ISSN 0001-4346, Mathematical Notes, 2015, Vol. 97, No. 1, pp. 3–11. © Pleiades Publishing, Ltd., 2015.
Original Russian Text © Ya. V. Abramov, 2015, published in Matematicheskie Zametki, 2015, Vol. 97, No. 1, pp. 3–12.

# Artin–Hasse Exponential Mapping, Algebraic Groups in Positive Characteristic, and the Nottingham Group

**Ya. V. Abramov**[*]

*Moscow State University, Moscow, Russia*

Received August 18, 2011; in final form, April 8, 2014

**Abstract**—Connected commutative subgroups of the prounipotent radical of the group of formal power series in one variable over an algebraically closed field of positive characteristic with respect to the operation of substitution are studied.

**DOI:** 10.1134/S0001434615010010

Keywords: *Artin–Hasse exponential mapping, prounipotent radical, group of formal power series, algebraically closed field.*

## 1. INTRODUCTION

Denote the set of formal power series without free term with coefficients in a commutative associative ring $R$ by $xR[[x]]$. Consider the binary operation of composition on the set $xR[[x]]$; to the series $f(x) = \sum_{i>0} a_i x^i$ and $g(x) = \sum_{i>0} b_i x^i$ this operation assigns the series

$$f(g(x)) = \sum_{i>0} c_i(a,b) x^i$$

in which

$$c_i(a,b) = a_1 b_i + a_i b_1^i + H_i(a_1,\dots,a_{i-1},b_1,\dots,b_{i-1}),$$
$$c_i(a,b) \in \mathbb{Z}[a_1,\dots,a_i,b_1,\dots,b_i].$$

This operation equips $xR[[x]]$ with the structure of an associative monoid.

Denote by $J(R)$ the set of formal power series with coefficients in $R$ and without free term in which the coefficient at $x$ is invertible as an element of the ring $R$. The operation of composition defines the structure of a group on $J(R)$. We refer to this group as the *group of jets*.

By a *proalgebraic group with countable base* [1] one means a group scheme which is the projective limit of a projective system consisting of countably many algebraic groups. Every proalgebraic group is equipped with the natural topology obtained as the projective limit of the Zariski topology on each of the groups entering the projective system from which the group itself is constructed. In what follows, all algebraic and proalgebraic group are regarded with this very topology. By a *regular homomorphism* of proalgebraic groups one means a morphism of these groups as group schemes. For the case in which $R = \Bbbk$ is a field, the group of jets is the group of $\Bbbk$-points of the proalgebraic group scheme $J$ which is the projective limit of the sequence of groups

$$J_1 \leftarrow J_2 \leftarrow J_3 \leftarrow \cdots,$$

where

$$J_n(\Bbbk) = \operatorname{Aut}(\Bbbk[x]/(x^{n+1}) : \Bbbk) \qquad \text{and} \qquad J_{n+l} \to J_n$$

[*] E-mail: zroslav@gmail.com

are the natural factorization homomorphisms. The group $J(\Bbbk)$ can be obtained as follows:

$$J(\Bbbk) = \mathrm{Aut}_{\mathrm{cont}}(\Bbbk[[x]] : \Bbbk) = \mathrm{Aut}_{\mathrm{cont}}(\Bbbk((x)) : \Bbbk),$$

where $\mathrm{Aut}_{\mathrm{cont}}$ stands for the group of automorphisms continuous in the $x$-adic topology on $\Bbbk[[x]]$ and $\Bbbk((x))$.

The group of jets contains the normal subgroup

$$N(\Bbbk) = \biggl\{x + \sum_{i>1} a_i x^i\biggr\},$$

which is referred to as the *Nottingham group* (after Nottingham University, where this group was intensively studied).

Everywhere below, the field $\Bbbk$ is assumed to be algebraically closed with $\operatorname{char}\Bbbk = p > 0$. The group $N(\mathbb{F}_p)$ with the profinite topology on it admits a closed embedding in $N(\Bbbk)$. As is well known, every pro-p-group with countable base admits a closed embedding in $N(\mathbb{F}_p)$ [2]. The problem of what commutative subgroups can be contained in $N(\mathbb{F}_p)$ has been studied intensively during the last years [3]–[9].

