TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 194, 1974

RATIONAL POINTS OF COMMUTATOR SUBGROUPS OF SOLVABLE ALGEBRAIC GROUPS

BY
AMASSA FAUNTLEROY(1)

ABSTRACT. Let G be a connected algebraic group defined over a field k. Denote by $G(k)$ the group of k-rational points of G. Suppose that A and B are closed subgroups of G defined over k. Then $[A,B](k)$ is not equal to $[A(k),B(k)]$ in general. Here $[A,B]$ denotes the group generated by commutators $aba^{-1}b^{-1}$, $a \in A$, $b \in B$.

We say that a field of k of characteristic p is p-closed if given any additive polynomial $f(x)$ in $k[x]$ and any element c in k, there exists an element α in k such that $f(\alpha) = c$.

Theorem 1. *Let G be a connected solvable algebraic group defined over the p-closed field k. Let A and B be closed connected subgroups of G, which are also defined over k, and suppose A normalizes B. Then $[A, B](k) = [A(K), B(K)]$.*

2. If G, A and B are as above and k is only assumed to be perfect then there exists a finite extension k_0 of k such that if K is the maximal p-extension of k_0, then $[A,B](K) = [A(K), B(K)]$.

Introduction. Let U be an algebraically closed field and k a subfield of U. It is well known that the commutator subgroup of the algebraic group $G = \mathrm{GL}_n(U)$ is the special linear group $\mathrm{SL}_n(U)$. If k is infinite, then the commutator subgroup of $G(k) = \mathrm{GL}_n(k)$, the group of k-rational points of G, is $\mathrm{SL}_n(k)$. This fact stated in another way says that $[G, G](k) = [G(k), G(k)]$.

On the other hand if we take for G the group $SO(n, U)$ this is of course no longer true. If k is any subfield of U then $[G, G](k) = G(k)$ and $G(k)/[G(k), G(k)]$ is isomorphic to $k^*/(k^*)^2$ where k^* is the group of units in k.

This paper investigates the following more general question. Suppose A and B are closed algebraic subgroups defined over k of $\mathrm{GL}_n(U)$. If A normalizes B, is $[A, B](k) = [A(k), B(k)]$? We will prove that the equality holds whenever A and B are connected and solvable provided certain restrictions are placed on the field of definition k.

We begin in §I with the study of unipotent algebraic groups. It is shown there that the above equality holds for connected unipotent groups provided k has the following property:

Given any additive polynomial in $k[x]$, say $f(x)$, and any element c in k, there exists an element y of k such that $f(y) = c$. A field with this property will be called p-closed.

Presented to the Society, May 8, 1972; received by the editors September 15, 1972.
AMS (MOS) subject classifications (1970). Primary 20G15, 14L15, 14G05, 12E10.
Key words and phrases. Algebraic groups, algebra, algebraic geometry.

(1) This paper consists of the author's Ph.D. dissertation (Northwestern University 1970) directed by Professor Maxwell Rosenlicht.

In §II the results of §I are extended to connected solvable algebraic groups. §III is devoted to the study of p-closed fields. The existence of nonalgebraically closed p-closed fields is established.

§IV could technically have been included in §§I and II but this would sacrifice comprehension for brevity. It essentially establishes the results of §§I and II for certain types of extensions of the field of definition when this field is not p-closed. Finally, we extend in §V the main results of §II to nonconnected solvable groups but under rather strong hypotheses (Theorem 5.3).

Notation. The language and conventions of algebraic geometry used throughout our investigations are essentially those of [B, Chapter A. G]. We denote by **Z**, **Q**, **R** and **C** the rational integers, rational, real, and complex number fields respectively. $\mathbf{A}^n$ denotes affine n-space. If k is any field, char(k) denotes the characteristic of k. If G is a group, g, h elements of G then by the commutator $[g, h]$ is meant $ghg^{-1}h^{-1}$. The brackets $\langle \cdots \rangle$ denote the abstract group generated by ....

Let G be a connected solvable algebraic group defined over k. Recall that G is split over k or k-split if there exists a composition series $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = e$ consisting of connected closed normal subgroups of G defined over k such that the successive quotients are k-isomorphic to either G_a–the additive group–or to G_m–the multiplicative group. A unipotent algebraic group defined over a perfect field is always split over that field of definition and the quotients are each isomorphic to G_a.

Finally we state some elementary and well-known facts concerning commutators for the sake of easy reference. Their proofs may be found in [G, Chapter I].

Theorem 0. *Let G be a group, x, y, z elements of G and H, K, and L subgroups of G.* $[\,]^y = y[\,]y^{-1}$. *Then:*

(1) $[xy, z] = [y, z]^x[x, z]$.

(2) $[x, yz] = [x, y][x, z]^y$.

(3) $[H, K]$ *is normal in* $\langle H, K\rangle$.

(4) $[H, K] = [K, H]$.

(5) H *normalizes* K *if and only if* $[H, K] \subset K$.

(6) K *normal in Gr and* G/K *abelian if and only if* $[G, G] \subset K$.

(7) *If* $K \subseteq H$ *are each normal in* G *then* $H/K \subset Z(G/K)$ *if and only if* $[H, G] \subset K$.

(8) *If* H, K, *and* L *are normal in* G, *then* $[HK, L] = [H, L][K, L]$.

(9) *If* K *is normal in* G *then* $\langle H, K\rangle = HK$.

I. Unipotent groups. We begin with an example to motivate our study. Let p be the characteristic of U and k any subfield. Let $f(x)$ in $k[X]$ be any additive polynomial; i.e.

$$f(t + s) = f(t) + f(s) \quad \text{all } t, s \text{ in } U.$$

Let n be a fixed positive integer. Then the following law of composition defines a unipotent algebraic group structure on affine 2-space.

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 + b_1, a_2 + b_2 + f(a_1^{p^n} b_1)).$$

The algebraic group G just defined is a connected unipotent algebraic group which is defined and even split over k.

Now let $g = (a_1, a_2)$ and $h = (b_1, b_2)$ be two elements of G. Their commutator $[g, h] = ghg^{-1}h^{-1}$ can be readily computed.

$$\begin{aligned}[g,h] &= (a_1, a_2) \cdot (b_1, b_2) \cdot (-a_1, f(a_1^{p^{n+1}}) - a_2) \cdot (-b_1, f(b_1^{p^{n+1}}) - b_2) \\ &= (0, f(a_1^{p^n} b_1 - b_1^{p^n} a_1)).\end{aligned}$$

Thus G is in general not commutative. Moreover, a product of commutators $c_i = [g_i, h_i], i = 1, \ldots, r$, has the form

$$\begin{aligned}\prod_{i=1}^{r} C_i &= \left(0, \sum_{i=1}^{r} f(a_i^{p^n} b_i - b_i^{p^n} a_i)\right) \\ &= \left(0, f\left(\sum_{i=1}^{r} (a_i^{p^n} b_i - b_i^{p^n} a_i)\right)\right)\end{aligned}$$

using the additivity of f.

It is readily seen that the commutator subgroup $[G, G]$ can be identified with the additive group G_a. Hence $[G, G](k) = G_a(k) = k$. Now suppose $[G, G](k) = [G(k), G(k)]$. Then given any c in k there exists $y = \sum_{i=1}^{s} (a_i^{p^n} b_i - b_i^{p^n} a_i)$ with a_i, b_i in $k, i = 1, \ldots, s$, such that $(0, c) = (0, f(y))$, i.e., $f(y) = c$.

Definition. Let k be a field and p its characteristic. We shall say k is *p-closed* if given any additive polynomial $f(x)$ in $k[X]$ and any element c in k, there exists an element y in k such that $f(y) = c$.

It is well known that the only additive polynomials in $k[X]$ are those of the form

$$f(x) = \begin{cases} aX, & a \in k \text{ if } p = 0, \\ \sum_{i=0}^{r} a_i X^{p^i}, & a_i \in k \text{ if } p > 0. \end{cases}$$

It follows that every field of characteristic zero is p-closed (0-closed). If $p > 0$, then since X^p is an additive polynomial, it follows that a p-closed field is perfect.

If F_q is the finite field with $q = p^m$ elements then $\varphi(x) = x^p - x$ gives an F_p-linear endomorphism of the finite dimensional F_p-vector space. Its kernel is F_p; hence φ is not surjective.

Corollary. *A p-closed field is infinite and perfect.*

We will take a closer look at p-closed fields in §III.

We now turn again to algebraic groups with the following:

Lemma 1. *Let k be a p-closed field. Let φ be a k-morphism from $\mathbf{A}^2$ into a connected commutative unipotent k-group W such that*

(i) *The image of φ generates W as an algebraic group,*

(ii) *φ is additive in each of its variables, i.e. $\varphi(x_1 + x_2, y) = \varphi(x_1, y) + \varphi(x_2, y)$ and $\varphi(x, y_1 + y_2) = \varphi(x, y_1) + \varphi(x, y_2)$ for all x, y, x_1, x_2, y_1, y_2 in $\mathbf{A}^1$, and*

(iii) *$\varphi(x, y) = -\varphi(y, x)$.*

Then W has the structure of a vector group over k and $W(k)$ is generated by the image under φ of $A^2(k) = k \times k$.

Proof. Recall that an algebraic group W is called a vector group (over k) if it is isomorphic (over k) to the direct product, $G_a^n = G_a \times \cdots \times G_a$, of n-copies of the additive group. If $\operatorname{char}(k) = 0$, then it follows from [MR-IV, Propositions 1 and 2] that W is isomorphic to a vector group over k. Since k is perfect and W is defined over k, it suffices by [ibid., Proposition 2] to show every element of W has order $p = \operatorname{char}(k)$.

But by (ii) for fixed $y \in \mathbf{A}^1$ we have the map $\varphi_y \colon \mathbf{A}^1 \to W$ given by $x \to \varphi(x, y)$. Now since $\mathbf{A}^1$ carries the structure of an algebraic group, G_a, it follows that φ_y is a morphism of algebraic groups. Every element of G_a has order p, so every element of the image of φ_y has order p. Letting y vary, every element of the image of φ has order p. Since the image of φ generates W by (i), and W is commutative, this implies that W has the structure of a vector group over k.

As we have seen W is generated by $\{\varphi_y(\mathbf{A}^1) \colon y \in \mathbf{A}^1\}$. Further, by (ii), $\varphi_y(\mathbf{A}^1)$ is a subgroup of W. Since k is infinite, $k \times k$ is Zariski dense in $\mathbf{A}^2$, hence $\mathbf{A}^1 \times k$ is dense in $\mathbf{A}^2$. Thus W is generated as an algebraic group by $\{\varphi_y(\mathbf{A}^1) \colon y \in k\}$; because the group closure of $\{\varphi_y(\mathbf{A}^1) \colon y \in k\}$ contains the group closure of $\{\varphi_y(\mathbf{A}^1) \colon y \in \mathbf{A}^1\}$.

Let $H_y = \varphi_y(\mathbf{A}^1)$, $y \in \mathbf{A}^1$. Since $\{H_y \colon y \in k\}$ generates W, by a dimension argument we can find $y_1, \ldots, y_n$ in k such that the closed subgroups $H_{y_i}, i = 1, \ldots, n$, generate W. Since W is commutative, we may write $W = H_{y_1} \cdots H_{y_n}$.

Further, since φ is given by a polynomial map, being a morphism of affine varieties φ_y is a k-morphism for $y \in k$. Identifying $\mathbf{A}^1$ with G_a we have $\varphi_y \colon G_a \to H_y$, $y \in k$, a k-morphism of affine algebraic groups. We will show $W(k) = \langle \varphi(k \times k) \rangle$ by induction on n.

