TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 248, Number 1, February 1979

ON A CASE OF EXTENSIONS OF GROUP SCHEMES

BY

B. WEISFEILER[1]

ABSTRACT. The extensions of a smooth connected commutative group scheme whose generic fiber is G_m by the additive group scheme are studied. The results are most explicit in the case when the basic scheme is the spectrum of an integral domain containing a field.

We compute in this note the group $\mathrm{Ext}(G_A(b), G_{a,A})$. Here A denotes an integral domain, and $G_{a,A}$ stands as usual for the additive group scheme over A (i.e., $A[G_{a,A}] = A[x]$, $\mu(x) = 1 \otimes x + x \otimes 1$). Further, $G_A(b)$ for $b \in A$ denotes the group scheme over A whose ring of the regular functions is $A[x, y]/x(by + 1) = 1$ and the comultiplication is given by $\mu(x) = x \otimes x$, $\mu(y) = 1 \otimes y + y \otimes 1 + by \otimes y$. We have $G_A(0) \cong G_{a,A}$, and if $b \in A^*$ then $G_A(b) \cong G_{m,A}$, the multiplicative group scheme over A. Thus the family of groups $G_A(b)$, $b \in A$, can be considered as a "deformation" of $G_{a,A}$ into $G_{m,A}$. (The deformation family is the group $G_{A[t]}(t)$.) The groups $G_A(b)$, $b \neq 0$, can be interpreted as the congruence subgroups modulo b of the group $G_A(b)$. (Namely, points of $G_A(b)$ over any A-algebra B which is an integral domain are elements $(by + 1) \in B^*$ with $y \in B$, i.e. elements $\equiv 1 \bmod bB$.) It could be shown (we do not use the fact below) that over a regular local domain A any smooth group scheme with connected fibres whose general fibre is G_m is isomorphic to a group $G_A(b)$, $b \neq 0$.

An example of nontrivial extension in the case $b \notin A^*$, $b \neq 0$, is the group G with ring $A[x, y, z]/x(by + 1) = 1$ and with the comultiplication $\mu(x) = x \otimes x$, $\mu(y) = y \otimes 1 + 1 \otimes y + by \otimes y$, $\mu(z) = z \otimes 1 + 1 \otimes z + y \otimes y$. Or, on the points: $(x, y, z)(x', y', z') = (xx', y + y' + byy', z + z' + yy')$; or, in the matrices

$$\begin{bmatrix} 1 & y & z \\ 0 & by + 1 & y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y' & z \\ 0 & by' + 1 & y' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & y + y' + byy' & z + z' + yy' \\ 0 & 1 + b(y + y' + byy') & y + y' + byy' \\ 0 & 0 & 1 \end{bmatrix}.$$

Received by the editors April 28, 1976.
AMS (MOS) subject classifications (1970). Primary 14L15, 20G10, 20G35.
[1]Supported by NSF.

0002-9947/79/0000-0058/$05.75

This example shows that there exist nontrivial extensions in the case $b \notin A^*$, $b \neq 0$. It is known, however (and follows from 4.6 below), that all extensions are trivial in the case $b \in A^*$ (then $G_A(b) \cong G_{m,A}$). In the case $b = 0$ we have $G_A(b) \cong G_{a,A}$ and the extensions in this case are described in [3, XV 3(iii)], [4, 4.7.4.7.3]. If $A \supseteq \mathbf{Q}$, the rational numbers we have $\mathrm{Ext}(G_A(b), G_{a,A}) = 0$ both for $b = 0$ and for $b \in A^*$. It is strange that this group $\mathrm{Ext}(G_A(b), G_{a,A})$ is not trivial in the intermediate cases $b \notin A^*$, $b \neq 0$.

Among other things it should be also noted that although the results below could be formulated without restrictions on the ring, which probably implies that there exist general proofs, our approach is by direct computation and it is based on the explicit description of some submodule of $\mathrm{Ext}(G_A(b), G_{a,A})$. But even after this explicit description is obtained, the proofs involve a lot of computation.

This paper and its author owe very much to several people. I. Dolgachov taught me the main concepts of the theory of group schemes and this paper is a by-product of our joint study of unipotent group schemes (cf. [4]). The results of this paper were discussed with D. Kazhdan whose sincere interest was stimulating and whose remarks were illuminating. Professor W. Messing made many corrections and essentially simplified proofs of Proposition 2, and Lemmas 3.4, 3.1 and 7.1 (the proofs of these statements given below are his), Professor H. Miyanishi also sent me many corrections and suggestions. I am grateful to I. Dolgachov, D. Kazhdan, W. Messing, M. Miyanishi for their interest and patience.

1. Notations and formulation of main results. Let K be the field of quotients of A, $T = \{f \in K[y] | f(0) = 0\}/\{f \in A[y] | f(0) = 0\}$ (A-module quotient). We shall represent elements of T as polynomials from $K[y]$ having zero constant term.

Let $Q(y) = \sum_{i=0}^{n} a_i y^i \in K[y]$. Set $Q^{[m]}(y) = \sum_{i=m}^{n} a_i \binom{i}{m} y^{i-m}$.

(REMARK (D. KAZHDAN). When it makes sense we have $Q^{[m]}(y) = (m!)^{-1}(d/dy)^m$. So in general we can represent $Q^{[m]}$'s as follows. Instead of the ring of differential operators (in one variable) with constant coefficients we take the ring of divided powers and make it act on $K[y]$. The $Q^{[m]}$'s are the results of application of some basic elements of this ring to Q. So the picture is similar (or dual to similar) to the relation to polynomial rings and divided power rings.)

Suppose that $b \neq 0$ and set

$$D_i(Q)(y) = (by + 1)^i Q^{[i]}(y) - Q^{[i]}(0)$$

and denote by R the A-algebra of operators on $K[y]$, generated by D_i, $i > 0$. We set $D_0 =$ identity operator.

The ring R evidently preserves $A[y]$. Hence it acts on T. We denote by T_R

the set of common zeros of all D_i, $i > 0$, on T, $T_R = \{P(y) \in T | R(P) = 0\}$ $= \{P(y) \in T | D_i(P) = 0 \ \forall i > 0\}$. Introduce polynomials $P_m(y) = b^{-m-1}\Sigma_{m \geqslant i \geqslant 1}(-yb)^i(i)^{-1} \in \mathbf{Z}[b^{-1}, (m!)^{-1}][y]$ where b is an indeterminate.

(REMARK. These polynomials are truncated series for $\log(1 + by)$ multiplied by b^{-m-1}.) When K is of characteristic $p > 0$, define F: $K[y] \to K[y]$ by $F(P(y)) = (P(y))^p$, so that $F\lambda = \lambda^p F$ for $\lambda \in K$. Denote by $\Pi(A)$ the set of primes which are not invertible in A.

Note that $\mathrm{Ext}(G_A(b), G_{a,A})$ is a module over the endomorphism ring of $G_{a,A}$. In particular, it is an A-module and if K is of characteristic $p > 0$ then it is an $A[F]$-module.

The main results of the present note are the following:

1.1. R is a commutative ring and it is generated by D_{p^i}, $i \geqslant 0, p \in \Pi(A)$ (cf. 4.1).

1.2. $\mathrm{Ext}(G_A(b), G_{a,A})$ contains an A-submodule isomorphic to T_R (cf. Proposition 2 and Lemma 3.3).

1.3. $\mathrm{Ext}(G_A(b), G_{a,A})$ is the union of its A-submodules annihilated by powers of b. In particular, it is zero if $b \in A^*$ (cf. 3.5, 3.6).

1.4. If $A \supseteq \mathbf{Q}$, then

(i) $R = A[D_1]$ (cf. 1.1).

(ii) $\mathrm{Ext}(G_A(b), G_{a,A}) \cong T_R$ (cf. 7.1, 8.1).

(iii) $T_R \cong A[b^{-1}]/A$ (cf. 7.1).