The main result of this paper is the following theorem.

**Theorem.** *Let $\Bbbk$ be an algebraically closed field of positive characteristic $p$. Then every closed finite-dimensional commutative connected subgroup of the Nottingham group $N(\Bbbk)$ can be isomorphic only to* $(\Bbbk, +)^m$.

Before passing to the proof of the theorem, recall the needed information on commutative connected algebraic groups in characteristic $p$.

## 2. WITT VECTORS

### *2.1. Definition and Main Properties of Witt Vectors*

Let $\mathbb{Z}_{(p)}$ be the ring of integer $p$-adic numbers. Write

$$w_n(X) = w_n(X_0, \dots, X_n) = \sum_{i=0}^{n} X_i^{p^{n-i}} p^i. \tag{1}$$

Obviously, there are polynomials $\Psi_n(X_0, \dots, X_n)$ with rational coefficients such that

$$X_n = \Psi_n(w_0(X), \dots, w_n(X)).$$

Write

$$s_n(X, Y) = s_n(X_0, \dots, X_n, Y_0, \dots, Y_n) = \Psi_n(w_0(X) + w_0(Y), \dots, w_n(X) + w_n(Y)),$$
$$m_n(X, Y) = m_n(X_0, \dots, X_n, Y_0, \dots, Y_n) = \Psi_n(w_0(X)w_0(Y), \dots, w_n(X)w_n(Y)).$$

**Theorem 2.1** (Witt, [10]). *We have*

$$s_i(X_0, \dots, X_i, Y_0, \dots, Y_i) \in \mathbb{Z}[X_0, \dots, X_i, Y_0, \dots, Y_i],$$
$$m_i(X_0, \dots, X_i, Y_0, \dots, Y_i) \in \mathbb{Z}[X_0, \dots, X_i, Y_0, \dots, Y_i].$$

Let $\mathbb{K}$ be an arbitrary field of characteristic $p > 0$. Introduce binary operations $+_W$ and $\cdot_W$ on the sequence space $\mathbb{K}^{\mathbb{Z}_{\geq 0}}$ as follows:

$$(X_0, \dots, X_n, \dots) +_W (Y_0, \dots, Y_n, \dots) = (s_0(X, Y), \dots, s_n(X, Y), \dots),$$
$$(X_0, \dots, X_n, \dots) \cdot_W (Y_0, \dots, Y_n, \dots) = (m_0(X, Y), \dots, m_n(X, Y), \dots).$$

**Theorem 2.2** (Witt, [10]). *The operations $\cdot_W$ and $+_W$ define on $\mathbb{K}^{\mathbb{Z}_{\geq 0}}$ the structure of a commutative associative local ring with unit, without zero divisors, and of characteristic* 0.

Following [10], we refer to the ring defined on the set $\mathbb{K}^{\mathbb{Z}_{\geq 0}}$ as the *ring of Witt p-vectors* and denote it by $W_{p^\infty}(\mathbb{K})$.

**Example 2.1.** We have $W_{p^\infty}(\mathbb{F}_p) = \mathbb{Z}_{(p)}$.

Let us also define on $\mathbb{K}^{n+1}$ the binary operations $+_W$ and $\cdot_W$ by

$$(X_0, \dots, X_n) +_W (Y_0, \dots, Y_n) = (s_0(X, Y), \dots, s_n(X, Y)),$$
$$(X_0, \dots, X_n) \cdot_W (Y_0, \dots, Y_n) = (m_0(X, Y), \dots, m_n(X, Y)).$$

**Theorem 2.3** (Witt, [10]). *The operations $\cdot_W$ and $+_W$ define on $\mathbb{K}^{n+1}$ the structure of a commutative associative local ring with unit.*

Following [10], we refer to the ring defined on the set $\mathbb{K}^{n+1}$ as the *ring of truncated Witt p-vectors* and denote it by $W_{p^{n+1}}(\mathbb{K})$.