If $n = 1$, then $y_1 \in k$, $\varphi_{y_1} \colon G_a \to H_{y_1}$ surjective. We assume $H_{y_1} \neq e$. Then $\dim H_{y_1} = 1$ and H_{y_1} is connected (being the image under a continuous map of a connected group). Thus, since k is perfect [B, Proposition 10.9], H_y is k-isomorphic to G_a. After making this identification we get φ_{y_1} a k-endomorphism of G_a, hence given by an additive polynomial in $k[T]$. Then $\varphi_{y_1}(k) = k$ since k is p-closed. Thus $W(k) = H_1(k) = \varphi(k, y_1) \subset \langle \varphi(k \times k) \rangle$.

If $n > 1$, say $W = H_{y_1} \cdots H_{y_n}$, then by the above we know $H_{y_i}(k) \subset \langle \varphi(k \times k) \rangle$ for all i. Consider then the k-morphism $\pi \colon W \to W/H_{y_1}$. This is defined and is a k-morphism since H_{y_1} and W are k-groups [MR-I, Theorem 4]. We then have

$\overline{\varphi}$: $\mathbf{A}^2 \to W/H_{y_1}$ given by $\overline{\varphi} = \pi \circ \varphi$. $\overline{\varphi}$ is clearly defined over k and satisfies the hypotheses (i), (ii) and (iii) of the lemma.

Now W/H_{y_1} is generated by $\pi(H_{y_2}), \ldots, \pi(H_{y_n})$ and hence by induction $W/H_{y_1}(k) = \langle \overline{\varphi}(k \times k) \rangle$. From the exact sequence

$$0 \to H_{y_1} \to W \xrightarrow{\pi} W/H_{y_1} \to 0$$

if $\alpha \in W(k)$, $\pi(\alpha) \in W/H_{y_1}(k)$. Hence there exists $\beta \in \langle \varphi(k \times k) \rangle$ such that $\pi(\beta) = \pi(\alpha)$. Then $\alpha = \beta \cdot \beta^{-1}\alpha$, $\beta^{-1}\alpha \in \operatorname{Ker} \pi = H_{y_1}$ and $\beta^{-1}\alpha$ is rational over k; hence $\beta^{-1}\alpha \in H_{y_1}(k) \subset \langle \varphi(k \times k) \rangle$. Thus $\alpha \in \langle \varphi(k \times k) \rangle$. This shows $W(k) \subset \langle \varphi(k \times k) \rangle$. The other inclusion is clear since φ is a k-morphism and this completes the proof of the lemma.

Proposition 1.2. *Let G be a connected unipotent group defined over the p-closed field k. Then $[G, G](k) = [G(k), G(k)]$.*

Proof. Let $G = G_0 \supset G_1 \supset \cdots \supset G_n = e$ be a composition series for G consisting of k-closed normal subgroups, connected, with G_i/G_{i+1} k-isomorphic to G_a and $[G, G_i] \subset G_{i+1}$. Such a composition series exists by [B, 10.6 and 10.8].

We prove the theorem by induction on the dimension of G. If $\dim G = 1$, G is k-isomorphic to G_a, hence commutative and there is nothing to prove.

Since G is nilpotent, by [MR-V] G_{n-1} is central in G. Let j be the smallest integer such that G_j is central in G. If $j = 0$, G is commutative and our proposition is trivial. Thus we may assume $j \neq 0$.

Let i_0 be the largest integer such that $0 \leq i_0 \leq j$ and $[G_{i_0}, G_{j-1}] \neq e$. Then $[G_{i_0}, G_{j-1}] \subset G_j$ which is central in G and $[G_{i_0+1}, G_{j-1}] = e$.

Consider the morphism

$$\varphi\colon G_{i_0} \times G_{j-1} \to W = [G_{i_0}, G_{j-1}] \subset G_j$$

given by $\varphi(g, h) = [g, h]$. φ is clearly defined over k since G is defined over k.

If g and g' are in G_{i_0} with $g = g't$, $t \in G_{i_0+1}$, then for all $h \in G_{j-1}$ we have

$$[g, h] = [g't, h] = [t, h]^{g'}[g', h] = [g', h]$$

since $[G_{i_0+1}, G_{j-1}] = e$. Similarly, if $h, h' \in G_{j-1}$, $h = h's$, $s \in G_j$, then for all $g \in G_{i_0}$, $[g, h] = [g, h's] = [g, h']$, by the definitions of G_{i_0}, G_j. The image of φ then is independent of the class of g mod G_{i_0+1} and the class of h mod G_j.

φ induces a k-morphism, which we will again call φ,

$$\varphi\colon G_{i_0}/G_{i_0+1} \times G_{j-1}/G_j \to W.$$

By definition the image of φ generates W. W is connected and defined over k by [B, 2.3] and commutative because $W \subset G_j$ which is central in G. Since G_{i_0}/G_{i_0+1} and G_{j-1}/G_j are k-isomorphic to G_a, after making the obvious identifications we have φ: $G_a \times G_a \to W$ defined over k.

We show φ satisfies the properties (i), (ii) and (iii) of Lemma 1. Let g_1 and g_2 be elements of G_{i_0} with images x_1 and x_2 in $G_{i_0}/G_{i_0+1} = G_a$. Let $h \in G_{j-1}$ with image y in G_a; then $\varphi(x_1 + x_2, y) = [g_1 g_2, h] = [g_2, h]^{g_1}[g_1, h] = [g_2, h][g_1, h]$, since $[g_2, h] \in W$, which is central in G.

$[g_2, h]\,[g_1, h] = [g_1, h]\,[g_2, h]$ since W is commutative. Thus $\varphi(x_1 + x_2, h) = \varphi(x_1, y) + \varphi(x_2, y)$. Since $[g, h] = [h, g]^{-1}$ it follows that $\varphi(x, y) = -\varphi(y, x)$ and that φ is additive in the second variable.

Applying Lemma 1, $W(k) = \langle \varphi(G_a(k) \times G_a(k)) \rangle$. Since G_{i_0+1} and G_j are connected and defined over k, by [B, p. 157] if $(x, y) \in G_a(k) \times G_a(k)$ we can find $g \in G_{i_0}(k)$ and $h \in G_{j-1}(k)$ with images x in $G_a(k)$ and $y \in G_a(k)$. Thus $[G_{i_0}(k), G_{j-1}(k)] = \langle \varphi(G_a(k) \times G_a(k)) \rangle = W(k)$.

Now consider the exact sequence

$$0 \to W \to G \xrightarrow{\alpha} G/W \to 0.$$

Since W is defined over k, α is also defined over k [MR-I, Theorem 4]. If $x \in [G, G](k)$, $\alpha(x) \in [G/W(k), G/W(k)]$ by induction. Since W is connected, α is surjective on k-rational points by [ibid.]. Then $\alpha(x) = \prod_{i=1}^{n} [a_i, b_i]$, $a_i, b_i \in G/W(k)$. Lift a_i, b_i to $g_i, h_i \in G(k)$. Then if $y = \prod_{i=1}^{n} [g_i, h_i], y \in [G(k), G(k)]$, $y^{-1}x \in W(k) \subset [G(k), G(k)]$ since $\alpha(y^{-1}x) = e$. Thus $x = y \cdot y^{-1}x \in [G(k), G(k)]$ which shows $[G, G](k) \subset [G(k), G(k)]$. The other inclusion is always valid, thus $[G, G](k) = [G(k), G(k)]$ and this completes the proof.

Corollary 1.2.1. *Let G be a connected unipotent group. Let V be the connected center of G. If the codimension of V in G is one, then $[G, G]$ has the structure of a vector group. If G is defined over the perfect field k, then $[G, G]$ may be given the structure of a vector group defined over k.*

Proof. If codim $V = 1$ in G, then consider the morphism φ defined in the proposition: φ: $G/V \times G/V \to [G, G]$. As shown in the course of the proof of Lemma 1, $[G, G]$ is a vector group defined over k if k is perfect.

Corollary 1.2.2. *Let G be a connected two dimensional unipotent group defined over a field of characteristic zero. Then G is commutative.*

Proof. Let V be the connected center of G. dim $V \geq 1$ by [MR-IV, p. 143]. If φ: $G/V \times G/V \to [G, G]$ is constructed as above, for fixed $y \in G/V$ we have φ_y: $G/V \to [G, G]$. Since G is connected and nilpotent $[G, G]$ is connected; and if $[G, G] \neq e$, $[G, G]$ is a proper subgroup of G hence has dim $= 1$, thus $V = [G, G]$.

Since $V = G_a$ and $G/V = G_a$ [B, 10.9], φ_y: $G_a \to G_a$ is an endomorphism, hence given by an additive polynomial say $\varphi_y = aT$ in $U[T]$. But then φ_y is an isomorphism.

Thus φ_y: $G_a \to G_a$ is bijective for all y. But if $y = 0$, φ_0: $G_a \to G_a$ is the 0-map, a contradiction. Hence $[G, G] = e$.

Let G, A and B be connected algebraic groups defined over the p-closed field k. Suppose that A and B are unipotent subgroups of G and that A normalizes B. We consider the statement '$[A, B](k) = [A(k), B(k)]$'. Since $[A, B] \subset \langle A, B\rangle$, we may as well assume that $G = AB$. We begin with some preliminary results on unipotent groups defined over p-closed fields. Recall that a homomorphism of algebraic groups is called an *isogeny* if it is surjective with finite kernel.

Proposition 1.3. *Let A and B be connected unipotent algebraic groups defined over the p-closed field k. Let $f\colon A \to B$ be a k-isogeny. Then f is surjective on k-rational points; i.e., $f(A(k)) = B(k)$.*

Proof. We argue by induction on the dimension of A. Since f is an isogeny, $\dim A = \dim B$.

Suppose $\dim A = \dim B = 1$. Then A and B can be identified (via a k-isomorphism) with G_a and f is given by an additive polynomial in $k[X]$. Thus if $y \in B(k) = G_a(k) = k$, we may choose $x \in k = G_a(k) = A(k)$ such that $f(x) = y$ since k is p-closed. It follows that f is surjective on k-rational points.

Now if $\dim A > 1$, let $A_1 \subset A$ be a connected closed normal subgroup of A defined over k with A/A_1 k-isomorphic to G_a. Such a subgroup exists by [B, 10.6]. Then $B_1 = f(A_1)$ is closed connected defined over k and normal in B. Moreover B/B_1 is connected and of dimension one, hence k-isomorphic to G_a.

Consider the commutative diagram of k-groups and k-morphisms

$$\begin{array}{ccc} A_1 & \xrightarrow{f} & B_1 \\ {\scriptstyle i}\downarrow & & {\scriptstyle i}\downarrow \\ A & \xrightarrow{f} & B \\ {\scriptstyle \pi}\downarrow & & {\scriptstyle \pi'}\downarrow \\ G_a = A/A_1 & \xrightarrow{\bar{f}} & B/B_1 = G_a \end{array}$$

where the horizontal maps are induced by f, i denotes inclusion and π, π' are the quotient morphisms.

Let b be an element of $B(k)$. Then $\pi'(b) \in B/B_1(k)$. Hence from the dimension one case, there exists $\bar{a}$ in $A/A_1(k)$ with $\bar{f}(\bar{a}) = \pi'(b)$. By [B, p. 157], we may choose $a \in A(k)$ with $\pi(a) = \bar{a}$. Then $\pi(f(a)) = \pi(b)$. Then $b^{-1} \cdot f(a)$ lies in the kernel of π', i.e., in $B_1(k)$.

By induction there exists a_1 in $A(k)$ with $f(a_1) = b^{-1}f(a)$. Then $b = f(a_1^{-1})f(a)$ $= f(a_1^{-1}a)$ lies in $f(A(k))$. This completes the proof.

Corollary 1.3.1. *Let A and B be connected unipotent algebraic groups defined over the p-closed field k. Let $f\colon A \to B$ be a surjective k-homomorphism. Then f is surjective on k-rational points.*

Proof. Let N be the kernel of f and N° its connected component. Since f is a k-morphism, N and N° are k-closed, hence, defined over k, since k is perfect.