(iv) The polynomials $P_m(y)$ generate the A-module T_R (cf. 6.1).

1.5. If $A \supseteq \mathbf{F}_p$, then

(i) $R = A[D_{p^i}, i \geqslant 0]$ (cf. 1.1).

(ii) $\mathrm{Ext}(G_A(b), G_{a,A}) \cong T_R$ (cf. 7.2, 8.2).

(iii) $T_R \cong A[F]/A[F]b^{p-1}$ (cf. 6.2.3).

(iv) $P_{p-1}(y)$ generates the $A[F]$-module T_R (cf. 6.2.3).

1.6. If $A \supseteq \mathbf{Z}$ then

$$\left(\prod_{p \in \Pi(A)} p^{[\log_p m]}\right) P_m(y) \in T_R \quad \text{(cf. 6.3)}.$$

1.7. Let $\tilde{A}$ be another integral domain and φ: $A \to \tilde{A}$ a ring homomorphism. Let

$$\varphi^*\colon \mathrm{Ext}(G_A(b), G_{a,A}) \to \mathrm{Ext}(G_{\tilde{A}}(\varphi(b)), G_{a,\tilde{A}})$$

be the induced homomorphism. If either $\varphi(b) \neq 0$ and $\tilde{A}$ contains a field, or $\tilde{A} \supseteq \mathbf{Q}$, or $\tilde{A}$ is a discrete valuation ring, or $\tilde{A}$ is a field of characteristic $p > 0$, or $\tilde{A}$ is a local integral domain which does not contain a field, then the image of φ^* generates the target module (cf. 9.2, 9.3).

The two last results give an estimate on the size of the group $\mathrm{Ext}(G_a(b), G_{a,A})$ also when A does not contain a field.

Notations. A, b (recall $b \neq 0$ throughout), $G_A(b)$, $G_{a,A}$, μ (comultiplication),

$K, x, y, R, D_i, T, T_R, P_m(y), F, \Pi(A)$ and also $N, \tilde{N}, \iota$ (coinversion), t, introduced below are fixed in the note. Since $G_K(b) \simeq G_{m,K}$ we write $K[G_A(b)] = K[t, t^{-1}]$. We assume (without loss of generality) that $x, y \in A[G_A(b)] \subseteq K[G_A(b)]$ are given by $x = t^{-1}$, $by + 1 = t$. We denote by ι the coinversion in $K[t, t^{-1}]$. It is given by $\iota(t) = t^{-1}$, $\iota(t^{-1}) = t$, $\iota(x) = by + 1$, $\iota(y) = -xy$. We denote by $\deg P(y)$ the degree of a polynomial $P(y)$ and by $\deg_A P(y)$ (the degree modulo $A[y]$) the highest power of y in $P(y)$ whose coefficient is not in A. We denote by $\binom{m}{i}$ binomial coefficients, i.e.,

$$(x + y)^m = \sum_{i=0}^{m} \binom{m}{i} x^i y^{m-i},$$

and we assume that $\binom{m}{i} = 0$ for $i < 0$ and $i > m$. We denote by $\mathbf{Z}$, $\mathbf{Z}^+$, $\mathbf{N}$, $\mathbf{Q}$ the set of integers, nonnegative integers, positive integers, rational numbers respectively.

2. Initial interpretation. Let N be the A-module of polynomials $Q(x, y) \in K[x, y]/x(by + 1) = 1$ which satisfy

$$\mu(Q(x, y)) - Q(x, y) \otimes 1 - 1 \otimes Q(x, y) \in A[x, y] \otimes A[x, y]. \quad (2.1)$$

Let further $\tilde{N} = A[x, y]/x(by + 1) = 1 \subset N$.

PROPOSITION. $\mathrm{Ext}(G_A(b), G_{a,A}) \cong N/\tilde{N}$.

PROOF (W. MESSING). Let G be the middle term of an exact sequence of commutative A-groups

$$1 \to G_{a,A} \to G \to G_A(b) \to 1.$$

Since the scheme $G_A(b)$ is affine and since $H^1(X, G_{a,A}) = 0$ for X affine (cf. [2, III, §4, 6.6]) we have $H^1(G_A(b), G_{a,A}) = 0$ whence it follows that the projection $G \to G_A(b)$ admits a regular section. (In particular, $G \simeq G_A(b) \times G_{a,A}$ as schemes and so G is affine.)

Now [2, III, §6, 2.4] says that $\mathrm{Ext}(G_A(b), G_{a,A}) \simeq H^2(G_A(b), G_{a,A})_{\mathrm{sym}}$, the set of symmetric two-cocycles modulo boundaries. A two-cocycle is a regular map

$$f\colon G_A(b) \times G_A(b) \to G_{a,A}.$$

Since $G_{a,A} = \mathbf{A}^1_A$, we can consider f as an element of $A[G_A(b) \times G_A(b)] = A[G_A(b)] \otimes A[G_A(b)]$.

Since any extension of $G_{a,K}$ by $G_{m,K}$ splits, i.e., $H^2(G_K(b), G_{a,K}) = 0$ (cf. [1, XVII, 5.1.1(d)]), we have f is a coboundary over K, i.e. there is $g \in K[G_A(b)]$ such that $f = \delta g$. If, on the other hand, $g \in K[G_A(b)]$ is such that $\delta g \in A[G_A(b)] \otimes A[G_A(b)]$ then δg is a cocycle and it is symmetric: $\delta g \in Z^2_{\mathrm{sym}}(G_A(b), G_{a,A})$.

Therefore we can identify $Z^2_{\mathrm{sym}}(G_A(b), G_{a,A})$ with $\delta(K[G_A(b)]) \cap$

$(A[G_A(b)] \otimes A[G_A(b)])$. Note now that

$$\delta\colon K[G_A(b)] \to K[G_A(b)] \otimes K[G_A(b)]$$

is given by $(\delta(g))(s_1, s_2) = g(s_1 s_2)g(s_1)^{-1}g(s_2)^{-1}$ or $\delta g = \mu(g) - g \otimes 1 - 1 \otimes g$.

We write $K[G_A(b)] = K[G_{m,K}] = K[t, t^{-1}]$ with $\mu(t) = t \otimes t$, $\mu(t^{-1}) = t^{-1} \otimes t^{-1}$. Let $g = \Sigma a_i t^i$. Then $\delta g = \mu(g) - g \otimes 1 - 1 \otimes g = \Sigma a_i t^i \otimes t^i - \Sigma a_i t^i \otimes 1 - 1 \otimes \Sigma a_i t^i$. It follows that $\delta g \neq 0$ for $g \neq 0$, $g \in K[G_A(b)]$. Therefore we can identify $Z^2_{\mathrm{sym}}(G_A(b), G_{a,A})$ with

$$N = \{ g \in K[G_A(b)] \mid \delta g \in A[G_A(b)] \otimes A[G_A(b)] \}.$$

Now the set of coboundaries is $\delta(A[G_A(b)])$ or with the above identification simply $\tilde{N} = A[G_A(b)] \subset N$. This concludes the proof of our assertion.

3. The beginning of computations.

3.1. LEMMA. (i) *Every* $Q(x, y) \in K[x, y]/x(by + 1) = 1$ *can be expressed in the form* $P(y)x^m$.

(ii) *If* $P(y)x^m = \tilde{P}(y)x^n$, $m \geqslant n$, *then* $P(y) = \tilde{P}(y)(by + 1)^{m-n}$.

(iii) *If* $P(y)x^m \in A[x, y]/x(by + 1) = 1$ *then* $P(y) \in A[y]$.

(iv) *If* $x^m \otimes x^n(\Sigma_i P_{1i}(y) \otimes P_{2i}(y)) \in A[x, y]/x(by + 1) = 1 \otimes A[x, y]/x(by + 1) = 1$ *then* $\Sigma P_{1i}(y) \otimes P_{2i}(y) \in A[y] \otimes A[y]$.