**Example 2.2.** We have $W_{p^n}(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$.

The groups of truncated Witt vectors, with respect to addition, are commutative unipotent algebraic groups that are remarkable due to the following fact.

**Theorem 2.4** (Serre, [11]). *Every connected commutative unipotent group over $\Bbbk$ is isomorphic to*

$$\biggl(\prod_{i=1}^{N} (W_{p^{n_i}}(\Bbbk), +_W)\biggr)/G,$$

*where $(W_{p^{n_i}}(\Bbbk), +_W)$ is the additive group of truncated Witt vectors and $G$ is the final subgroup in the above product.*

### 2.2. Classification of the Additive Homomorphisms of Witt Vectors to Witt Vectors

In what follows, we need a complete classification of the regular homomorphisms from the group $W_{p^N}(\Bbbk)$ to the group $W_{p^M}(\Bbbk)$ for $N \geq M$. Let us present several examples of endomorphisms of the group $W_{p^{N+1}}(\Bbbk)$.

**Example 2.3.** We have $a \in \Bbbk$, $\widehat{a}\colon (X_0, X_1, \dots X_N) \mapsto (aX_0, a^p X_1, \dots, a^{p^N} X_N)$.

**Example 2.4.** We have $V\colon (X_0, X_1, \dots, X_N) \mapsto (0, X_0, \dots, X_{N-1})$.

**Example 2.5.** We have $F\colon (X_0, X_1, \dots, X_N) \mapsto (X_0^p, X_1^p, \dots, X_N^p)$.

**Lemma 2.1.** *$FV = VF$, and this composition is the multiplication by p in the ring $W_{p^n}(\Bbbk)$.*

**Lemma 2.2** ([10]). *The maximal order of an element of $(W_{p^N}(\Bbbk), +_W)$ is equal to $p^N$.*

**Example 2.6.** An example of a homomorphism $W_{p^N}(\Bbbk) \to W_{p^M}(\Bbbk)$ is given by the factorization $Q_{NM}$ by the subgroup $V^{N-M}(W_{p^N}(\Bbbk))$.

**Theorem 2.5.** *Every regular homomorphism from $W_{p^N}(\Bbbk)$ to $W_{p^M}(\Bbbk)$ for $N \geq M$ is of the form*

$$\sum_{n,m} \widehat{a}_{n,m} F^n V^m Q_{NM},$$

*where $\widehat{a}_{n,m}$ is as in Example 2.3, $F$ as in Example 2.4, $V$ as in Example 2.5, and $Q_{NM}$ as in Example 2.6.*

**Corollary 2.1.** *Every regular endomorphism of $W_{p^N}(\Bbbk)$ is of the form*

$$\sum_{i,j} \widehat{a}_{ij} F^i V^j.$$

**Corollary 2.2.** *Every homomorphism $W_{p^N}(\Bbbk) \to W_{p^M}(\Bbbk)$, $N \geq M$, can be lifted to a homomorphism $W_{p^N}(\Bbbk) \to W_{p^K}(\Bbbk)$, where $N \geq K \geq M$, and is given by the rule*

$$\sum_{nm} \widehat{a}_{n,m} F^n V^m Q_{NK}.$$

**Proof of Theorem 2.5.** Let

$$H\colon X = (X_0, \dots, X_{N-1}) \mapsto (H_0(X), \dots, H_{M-1}(X))$$

be a regular homomorphism from the group $W_{p^N}(\Bbbk)$ to the group $W_{p^M}(\Bbbk)$. Recall that the maximal order of an element of the group $W_{p^N}(\Bbbk)$ is equal to $p^N$. Moreover, under a homomorphism, the order of the image of an element cannot exceed the order of the element itself. The composition of the homomorphism

$$H\colon W_{p^N}(\Bbbk) \to W_{p^M}(\Bbbk)$$

and the projection

$$Q_{Mi}\colon W_{p^M}(\Bbbk) \to W_{p^i}(\Bbbk)$$

takes the elements of the subgroup $V^{i+1}(W_{p^N}(\Bbbk))$ to 0 (because these are the $p^{i+1}$th powers of elements of the group $(W_{p^N}(\Bbbk), +_W)$). Therefore, $H_i(X)$ depends only on $X_0, \dots, X_i$.

