, then $\text{card } L(T) = 0$ if $\dim T > 1$ and $\text{card } L(T) = 1$ if $\dim T \leq 1$. In addition $\dim k/L_{ib}(k)$ is infinite for every $b \in T_k$. Therefore $\text{card } E_k(G_F) = 0$ if $\dim T > 1$, and $\text{card } E_k(G_F) \geq 1$ if $\dim T \leq 1$ (and $G \neq 1$).

REFERENCES

1. M. Hall, *The theory of groups*, Macmillan, New York, 1959. MR 21 #1996.
2. E. R. Kolchin and S. Lang, *Existence of invariant bases*, Proc. Amer. Math. Soc. **11** (1960), 140–148. MR 30 #84.
3. J. Kovacic, *The inverse problem in the Galois theory of differential fields*, Ann. of Math. (2) **89** (1969), 583–608. MR 39 #5535.
4. ———, *On the inverse problem in the Galois theory of differential fields. II*, Ann. of Math. (2) **93** (1971), 269–284. MR 44 #2732.
5. S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR 19, 174.
6. ———, *Algebra*, Addison-Wesley, Reading, Mass., 1965. MR 33 #5416.
7. M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math. **78** (1956), 401–443. MR 18, 514.
8. ———, *Some rationality questions on algebraic groups*, Ann. Mat. Pura Appl. (4) **43** (1957), 25–50. MR 19, 767.
9. J.-P. Serre, *Groupes algébriques et corps de classes*, Publ. Inst. Math. Univ. Nancago, VII, Actualités Sci. Indust., no. 1264, Hermann, Paris, 1959. MR 21 #1973; errata, 30, 1200.
10. I. R. Šafarevič, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR Ser. Mat. **18** (1954), 525–578; English transl., Amer. Math. Soc. Transl. (2) **4** (1956), 185–237. MR 17, 131.
11. J. Tits, *Lectures on algebraic groups*, Lecture notes, Yale University, New Haven, Conn., 1966–67.
12. E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n* , J. Reine Angew. Math. **176** (1937), 126–140.

DEPARTMENT OF MATHEMATICS, FORDHAM UNIVERSITY, BRONX, NEW YORK 10458

Current address: Department of Mathematics, Brooklyn College (CUNY), Brooklyn, New York 11210