Consider the sequence of k-groups and k-morphisms

$$0 \to N^\circ \to A \xrightarrow{f_1} A/N^\circ \xrightarrow{f_2} A/N = B \to 0.$$

The composite $f_2 \circ f_1$ is clearly equal to f. But f_1 is surjective on k-rational points by [B, p. 157]. The kernel of f_2, N/N°, is finite; hence f_2 is a k-isogeny and surjective on k-rational points by Proposition 1.3. It follows that f is surjective on k-rational points.

Proposition 1.4. *Let G, A and B be connected unipotent algebraic groups defined over the p-closed field k. Assume that A and B are closed, B is normal in G, and $G = AB$. Then $G(k) = A(k)B(k)$.*

Proof. Consider the commutative diagram of k-groups and k-morphisms,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A \cap B & \longrightarrow & A & \xrightarrow{\pi} & A/A \cap B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle i} & & \downarrow & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & B & \xrightarrow{i} & G & \xrightarrow{\pi} & G/B & \longrightarrow & 0 \end{array}$$

where i denotes inclusion and π is the quotient morphism (restricted to A where necessary). By [MR-I, Theorem 8], f is an isomorphism (clearly defined over k).

Let x be any element of $G(k)$. Then $y = \pi(x)$ is in $G/B(k) = A/A \cap B(k)$. By Corollary 1.3.1, there exists a in $A(k)$ with $\pi(a) = y$. Then $\pi(a^{-1}x) = e$. So $a^{-1}x \in B(k)$. But $x = a \cdot a^{-1}x$; hence $x \in A(k)B(k)$. This shows that $G(k) \subset A(k)B(k)$. Since the other inclusion always holds the equality follows.

Corollary 1.4.1. *Let $H_1, \ldots, H_n$ be k-closed connected normal subgroups of the unipotent algebraic group G. Suppose $G = H_1 \cdots H_n$. Then $G(k) = H_1(k) \cdots H_n(k)$.*

Proof. This follows from the proposition by induction.

We need one more preliminary result before we can prove the main result of this section.

Lemma 1.5. *Let A and B be k-closed connected subgroups of the connected unipotent group G. Assume B is normal in $G = AB$ and k is p-closed. Let H be a k-closed connected subgroup of G such that $H(k) \subset [A(k), B(k)]$. Let N be the smallest normal subgroup of G containing H and assume H is normal in N. Then $N(k) \subset [A(k), B(k)]$.*

Proof. From [B, p. 108] we know $N = H \cdot [G, H]$ and hence by [B, 2.3] that N is k-closed and connected. Further, since $[A, B]$ is normal in G, $N \subset [A, B]$. Now N is generated, as an algebraic group, by the subgroups $H^x = xHx^{-1}$, $x \in G$. In fact, we claim N is generated by $\{H^x : x \in G(k)\}$.

To see this consider the morphism φ: $H \times G \to N$ given by $\varphi(h, x) = xhx^{-1}$. If M is the image of φ, then the group closure of M is N. Let M' be the image of $H \times G(k)$ under φ. Then $\varphi^{-1}(\overline{M'}) \supset \overline{H \times G(k)} = H \times G$ since $G(k)$ is Zariski dense in G. Thus $\varphi(\varphi^{-1}(\overline{M'})) = M$ and $M \subset \overline{M'}$. It follows that the group closure of M' is N. This establishes our claim.

For dimension reasons there exist $x_1, \ldots, x_n$ in $G(k)$ with $N = \langle H^{x_i} : 1 \leq i \leq n \rangle$. But since H is normal in N, $N = H^{x_1} \cdots H^{x_n}$. Since H is k-closed and the x_i are rational over k, H^{x_i} is clearly k-closed, $i = 1, \ldots, n$. Thus by Corollary 1.4.1, $N(k) = H^{x_1}(k) \cdots H^{x_n}(k)$. Our proof will be complete if we can show $H^{x_i}(k) \subset [A(k), B(k)]$.

But $x_i \in G(k)$; hence $x_i = a_i b_i$, $a_i \in A(k)$, $b_i \in B(k)$, $i = 1, \ldots, n$, by Proposition 1.4. It suffices to show $H^z(k) \subset [A(k), B(k)]$ for $z \in A(k)$ or $z \in B(k)$.

If $z \in A(k)$ we have for any $a \in A(k)$, $b \in B(k)$, $[a,b]^z = [za, b][z,b]^{-1} \in [A(k), B(k)]$. Similarly, if $z \in B(k)$, $[a,b]^z = [a,z]^{-1}[a,zb] \in [A(k), B(k)]$. Thus, for all $x \in G(k), H^x(k) \subset [A(k), B(k)]$ and hence $N(k) = H^{x_1}(k) \cdots H^{x_n}(k) \subset [A(k), B(k)]$.

Now the main result of this section:

Theorem 1.6. *Let A and B be connected closed subgroups of the unipotent algebraic k-group G. Suppose that A and B are defined over the p-closed field k and that A normalizes B. Then $[A,B](k) = [A(k), B(k)]$.*

Proof. Since $[A,B] \subset AB$, we may assume $G = AB$ and is defined over k. Let us first assume $[A, B]$ is commutative.

Choose a composition series $A = A_0 \supset A_1 \supset \cdots \supset A_m = e$ in A consisting of k-closed connected normal subgroups of A with A_j/A_{j+1} k-isomorphic to G_a, $j = 0, \ldots, m-1$. Choose a composition series for $B = B_0 \supset B_1 \supset \cdots \supset B_n = e$ with B_i k-closed, connected and normal in G, $[G, B_i] \subset B_{i+1}$, and B_i/B_{i+1} k-isomorphic to G, $i = 0, \ldots, n-1$. We assume $[A,B] \neq \{e\}$, else there is nothing to prove. We argue by induction on the dimension of $[A, B]$.

Let i_0 be the unique integer such that $[A, B_{i_0}] \neq e$, but $[A, B_{i_0+1}] = e$. Similarly let j_0 be the unique integer such that $[A_{j_0}, B_{i_0}] \neq e$, but $[A_{j_0+1}, B_{i_0}] = e$. Then, just as in the proof of Proposition 1.2, we have the morphism

$$\varphi\colon A_{j_0} \times B_{i_0} \to [A,B]$$

given by $(a,b) \to [a,b] = aba^{-1}b^{-1}$. φ induces a morphism, again called φ,

$$\varphi\colon A_{j_0}/A_{j_0+1} \times B_{i_0} \times B_{i_0+1} \to [A,B].$$

Now φ is clearly defined over k. It is also clear that $\varphi(x,y) = -\varphi(y,x)$ (recall $[A, B]$ is assumed commutative hence the additive notation). We show that φ is additive in each variable.

If $x_1, x_2 \in A_{j_0}$, $z \in B_{i_0}$ then

$$[x_1 x_2, z] = [x_2, z]^{x_1}[x_1, z] = [x_1, z][x_2, z]^{x_1}$$

since $[A, B]$ is commutative. Now $[x_2, z] \in [G, B_{i_0}] \subset B_{i_0+1}$ and, by the definition of B_{i_0+1}, $[A, B_{i_0+1}] = e$. Thus $[x_2, z]^{x_1} = [x_2, z]$. φ is then additive in the first variable. Since $\varphi(x,y) = -\varphi(y,x)$ it follows that φ is additive in the second variable.

Now identifying A_{j_0}/A_{j_0+1} and B_{i_0}/B_{i_0+1} (via k-morphisms) with G_a we have $\varphi\colon G_a \times G_a \to [A_{j_0}, B_{i_0}] = W$, φ satisfying the conditions of Lemma 1.1. It follows that $W(k) = [A_{j_0}, B_{i_0}](k) = [A_{j_0}(k), B_{i_0}(k)] \subset [A(k), B(k)]$. Now $W \subset B_{i_0+1}$ which is normal in G. $W \subset A_{j_0} B_{i_0} = G'$ and is clearly normal in G'. Thus W is normal in B_{i_0}. Let N be the smallest normal subgroup of G containing W. Since $N \subset B_{i_0}$ and W is normal in B_{i_0}, hence in N, we may apply Lemma 1.5. Thus $N(k) \subset [A(k), B(k)]$.

Since N is connected, k-closed and normal in G, by [MR-IV, p. 143] N contains a connected k-closed central subgroup V of G with $V \neq e$, since $N \neq e$.

Consider the exact sequences of k-groups and k-morphisms

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \longrightarrow & [A, B] & \xrightarrow{\pi} & [A, B]/V & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle i} & & \downarrow & & \\ 0 & \longrightarrow & V & \longrightarrow & G & \xrightarrow{\pi} & G/V & \longrightarrow & 0 \end{array}$$

If $x \in [A,B](k)$ then $\pi(x) \in [A,B]/V(k) = [\pi(A), \pi(B)](k) = [(\pi A)(k), (\pi B)(k)]$ by induction on $\dim[A, B]$. Since V is connected and k-closed by [B, p. 157] $\pi\colon B \to B/V$ is surjective on k-rational points thus; $(\pi B)(k) = \pi(B)(k)$. We also have $(\pi A)(k) = \pi(A(k))$, by Corollary 1.3.1.

Thus $\pi(x) \in [\pi(A(k)), \pi(B(k))]$. Then there exist $a_i \in A(k)$, $b_i \in B(k)$, $i = 1, \ldots, n$, with $y = [a_1, b_1] \cdots [a_n, b_n] \in [A(k), B(k)]$ and $\pi(y) = \pi(x)$. Now $\pi(y^{-1}x) = e$, so $y^{-1}x \in \operatorname{Ker} \pi$, i.e., $y^{-1}x \in V(k) \subset [A(k), B(k)]$. Thus $x = yy^{-1}x \in [A(k), B(k)]$; hence $[A, B](k) \subset [A(k), B(k)]$. The reverse inclusion is clear; thus $[A, B](k) = [A(k), B(k)]$.

To complete the proof of the theorem we must establish the result for $[A, B]$ not commutative. For this we need the following

Lemma. *Let k be p-closed. Let H be a k-closed connected normal unipotent subgroup of the algebraic group G defined over k. Let $\psi\colon G \to G' = G/[H, H]$ be the canonical projection and L a subset of $G(k)$. If $\psi(L)$ generates $G'(k)$, then L generates $G(k)$.*

Granting the lemma we let $H = [A, B]$ and $\psi\colon G \to G' = G/[H, H]$. Then in G', $[\psi(A), \psi(B)]$ is commutative; hence $[\psi(A), \psi(B)](k) = [\psi(A)(k), \psi(B)(k)]$. Let $L = [A(k), B(k)]$, $\psi(L) = [\psi(A)(k), \psi(B)(k)]$ by [B, p. 157] and Corollary 1.3.1. Restricting ψ to H we apply the above lemma with $H = G$. Then $\psi\colon H \to H/[H, H]$, $\psi(L)$ generates $H/[H, H](k)$; hence L generates $H(k) = [A, B](k)$.

It remains to prove

Lemma 1.7. *Let k be p-closed, H a k-closed connected unipotent subgroup of the algebraic group G defined over k. Suppose H is normal in G and let $\psi\colon G \to G' = G/[H, H]$ be the canonical projection. Then if $\psi(L)$ generates $G'(k)$, L generates $G(k)$.*

Proof. (*Note*: The lemma was proven for char $k = 0$ by Borel and Tits in [B-

T, 13.3]. Their proof, given here, holds word for word for p-closed fields once Proposition 1.2 has been established.)

We argue by induction on dim G. If dim $G = 1$ this is clear. If H is commutative there is nothing to prove. Hence assume $[H, H] \neq e$. Let $V \subset H$ be the last nontrivial term in the descending central series for H. V is connected, defined over k, and normal in G.