Let us prove the assertion of the theorem by induction on $M$.

For $M = 0$, the mapping $X_0 \mapsto H_0(X_0)$ is a regular endomorphism of the additive group of the field, and hence it is of the form $H_0(X_0) = \sum_{j=0} b_j X_0^{p^j}$. Let us now make the passage from $M-1$ to $M$. Write

$$H' = H - \sum \widehat{b}_j F^j Q_{NM}.$$

Let

$$H'\colon X = (X_0, \dots, X_{N-1}) \mapsto (H'_0(X), \dots, H'_{M-1}(X)).$$

It is clear that $H'_0(X) = 0$. Thus, $\operatorname{Im} H'$ belongs to $V(W_{p^M}(\Bbbk)) \cong W_{p^{M-1}}(\Bbbk)$. This completes the induction. □

### 2.3. Artin–Hasse Exponential Mapping

**Definition 2.1** (see [12]). By the *Artin–Hasse exponential function* one means the expression

$$E_p(T) = \exp\biggl(\sum_{i \geq 0} \frac{T^{p^i}}{p^i}\biggr) \in \mathbb{Q}[[T]].$$

For the following results, see, e.g., [12].

**Theorem 2.6.** *$E_p(T) \in \mathbb{Z}_{(p)}[[T]]$, i.e., the denominators of all coefficients of this series are not divisible by $p$.*

**Theorem 2.7.** $(E_p(T))^p \equiv E_p(T^p) \pmod p$.

**Theorem 2.8.** *There is an Artin–Hasse logarithm*

$$L_p(1+T) \in T\mathbb{Z}_{(p)}[[T]]$$

*such that $L_p(E_p(T)) = T$ and $E_p(L_p(1+T)) = 1+T$.*

By an *upper niltriangle matrix* we mean an upper triangular matrix with zeros on the main diagonal. By an *upper unitriangle matrix* we mean an upper triangular matrix with identity elements on the main diagonal. Note that, if $N$ is an upper niltriangular matrix over the field $\Bbbk$ of characteristic $p$, then $E_p(N)$ is an upper unitriangular matrix over the same field.

**Definition 2.2** (see [11]). Write

$$\begin{aligned} E_p(X,T) &= E_p((X_0,\dots,X_n,\dots),T) = E_p(X_0T)E_p(X_1T^p)\cdots E_p(X_nT^{p^n})\cdots \\ &= \exp\biggl(\sum_{n\ge 0} T^{p^n}\sum_{i=0}^{n}\frac{X_{n-i}^{p^i}}{p^i}\biggr) = \exp\biggl(\sum_{n\ge 0} T^{p^n}\frac{w_n(X)}{p^n}\biggr), \end{aligned}$$

where $w_n(X)$ are defined in (1).

Obviously,

$$E_p(X\oplus Y,T) = E_p(X,T)E_p(Y,T).$$

**Theorem 2.9** (see [13]). *Set*

$$E_p(X,T) = 1 + \sum_{n>0} c_n(X)T^n.$$

*Then*

*1)* $c_i(X) = X_0^i/i!$, $0 < i < p$;

*2)* $c_i(X) \in \mathbb{Z}_{(p)}[X_0,\dots X_{j-1}]$, $0 < i < p^j$;

*3)* $c_{p^j}(X) - X_j \in \mathbb{Z}_{(p)}[X_0,\dots,X_{j-1}]$.

Everywhere below, denote by $U_\infty(\Bbbk)$ the group of infinite upper unitriangular matrices. As we shall see in part 3.1 of the present text, this group can be equipped with the structure of a proalgebraic group.