PROOF. The first two assertions are evident. The third and the fourth ones follow from

3.1.1. LEMMA (W. MESSING). *Let* $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ *and* $f(0, 0, \ldots, 0) \in A^*$. *Let* $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ *be such that* $f^s \cdot g \in A[x_1, \ldots, x_n]$. *Then* $g(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$.

PROOF OF LEMMA 3.1.1. If $s \leqslant 0$, then there is nothing to prove. Suppose that $s > 0$. Then it is sufficient to consider the case $s = 1$ (otherwise we replace g by $f^{s-1}g$ and apply induction on s). So let $s = 1$. Let x^q (where $q = (q_1, \ldots, q_n)$) be the product of x_i's to the q_ith powers. Suppose that x^r is the term of smallest total degree in g whose coefficient a_r does not belong to A. But the coefficient of x^r in $f \cdot g$ does belong to A. This latter coefficient is congruent mod A to $f(0, \ldots, 0)a_r$, i.e. $a_r \in A$, a contradiction.

3.1.2. THE PROOF OF LEMMA 3.1 CONTINUED. In case (iii) we apply Lemma 3.1.1 with $n = 1$, $f(x_1) = bx_1 + 1$. Indeed our condition means $P(y) \cdot (by + 1)^{-m} \in A[y]_{by+1}$ (= localization of $A[y]$ at $(by + 1)$). This means that $P(y) = P'(y)(by + 1)^q$ with $P'(y) \in A[y]$. So there is nothing to prove if $q \geqslant 0$. If $q < 0$, then $P(y)(by + 1)^{-q} \in A[y]$ and we are in conditions of Lemma 3.1.1.

In case (iv) we consider $\Sigma P_{1i}(y) \otimes P_{2i}(y)$ as a polynomial $P(y_1, y_2)$ in two

variables. Then we have

$$P(y_1, y_2) \cdot (by_1 + 1)^{-m}(by_2 + 1)^{-n} \in A[y_1, y_2]_{by_1+1,\, by_2+1}$$

and we argue as above using Lemma 3.1.1 with $f(x_1, x_2) = (bx_1 + 1)(bx_2 + 1)$.

3.2. LEMMA. $\mu(P(y)) = \Sigma_{i\geqslant 0}(by + 1)^i P^{[i]}(y) \otimes y^i$.

PROOF. The expression is linear in $P(y)$. Hence it is sufficient to check it for a basis of $K[y]$. We have $\mu((by + 1)^m) = (by + 1)^m \otimes (by + 1)^m$. On the other hand $((by + 1)^m)^{[i]} = b^i \binom{m}{i}(by + 1)^{m-i}$. Hence the right-hand side of the formula has the form

$$\sum_{i>0} (by + 1)^i b^i \binom{m}{i}(by + 1)^{m-i} \otimes y^i = \sum_{i>0} (by + 1)^m \otimes \binom{m}{i} b^i y^i$$
$$= (by + 1)^m \otimes (by + 1)^m.$$

3.3. LEMMA. *Let $Q(x, y) = P(y)x^m$. The condition $Q(x, y) \in N$ is equivalent to the following condition*

$$\sum_{i>1} D_i(P)(y) \otimes y^i - \big((by + 1)^m - 1\big) \otimes P(y)$$
$$- P(y) \otimes \big((by + 1)^m - 1\big) - P(0) \otimes 1 \in A[y] \otimes A[y]. \quad (3.3.1)$$

In particular, $P(0) = 0$, and $T_R \subseteq \mathrm{Ext}(G_A(b), G_{a,A})$.

PROOF. We have

$$\mu(P(y)x^m) - P(y)x^m \otimes 1 - 1 \otimes P(y)x^m$$
$$= x^m \otimes x^m\big(\mu(P(y)) - P(y) \otimes (by + 1)^m - (by + 1)^m \otimes P(y)\big).$$

By Lemma 3.1(iv), (2.1) takes the form

$$\mu(P(y)) - P(y) \otimes (by + 1)^m - (by + 1)^m \otimes P(y) \in A[y] \otimes A[y].$$

We have further

$$\mu(P(y)) = P(y) \otimes 1 + \sum_{i>1} (by + 1)^i P^{[i]}(y) \otimes y^i$$
$$= P(y) \otimes 1 + \sum_{i>1} D_i(P)(y) \otimes y^i + \sum_{i>1} P^{[i]}(0) \otimes y^i$$
$$= P(y) \otimes 1 + \sum_{i>1} D_i(P)(y) \otimes y^i + 1 \otimes (P(y) - P(0))$$

whence our assertion follows (the inclusion of T_R in $\mathrm{Ext}(G_A(b), G_{a,A})$ being the case when $m = 0$).

3.4. Let ι be the coinversion in $K[t, t^{-1}]$, $\iota(t) = t^{-1}$, $\iota(t^{-1}) = t$. It is an automorphism of the ring $K[t, t^{-1}]$. We have $\iota(x) = by + 1$, $\iota(y) = -xy$.

Thus ι determines the multiplication by -1 in the group scheme $G_A(b)$. In particular, ι acts on $\mathrm{Ext}(G_A(b), G_{a,A})$ and, since Ext is an additive functor we get the following:

LEMMA. *ι acts as (-1) on* $\mathrm{Ext}(G_A(b), G_{a,A})$.

3.5. Denote by N_b the A-submodule in N which consists of $Q(x,y) \in A[b^{-1}][x,y]/x(by+1) = 1$.

PROPOSITION. $\mathrm{Ext}(G_A(b), G_{a,A}) \cong N_b/\tilde{N}$. *In particular,* $\mathrm{Ext}(G_A(b), G_{a,A})$ *is the inductive limit of submodules annihilated by powers of* b.

PROOF. Let $x^m P(y) \in N$, $P(y) = \Sigma_{i=0}^r a_i y^i$. Applying ι (cf. 3.4 above), we can assume $m < r$. Then for $r \geqslant 1$ the coefficient of $y^r \otimes y^r$ in (3.3.1) is $a_r b^r$ (this term is contained only in $D_r(P)(y) \otimes y^r$). Hence by 3.3 we have $a_r b^r \in A$, that is, $b^r x^m P(y)$ can be represented modulo $\tilde{N}$ in a form $x^{m_1} R(y)$, where $\deg R(y) < \deg P(y)$. By induction on $r = \deg P$ we see, using 3.1(iii) that $b^M P(y) \in A[y]$ for some M, as asserted.

3.6. COROLLARY. *If $b \in A^*$ then* $\mathrm{Ext}(G_A(b), G_{a,A}) = 0$.

4. Structure of $R = A[D_i, i > 0]$.

4.1. THEOREM. (i) $D_i D_j = \Sigma_{r=0}^i \binom{i}{r}\binom{j+r}{i} b^{i-r} D_{j+r}$.
(ii) $D_i D_j = D_j D_i$.
(iii) $R = A[D_{p^i}, i = 0, 1, \ldots, ; p \in \Pi(A)]$.