Let L^* denote the subgroup of G generated by L. We know $G/V(k) = G(k)/V(k)$ [B, p. 157]. We have for φ: $G \to G/V$, by our inductive assumption, $\varphi(L) = G/V(k) = G(k)/V(k)$ so $G(k) = L^* \cdot V(k)$. Thus $H(k) = (L^* \cap H(k)) \cdot V(k)$. But if $x = av$, $y = bw$ with $a, b \in L^* \cap H(k)$, $v, w \in V(k)$, we have, since v and w are central in H, $[x,y] = [a,b]$ which implies that $[H,H](k) = [H(k), H(k)]$ (by Proposition 1.2) is contained in L^*. But $V(k) \subset [H,H](k)$, so $V(k) \subset L^*$ and thus $H(k) \subset L^*$, i.e., $G(k) = L^*$.

Corollary 1.8. *Let H be a k-closed connected subgroup of the connected unipotent group G. Assume k is p-closed and G is defined over k. Then $[G,H](k) = [G(k), H(k)]$.*

Proof. Take $A = H$, $B = G$ in the proposition.

Corollary 1.9. *Let G be a connected nilpotent group defined over the p-closed field k. Let A and B be k-closed connected subgroups of G with A normalizing B. Then $[A,B](k) = [A(k), B(k)]$.*

Proof. Since G, A and B are nilpotent, from the structure theorems for such groups, we know that toroidal elements are central. It follows that $[A,B] = [A_u, B_u]$. But A_u and B_u are defined over k by [B, 10.6]. Hence, by the proposition, $[A,B](k) = [A_u, B_u](k) = [A_u(k), B_u(k)]$. Consequently, $[A,B](k) \subset [A(k), B(k)]$, and the desired equality follows from this inclusion.

II. **Solvable groups.** In this chapter we shall extend Proposition 1.6 to connected solvable groups defined over p-closed fields. It is well known that a connected solvable algebraic group is the semidirect product of a torus and a unipotent group. The action of tori on unipotent groups plays a crucial role in our investigation of solvable groups.

2.1. *Tori acting on commutative unipotent groups.* Let T be a torus defined over the infinite perfect field k. Let W be a connected commutative unipotent k-group on which T acts k-morphically, i.e., there exists a k-morphism of k-varieties φ: $T \times W \to W$ such that $w \to \varphi(t,w)$ is an automorphism of W for each t in T. The semidirect product (i.e., $T \times W$ with multiplication given by $(t,w) \cdot (t',w') = (tt', \varphi(t',w)w')$) is then a connected solvable algebraic group, and it is clearly defined over k.

Since k is infinite, by [B, Corollary 9.5], there exists t in $T(k)$ such that $Z_W(t)^\circ$, the connected component of the centralizer of t in W, equals $Z_W(T)^\circ$. (Here T and W are considered to be subgroups of the semidirect product $T \cdot W$.)

Let c_t: $W \to W$ be the morphism defined by $c_t(w) = twt^{-1}w^{-1}$. This mor-

phism is defined over k since t is in $T(k)$. Further, if $w_1, w_2 \in W$, then $c_t(w_1 w_2) = c_t(w_1)w_1 c_t(w_2)w_1^{-1} = c_t(w_1)c_t(w_2)$ using elementary properties of commutators and the commutativity of W. Let $M = c_t(W)$ be the image of the homomorphism c_t. Then M is defined over k. Moreover, by [B, Proposition 9.3] W is isomorphic to $M \times Z_W(t)$ over k and $c_t\colon M \to M$ is an isomorphism. Since c_t is defined over k, given $x \in M(k)$, there exists $y \in M(k)$ such that $c_t(y) = x$. This shows that $M(k) \subset [t, W(k)] \subset [T(k), W(k)]$.

But $Z_W(t)$ is connected by [ibid.], and equals $Z_W(T)^\circ$ by the choice of t. Thus, $[T, W] = [T, M \cdot Z_W(t)] = [T, M] \subset M$. But then $[T, W](k) \subset M(k) \subset [t, M(k)] \subset [T(k), W(k)]$. The inclusion $[T(k), W(k)] \subset [T, W](k)$ always holds. Hence we have proved the following:

Proposition 2.1. *Let T be a torus defined over the infinite perfect field k. Let W be a connected commutative unipotent k-group on which T acts k-morphically. Let $G = T \cdot W$ and consider T and W as subgroups of G. Then $[T, W](k) = [T(k), W(k)]$.*

Corollary 2.2. *Let T be a torus defined over the p-closed field k. Let W be a connected unipotent k-group on which T acts k-morphically and let $G = T \cdot W$. Then $[T, W](k) = [T(k), W(k)]$.*

Proof. Let $M = [T, W]$. By [T, Proposition 3.3.2, p. 149], M is normal in G and $[T, M] = M$. M is clearly connected and defined over k.

If M is commutative, then by the proposition, $M(k) = [T, M](k) = [T(k), M(k)]$. Hence $[T, W](k) = M(k) \subset [T(k), W(k)]$ and the desired equality follows from this inclusion.

If M is not commutative we consider the quotient $N = M/[M, M]$. T acts on N and $[T, N](k) = [T(k), N(k)]$ by the proposition. Let $L = [T(k), M(k)]$. $[M, M]$ is connected and defined over k. Hence the k-morphism $\pi\colon M \to N$ is surjective on k-rational points [B, p. 157]. It follows that the map $T \cdot M \to T \cdot N$ induced by π is surjective on k-rational points, and that $\pi(L) = [T(k), N(k)]$.

We now apply Lemma 1.7 to the k-morphism $\pi\colon M \to N$ and $L \subset M(k)$. We thus have $L = M(k)$. Then $[T, W](k) = M(k) = [T(k), M(k)] \subset [T(k), W(k)]$. Again we have established the vital inclusion. The desired equality follows.

Lemma 2.3. *Let G be a connected solvable group defined over the p-closed field k and N a k-closed connected normal unipotent subgroup of G. Let $\pi\colon G \to G/N$ be the canonical quotient morphism. Then if A is any k-closed connected subgroup of G, $\pi|_A$ is surjective on k-rational points.*

Proof. If A is unipotent the lemma follows from Corollary 1.3.1. If A is a k-torus then $\pi|_A$ is an isomorphism because $A \cap N = e$. Thus if A is a torus defined over k, $\pi(A(k)) = \pi(A)(k)$.

Given any k-closed subgroup A of G, there exists a maximal torus, $S \subset A$, which is defined over k by [MR-III, Theorem 5]. A is then the semidirect product

of S and A_u, the unipotent radical of A. Then $\pi(A) = \pi(S \cdot A_u) = \pi(S) \cdot \pi(A_u)$, and it follows that $\pi(A(k)) = \pi(S(k)) \cdot \pi(A_u(k)) = \pi(S)(k) \cdot \pi(A_u)(k) = \pi(A)(k)$. This proves the lemma.

Theorem 2.4. *Let G be a connected solvable algebraic group defined over the p-closed field k. Suppose that A and B are k-closed connected subgroups of G with B normal in $G = AB$. Then $[A,B](k) = [A(k), B(k)]$.*

Proof. Let $H = [A,B]$. Let $V \subset H$ be a k-closed connected normal subgroup of G. Then V is unipotent. Let $\pi\colon G \to G/V$ be the quotient morphisms and suppose that $[\pi(A),\pi(B)](k) = [\pi(A)(k),\pi(B)(k)]$. Then, by Lemma 2.3, $\pi[A(k), B(k)] = [\pi(A)(k),\pi(B)(k)]$ generates $\pi(H)(k)$. If we restrict π to H, then it follows from Lemma 1.7 that $[A,B](k) = [A(k), B(k)]$.

We shall use this reduction procedure to pass to quotient groups of G. In particular we may assume (passing to the quotient of G by $[H, H]$) that H is commutative.

Let T be a maximal torus of G which is defined over k. Then $T \cdot H$ is k-closed solvable and connected. Moreover $H = [T,H] \times Z_H(T)$ by [B, 9.3]. It follows that $[T, H]$ is normal in G and obviously contained in H. Hence we may further assume (again, passing to the quotient of G by $[T, H]$ if necessary) that $[T,H] = e$.

Now suppose that $Q \subset B$ is a maximal torus in B which is defined over k. By [B-T, 11.5] some conjugate of Q by an element, say x, of $G(k)$ lies in T. Thus $Q^x \subset B^x = B$, and we may assume without loss that $Q \subset T$. Let $S \subset A$ be a maximal torus of A which is defined over k. Some conjugate of S by an element, say y, of $G(k)$ also lies in T. Since $[A, B]$ is normal in G, $[A,B] = [A,B]^y = [A^y, B^y] = [A^y, B]$. Hence we may also assume without loss of generality that $S \subset T$.

Now let $a \in A$ and $b \in B$. Then by [B, Theorem 10.6] we may write $a = su$ and $b = qv$ with $s \in S$, $q \in Q$, $u \in A_u$ and $v \in B_u$. We then have, using elementary group theory

$$[a,b] = [su, qv] = [u, qv]^s[s, qv] = [u, qv][s, qv]$$

(since $S \subset T$ and $[T,H] = e$). Expanding further and using the facts that $[T,H] = e$ and $[S,Q] = e$ we get

$$[a,b] = [u,q][u,v][s,v].$$

This last equality shows that H is generated by the subgroups $H_1 = [Q, A_u]$, $H_2 = [A_u, B_u]$ and $H_3 = [S, B_u]$. It follows from Corollary 1.4.1 that $H(k) = H_1(k)H_2(k)H_3(k)$.

Now $H_2(k) = [A_u(k), B_u(k)] \subset [A(k), B(k)]$ by Proposition 1.6 and $H_3(k) = [S(k), B_u(k)]$ by Corollary 2.2.

Since $Q(k)$ is dense in Q, it follows that $[Q, A_u]$ is generated by the subsets $[t, A_u] = \{tut^{-1}u^{-1} \mid u \in A_u\}$ as t runs through the elements of $Q(k)$. For

dimension reasons there exists a finite number of elements $t_i \in Q(k), i = 1, \ldots, n$, such that the subsets $[t_i, A_u]$ generate $[Q, A_u]$.

Let $N = H/H_2H_3$ and $\pi: H \to N$ be the quotient map. Define maps $\varphi_i(a) = \pi([t_i, a]), i = 1, \ldots, n$. Then since the sets $[t_i, A_u]$ generate $[Q, A_u]$ the images of the φ_i generate N. Furthermore $\varphi_i(aa') = \pi([t_i, aa']) = \pi([t_i, a][t_i, a']^a) = \pi([t_i, a]) \cdot \pi([t_i, a']) = \varphi_i(a)\varphi_i(a')$ since $H_2 = [A_u, B_u]$. Let N_i be the image of φ_i so that $N = N_1 \cdots N_r$. Each $N_i(k) = \varphi_i(A_u(k))$ by Lemma 2.3 and $N(k) = N_1(k) \cdots N_r(k)$. Thus the map $[Q(k), A_u(k)] \to^{\pi} N(k)$ is surjective.

Now consider the exact sequence

$$0 \to H_2H_3 \to H \xrightarrow{\pi} N \to 0.$$

If $x \in H(k) = [A, B](k)$, then $\pi(x) \in N(k)$. Hence there exists $y \in [Q(k), A_u(k)]$ such that $\pi(y) = \pi(x)$. Then $xy^{-1} \in H_2H_3(k) = H_2(k)H_3(k) \subset [A(k), B(k)]$. It follows that $x = xy^{-1}$, $y \in [A(k), B(k)]$. This proves the critical containment $[A, B](k) \subset [A(k), B(k)]$, and hence the theorem.

III. ***p*-closed fields.** In this chapter we establish the existence of nonalgebraically closed p-closed fields. Since every field of characteristic zero is p-closed, we restrict our attention to fields of positive characteristic.

Recall that a pro-finite group is a topological group which is the projective (direct) limit of finite groups, each with the discrete topology. Such a group is compact and totally disconnected. For example, if k^s is the separable closure of a field k, then the galois group–$G = \mathrm{Gal}(k^s/k)$–of k^s over k is a pro-finite group. G is the direct limit of the groups $G_i = \mathrm{Gal}(k_i/k)$ where k_i is a finite galois extension of k.