**Theorem 2.10** (see [13]). *For an infinite upper niltriangular matrix $N$ over $\Bbbk$, the image of the mapping*

$$(X_0,\dots,X_n,\dots) \mapsto E_p(X,N)$$

*is contained in $U_\infty(\Bbbk)$, and the mapping by itself,*

$$E_p(\,\cdot\,,N)\colon W_{p^\infty}(\Bbbk) \to U_\infty(\Bbbk),$$

*is a regular group homomorphism.*

## 3. CLASSIFICATION OF ALL REGULAR HOMOMORPHISMS OF THE WITT GROUP TO THE GROUP OF INFINITE UNITRIANGULAR MATRICES

### *3.1. Reduction of Homomorphisms*

Let $H\colon W_{p^\infty}(\Bbbk) \to U_\infty(\Bbbk)$ be an arbitrary regular homomorphism of the group of Witt vectors to the group of infinite upper unitriangular matrices. Let us define the operation of reduction of such a homomorphism as follows.

On the group $U_\infty(\Bbbk)$, consider an infinite filtration by normal subgroups of the form

$$U_n = \left\{ \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & \ast & \ast & \ast & \ldots & \ast & \ldots \\ 0 & 1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & \ast & \ast & \ast & \ldots & \ast & \ldots \\ 0 & 0 & 1 & \ldots & 0 & 0 & 0 & \ldots & 0 & \ast & \ast & \ast & \ldots & \ast & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 & 0 & \ldots & 0 & \ast & \ast & \ast & \ldots & \ast & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 & 0 & \ast & \ast & \ldots & \ast & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 1 & \ldots & 0 & 0 & \ast & \ast & \ldots & \ast & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 1 & 0 & \ast & \ast & \ldots & \ast & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 1 & \ast & \ast & \ldots & \ast & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 0 & 1 & \ast & \ldots & \ast & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 1 & \ldots & \ast & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{pmatrix} \right\},$$

where a triangle of zeros formed by $m$ columns in succession is placed above the diagonal. In the next column with the index $(m+2)$, there can be $k$ zeros placed in succession over the diagonal, and the other elements are arbitrary. Thus, the total number of fixed zeros over the diagonal is equal to $n = m(m+1)/2 + k$, where $k < m+2$. Note that

$$U_n/U_{n+1} \cong (\Bbbk, +).$$

**Remark.** This filtration is a partial case of Serre's filtration [14].

Let $\operatorname{Im} H$ be completely contained in $U_n$ and not completely contained in $U_{n+1}$. Then there is a regular homomorphism of the group of the Witt vectors to the quotient group

$$H/U_{n+1} \colon W_{p^\infty}(\Bbbk) \to U_n/U_{n+1} \cong \Bbbk.$$

This homomorphism is of the form

$$H/U_{n+1} \colon X \mapsto f(X_0) = \sum_{i=0}^{n_0} a_{0i} X_0^{p^i}.$$

By Corollary 2.2, one can lift the homomorphism $W_{p^\infty}(\Bbbk) \to \Bbbk$ in question to a homomorphism $S \colon W_{p^\infty}(\Bbbk) \to W_{p^\infty}(\Bbbk)$,

$$S(X) = \sum_{i=0}^{n_0} \widehat{a}_{0i} F^i(X)$$

(let us use a lifting in the very form used in the proof of Theorem 2.5; below this is of importance in our constructions). Let $u_0 \in \operatorname{Im} H$, and let the coset of $u_0$ in $U_n/U_{n+1} \cong \Bbbk$ be equal to 1 in the field $\Bbbk$. Note that the analytic function of an element of the commutative subgroup of $U_\infty(\Bbbk)$ commutes with all elements of this subgroup. Therefore, $E_p(X, L_p(u_0))$ commutes with every element of $\operatorname{Im} H$ for any $X \in W_{p^\infty}(\Bbbk)$. Write

$$H_1(X) = H(X) \cdot E_p(S(X), L_p(u_0))^{-1},$$

where

$$S(X) = \sum_{i=0}^{n_0} \widehat{a}_{0i} F^i(X).$$

Then $H_1$ is a group homomorphism, because it is the ratio of homomorphisms for which every element in the image of the first homomorphism commutes with every element in the image of the other. Here $\operatorname{Im} H_1$ is entirely contained in $U_{n+1}$. The homomorphism $H_1$ thus constructed is referred to as the *reduction* of the homomorphism $H$.

If, using this reduction, we pass from $H_1$ and $H_2$, then from $H_2$ to $H_3$, etc., then we obtain the following result.