PROOF. (i) One has (where we set $r = i - s$)

$$\begin{aligned}
\big((by+1)^j P^{[j]}(y)\big)^{[i]} &= \sum_{s=0}^{i} \binom{i}{s} b^s (by+1)^{j-s} \cdot \frac{j(j-1)\ldots(j-s+1)}{i!} \\
&\quad \cdot \frac{1}{j!} \frac{d^{i+j-s} P(y)}{dy^{i+j-s}} \\
&= \sum_{s=0}^{i} \binom{i}{s} b^s (by+1)^{j-s} \frac{j(j-1)\ldots(j-s+1)}{i!} \\
&\quad \cdot \frac{(j+i-s)\ldots(j+1)}{(j+i-s)!} \cdot \frac{d^{i+j-s} P(y)}{dy^{i+j-s}} \\
&= \sum_{s=0}^{i} \binom{i}{s} b^s (by+1)^{j-s} \binom{j+i-s}{i} P^{[i+j-s]}(y) \\
&= \sum_{r=0}^{i} \binom{i}{r} b^{i-r} (by+1)^{j-i+r} \binom{j+r}{i} P^{[j+r]}(y) \\
&= \sum_{r=0}^{i} \binom{i}{r}\binom{j+r}{i} b^{i-r} \big[(by+1)^{j-i+r} P^{[j+r]}(y)\big].
\end{aligned}$$

Now

$$(D_iD_jP)(y) = (by + 1)^i\left[(by + 1)^jP^{[j]}(y)\right]^{[i]} - \left[(by + 1)^jP^{[j]}(y)\right]^{[i]}|_{y=0}$$

$$= \sum_{r=0}^{i}\binom{i}{r}\binom{j+r}{i}b^{i-r}\left[(by + 1)^{j+r}P^{[j+r]}(y)\right]$$

$$- \sum_{r=0}^{i}\binom{i}{r}\binom{j+r}{i}b^{i-r}P^{[j+r]}(0)$$

$$= \sum_{r=0}^{i}\binom{i}{r}\binom{j+r}{i}b^{i-r}D_{j+r}P(y)$$

$$+ \sum_{r=0}^{i}\binom{i}{r}\binom{j+r}{i}b^{i-r}P^{[j+r]}(0)$$

$$- \sum_{r=0}^{i}\binom{i}{r}\binom{j+r}{i}b^{i-r}P^{[j+r]}(0),$$

whence (i).

(ii) Using the identity

$$\binom{i}{m}\binom{j+i-m}{i} = \binom{j}{m}\binom{j+i-m}{j}$$

one has

$$D_iD_j = \sum_{r=0}^{i}\binom{i}{r}\binom{j+r}{i}b^{i-r}D_{j+r} = \sum_{m=i}^{0}\binom{i}{i-m}\binom{j+i-m}{i}b^mD_{i+j-m}$$

(by our convention on binomial coefficients, the terms with $m > \min(i, j)$ vanish and this equals)

$$= \sum_{m=j}^{0}\binom{j}{j-m}\binom{i+j-m}{j}b^mD_{i+j-m} = \sum_{r=0}^{j}\binom{j}{r}\binom{i+r}{j}b^{j-r}D_{i+r} = D_jD_i.$$

(iii) Suppose that n is not a power of a prime in $\Pi(A)$. Let us show that $D_n \in A[D, \ldots, D_{n-1}]$ in this case. Then (iii) evidently follows.

For every pair $i, j \in \mathbf{N}$ such that $i + j = n$ we have $D_iD_j = \binom{n}{i}D_n$ mod $\Sigma_{i<n} AD_i$. It follows from our choice of n that $\mathrm{GCD}_{i\in[1,n-1]}\{\binom{n}{i}\}$ is invertible in A. Hence there exist $a_1, \ldots, a_{n-1} \in \mathbf{Z}$ such that $\Sigma_{0<i<n} a_iD_iD_{n-i} \equiv \varepsilon D_n$ mod $\Sigma_{i<n} AD_i$ where $\varepsilon \in A^*$. Hence $D_n \in A[D_1, \ldots, D_{n-1}]$ as asserted.

4.2. COROLLARY. *$R \otimes A/(b)$ is a quotient of the free divided power algebra on one generator.*

Evident.

4.3. COROLLARY. $nD_n = D_1(\Sigma_{i=0}^{n-1}(-b)^i D_{n-i-1})$.

PROOF (BY INDUCTION). Suppose that our assertion is proved for n and let us prove it for $n + 1$. We have by 4.1(i)

$$D_1 D_n = (n + 1)D_{n+1} + nbD_n.$$

By the induction hypothesis we have

$$D_1 D_n = (n + 1)D_{n+1} + bD_1\left(\sum_{i=0}^{n-1}(-b)^i D_{n-i-1}\right)$$

whence our assertion.

4.4. COROLLARY. $(n!)D_n \equiv D_1^n \bmod bR$.

The proof follows immediately from 4.3.

5. Action of R on $A[y]$.

5.1. LEMMA. (i) $D_r(y^m) = \binom{m}{r} y^{m-r}(by + 1)^r$ *if* $m > r$.
(ii) $D_r(y^r) = (by + 1)^r - 1$.
(iii) $D_r(y^m) = 0$ *if* $m < r$.

Evident.

5.2. LEMMA. $(D_1 P_m)(y) = (-y)^m$.

PROOF. One has

$$(by + 1)\frac{d}{dy}\left[b^{-m-1}\sum_{i=1}^{m}\frac{(-by)^i}{i}\right] = (by + 1)b^{-m-1}\cdot\sum_{i=1}^{m}(-by)^{i-1}\cdot(-b)$$

$$= -b^{-m}\left(\sum_{i=1}^{m}(-by)^{i-1} - \sum_{i=1}^{m}(-by)^i\right) = -b^{-m} + b^{-m}(-by)^m.$$

Hence

$$(D_1 P_m)(y) = (by + 1)P_m^{[1]}(y) - P_m^{[1]}(0) = (-y)^m$$

as asserted.

5.3. LEMMA.
(i) $n(D_n P_m)(y) = (-1)^m \Sigma_{i=0}^{n-1}(-b)^i \binom{m}{n-i-1} y^{m-n+i+1}(by + 1)^{n-i-1}$ *if* $n < m$.
(ii) $m(D_m P_m)(y) = (-1)^m(by + 1)^m b^{-1} - (-1)^m b^{-1}$.
(iii) $(D_n P_m)(y) = 0$ *if* $n > m$.

PROOF. Using 4.3, 4.1(ii) and then 5.1 we get for $n < m$

$$n(D_nP_m)(y) = D_1\left(\sum_{i=0}^{n-1}(-b)^iD_{n-i-1}\right)P_m(y)$$
$$= \left(\sum_{i=0}^{n-1}(-b)^iD_{n-i-1}\right)(-y)^m$$
$$= (-1)^m\cdot\left(\sum_{i=0}^{n-1}(-b)^i\binom{m}{n-i-1}y^{m-n+i+1}(by+1)^{n-i-1}\right).$$

This proves the first equation. The remaining equations are evident.

6. Computation of T_R.

6.1. *The case* $\mathbf{Q} \subseteq A$.

PROPOSITION. *The A-module T_R is isomorphic to $A[b^{-1}]/A$. The images of polynomials $P_m(y)$ generate T_R over A.*

PROOF. By 4.1(iii), $R = A[D_1]$. By 5.2 we have $P_m(y) \in T_R$. Take now $P(y) = \Sigma_{i=1}^m a_iy^i \in T_R$. Then

$$(by+1)P^{[1]}(y) - P^{[1]}(0) \in A[y]$$

implies that $mba_m \in A$ where a_m is the coefficient of the highest power of y. Hence

$$\deg\left[P(y) + (-1)^{m-1}mba_mP_m(y)\right] < \deg P(y).$$

Applying the same method m times we get $P(y) \in \Sigma_{i=1}^m AP_i(y)$, i.e., $T_R = \Sigma_{i\geqslant 1} AP_i(y)$. This proves the second assertion of Proposition 6.1.

Note that $bP_m(y) \equiv P_{m-1}(y) \bmod A[y]$. It implies that T_R is the direct limit of $A/(b^i)$ with respect to inclusions $A/(b^i) \to A/(b^{i+r})$ given by $\lambda \mapsto \lambda b^r$. This direct limit is clearly isomorphic to $A[b^{-1}]/A$.

6.2. *The case* $\mathbf{F}_p \subseteq A$.