Following [S], a *super natural number* will be a formal product, $\Pi_{\mathrm{allprimes};q} q^{n_q}$, where n_q is either nonnegative or infinite. One speaks of the l.c.m. or g.c.d. of two or more super natural numbers in the obvious manner.

Recall also that if $U \subset G$ is an open normal subgroup of the pro-finite G, then G/U is finite; and conversely, if H is a finite factor group of G, then $H = G/U$ for some $U \subset G$ open and normal. If $N \subset G$ is a closed subgroup of G, we define the *index of N in G* to be the super natural number which is the l.c.m. of the indices $(G/U\colon H/H \cap U)$ as U runs through the set of open normal subgroups of G. The index of N in G will be denoted $(G\colon N)$. The *order of a pro-finite group* is by definition $(G\colon e)$.

Let p be a prime number. A pro-finite group H is called a *pro-p-group* if it is the direct limit of finite p-groups, or, equivalently, if its order is a (possibly infinite) power of p. A closed subgroup P of G is called a *p-Sylow subgroup* if it is a pro-p-group and if $(G\colon P)$ is prime to p.

Proposition [S, Chapter I, Proposition 3]. *Every pro-finite group possesses p-Sylow subgroups and any two of these are conjugate. Every pro-p-subgroup of a pro-finite group is contained in p-Sylow subgroup.*

Theorem 3.1. *Let K be an infinite perfect field and $G = \mathrm{Gal}(\bar{k}/k)$ the galois*

group of the algebraic closure, $\bar{k}$, of k. Let N be any closed subgroup of G whose order is prime to the characteristic p of k. Then $K = \bar{k}^N$ is p-closed.

Proof. Recall that K is p-closed if and only if given any polynomial $\varphi(X) \in K[X]$ of the form $\varphi(X) = \sum_{i=0}^{n} a_i X^{p^i}$ and any $c \in K$, there exists $y \in K$ such that $\varphi(y) = c$.

Let $\varphi(X) \in K[X]$ and $c \in K$ be as just described. If $c = 0$, then $X = 0$ solves our problem. We may thus assume that $c \neq 0$. Say $\varphi(X) = \sum_{i=0}^{n} a_i X^{p^i}$ with $a_m \neq 0$ but $a_i = 0$ for $i < m$. Then $\varphi(X) = \sum_{i=m}^{n} a_i X^{p^i}$. Further, since K is perfect $c^{1/p^m} \in K$. Put $\psi(X) = (\varphi(X))^{1/p^m}$ so that $\psi(X) = a'_m X + a'_{m+1} X^p + \cdots + a'_n X^{p^{n-m}}$ where $a'_i = a_i^{1/p^m}$ for $m \geq i \leq n$. It is immediate that $\psi(X)$ is again an additive polynomial. If $\beta \in K$ and $\psi(\beta) = c^{1/p^m}$, then $\varphi(\beta) = c$. We may assume then that $\varphi(X) = \sum_{i=0}^{n} a_i X^{p^i}$ with $a_0 \neq 0$ and thus that $\varphi(X)$ is a separable polynomial.

Now by definition $\mathrm{Gal}(\bar{K}/K) = N$ and the order of N is prime to p. If L is any finite extension of K with $L \subset \bar{K}$, then $[L\colon K]$ is prime to p; for L is clearly contained in a finite galois extension E of K and, since $[L\colon K]$ divides $[E\colon K]$ which is prime to p, $[L\colon K]$ is also prime to p.

Now consider the equation $\varphi(X) - c = 0$ where $\varphi(X)$ is our given separable additive polynomial in $K[X]$ and $c \in K$, $c \neq 0$. Since the degree of $f(X) = \varphi(X) - c$ is p^n, $f(X)$ cannot be irreducible in $K[X]$. For if it were, adjoining a root γ of $F(X)$ to K would give $L = K(\gamma)$, $[L\colon K] = p^n$, contradicting what has been established above. Thus $f(X)$ factors in $K[X]$, say $f(x) = f_1(x) \cdots f_r(x)$ with $f_i(x)$ irreducible and separable for $i = 1, \ldots, r$.

Consider now $f_1(x)$. If the degree of $f_1(x)$ is one we have a root. In any case the degree of f_1 must be prime to p by the same argument used above. Let m be the degree of f_1. Let $\alpha_1, \ldots, \alpha_m$ be the roots of f_1. They are all distinct since f_1 is separable.

Let $E = K(\alpha_1, \ldots, \alpha_m)$. Now each $\alpha_i (1 \leq i \leq m)$ is a root of $f(x) = \varphi(x) - c$. Hence $\varphi(\alpha_i) = c$ for $1 \leq i \leq m$. Let $\gamma = \mathrm{tr}_K^E(\alpha_1) = \alpha_1 + \cdots + \alpha_m$ be the trace of α_1 from E to K. Then $\gamma \in K$ and $\varphi(\gamma) = \varphi(\alpha_1 + \cdots + \alpha_m) = \varphi(\alpha_1) + \cdots + \varphi(\alpha_m) = \bar{m}c$. Here $\bar{m}$ is the class of m mod p.

Since m is prime to p, there exists $s \in F_p$ with $s\bar{m} = 1$. Then if $y = s \cdot \gamma$ we have $\varphi(y) = \varphi(s\gamma) = s\varphi(\gamma) = s\bar{m}c = c$. We have thus constructed a root, y, of $f(x) = \varphi(x) - c$, $y \in K$, and hence K is p-closed.

We give another description of those closed subgroups of G whose orders are prime to p. The discrete abelian groups on which G acts continuously form an abelian category. One thus has a cohomology theory which associates to such a G-module A, the cohomology complex of abelian groups, $H^n(G, A)$, $n = 0, 1, 2, \ldots$, called the cohomology groups of G with coefficients in A.

Now if p is a prime integer, the *p-cohomological dimension* of G, denoted $\mathrm{cd}_p(G)$, is the least upper bound of all integers m satisfying:

(*) For every discrete torsion G-module A and all $n > m$, the p-primary component of $H^n(G, A)$ is zero.

Proposition [S, Chapter I, p. 21]. *If* $\mathrm{cd}_p(G) = 0$ *then the order of* G *is prime to* p *and conversely.*

Hence Theorem 3.1 could have been stated in cohomological terms:

Let k be an infinite perfect field of characteristic p and $G = \mathrm{Gal}(\bar{k}/k)$. If N is a closed subgroup of G such that $\mathrm{cd}_p(N) = 0$, then the fixed field of N is p-closed.

We do not know at present whether or not the converse holds.

Maximal p-extensions. Let k be a perfect field (of arbitrary characteristic) and let $G = \mathrm{Gal}(\bar{k}/k)$ be its galois group. If p is any prime number we denote by $G^{[p]}$ the largest quotient of G which is a pro-p-group. If $G^{[p]} = G/N$ then we call $\bar{k}^N$, denoted $k^{[p]}$, the *maximal p-extension of k.* By definition $k^{[p]}$ is normal.

We now give some examples to illustrate these concepts.

Example 3.2. Let p be a prime number and F_p the prime field of characteristic p. Then, as is well known (see for example [L]), $G = \mathrm{Gal}(\bar{F}_p/F_p) = \hat{\mathbf{Z}} \cong \prod_{q\,\text{prime}} \hat{\mathbf{Z}}_q$, where $\hat{\mathbf{Z}}_q$ is the completion of the integers at the prime q. If $N = \prod_{q \neq p} \hat{\mathbf{Z}}_q$, it is not hard to see that $G/N \cong \hat{\mathbf{Z}}_p$ is the largest quotient of G which is a pro-p-group. A straightforward computation also shows that the order of N is prime to p. It follows then that $K = F_p^{[p]}$ is infinite and perfect and, since $\mathrm{cd}_p(N) = 0$, that K is p-closed.

The procedure of taking the maximal p-extension of a field of characteristic p does not yield, in general, a p-closed field however. Consider the following example.

Example 3.3. Let k_0 be an algebraically closed field of characteristic $p > 0$. Let $k_1 = k_0(t)$, t transcendental over k_0, and let k be the perfect closure of k_1. Finally let $K = k^{[p]}$ be the maximal p-extension of k. We will show that the polynomial $X^p - tX - t$ has no root in K and thus that K is not p-closed.

First we show that $X^p - tX - t$ is irreducible over k. Suppose $X^p - tX - t = g(x)h(x)$ factors in $k[X]$. Then the degree of g (and h) must be prime to p. The trace argument used in the proof of Theorem 3.1 then shows that there exists a root of $X^p - tX - t$ in k. Since our polynomial is separable this root must lie in $k_1 = k_0(t)$ since k/k_1 is purely inseparable.

Suppose then that $\gamma = \alpha(t)/\beta(t)$ is a root of $f(X) = X^p - tX - t$. We may assume $\alpha(t)$ and $\beta(t)$ are relatively prime in $k_0[t]$. Now since γ is a root we have

$$\alpha^p/\beta^p - t\alpha/\beta - t = 0,$$

which yields

$$\alpha^p - t\alpha\beta^{p-1} - t\beta^p = 0,$$

i.e., $\alpha^p = t\alpha\beta^{p-1} + t\beta^p$. Thus β divides α contradicting our assumption that $(\alpha, \beta) = 1$. Thus $X^p - tX - t$ is irreducible over k.

Now if $f(X)$ has one root in K it has all of its roots in K since K is normal over k. Suppose $\alpha_1, \ldots, \alpha_p$ are these roots. Then $\beta_i = \alpha_1 - \alpha_i, i = 1, \ldots, p$, are all distinct and roots of $X^p - tX$; for

$$\begin{aligned}\beta_i^p - t\beta_i &= (\alpha_1^p - \alpha_i^p) - t(\alpha_1 - \alpha_i)\\ &= \alpha_1^p - t\alpha_1 - (\alpha_i^p - t\alpha_i)\\ &= t - t = 0.\end{aligned}$$

Thus $X^p - tX$ splits in K, i.e., $X^{p-1} - t$ splits in K. Now $X^{p-1} - t$ is clearly irreducible in $k[X]$ and hence, if E is its splitting field, $p - 1$ divides $[E: k]$. But $[K: k]$ is a power of p and $E \subset K$ is a contradiction. Hence $X^p - tX - t$ has no root in K.

Let K be a p-closed field and assume that $\mathrm{cd}_p(K) = \mathrm{cd}_p(\mathrm{Gal}(\overline{K}/K)) = 0$. Let E be a finite extension of K. Then if $H = \mathrm{Gal}(\overline{K}/E)$, since $H \subset \mathrm{Gal}(\overline{K}/K)$, $\mathrm{cd}_p(H) = 0$ also. Thus E is p-closed by Theorem 3.1. We have even more.

Theorem 3.4. *Let K be a p-closed field. Then the following conditions are equivalent*

(i) *Every finite extension of K is p-closed.*

(ii) *Every finite extension E of K with $[E:K]$ prime to p is p-closed.*

(iii) $\mathrm{cd}_p(K) = 0$.

Proof. We have just seen that (iii) implies (i) and (ii). Also, that (i) implies (ii) is clear. We show now that (ii) implies (iii).

Let E be a finite galois extension of K and suppose that p divides $[E:K]$. Let $G = \mathrm{Gal}(E/K)$ and G_p a p-Sylow subgroup.

Then we have

$$\begin{array}{c} E \\ | \\ E_p = E^{G_p} \\ | \\ K \end{array}$$

with $[E: E_p] = p^n$ and E/E_p galois with group G_p. By (ii) and the fact that $[E_p: K]$ is prime to p, E_p is p-closed. Since G_p is a p-group it is nilpotent. Hence there exists $H_p \subset G_p$, normal, with $G_p/H_p = \mathbf{Z}/p\mathbf{Z}$. Then $L = E_p^{H_p}$ is a cyclic extension of E_p of degree p. By Artin-Schreier theory [L, Chapter 8, Theorem 11] such an extension is the splitting field of an equation of the type $X^p - X + a$, $a \in E_p$.