**Theorem 3.1.** *Every regular homomorphism $H\colon W_{p^\infty}(\Bbbk) \to U_\infty(\Bbbk)$ is of the form*

$$H(X) = \prod_{i=0}^{n} E_p(\sigma_i(X), N_i),$$

*where $n$ is a positive integer or infinity,*

$$\sigma_i \in \operatorname{End}(W_{p^\infty}(\Bbbk)), \qquad \sigma_i = \sum_j \widehat{a}_{ij} F^j,$$

*and $\{N_i\}_i$ is a family, linearly independent over $\Bbbk$, of infinite upper niltriangular matrices such that $1 + N_i \in U_{n_i} \setminus U_{n_i+1}$ and $n_i \in \mathbb{N}$ increase.*

Thus, we have described not only all homomorphisms $W_{p^\infty}(\Bbbk) \to U_\infty(\Bbbk)$, but also all homomorphisms $W_{p^N}(\Bbbk) \to U_\infty(\Bbbk)$.

### *3.2. Tangent Algebra to the Image of a Homomorphism*

For the definition of tangent algebra $\operatorname{Lie}(G)$ of a group scheme $G$ over the field $\Bbbk$ and of tangent vector to a scheme over $\Bbbk$, see [15].

Let us describe the tangent algebra to the image of the group $W_{p^\infty}(\Bbbk)$ under the homomorphism $H$ from Theorem 3.1. We have $\sigma_i(X)_0 = \sum_j a_{ij} X_0^{p^j}$. We may assume that $a_{i0} \neq 0$ for at least one $i$; otherwise, by the construction of $\sigma_i$, the homomorphism $H$ depends on $X_0^p$ rather than on $X_0$, i.e., $H$ is the composition of another homomorphism $\widetilde{H}$ and the Frobenius homomorphism, and we can replace $H$ by $\widetilde{H}$.

Then

$$\frac{\partial}{\partial X_0} \prod_i E_p(\sigma_i(X), N_i)\big|_{X=0} = \sum_i \frac{\partial}{\partial X_0} E_p(\sigma_i(X), N_i)\big|_{X=0} = \sum_i a_{i0} N_i.$$

Let us take $\sum_i a_{i0} N_i$ for the first tangent vector at the identity to the image of $W_{p^\infty}(\Bbbk)$. Note that the operation of taking to the power $p$ in the additive group of Witt vectors is the composition $F \circ V = V \circ F$. The image of this endomorphism is a subgroup of codimension 1. Here

$$\Bigl(\prod_i E_p(\sigma_i(X), N_i)\Bigr)^p = \prod_i E_p(F(V(\sigma_i((X)))), N_i) = \prod_i E_p(F(\sigma_i((X)), N_i^p).$$

Take $\sum_i a_{i0}^p N_i^p$ as the second tangent vector to the image of $W_{p^\infty}(\Bbbk)$. By analogy, one can also construct the tangent vectors $\sum_i a_{i0}^{p^j} N_i^{p^j}$. Since $\operatorname{codim}_{W_{p^N}}(V(W_{p^N})) = 1$, these vectors span the entire tangent algebra, and the nonzero vectors among them form a basis of the algebra. Thus, the following assertion holds.

**Theorem 3.2.** *The tangent algebra of every closed subgroup of $U_\infty(\Bbbk)$ which is a quotient of the group $W_{p^\infty}(\Bbbk)$ has a basis of the form $\{N^{p^i}\}$ for some element $N$ of this tangent algebra.*

## 4. COMMUTATIVE SUBGROUPS OF THE NOTTINGHAM GROUP

### *4.1. Proof of the Main Result*

Suppose the contrary. As follows from Theorem 2.4, there must be an $n > 1$ such that some homomorphism $W_{p^n}(\mathbb{k}) \to N(\mathbb{k})$ has at most a discrete kernel. The group $N(\mathbb{k})$ admits the following natural regular embedding in $U_\infty(\mathbb{k})$. The action $r(x) \mapsto r(g^{-1})$ embeds $N(\mathbb{k})$ in the infinite lower triangular unitriangular matrices. The mapping $A \mapsto (A^T)^{-1}$ isomorphically takes the lower triangular matrices to the upper triangular ones.