6.2.1. *An expression for* $(D_{p^q}P)(y)$. To avoid, at least partially, what the referee called a typographical *nightmare* we use notation $Q = p^q$. Take $P(y) = \Sigma_{i=1}^m a_iy^i$ and set $(D_QP)(y) = \Sigma_{i=1}^m b_{iq}y^i$. Suppose that $Q = p^q \leqslant m$ (otherwise the result is zero by 5.3). We have

$$(D_QP)(y) = (by+1)^QP^{[Q]}(y) - P^{[Q]}(0)$$
$$= (b^Qy^Q+1)P^{[Q]}(y) - P^{[Q]}(0)$$
$$= \sum_{i=Q}^m\binom{i}{Q}a_ib^Qy^i + \sum_{i=Q}^m\binom{i}{Q}a_iy^{i-Q} - a_Q$$
$$= \sum_{i=1}^{Q-1}\binom{i+Q}{Q}a_{i+Q}y^i + \sum_{i=Q}^{m-Q}\left(\binom{i}{Q}b^Qa_i + \binom{1+Q}{Q}a_{i+Q}\right)y^i$$
$$+ \sum_{i=m-Q+1}^m\binom{i}{Q}a_ib^Qy^i.$$

This gives us for $1 \leqslant (rp + d)Q \leqslant m - Q$

$$b_{(rp+d)Q,\,q} = \binom{(rp + d)Q}{Q} b^{Q} a_{(rp+d)Q} + \binom{(rp + d + 1)Q}{Q} a_{(rp+d+1)Q}.$$

Using the relation $\binom{(rp+d)Q}{Q} \equiv d \pmod{p}$ we get

$$b_{(rp+d)Q,\,q} = db^{Q} a_{(rp+d)Q} + (d + 1)a_{(rp+d+1)Q} \quad \text{for } 1 \leqslant (rp + d). \quad (*)$$

It is assumed in this relation that $a_i = 0$ for $i > m$.

6.2.2. LEMMA. *If* $P(y) \in T_R$ *then* (i) $a_{rQ} \in A$ *for* $(r, p) = 1$, $r > p$ *and* (ii) $b^{(p-r)Q} a_{rQ} \in A$ *for* $r = 1, 2, \ldots, p - 1$.

PROOF. Since $P(y) \in T_R$, we have $b_{iq} \in A$ for all i and q. Applying successively $(*)$ from 6.2.1 with $d = 0, 1, \ldots, p - 2$, we get (i). Applying now $(*)$ from 6.2.1 with $r = 0$ and $d = p - 1, p - 2, \ldots, 1$ successively, we get the second relation.

6.2.3. PROPOSITION. *Assume* $\mathbf{F}_p \subseteq A$. *Then* T_R *is an* $A[F]$*-module isomorphic to* $A[F]/A[F]b^{p-1}$. *The polynomials* P^{Q}_{p-1}, $q \geqslant 0$, *generate* T_R *over* A.

PROOF. By 5.1(iii), $R = A[D_{p^i}, i = 0, 1, \ldots,]$. It is clear that $(D_{p^i} P^{Q}_{j})(y) = 0$ if $j \in [1, p - 1]$ and $i \neq q$. For $i = q$ we have $(D_Q P^{Q}_{j})(y) = (-1)^{jQ} y^{jQ}$ for $j \in [1, p - 1]$.

Indeed, we have

$$P^{Q}_{j}(y) = b^{-Q(j+1)} \sum_{j \geqslant i \geqslant 1} (-by)^{Qi-1}.$$

So

$$\left(P^{Q}_{j}\right)^{[Q]}(y) = b^{-Q(j+1)} \sum_{j \geqslant i \geqslant 1} \binom{Qi}{Q} (-b)^{Qi} y^{Q(i-1)i-1}$$

$$= b^{-Q(j+1)} \sum_{j \geqslant i \geqslant 1} (-b)^{Qi} y^{Q(i-1)}$$

whence (cf. 5.2)

$$\left(D_Q P^{Q}_{j}\right)(y) = \left(b^{Q} y^{Q} + 1\right)\left(P^{Q}_{j}\right)^{[Q]}(y) - \left(P^{Q}_{j}\right)^{[Q]}(y)$$

$$= b^{-Q(j+1)}\left(\sum_{j \geqslant i \geqslant 1} (-1)^{Qi} b^{Q(i+1)} y^{Qi} + (-1)^{Qi} b^{Qi} y^{Q(i-1)} \right) - b^{Qj} \cdot (-1)^{Q}$$

$$= b^{-Q(j+1)} (-1)^{Qj} b^{Q(j+1)} y^{Qj} = (-1)^{Qj} y^{Qj}.$$

So $P^{Q}_{j}(y) \in T_R$ for all $q \geqslant 0$ and every $j \in [1, p - 1]$.

Assume now that $P(y) \in T_R$, $m = \deg_A P(y)$, $a_m \notin A$. We can assume at once that $m = \deg P(y)$. By 6.2.2(ii) we have $m = dQ$, $d \in [1, p - 1]$, $q \geqslant 0$.

Using (*) from 6.2.1 we get $b_{m,Q} = d \cdot b^Q a_m \in A$ whence it follows that

$$\deg\big[P(y) - \lambda P_d^Q(y)\big] < \deg P(y)$$

for some $\lambda \in A$. Applying now the induction on deg $P(y)$ we see that $P_i^Q(y)$, $i \in [1, p-1]$, $q \geqslant 0$, generate T_R. Since $b^i P_{p-1}(y) \equiv P_{p-1-i}(y) \bmod A(y)$ for $0 \leqslant i \leqslant p-1$, we get that $P_{p-1}^Q(y)$, $q \geqslant 0$, generate T_R. This proves the last assertion.

It follows now that T_R is an $A[F]$-module with one generator $P_{p-1}(y)$. (Recall that we set $F(P(y)) = P^p(y)$.) Since $b^{p-1}P_{p-1}(y) \in A[y]$, T_R is a quotient of $A[F]/A[F]b^{p-1}$. If $\Sigma_{i=r}^{s} \lambda_i F^i P_{p-1}(y) \in A[y]$ one shows inductively that each λ_i is a multiple of $b^{p^i(p-1)}$ and thus establishes the first assertion.

6.3. *The case* $\mathbf{Z} \subseteq A$.

PROPOSITION. $\Pi_{p \in \Pi(A)} p^{[\log_p m]} \cdot P_m(y) \in T_R$.

PROOF. By 5.3, $(nD_n P_m)(y) \in A[y]$ for all n. Since $(D_n P_m)(y) = 0$ for $n > m$, we have only to check that $n^{-1} \cdot \Pi_{p \in \Pi(A)} p^{[\log_p m]} \in A$ for $n < m$. This is clear.

6.3.1. REMARK. If p is the smallest prime in $\Pi(A)$ and $p | b^{p-1}$ then $P_p(y) \in T_R$ (since $(D_1 P_p)(y) = (-y)^p$ and $(D_p P_p)(y) = (-1)^p[(by+1)^p - 1]/pb$).

7. The kernel of the map $T_R + \iota T_R \to \mathrm{Ext}(G_A(b), G_{a,A})$. Denote this map by τ (cf. 3.4 for the definition of ι).

7.1. LEMMA. Ker τ *is generated by elements* $P + \iota P$, $P \in T_R$.

PROOF. This is evident, as ι acts as -1 on $\mathrm{Ext}(G_A(b), G_{a,A})$; see 3.4.

7.2. PROPOSITION.

$$\sum_{j=1}^{m-d} \frac{(-1)^j \binom{m}{d+j}\binom{m-j}{d}}{j} = 0, \qquad d = 0, 1, \ldots, m-1.$$

REMARK. I was not able to prove these identities directly, nor to find them in books. So the proof below can be considered either as the proof of these identities (by one who does not know them) or as an alternative proof of 7.1 in the case $A \supseteq \mathbf{Q}$ (by one who knows them).