But E_p is p-closed; hence $X^p - X + a$ splits in E_p. Thus $L = E_p$ and hence $[E: K]$ must have order prime to p. This means that if U is any open normal subgroup of $G' = \mathrm{Gal}(\overline{K}/K)$, then the order of G'/U is prime to p. For given such a U, $E = \overline{K}^U$ is a finite galois extension of K and the order of $G'/U = [E: K]$. This implies that the order of G' is prime to p, i.e., $\mathrm{cd}_p(G') = \mathrm{cd}_p(K) = 0$.

Corollary 3.5. *If K is p-closed then $K = K^{[p]}$.*

Proof. Let L be a finite galois extension of K with $[L: K] = p^n$ and galois group

G. Then since G is a p-group, hence nilpotent, there is a normal subgroup $G_1 \subset G$ with $G/G_1 \cong \mathbf{Z}/p\mathbf{Z}$.

Let $K_1 = L^{G_1}$. Then K_1/K is galois and cyclic of degree p. By Artin-Schreier theory again we conclude that K_1 is the splitting field of a polynomial of the form $X^p - X + a$, $a \in K$. But since K is p-closed such a polynomial has a root in K. This contradiction shows that K has no finite galois extensions of degree p^n and hence $K = K^{[p]}$.

Minimal p-closed extensions. Let k be a perfect field. An algebraic extension K of k will be called a *minimal p-closed extension* of k if K is p-closed and is contained in any other p-closed field (inside $\bar{k}$) containing k.

Proposition 3.6. *Let k be a perfect field. Let K be a minimal p-closed extension of k. Then $K = k^{[p]}$.*

Proof. Let $G = \mathrm{Gal}(\bar{k}/K)$ and $N = \mathrm{Gal}(\bar{k}/k)$. If q is any prime not equal to p, then the q-Sylow subgroup G_q has order prime to p. Thus, by Theorem 3.1, $\bar{k}^{G_q}$ is p-closed. It follows that $K \subset \bar{k}^{G_q}$, i.e., $G_q \subset N$.

Since any conjugate of G_q is also a q-Sylow subgroup, N contains all q-Sylow subgroups for all primes different from p. Moreover, if $\lambda \in G$, and $N^\lambda = \lambda N \lambda^{-1}$, then $K^\lambda = \bar{k}^{N^\lambda} = \lambda K$ is p-closed; hence $N^\lambda \subset N$. Thus N is normal.

From this it follows that G/N is a pro-p-group. But then by the definition of $k^{[p]}$ we must have $K \subset k^{[p]}$. Alas, Corollary 3.5 tells us that $K \supset k^{[p]}$, and hence $K = k^{[p]}$.

Theorem 3.7. *Let k be a perfect field of positive characteristic. Let $f_1, \ldots, f_n$ be additive polynomials in $k[X]$. Then there exists a finite extension, k_0, of k such that $k \subset k_0 \subset \bar{k}$ and the maximal p-extension $K = k_0^{[p]}$ of k_0 satisfies the following property:*

Given $c \in K$ and any f_i, $1 \leqslant i \leqslant n$,
there exists $\alpha_i \in K$ such that $f_i(\alpha_i) = c$.

Proof. Since k is perfect, we may assume, as in the proof of Theorem 3.1, that $f_1, \ldots, f_n$ are separable. Let k_0 be the splitting field of the set of polynomials $\{f_1, \ldots, f_n\}$. Let $K = k_0^{[p]}$. We must show that given $c \in K$ and any f_i, there exists a root of $g_i(x) = f_i(x) - c$ in K.

Fix i. Suppose first that $g_i(x)$ is irreducible. Let γ be any root of $g_i(x)$. Then $K(\gamma)$ has degree $p^n = \deg(g_i) = \deg(f_i)$ over K. We claim $K(\gamma)$ is normal; indeed, if $\beta_1, \ldots, \beta_{p^n}$ are the roots of $f_i(X)$, then, since f_i is additive and separable, $\gamma + \beta_1, \ldots, \gamma + \beta_{p^n}$ are p^n distinct roots of $g_i(x)$. Each $\gamma + \beta_j$, $1 \leq j \leq p^n$, lies in $K(\gamma)$; hence $K(\gamma)$ is normal.

Since $K = k_0^{[p]}$, K has no normal extensions of degree p^n. Hence $K = K(\gamma)$ and $g_i(x)$ has not only one, but all of its roots in K.

Now suppose $g_i(x)$ were reducible. Say $g_i(x) = h_1(x) \cdots h_r(x)$ with $h_j \in K[X]$. If γ_j is a root of h_j, then the above argument again shows that $K(\gamma_j)$ splits $g_i(x)$.

Thus adjoining any root of any of the h_j's leads to the same extension of K–the splitting field of $g_i(x)$.

In particular this shows that $\deg h_1 = \deg h_2 = \cdots = \deg h_r$. Let s be this common degree. It follows from the fact that $g_i(x) = h_1(x) \cdots h_r(x)$ that $p^n = s \cdot r$, and therefore $s = p^t$ for some $t \geq 0$. If $t = 0$ then $s = 1$ and all roots lie in K. If t were not zero, then $K(\gamma_j)$ would be an extension of degree p^t. But this contradicts the fact that $K = k_p^{[p]}$ has no normal extensions of degree p^t. Thus in any case K splits $g_i(x)$ and this completes the proof.

Remark. If $K = k_0^{[p]}$ is as in the proof of the theorem and if k_1/k_0 is finite, then it is clear that $K_1 = k_1^{[p]}$ satisfies the same properties relative to $f_1, \ldots, f_n$ as K does.

IV. Almost finite extensions. Many rationality questions involving algebraic groups and morphisms of these groups may not be answerable over arbitrary fields of definition for these groups and morphisms. Often, however, these same questions are answerable over finite algebraic extensions of a given field of definition. For example, a connected solvable algebraic group defined over a field k splits over a finite extension of k [B, 18.4].

We ask a similar question here concerning the group of rational points of commutator subgroups in solvable groups. More precisely, let A and B be closed connected subgroups of the solvable algebraic group G. Suppose G, A and B are defined over k and that B is normal in $G = AB$. Is there a finite extension of k, say K, such that $[A,B](K) = [A(K), B(K)]$? More generally, what are the 'minimal extensions' of k for which the above equality holds?

In general, finite extensions of k will not suffice as the following example illustrates.

Example 4.1. Let $k = F_p(t)^{1/p^\infty}$ be the perfect closure of the function field $F_p(t)$. Let G be the unipotent group defined in the example of §I with $f(T) = T^p - T$.

Recall that an element of the commutator subgroup of G can be expressed as a sum of elements of the form $(0, x^p - x)$, where $x = a^p b - b^p a$ for some a and b in $\mathbf{A}'$. A sum of such elements still has the same form, i.e., $(0, t^p - t)$, $t = \sum_{i=1}^n a_i^p b_i - b_i^p a_i$ with a_i, b_i in $\mathbf{A}'$.

Suppose K is a finite extension of k such that $[G,G](K) = [G(K), G(K)]$. It follows, then, that given any c in K, there exists a root of $T^p - T - c$ in K. By Artin-Schreier theory, all roots of $T^p - T - c$ then lie in K. It follows (from Artin-Schreier again) that K has no cyclic extension of degree p, i.e., $K = K^{[p]}$. Since $K \supset k$, $K = K^{[p]} \supset k^{[p]}$. Thus $[k^{[p]}: k]$ is finite. But $F_p \subset F_p^{[p]} \subset k^{[p]}$ and $[F_p^{[p]}: F_p]$ is not finite. Since F_p and k are linearly disjoint over $F_p^{[p]} \subset \overline{F}_p$, $[k^{[p]}: k]$ cannot be finite. Hence there exists no finite extension K of k with $[G,G](K) = [G(K), G(K)]$.

Suppose we are considering some 'rationality question,' say (S, k) concerning algebraic groups and morphisms of these groups defined over k. We shall say that the question (S, k) admits a *finite k-solution* if:

(i) There exists a finite algebraic extension k_0 of k which makes (S, k_0) a true statement in the obvious sense.

(ii) If k_1 is any finite extension of k_0 then (S, k_1) is also a true statement.

For example the problem of splitting a torus T defined over k is finitely k-solvable [B, 8.11].

We shall say the rationality question (S, k) admits an *almost finite k-solution* if

(i) There exists a finite extension k_0 of k such that $(S, k_0^{[p]})$ becomes a true statement in the obvious sense.

(ii) If k_1 is a finite extension of k_0, then $(S, k_1^{[p]})$ also becomes a true statement.

A field K, $k \subset K \subset \bar{k}$, will be called an *almost finite p-extension* if $K = k_0^{[p]}$ with $[k_0 : k] < \infty$. If K is an almost finite p-extension and $K = k_0^{[p]}$, we shall call k_0 the finite part of K (it is unique because $k_0^{[p]}$ is determined by a unique closed subgroup of $\mathrm{Gal}(\bar{k}/k)$; see §III).

Proposition 4.2. *Let k be an infinite perfect field. Let φ be a k-morphism of varieties, $\varphi: A^2 \to W$, W a connected commutative unipotent k-group. Suppose that*

(i) *The image of φ generates W, $W \neq e$.*

(ii) *φ is additive in each variable.*

(iii) *$\varphi(x,y) = -\varphi(y,x)$ all $(x,y) \in \mathbf{A}^2$.*

Then W has the structure of a vector group over k. Further the equality $\langle \varphi(\mathbf{A}^2(K)) \rangle = W(K)$ admits an almost finite k-solution.

Proof. The first statement follows from the proof of the analogous Lemma 1 of §I, since only the perfectness of k was used here.

We proceed by induction on the dimension of W. If $\dim W = 1$, then as in Lemma 1.1, there exists $x \in \mathbf{A}'(k)$ with $\varphi_x: G_a \to W$ given by $\varphi_x(y) = \varphi(x,y)$. φ_x is defined over k and nonzero. φ_x is a homomorphism of algebraic groups by (ii), and since $W \cong G_a$ over k we have, after making this identification, $\varphi_x: G_a \to G_a$. Thus φ_x is given by an additive polynomial in $k[T]$, say $\varphi_x = P(T) \in k[T]$.

Let k_0 be the splitting field of $P(T)$. Let $K = k_0^{[p]}$. By Theorem 3.7, given $c \in K$ there exists $y \in K$ such that $P(y) = c$. It follows, as in Lemma 1.1, that $\langle \varphi(\mathbf{A}^2(K)) \rangle = W(K)$. The remark following Theorem 3.7 shows that K is indeed an almost finite k-solution.

If $\dim W > 1$, we can find $x_1, \ldots, x_n \in \mathbf{A}^1(k)$, just as in Lemma 1.1, such that if $H_i = \varphi_{x_i}(\mathbf{A}^1), i = 1, \ldots, n$, $H_i \neq e$ then $W = H_1, \ldots, H_n$. Then consider the exact sequence

$$0 \to H_1 \to W \xrightarrow{\pi} W/H_1 \to 0.$$

It is clear that $\pi \circ \varphi: \mathbf{A}^2 \to W/H_1$ satisfies the hypothesis of our lemma; hence by induction there exists an almost finite k-solution $K_0 = k_0^{[p]}$ of $W/H_1(K_0) = \langle \pi \circ \varphi(\mathbf{A}^2(K_0)) \rangle$. Let k_0 be the finite part of K_0. By the dimension one case there exists a finite extension k_1 of k such that $\varphi x_1(A_1(k_1^{[p]})) = H_1(k_1^{[p]})$. Now put $k_2 = k_0 k_1$. Then $[k_2 : k] < \infty$ and $K = k_2^{[p]}$ is an almost finite k-solution.