The tangent algebra $N(\mathbb{k})$, regarded as a subalgebra of $\mathrm{Lie}(U_\infty(\mathbb{k}))$, is of the form

$$\left\{\sum_{i>1} a_i x^i \frac{d}{dx}\right\}$$

with the bracket

$$\left[r(x)\frac{d}{dx}, q(x)\frac{d}{dx}\right] = (rq' - r'q)\frac{d}{dx} = r^2\left(\frac{q}{r}\right)'\frac{d}{dx}.$$

The centralizer of the tangent vector $r(x)d/dx$ is of the form

$$\left\{g(x^p)r(x)\frac{d}{dx} \;\middle|\; g(x) \in \mathbb{k}((x)),\ r(x)g(x^p) \in x^2\mathbb{k}[[x]]\right\}.$$

**Lemma 4.1.** *Let $g(x)d/dx$ be a tangent vector to $N(\mathbb{k})$. Then $(g(x)d/dx)^p$ is also a tangent vector to $N(\mathbb{k})$. It is of the form $g(x)h(x^p)d/dx$, $h(x) \in \mathbb{k}[[x]]$.*

**Proof.** Indeed, the $p$th power of any derivation $D$ of an arbitrary algebra over the field of characteristic $p$ is also a derivation of the algebra,

$$D^p(fg) = \sum_{j=0}^{p} \binom{p}{j} D^j(f)D^{p-j}(g) = D^p(f)g + fD^p(g).$$

$D^p$ commutes with $D$, and the least $n$ such that $x^n d/dx$ enters the representation of $D^p$ with nonzero coefficient is not less than that for $D$ and, therefore, $D^p$ has the desired form. □

Let us now continue the proof of the theorem. By Theorem 3.2, some derivations $D^{p^i}$, $i = 0, \dots, n$, are tangent vectors to the connected commutative subgroup in question. Thus, there is a derivation $D$ of the algebra $\mathbb{k}[[x]]$ such that $D^{p^n} \neq 0$ and $D^{p^{n+1}} = 0$. Let

$$D^{p^{n-1}} = f(x)\frac{d}{dx}.$$

Then

$$D^{p^n} = f(x)h(x^p)\frac{d}{dx} \neq 0.$$

Note that the operator of multiplication by $h(x^p)$ commutes with the operator $d/dx$. Therefore,

$$D^{p^{n+1}} = f(x)h(x^p)^{p+1}\frac{d}{dx} \neq 0,$$

which contradicts our assumption. Hence, a connected commutative subgroup of $N(\mathbb{k})$ can be only of the form $\mathbb{k}^n/G$, where $G$ is a finite subgroup. The theorem now results from the following lemma.

**Lemma 4.2.** *Let $G$ be a finite subgroup of $(\mathbb{k}, +)^l$. Then $(\mathbb{k}, +)^l/G \cong (\mathbb{k}, +)^l$.*

**Proof.** Note that $G \cong (\mathbb{Z}/p\mathbb{Z})^m$. Therefore, it suffices to prove the assertion for $G \cong \mathbb{Z}/p\mathbb{Z}$. Choose a generating element $e$ in $G$. To this element, there corresponds some vector $v$ in $\mathbb{k}^n$. Including $v$ into some basis, we obtain $\mathbb{k}^l/G \cong (\mathbb{k}/(\mathbb{Z}/p\mathbb{Z})) \oplus \mathbb{k}^{l-1}$ (after this linear change, $v$ becomes 1 in the field $\mathbb{k}$). At the same time, $M\colon x \to x^p - x$ is an endomorphism of $\mathbb{k}$ whose kernel is precisely $\mathbb{Z}/p\mathbb{Z}$ and the image is the entire $\mathbb{k}$, as was to be proved. □

### *4.2. Open Questions*

The question of what are the numbers $n$ for which the Nottingham group contains a subgroup isomorphic to $\mathbb{k}^n$ remains open. For $n = 1$, these subgroups exist; they are subgroups of the form

$$f_{\lambda,l}(x) = \sqrt[l]{\frac{x^l}{1+\lambda x^l}}, \qquad \lambda \in \mathbb{k}, \quad l \in \mathbb{N}, \quad (l,p) = 1, \qquad f_{\lambda,l} \circ f_{\mu,l} = f_{\lambda+\mu,l}.$$

The question of what infinite-dimensional connected Abelian subgroups are in the Nottingham group also remains open. Is the group $W_{p^\infty}(\mathbb{k})$ realizable in the Nottingham group? Are some its quotient groups by prodiscrete subgroups realizable?