PROOF. Take $A = \mathbf{Q}[[b]]$, b an independent variable, and use 7.1 with $P = P_m$. We have

$$P_m(y) + P_m(-xy) = b^{-m-1}\left[\sum_{i=1}^{m} i^{-1}\left((-by)^i + (bxy)^i\right)\right]$$

$$= b^{-m-1}x^m \sum_{i=1}^{m} i^{-1}(-by)^i\left[(by+1)^m + (-1)^i(by+1)^{m-i}\right]$$

$$= b^{-m-1}x^m \sum_{i=1}^{m} i^{-1}(-by)^i\left[\sum_{j=0}^{m}\binom{m}{j}b^j y^j + (-1)^i\sum_{j=0}^{m-i}\binom{m-i}{j}b^j y^j\right]$$

$$= b^{-m-1}x^m \sum_{j\geq 1} b^j y^j\left[\sum_{r=0}^{j-1}(j-r)^{-1}\left((-1)^{j-r}\binom{m}{r} + \binom{m-j+r}{r}\right)\right].$$

The condition $P_m(y) + P_m(-xy) \in A[x,y]/(by+1)x = 1$ is now equivalent to

$$\sum_{r=0}^{j-1}(j-r)^{-1}\left((-1)^{j-r}\binom{m}{r} + \binom{m-j+r}{r}\right) = 0 \quad \text{for } j = 1, \ldots, m.$$

Set $s = j - r$, $d = m - j$. Then we finally have

$$\sum_{r=0}^{j-1}(j-r)^{-1}\left((-1)^{j-r}\binom{m}{r} + \binom{m-j+r}{r}\right)$$

$$= \sum_{s=1}^{j} s^{-1}\left((-1)^s\binom{m}{j-s} + \binom{m-s}{j-s}\right)$$

$$= \sum_{s=1}^{j} s^{-1}\left((-1)^s\binom{m}{m-j+s} + \binom{m-s}{m-s-j-s}\right)$$

$$= \sum_{s=1}^{m-d} s^{-1}\left((-1)^s\binom{m}{d+s} + \binom{m-s}{d}\right).$$

8. The surjectivity of τ in the equicharacteristic case.

8.1. *The case* $\mathbf{Q} \subseteq A$.

PROPOSITION. *τ is surjective.*

PROOF. Let $P(y)x^m \in N$ and let $d = \deg P(y)$. If $d \leqslant m$ then $P(y)x^m \in K[t^{-1}]$, hence $P(y)x^m \in \iota(T_R)$ and we are done.

Therefore it can (and will) be assumed that $d > m$. Write $P(y) = \sum_{i=0}^{d} a_i y^i$. Consider in (3.3.1) the coefficient of $y^d \otimes y$. It is contained only in the summands $D_1(P)(y) \otimes y$ and $P(y) \otimes ((by+1)^m - 1)$. Corresponding coefficient is $dba_d - mba_d = b(d-m)a_d$. It follows now from 3.1(iv) that $ba \in A$.

8.1.1. LEMMA. *$P_d(y)(by + 1)^m$ is equivalent modulo $A[y]$ to a polynomial of degree d with highest coefficient $((-1)^d/b) \cdot ((-1)^m/(d \cdot \binom{d-1}{m}))$.*

Before proving Lemma 8.1.1 let us show how our proposition follows from it. One has $P_d(y) = P_d(y)(by + 1)^m x^m \in T_R \subset N$. Subtracting an appropriate multiple of $P_d(y)x^m$ from $P(y)x^m$ and using $ba_d \in A$ we get a polynomial of lower degree and our assertion follows by induction, since we get at last polynomials of degree $d \leqslant m$.

8.1.2. PROOF OF 8.1.1. Since $bP_d(y) \equiv P_{d-1}(y) \bmod A[y]$, we have $\deg_A(P_d(y)(by + 1)^m) \leqslant d$. Let $\sigma_{i,d} \cdot b^{-1}$ be the coefficient mod A of y^d in $P_d(y)(by + 1)^i$. Since $bP_d(y) \equiv P_{d-1}(y) \bmod A[y]$, we have $\sigma_{i+1,d} = \sigma_{i,d} + \sigma_{i,d-1}$. Clearly $\sigma_{0,d} = (-1)^d \cdot d^{-1}$. We can now apply induction on i (the case $i = 0$ being checked). We have

$$\sigma_{i+1,d} = \sigma_{i,d} + \sigma_{i,d-1}$$

$$= (-1)^{i+d}\left[\frac{i!}{d(d-1)\ldots(d-i)} - \frac{i!}{(d-1)\ldots(d-i-1)}\right]$$

$$= \frac{(-1)^{i+d}(d-i-1-d)i!}{d(d-1)\ldots(d-i-1)}$$

$$= (-1)^{i+d+1}\frac{(i+1)!}{d(d-1)\ldots(d-i-1)}$$

as asserted.

8.2. *The case $\mathbf{F}_p \subseteq A$.*

PROPOSITION. *τ is surjective.*

We use below notation $M = p^n$, $Q = p^q$ (cf. 6.2.1).

8.2.1. PROOF. Let $P(y)x^s \in N$. Replacing, if necessary, s by p^n ($\geqslant s$) and $P(y)$ by $P(y)(by + 1)^{p^n - s}$ we can assume that $s = p^n$. Then (3.3.1) takes the form

$$\sum_{i>1}(D_iP)(y) \otimes y^i - b^M y^M \otimes P(y) - P(y) \otimes b^M y^M - P(0) \otimes 1 \in A[y] \otimes A[y]. \qquad (*)$$

Let us use the notations of 6.2.1 for $P(y)$ and $(D_Q p)(y)$.

8.2.2. LEMMA. (i) *$b_{i,q} \in A$ for $i \neq M$, $q \neq n$.*
(ii) *$b_{i,n} - b^M a_i \in A$ for $i \neq M$.*
(iii) *$b_{M,q} - b^M a_Q \in A$ for $q \neq n$.*
(iv) *$b_{M,n} - 2b^M a_M \in A$.*

PROOF OF LEMMA. We use (*) from 8.2.1. If $i \neq M$, $q \neq n$, then $(\ldots)y^i \otimes y^Q$ is contained only in $(D_Q P)(y) \otimes y^Q$, whence (i). If $i \neq M$ then $(\ldots)y^i \otimes y^M$ is contained only in $(D_M P)(y) \otimes y^M - P(y) \otimes b^M y^M$ whence (ii). If $q \neq n$, then $y^M \otimes y^Q(\ldots)$ is contained only in $(D_Q P)(y) \otimes y^Q - b^M y^M \otimes P(y)$, whence (iii). An expression of the form $\lambda y^M \otimes y^M$ is contained in $(D_M P)(y) \otimes y^M - b^M y^M \otimes P(y) - P(y) \otimes b^M y^M$, whence (iv).

8.2.3. LEMMA. *If* $q > n$ *then* (i) $a_{rQ} \in A$ *for* $(r, p) = 1$, $r > p$, *and* (ii) $b^{(p-r)Q} a_{rQ} \in A$ *for* $r \in [1, p-1]$.

PROOF OF LEMMA. Apply 8.2.2(i) and (*) from 6.2.1 successively with $d = 0, 1, \ldots, p-2$ and get (i). Apply now 8.2.2(i) and (*) from 6.2.1 with $r = 0$ and $d = p-1, p-2, \ldots, 1$ successively and get (ii).

8.2.4. LEMMA. *If* $q \neq n$ *then* (i) $a_{rQ} \in A$ *for* $(r, p) = 1$, $r > p$ *and* (ii) $b^{(p-r)Q} a_{rQ} \in A$ *for* $r \in [1, p-1]$.

PROOF OF LEMMA. By 8.2.3 it is sufficient to prove the assertion for $q < n$. So we shall assume that $q < n$. If $i < M$ the same proof as in 8.2.3 goes through (since we use only 8.2.2(i)).

If $i = p^n$ we use 8.2.2(iii). It gives us $b_{M,q} - b^M a_q \in A$. But since $Q < M$, we have by the previous paragraph (with $i = Q$, i.e. $r = 1$) that $b^{(p-1)Q} a_Q \in A$. Hence 8.2.2 is reduced to $b_{M,q} \in A$ and the proof goes through for the remaining values of i.