Proposition 4.3. *Let A and B be connected unipotent groups defined over the perfect field k. Let φ be a k-isogeny from A onto B. Then the statement 'φ is surjective on K-rational points' admits an almost finite k-solution.*

Proof. We induct on the dimension of A. If $\dim A = \dim B = 1$ then A and B are k-isomorphic to G_a [B, Proposition 10.9]. It follows that φ is given by an additive polynomial and our proposition then follows from the proof of Lemma 4.2 ($\dim W = 1$).

If $\dim A > 1$, let $A_1 \subset A$ be connected normal and defined over k with A/A_1 k-isomorphic to G_a. $B_1 = \varphi(A_1)$ has the corresponding properties in B [B, 1.4].

Consider the commutative diagram of k-groups and k-morphisms

$$\begin{array}{ccc} A_1 & \xrightarrow{\varphi} & B_1 \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} \\ A & \xrightarrow{\varphi} & B \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ A/A_1 & \xrightarrow{\bar{\varphi}} & B/B_1 \end{array}$$

where i denotes inclusion, π the canonical projections and $\bar{\varphi}$ the induced map on quotients. By induction there exists an almost finite k-solution, $k_1^{[p]}$, such that $\varphi(A_1(k_1^{[p]})) = B_1(k_1^{[p]})$. By the dimension one case, there exists $k_2^{[p]}$, such that $\bar{\varphi}$ is surjective on $k_2^{[p]}$-rational points, $k_2^{[p]}$ being an almost finite k-solution. Then by a diagram chase similar to that of Lemma 1.3, $k_3^{[p]}, k_3 = k_1 k_2$, is an almost finite k-solution of our problem.

Proposition 4.4. *Let A and B be connected subgroups of the unipotent algebraic group G with B normal in $G = AB$. Suppose G, A and B are defined over the perfect field k. Then the equality '$G(K) = A(K)B(K)$' admits an almost finite k-solution.*

Proof. As in the proof of Proposition 1.4, the crucial point is that a certain isogeny be surjective on k-rational points, i.e.,

$$A/(A \cap B)^\circ \to A/A \cap B \quad \text{is a } k\text{-isogeny.}$$

The proposition follows from Proposition 4.3, and the diagram chase of Proposition 1.4.

Corollary 4.5. *Let G be connected unipotent and defined over the perfect field k. Let $H_1, \ldots, H_n$ be closed normal k-subgroups of $G = H_1, \ldots, H_n$. Then the equality $G(K) = H_1(K) \cdots H_n(K)$ admits an almost finite k-solution.*

Lemma 4.6. *Let G, A and B be as in Proposition 4.4. We assume k is perfect and infinite. Let $H \subset [A, B]$ be a closed connected k-subgroup of G and suppose the inclusion '$H(K) \subset [A(K), B(K)]$' admits an almost finite k-solution $k_0^{[p]}$. Let N be the smallest normal subgroup of G containing H and assume it is normal in N. Then the inclusion '$N(K) \subset [A(K), B(K)]$' admits an almost finite k-solution.*

Proof. Since k_0 is a finite extension of k, k_0 is infinite and perfect. Hence just as in the proof of Lemma 1.5, we can find $x_1, \ldots, x_n$ in $G(k_0)$ such that if $H_i = x_i H x_i^{-1}$, then $N = H_1 \cdots H_n$. Each H_i is clearly normal in N.

By Corollary 4.5 we can find a finite extension k_1 of k_0 such that $k_1^{[p]}$ is an almost finite k_0-solution of the equality '$N(K) = H_1(K) \cdots H_n(K)$'. By Proposition 4.4 we may find an almost finite k_1-solution, $k_2^{[p]}$, of the equality '$G(K) = A(K)B(K)$'. It follows that if $K = k_2^{[p]}$ then

(a) $G(K) = A(K)B(K)$,

(b) $N(K) = H_1(K)H_2(K) \cdots H_n(K)$,

(c) $H(K) \subset [A(K), B(K)]$.

We must show $N(K) \subset [A(K), B(K)]$. It clearly suffices to show $H_i(K) \subset [A(K), B(K)]$ for all i.

Now $H_i = x_i H x_i^{-1}$, $x_i \in G(k) \subset G(K)$. Write $x_i = a_i b_i$ with $a_i \in A(K)$, $b_i \in B(K)$. It will suffice to show, then, that $(zHz^{-1})(K) \subset [A(K), B(K)]$ for $Z \in A(K)$ or $Z \in B(K)$. But this follows by arguments similar to those of the proof of Lemma 1.5.

Proposition 4.7. *Let k be an infinite perfect field. Let G be a connected unipotent k-group. Then the equality '$[G, G](K) = [G(K), G(K)]$' admits an almost finite k-solution.*

Proof. The proof is analogous to that of Proposition 1.2. If G is commutative, there is nothing to prove. Thus we assume $[G, G] \neq e$ and argue by induction on the dimension of $[G, G]$.

Choose as in Proposition 1.2 a composition series exhibiting the k-splitting of G,

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = e,\ G_i \text{ a connected normal } k\text{-subgroup of } [G, G_i] \subset G_{i+1}, i = 1, \cdots, n-1.$$

Let G_{i_0} and G_j be as defined in the proof of Proposition 1.2. The k-morphism

$$\varphi\colon G_{i_0}/G_{i_0} \times G_{j-1}/G_j \to V = [G_{i_0}, G_{j-1}]$$

induced by $(g, h) \to [g, h]$ satisfies the properties of Proposition 4.2. $\dim V \geq 1$ by construction and hence if $\dim[G, G] = 1$, we have $V = [G, G]$. It follows from Proposition 4.2 that

$$\langle \varphi(G_{i_0}/G_{i_0+1}(k_1^{[p]}), G_{j-1}/G_j(k_1^{[p]})) \rangle = V(k_1^{[p]})$$

and since $k_1^{[p]}$ is infinite and perfect, G_{i_0+1} and G_j connected, that $[G_{i_0}(k_1^{[p]}), G_{j-1}(k_1^{[p]})] = V(k_1^{[p]})$ where $k_1^{[p]}$ is an almost finite k-solution.

If $\dim[G, G] > 1$, using the above results, we still obtain $V(k_1^{[p]}) = [G_{i_0}(k_1^{[p]}), G_{j-1}(k_1^{[p]})]$. Then from the exact sequence

$$0 \to V \to G \xrightarrow{\pi} G' = G/V \to 0,$$

we get, since $\dim[G', G'] < \dim[G, G]$, the existence of an almost finite k_1-

solution, $k_2^{[p]}$, such that $[G'(k_2^{[p]}), G(k_2^{[p]})] = [G', G'](k_2^{[p]})$. Then also, $V(k_2^{[p]}) \subset [G(k_2^{[p]}), G(k_2^{[p]})]$ since k_2 is a finite extension of k_1, which is the finite part of an almost finite k-solution to the inclusion '$V(K) \subset [G(K), G(K)]$'. The proof is now completed by repeating the argument at the end of the proof of Proposition 1.2.

Lemma 4.8. *Let G be a linear algebraic group defined over the infinite perfect field k. Let H be a closed connected normal unipotent subgroup of G which is defined over k. Let ψ: $G \to G/[H,H]$ be the canonical projection. Finally, suppose $K = k_0^{[p]}$ is an almost finite k-solution of the equality $[H,H](K) = [H(K), H(K)]$ and L a subset of $G(K)$. Then if $\psi(L)$ generates $G/[H,H](K)$, then L generates $G(K)$.*

Proof. The proof is obtained by repeating the arguments of Lemma 1.7, replacing the k there by K.

Lemma 4.9. *Let G be a connected solvable group defined over the infinite perfect field k. Let W be the unipotent radical of G and T a maximal torus of G which is defined over k. Then there exists an almost finite k-solution of the equality $[T,W](K) = [T(K), W(K)]$.*

Proof. Let $H = [T,W]$ and K an almost finite k-solution of the equality $[H,H](K) = [H(K), H(K)]$. The lemma now follows by replacing the field k by K in the argument of Proposition 2.1 and Corollary 2.2.

Theorem 4.10. *Let G be a connected solvable algebraic group defined over the infinite perfect field k. Let A and B be closed connected subgroups of G defined over k. Suppose B is normal in $G = AB$. Then there eixists an almost finite k-solution K to the equality '$[A,B](K) = [A(K), B(K)]$'.*

Proof. As in the proof of Theorem 2.3, A and B contain maximal tori, $S \subset A$ and $Q \subset B$, which are defined over k. Let V and W be the unipotent radicals of A and B respectively. Put $H = [A,B]$, $H_1 = [V,W]$, $H_2 = [Q,W]$ and $H_3 = [S,W]$.

We have seen in the course of the proof of Theorem 2.3 that if H is commutative, $H = H_1 H_2 H_3$.

Assuming that H is commutative it suffices to find almost finite k-solutions for the following:

(1) $H_1(K) = [V(K), W(K)]$,
(2) $H_2(K) = [Q(K), W(K)]$,
(3) $H_3(K) = [S(K), W(K)]$,
(4) $H(K) = H_1(K)H_2(K)H_3(K)$.

The solutions for (2) and (3) follow from Lemma 4.9 and that of (4) from Corollary 4.5. We assume, for the moment, that we can find an almost finite k-solution of (1). Let $k_1^{[p]}$, $k_2^{[p]}$, $k_3^{[p]}$, and $k_4^{[p]}$ be almost finite k-solutions for (1), (2), (3) and (4) respectively. If k_0 is the composite of the k_i $(i = 1,2,3,4)$, then $K = k_0^{[p]}$ solves (1), (2), (3) and (4) simultaneously. Hence $H(K) \subset [A(K), B(K)]$ and this inclusion implies the desired equality.

If H is not commutative we may find an almost finite k-solution of the equality $[H,H](K) = [H(K),H(K)]$ by Proposition 4.7. Let $K_0^{[p]}$ be such a k-solution, then in $G' = G/[H,H]$ we may use the above arguments to find an almost finite k_0-solution $k_1^{[p]}$ such that $[A',B'](k_1^{[p]}) = [A'(k_1^{[p]}),B'(k_1^{[p]})]$. Then the proof is completed by letting $L = [A(k_1^{[p]}),B(k_1^{[p]})]$ and applying Lemma 4.8.

It remains to show that (1) has an almost finite k-solution. For this we prove the following proposition from which (1) follows.

Proposition 4.11. *Let G be a connected unipotent group defined over the infinite perfect field k. Let A and B be closed connected k-subgroups of G with G normal in $G = AB$. Then the equality $[A,B](K) = [A(K),B(K)]$ admits an almost finite k-solution.*

Proof. We use the notation of the analogous Theorem 1.6. Assume $[A, B]$ commutative. Let A_{j_0}, A_{j_0+1}, B_{i_0}, B_{i_0+1} and the k-morphism φ: $A_{j_0}/A_{j_0+1} \times B_{i_0}/B_{i_0+1} \to [A_{j_0}, B_{i_0}]$ be as in Theorem 1.6. The definitions and properties of these groups and of φ did not depend on the fact that in Lemma 1.5 k was assumed p-closed. We argue as in Theorem 1.6 on the dimension of $[A, B]$. If $\dim[A, B] = 1$ then, as was shown in Theorem 1.6, φ satisfies the hypothesis of Lemma 4.2. Thus it follows that

$$[A_{j_0}(k_1^{[p]}), B_{i_0}(k_1^{[p]})] = [A_{j_0}, B_{i_0}](k_1^{[p]}) = [A,B](k_1^{[p]}),$$

where $k_1^{[p]}$ is an almost finite k-solution, by arguments used in Theorem 1.6 and elsewhere.