For example, $N(\mathbb{k})$ has a closed subgroup isomorphic to the group $(\{1 + \sum_{i=1}^{\infty} a_i T^i \mid a_i \in \mathbb{F}_p\}, \cdot\,)$ and realizable in the form $\{x + \sum a_i x^{p^i} \mid a_i \in \mathbb{F}_p\}$ in the Nottingham group (see [16]). It has infinite order, but it is not connected.

## ACKNOWLEDGMENTS

The author is very thankful to his research supervisor É. B. Vinberg and also to D. A. Timashev, A. Ya. Kanel-Belov, and M. V. Ershov for useful discussions in connection with this paper.

The work was supported by the Laboratory of Algebraic Geometry and Its Applications of the National Research University Higher School of Economics (grant of the Russian Federation, agreement 11. G34.31.0023) and by the Russian Foundation for Basic Research (grants nos. 10-01-00836, 12-01-33101, and 12-01-31233).

## REFERENCES

1. J. P. Serre, *Groupes proalgébriques*, Publ. Math. IHES, No. 7 (1990).
2. R. Camina, "Subgroups of the Nottingham group," J. Algebra **196**, 101–113 (1997).
3. B. Klopsch, "Automorphisms of the Nottingham Group," J. Algebra **223** (1), 37–56 (2000).
4. P. P. Palfy, "The number of conjugacy classes in some quotients of the Nottingham group," Proc. Edinburgh Math. Soc. (2) **41** (02), 369–384 (1998).
5. M. Ershov, "New just-infinite pro-$p$ groups of finite width and subgroups of the Nottingham group," J. Algebra **275** (1), 419–449 (2004).
6. M. Ershov, "On subgroups of the Nottingham group of positive Hausdorff dimension," Comm. Algebra **35** (1), 193–206 (2007).
7. I. Fesenko, "On just infinite pro-$p$-groups and arithmetically profinite extensions of local felds," J. Reine Angew. Math. **517**, 61–80 (1999).
8. J.-P. Wintenberger, "Extensions abéliennes et groupes d'automorphismes de corps locaux," C. R. Acad. Sci. Paris Sér. A-B **290** (5), A201–A203 (1980).
9. I. K. Babenko, "Algebra, geometry, and topology of the substitution group of formal power series," Uspekhi Mat. Nauk **68** (1), 3–76 (2013) [Russian Math. Surveys **68** (1), 1–68 (2013)].
10. M. Hazewinkel, *Witt Vectors. Part* 1 `math. RA/ 0804.3888v1`.
11. J. P. Serre, *Groupes algébriques et corps de classes* (Hermann, Paris, 1959; Mir, Moscow, 1968; *Algebraic Groups and Class Fields*, Springer-Verlag, New York–Berlin, 1988).
12. A. M. Robert, *A Course in p-Adic Analysis*, in *Grad. Texts in Math.* (Springer, New York, 2000), Vol. 198.
13. R. Proud, "Witt groups and unipotent elements in algebraic groups," Proc. London Math. Soc. (3) **82** (3), 647–675 (2000).
14. J. E. Humphreys, *Linear Algebraic Groups* (Springer-Verlag, New York–Heidelberg, 1975; Nauka, Moscow, 1980).
15. J. C. Jantzen, *Representations of Algebraic Groups*, in *Pure Appl. Math.* (Academic Press, Boston, MA, 1987), Vol. 131.
16. Y. Barnea and B. Klopsch, "Index-subgroups of the Nottingham group," Adv. Math. **180** (1), 187–221 (2003).