8.2.5. LEMMA. *If* $q \geqslant n$ *and* $rp^{q-n} + d > 1$ *then* $(d-1)b^M a_{rQ+dM} + (d+1)a_{rQ+(d+1)M} \in A$.

PROOF. In (*) from 6.2.1 set $q := n$, $r := rp^{q-n-1}$ and substitute the resulting expression in 8.2.2(ii) (where we put $i := (rp^{q-n} + d)p^n$). The result is our assertion.

8.2.6. LEMMA. *If* $q > n$ *and* $r > 0$ *then*

$$a_{rQ+dM} \in A \quad \text{for } d \not\equiv 0, 1 \pmod{p^{q-n}}.$$

PROOF. We will prove by induction that if $i < q - n$ then $a_{rQ+dM} \in A$ for $d \not\equiv 0, 1 \bmod p^{i+1}$. To prove our statement for $i = 0$ (the beginning of induction) we set in 8.2.5 successively $d = jp + 1, jp + 2, \ldots, (j+1)p - 2$ for fixed, but arbitrary, $j \geqslant 0$. We get then that

$$a_{rQ+dM} \in A \quad \text{for } d = jp + 2, \ldots, (j+1)p - 1,$$

that is for all d except $d \equiv 0$ or $d \equiv 1 \pmod p$. Thus the inductive assumption holds for $i = 0$.

Suppose it holds for all $i \leqslant j$ and let us prove it for $j + 1$ (if $j + 1 < q -$

n, otherwise we are done). We have to prove that

$$a_{rQ+dM} \in A \quad \text{for } d \equiv 0, 1 \pmod{p^{j+1}},\ d \not\equiv 0, 1 \pmod{p^{j+2}}.$$

Since $j + 1 < q - n$ we set in 8.2.3(i): $q := n + j + 1$, $r := rp^{q-n-j-1} + d$ (with $(d, p) = 1$). Then we get that $a_s \in A$ with $s = rp^q + dp^{n+j+1}$, $d > 0$, $(d, p) = 1$. In particular (when $d = 1$) we get our inductive statement with $d \equiv 0 \pmod{p^{j+1}}$, $d \not\equiv 0 \pmod{p^{j+2}}$. Substituting this result in 8.2.5 we get that $a_{rQ+dM} \in A$ also for $d \equiv 1 \pmod{p^{j+1}}$, $d \not\equiv 1 \pmod{p^{j+2}}$. This concludes the inductive step.

8.2.7. COROLLARY. *Let* $m = \deg_A P(y)$. *Then* $m = \tilde{r}p^{\tilde{q}} + \tilde{d}p^n$ *with* $\tilde{r} \in [1, p - 1]$, $\tilde{q} \geqslant n$. *Moreover*:

(i) *If* $\tilde{q} > n$ *then* $\tilde{d} = 0$ *or* 1.

(ii) *If* $\tilde{q} = n$ *then* $\tilde{d} + \tilde{r} \in [2, p - 1]$.

We will use notation $\tilde{Q}$ for $p^{\tilde{q}}$.

PROOF. If $m \leqslant p^n = M$ then $P(y)x^M \in \iota(T_R)$ and we are done. So take $m > p^n$. Let $m = \Sigma_{0 \leqslant i \leqslant q} r_i p^i$, $r_i \in [1, p - 1]$, be the p-adic expansion of m. If $r_i \neq 0$ for $i < n$ then 8.2.4(i) yields $a_m \in A$, a contradiction. So $r_i = 0$ for $i < n$, i.e., $m = r_{\tilde{q}}p^{\tilde{q}} + \tilde{d}p^n$. We set $\tilde{r} = r_{\tilde{q}}$. Then if $\tilde{q} > n$ we have by 8.2.6 that $\tilde{d} = 0$ or 1. If $\tilde{q} = n$ then $m > p^n$ implies $\tilde{d} + \tilde{r} \in [2, p - 1]$.

8.2.8. LEMMA. *Let* $\tilde{q} > n$. *Then*

(i) $b^{\tilde{Q}}a_{\tilde{r}\tilde{Q}} \in A$.

(ii) $-b^M a_{\tilde{r}\tilde{Q}} + a_{\tilde{r}\tilde{Q}+M} \in A$.

(iii) $b^{\tilde{Q}-M}a_{\tilde{r}\tilde{Q}+M} \in A$.

PROOF. To get (i) set $r := Q$, $d := \tilde{r}$ in $(*)$ from 6.2.1 and substitute it in 8.2.2(i). To get (ii) set $d := 0$ in 8.2.5. To get (iii) apply (i) to (ii).

8.2.9. *Elimination of the case* $\tilde{q} > n$, $\tilde{d} = 1$. Using 8.2.8(iii) we can find $\lambda \in A$ such that

$$\deg_A\left[P(y) - \lambda P_{\tilde{r}}^{\tilde{Q}}(y)(by + 1)^M\right] < \deg_A P(y).$$

So in this case we can lower the degree of $P(y)$.

8.2.10. *Elimination of the case* $\tilde{q} = n$. In this case $m = (\tilde{r} + \tilde{d})p^n$ with $\tilde{r} + \tilde{d} \in [2, p - 1]$ (cf. 8.2.7). By 8.2.2(ii) (with $i := (\tilde{r} + \tilde{d})p^n > p^n$) and by 8.2.5 (where $r := 0$, $d := \tilde{r} + \tilde{d}$) we have $(\tilde{r} + \tilde{d} - 1)b^M a_{(\tilde{r}+\tilde{d})M} \in A$, since $a_j = 0$ for $j > m$. Since $\tilde{r} + \tilde{d} - 1 \neq 0$ in $\mathbf{F}_p$ we have $b^M a_{(\tilde{r}+\tilde{d})M} \in A$. It follows now from 8.1.1 that

$$\deg_A\left[P(y) - \lambda(by + 1)^M P_{\tilde{r}+\tilde{d}}^M(y)\right] < \deg_A P(y)$$

for an appropriate $\lambda \in A$.

8.2.11. *Elimination of the case* $\tilde{q} > n$, $\tilde{d} = 0$. We have in this case $m = \tilde{r}p^{\tilde{q}} (= \tilde{r}\tilde{Q})$. We get at once from 8.2.8(ii):

(a) $b^M a_{\tilde{r}\tilde{Q}} \in A$.

Let us replace $P(y)$ by $\tilde{P}(y) = P(y)(by + 1)^{\tilde{Q}-M}$ and (consequently) $P(y)x^M$ by $\tilde{P}(y)x^{\tilde{Q}}$.

(b) LEMMA. $\deg_A \tilde{P}(y) \leqslant \deg_A P(y)$.

PROOF. If $\tilde{r} > 1$, apply 8.2.6 with $r := \tilde{r} - 1$, $q := \tilde{q}$. Then we have from 8.2.6:

$$a_{(\tilde{r}-1)\tilde{Q}+dM} \in A \quad \text{for } 1 < d < p^{\tilde{q}-n}.$$

Therefore there is only one term of $\tilde{P}(y)$ of degree $> m$ which may be outside $A[y]$. It is $a_{\tilde{r}\tilde{Q}}\, b^{\tilde{Q}-M} y^{(\tilde{r}+1)\tilde{Q}-M}$. But it also belongs to $A[y]$ by (a) above and since $\tilde{Q} - M \geqslant M$.

If $\tilde{r} = 1$, $\tilde{q} > n + 1$, then we have from 8.2.6 with $r := p - 1$, $q := \tilde{q} - 1$ that

$$a_{(p-1)Q+dM} \in A \quad \text{if } 1 < d < p^{\tilde{q}-n-1}.$$

So this case is completed in the same way as the previous one.