If $\dim[A,B] > 1$ we still have $[A_{j_0}, B_{i_0}](k_1^{[p]}) = [A_{j_0}(k_1^{[p]}), B_{i_0}(k_1^{[p]})]$. Let $H = [A_{j_0}, B_{i_0}]$. Then H is normal in B_{i_0} (since it is normal in $\langle A_{j_0}, B_{i_0}\rangle$). Hence H is normal in the smallest normal subgroup of G containing it since B_{i_0} is normal in G. Then we may apply Lemma 4.6 to obtain N normal in G with $H \subset N$, H normal in N and $N(k_2^{[p]}) \subset [A(k_2^{[p]}),B(k_2^{[p]})], k_2^{[p]}$ an almost finite k-solution. Then, assuming $[A, B]$, is commutative still we consider the diagram of k-groups and k-morphisms

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & [A,B] & \xrightarrow{\pi} & [A,B]/N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{\pi} & G/N & \longrightarrow & 0 \end{array}$$

the vertical maps being inclusions and π the canonical projections. In G/N we have lowered the dimension of $[\pi A, \pi B]$. Hence we may find an almost finite k-solution, $k_3^{[p]}$, or the equality $[(\pi A)(K),(\pi B)(K)] = [\pi A, \pi B](K)$.

Now $\pi(A) = A/A \cap N$ is given by the composition $A \to A/(A \cap N)^\circ \to^{\sigma} A/A \cap N$, σ being a k-isogeny since A, N and hence $A \cap N$ and $(A \cap N)^\circ$ all are defined over k. By Proposition 4.4 choose $k_4^{[p]}$ such that σ is surjective on $k_4^{[p]}$ rational points.

Now put $k_5 = k_0k_1k_2k_3k_4$ (the composite of these fields) and let $K = k_5^{[p]}$. This is an almost finite k-solution of the following statements.

(a) $N(K) \subset [A(K), B(K)]$,

(b) $\pi(A(K)) = (\pi A)(\pi K)$,

(c) $[(\pi A)(K), (\pi B)(K)] = [\pi A, \pi B](K)$,

(d) $\pi(B(K)) = (\pi B)(K)$.

(d) follows because $N \subset [A, B] \subset B$ is a connected k-closed subgroup and hence from [B, p. 157] the result.

Now if $x \in [A, B(K)]$, $\pi(x) \in [\pi A, \pi B](K) = [(\pi A)(K), (\pi B)(K)]$ $= [\pi(A(K)), \pi(B(K))]$. Hence there exist $y \in [A(K), B(K)]$ with $\pi(y) = \pi(x)$. $y^{-1}x \in (\operatorname{Ker}\pi)(K) = N(K) \subset [A(K), B(K)]$; hence $x = y \cdot y^{-1}x \in [A(K), B(K)]$ and this yields the desired equality.

Finally, if $H = [A, B]$ is not commutative, then let $k_6^{[p]}$ be an almost finite k-solution to the equality '$[H, H](K) = [H(K), H(K)]$' by Proposition 4.7. Then applying the above results to $G' = G/[H, H]$ and using Lemma 4.8 with $L = [A(E), B(E)]$, $E = (k_5 \cdot k_6)^{[p]}$ we obtain the desired results with $(k_5 \cdot k_6)^{[p]}$ the almost finite k-solution.

V. Some final observations and examples. We make some final observations concerning the extension of Theorem 2.4 to wider classes of linear algebraic groups.

5.1. *Nonconnected solvable groups.*

Example 5.1. Let G be a linear algebraic group defined over a field k. The definitions we have been using do not imply that every component of G is defined over k. This, of course, is true if G is connected. It is not hard to construct counterexamples to Theorem 2.4 using this definition of field of definition. For example, let $A \subset G_m$ be the subgroup defined over $k = \mathbf{Q}$, by:

$$x \in A \quad \text{if and only if} \quad x^3 = 1.$$

Let $G = G_m \cdot G_a$, where G_m acts via multiplication. Then $A(k) = A(Q) = e$. But A does not centralize $B = G_a \subset G$. Hence $[A, B]$ is connected, contained in B, and therefore equal to B (since it is nontrivial). Then $B(k) = [A, B](k) \neq e$ $= [A(k), B(k)] = [e, B(k)]$. One may question this definition of 'defined over k'. An algebraic k-group is said to be defined over k, by some authors, only when each component of G is defined over k. Using such a definition here does not entirely remove the difficulty, however.

Example 5.2. Let $G = \mathrm{GL}_2(\mathbf{C})$. Let A be the subgroup of G generated by the matrix $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. A is finite of order 2. Let B be the subgroup of G consisting of diagonal matrices of determinant one. G is isomorphic over $\mathbf{Q}$ to G_m. $A \cdot B \subset G$ is clearly solvable and the k-rational points of AB are dense in AB.

A acts on B via conjugation. We compute the commutator of a typical pair of elements in A and B.

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x^{-1} & 0 \\ 0 & x \end{bmatrix}$$

$$= \begin{bmatrix} x^{-1} & 0 \\ 0 & x \end{bmatrix} \begin{bmatrix} x^{-1} & 0 \\ 0 & x \end{bmatrix} = \begin{bmatrix} x^{-2} & 0 \\ 0 & x^2 \end{bmatrix}.$$

Thus $[A, B]$ is nontrivial, hence connected and equal to $B(= G_m)$. A and B are both defined over $k = \mathbf{Q}$. But $[A, B](k)$ is not equal to $[A(k), B(k)]$ because every element of $\mathbf{Q}$ is certainly not a square.

Under suitable hypotheses Theorem 2.4 does generalize to nonconnected solvable groups.

Theorem 5.3. *Let G be a solvable linear algebraic group defined over the p-closed field k. Let A and B be closed subgroups of $G = AB$, B normal in G. Suppose that*

(a) *A and B are defined over k,*

(b) *A and B are simultaneously triagonalizable over k, and*

(c) *each component of A (resp. B) contains a point rational over k.*

Then $[A, B](k) = [A(k), B(k)]$.

Proof. We shall use a reduction procedure similar to that used in the proof of Theorem 2.4. Let $V \subset [A, B]$ be a connected normal k-closed subgroup of G and $\pi\colon G \to G/V$ the quotient morphism. By Lemma 2.3, $\pi(A^\circ(k)) = \pi(A^\circ)(k)$. The hypothesis (c) implies that A/A° consists of k-rational points, because A° is defined over k and the cosets of A° are the components of A. The map π, when restricted to A, clearly induces a surjective k-morphism from A/A° to $\pi(A)/(\pi(A))^\circ$.

Consider the commutative diagram of k-morphisms and k-groups

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^\circ & \xrightarrow{i} & A & \xrightarrow{\nu} & A/A^\circ & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & \\ 0 & \longrightarrow & \pi(A)^\circ & \longrightarrow & \pi(A) & \xrightarrow{\mu} & \pi(A)/\pi(A)^\circ & \longrightarrow & 0 \end{array}$$

If $x \in \pi(A)(k)$, then $\mu(x)$ is rational over k (since every element of A/A° and $\pi(A)/\pi(A)^\circ$ is rational over k). There exists $\bar{a} \in A/A^\circ$ with $\pi(\bar{a}) = \mu(x)$. Let $a \in A(k)$ be such that $\nu(a) = \bar{a}$. Then $\pi(a)x^{-1}$ lies in the kernel of μ, i.e., $\pi(a)x^{-1} \in \pi(A)^\circ(k)$. But there exists $y \in A^\circ(k)$ such that $\pi(y) = \pi(a)x^{-1}$ by Lemma 2.3. It follows that $x = \pi(y^{-1}a) \in \pi(A(k))$, and this shows that $\pi(A(k)) = \pi(A)(k)$.

A similar argument shows that $\pi(B(k)) = \pi(B)(k)$. Now suppose that $[\pi(A)(k), \pi(B)(k)]$ generates $\pi([A, B])(k)$. Then we may apply Lemma 1.7 to π restricted to $[A, B]$ to conclude that $[A(k), B(k)] = [A, B](k)$.

The point is that it will suffice to establish the theorem in quotient groups of G by k-closed connected normal subgroups contained in $[A, B]$. We remark that the hypotheses do in fact remain valid in quotient groups (by k-closed subgroups). Everything is clear except perhaps (b). To see that this remains valid

when we pass to quotient groups we recall the well-known fact (cf. Rosenlicht, *On the definition of field of definition*, Bol. Soc. Mat. Mexicana **2** (1962), that a matrix group is triagonalizable if and only if it is solvable and its commutator subgroup consists of unipotent elements. These properties are clearly preserved under homomorphic images.

We now begin the proof. Since $[A, B]$ is normal in $G = A \cdot B$, $[A, B]^\circ$ is normal in G. Thus $[B,[A,B]^\circ]$ is connected [B, 2.3], normal, k-closed and contained in $[A, B]$. Passing to the quotient cf G by $[B,[A,B]^\circ]$ we may thus assume that $[B,[A,B]^\circ] = e$. Now $[A,B^\circ]$ is also connected and k-closed. Moreover $[A,B^\circ] \subset [A,B]^\circ$. It is normalized by A (since it is contained in $\langle A,B\rangle^\circ$) and by B since $[B,[A,B^\circ]] \subset [B,[A,B]^\circ] = e$. Thus we may also assume that $[A,B^\circ] = e$. It follows now that $[A^\circ,B^\circ] = e$ also.

We consider the map $\sigma\colon A \times B \to [A,B]$ given by $\sigma(a,b) = aba^{-1}b^{-1}$. Our assumptions tell us that $\sigma(a,b)$ is independent of the class of a modulo A° and also of the class of b modulo B°. Thus σ gives a well-defined map, again denoted σ,

$$\sigma\colon A/A^\circ \times B/B^\circ \to [A,B].$$

We have $\sigma(\bar{a},\bar{b}) = aba^{-1}b^{-1}$, where a and b are any representatives of $\bar{a} \in A/A^\circ$ and $\bar{b} \in B/B^\circ$. By hypothesis (c) these representatives may be chosen to be rational over k. It follows that the image of σ consists of a finite number of k-rational points rational over k. Thus $[A,B] = [A,B](k) = [A(k),B(k)]$ and this completes the proof of the theorem.

References

[B] A. Borel, *Linear algebraic groups*, Benjamin, New York, 1969. MR **40** #4273.

[B-T] A. Borel and J. Tits, *Groupes reductifs*, Inst. Hautes Études Sci. Publ. Math. No. 27 (1965), 55–150. MR **34** #7527.

[F] W. Fulton, *Algebraic curves*, Benjamin, New York, 1969.

[G] D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968. MR **38** #229.

[H-K] K. Hoffman and R. Kunze, *Linear algebra*, Prentice-Hall Math. Series, Prentice-Hall, Englewood Cliffs, N.J., 1961. MR **23** #A3146.

[L] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965. MR **33** #5416.

[MR-I] M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math. **78** (1956), 401–443. MR **18**, 514.

[MR-II] ———, *Some rationality questions on algebraic groups*, Ann. Mat. Pura Appl. (4) **43** (1957), 25–50. MR **19**, 767.

[MR-III] ———, *Questions of rationality for solvable algebraic groups over nonperfect fields*, Ann. Mat. Pura Appl. (4) **61** (1963), 97–120. MR **28** #2113.

[MR-IV] ———, *Extensions of vector groups by Abelian varieties*, Amer. J. Math. **80** (1958), 685–714. MR **20** #5780.

[MR-V] ———, *Nilpotent linear algebraic groups*, Seminari 1962/63 Anal. Alg. Geom. e Topol., Vol. 1, Ist. Naz. Alta Mat., Ediz. Cremonese, Rome, 1965, pp. 133–152. MR **32** #5740.

[S] J. P. Serre, *Cohomologie galoisienne*, 3rd ed., Lecture Notes in Math., vol. 5, Springer-Verlag, Berlin and New York, 1965. MR **34** #1328.

[T] J. Tits, *Lectures on algebraic groups*, Yale Lecture Notes, 1967.

Department of Mathematics, University of Illinois, Urbana, Illinois 61801