If $\tilde{r} = 1$ and $\tilde{q} = n + 1$, then we have from 8.2.5 with $r := 0$ where we put successively $d = p - 1, p - 2, \ldots, 2$ that (compare with 8.2.3(ii))

$$b^{M(p-i)} a_{Mi} \in A \quad \text{for } i = 2, \ldots, p - 1.$$

Now we have

$$\begin{aligned}
\tilde{P}(y) &= \left(\sum_{p \geqslant i \geqslant 1} a_{iM} y^{iM} \right) (b^M y^M + 1)^{p-1} \\
&= \left(\sum_{p \geqslant i \geqslant 1} a_{iM} y^{iM} \right) \left(\sum_{p-1 \geqslant j \geqslant 0} \binom{p-1}{j} b^{Mj} y^{Mj} \right) \\
&= \sum_{2p-1 \geqslant s \geqslant 1} \left(\sum_{i+j=s} \binom{p-1}{j} b^{Mj} a_{iM} \right) y^{Ms}.
\end{aligned}$$

We have to show that if $s > p$ then $\Sigma_{i+j=s} \binom{p-1}{j} b^{Mj} a_{iM} \in A$. But if $s > p$ we just proved that $b^{Mj} a_{iM} \in A$ in this case.

(c) Thus we have $\tilde{P}(y)x^{\tilde{Q}} = P(y)x^M$ and $\deg_A \tilde{P}(y) \leqslant \tilde{r}\tilde{Q}$. By 8.2.7 we are in conditions of 8.2.10 and therefore we are done.

8.2.12. END OF THE PROOF OF PROPOSITION 8.2.1. We have shown that in all cases we can assume (possibly changing M) that for $P(y)x^M$ there exist $\lambda \in A$ and $P_i^{\tilde{Q}}(y)$ such that

$$\deg_A \left(P(y) - \lambda P_i^{\tilde{Q}}(y)(by + 1)^M \right) < \deg_A P(y).$$

Now the same argument as in 8.1 (after Lemma 8.1.1) completes the proof of Proposition 8.2.1.

9. Base change.

9.1. *An auxiliary lemma.*

LEMMA. *Let* $M = p^{n-1}$.

(i) $MP_{pM-1}(y) \in T_R$.

(ii) $MP_{pM-1}(y) \equiv P^M_{p-1}(y) \bmod p$.

(iii) $\mu(MP_{pM-1}(y)) \equiv 1 \otimes MP_{pM-1}(y) + MP_{pM-1}(y) \otimes 1 + \Sigma_{p>i>0} p^{-1}\binom{p}{i} y^{(p-i)M} \otimes y^{iM} \bmod (pA + bA)$.

PROOF. The first assertion is contained in 6.3 (with $m = p^n - 1$). We have

$$\begin{aligned} MP_{pM-1}(y) &= b^{-pM} \sum_{M>i>0} (-by)Mi^{-1} \\ &\equiv b^{-pM} \sum_{p>j>0} (-by)^{jM} j^{-1} \bmod p \\ &\equiv \left[b^{-p} \sum_{p>j>0} (-by)^j j^{-1} \right]^M \bmod p \\ &\equiv P_j^M(y) \bmod p. \end{aligned}$$

This proves (ii).

Using (ii) we see that it is sufficient to prove (iii) only in the case $M = 1$. We have then (using 3.2 and 5.3)

$$\begin{aligned} \mu(P_{p-1}(y)) - P_{p-1}(y) \otimes 1 - 1 \otimes P_{p-1}(y) &= \sum_{n>0} (D_n P_{p-1})(y) \otimes y^n \\ &= (-1)^{p-1} \sum_{p-1>n>0} \frac{1}{n} \left(\sum_{n>i\geq 0} \binom{p-1}{n-i-1} (-b)^i y^{p-n+i} (by+1)^{n-i-1} \right) \otimes y^n \\ &\quad + \frac{1}{p-1} \cdot \left[\frac{(-1)^{p-1}}{b} (by+1)^{p-1} - \frac{(-1)^{p-1}}{b} \right] \otimes y^{p-1} \\ &\equiv (-1)^{p-1} \sum_{p-1>n>0} \frac{1}{n} \binom{p-1}{n-1} y^{p-n} \otimes y^n + (-1)^{p-1} y \otimes y^{p-1} \bmod bA \\ &\equiv (-1)^{p-1} \sum_{p>n>0} \frac{1}{n} \frac{(p-1)!}{(p-n)!\,(n-1)!} y^{p-n} \otimes y^n \bmod bA. \end{aligned}$$

Now it remains to remark that $(-1)^{p-1} \equiv 1 \pmod p$ and

$$\frac{1}{n} \frac{(p-1)!}{(p-n)!\,(n-1)!} = \frac{(p-1)!}{(p-n)!\,n!} = \frac{1}{p}\binom{p}{n}.$$

9.2. *The case* $\varphi(b) = 0$. Let $\tilde{A}$ belong to one of the following classes of rings:

(a) $\tilde{A} \supseteq \mathbf{Q}$.

(b) $\tilde{A}$ is an integral domain containing $\mathbf{Z}$ with a unique prime, say p, which is not invertible in A.

(c) $\tilde{A}$ is a discrete valuation ring with residual characteristic $p > 0$.

(d) $\tilde{A}$ is a field of characteristic p.

Let A be an integral domain, $b \in A$, $b \neq 0$, and φ: $A \to \tilde{A}$ be a ring homomorphism such that $\varphi(b) = 0$. (In particular, $\varphi_*(G_A(b)) = G_{a,\tilde{A}}$.)

PROPOSITION. *The image of* φ^*: $\mathrm{Ext}(G_A(b), G_{a,A}) \to \mathrm{Ext}(G_{a,\tilde{A}}, G_{a,\tilde{A}})$ *generates its target as an* $\tilde{A}$*-module. Moreover, if* φ *is surjective then* φ^* *is surjective.*

PROOF. Suppose first that we are in cases (b), (c) or (d) with a unique prime, p, noninvertible in $\tilde{A}$. Using 9.1(iii) we see that our result follows from [**2**, II.3, 4.6] in the case (d) and from [**4**, 4.7, 4.7.3] in the cases (b), (c). If $\tilde{A} \supseteq \mathbf{Q}$ then $\mathrm{Ext}(G_{a,\tilde{A}}, G_{a,\tilde{A}}) = 0$ by [**3**, XV, 3 (iii)] and there is nothing to prove.

9.3. *The case* $\varphi(b) \neq 0$. Let $\tilde{A}$ be an integral domain which contains a field, A be an integral domain and φ: $A \to A$ be a homomorphism such that $\varphi(b) \neq 0$.

PROPOSITION. $\mathrm{Ext}(G_{\tilde{A}}(\varphi(b)), G_{a,\tilde{A}})$ *is generated by the image of* φ^*. *If* φ *is surjective, then* φ^* *is also surjective.*

PROOF. By 8.1, 8.2 $\mathrm{Ext}(G_{\tilde{A}}(\varphi(b)), G_{a,\tilde{A}})$ is generated by the image of $T_{R,\tilde{A}}$. If $A \supseteq \mathbf{Q}$, then the $P_m(y)$ generate $T_{R,\tilde{A}}$ (by 6.1). By 6.3, the $P_m(y)$ are certainly contained in the image of φ, whence the assertion.

If $\tilde{A} \supseteq \mathbf{F}_p$ and $A \supseteq \mathbf{F}_p$ then we are done by 6.2.3. Consider the case $\tilde{A} \supseteq \mathbf{F}_p$, $A \supseteq \mathbf{Z}$. Then we are done by 9.1(i), (ii).

REFERENCES

1. Séminaire de Géométrie Algébrique 1962/1964 dirigé par M. Demazure et A. Grothendieck, *Schémas en groupes*. II, Lecture Notes in Math., vol. 152, Springer-Verlag, Berlin, 1970.

2. M. Demazure and P. Gabriel, *Groupes algébriques*, North-Holland, Amsterdam, 1970.

3. M. Raynaud, *Faisceaux amples sur les schémas en groupes et les espaces homogènes*, Lecture Notes in Math., vol. 119, Springer-Verlag, Berlin, 1970.

4. B. Weisfeiler and I. Dolgachov, *Unipotent group schemae over integral domains*, Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), 757–799. (Russian)

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PENNSYLVANIA 16802