J. Math. Soc. Japan
Vol. 24, No. 3, 1972

On commutative unipotent groups defined by Seligman

By Tetsuo NAKAMURA

(Received Nov. 25, 1970)

Let F be a field of prime characteristic p, and $\boldsymbol{L}$ a given commutative Lie p-algebra over F whose p-power is nilpotent of exponent m. In [1] Seligman constructs a commutative unipotent group defined over F, of exponent p^m, whose Lie algebra is F-isomorphic to $\boldsymbol{L}$. In general this commutative unipotent group is not isomorphic to direct sum of Witt groups over the base field. (cf. example in [1].) The aim of the paper is to show that this group is isomorphic to direct sum of Witt groups over a purely inseparable extension of the base field.

The author wishes to thank Professor T. Kanno for his invaluable conversations and advice.

§ 1. Preliminaries and construction of the isomorphism.

At first we shall introduce the notations of [1] (for details see [1] § 2). Let m be a fixed positive integer, p a fixed rational prime. For each integer k, $1 \leqq k \leqq m$, let d_k be a fixed positive integer. (cf. Remark at the end of the paper.) Let R be the set of symbols

$$a=\binom{(k)}{ij}$$

where $1 \leqq k \leqq m$, $1 \leqq i \leqq d_k$, $0 \leqq j \leqq m-k$. We write $k=k(a)$, $i=i(a)$, $j=j(a)$ in the above setting, and if $j(a)>0$ we write $a-1$ for the symbol

$$\binom{(k(a))}{i(a)j(a)-1}.$$

Let S be the set of symbols

$$\binom{(k,\, r)}{ij,\, \nu},$$

where $a=\binom{(k)}{ij}$ and $b=\binom{(r)}{\nu,\, m-r}$ are in R and where $j>m-r$. We write

$$(a\,;\, b)=\binom{(k,\, r)}{ij,\, \nu}.$$

Let $x(a)$, $y(a)$, $z(a)$, $u(s)$ $(a \in R,\ s \in S)$ be $(3|R|+|S|)$ algebraically independent indeterminates over the rational field $\boldsymbol{Q}$ and we put $t(s)=u(s)^{p^{m-1}}$ for all $s\in S$.

We define a family of polynomials $\varphi_a(x, t)\in \boldsymbol{Z}[x, t]$ for $a\in R$ by induction on $j(a)$, as follows:

If $j(a)=0$, $\varphi_a(x, t)=x(a)$, and for $j(a)>0$

$$\varphi_a(x, t)=p^{j(a)}x(a)+\varphi_{a-1}(x^p, t^p) + \sum_{\substack{b\in R\\ j(b)=m-k(b)\\ j(b)<j(a)}} p^{j(a)-j(b)-1}t((a\,;\,b))\varphi_b(x^p, t^p)\,.$$

It follows that $\varphi_a(x, t)-p^{j(a)}x(a)\in \boldsymbol{Z}[\{x(c)\,;\,j(c)<j(a)\}, t]$. There are uniquely determined polynomials $\psi_a(x, t)$ in $\boldsymbol{Q}[x, t]$ $(a\in R)$ such that $x(a)=\psi_a(\varphi(x, t), t)=\varphi_a(\psi(x, t), t)$ for all $a\in R$. For each $a\in R$, put $f_a(x, y, t)=\psi_a(\varphi(x, t)+\varphi(y, t), t)$ and $g_a(x, t)=\psi_a(-\varphi(x, t), t)$. Then $f_a(x, y, t)$ and $g_a(x, t)$ are well-defined elements of $\boldsymbol{Z}[x, y, t]$ satisfying the relations;

(1) $\qquad \varphi_a(f(x, y, t), t)=\varphi_a(x, t)+\varphi_a(y, t)\,;\ \varphi_a(g(x, t), t)=-\varphi_a(x, t)$ for all a

and

$$f(f(x, y, t), z, t)=f(x, f(y, z, t), t)\,;$$
$$f(x, y, t)=f(y, x, t)\,;$$
$$f(o, x, t)=x\,;\qquad g(o, t)=0\,;$$
$$g(g(x, t), t)=x\,;\qquad f(g(x, t), x, t)=0\,.$$

Moreover we have

$$f_a(x, y, t)-x(a)-y(a)\in \boldsymbol{Z}[\{x(c), y(c)\,;\,j(c)<j(a)\}, t]\,,$$
$$g_a(x, t)+x(a)\in \boldsymbol{Z}[\{x(c)\,;\,j(c)<j(a)\}, t]\,.$$

In the followings we write $\varphi_a(x, u)$, $\psi_a(x, u)$, $f_a(x, y, u)$ and $g_a(x, u)$ for $\varphi_a(x, t)$, $\psi_a(x, t)$, $f_a(x, y, t)$ and $g_a(x, t)$, respectively, since they are also contained in $\boldsymbol{Q}[x, u]$ where $u(s)$ are such that $u(s)^{p^{m-1}}=t(s)$.

Now we define some new notations as follows;

For each $a\in R$ we write a^* for the symbol

$$\begin{pmatrix} & (k(a)) & \\ i(a) & & m-k(a)\end{pmatrix}.$$

If $k(a)<m$ and $j(a)<m-k(a)$, we write a' for the symbol

$$\begin{pmatrix} & (k(a)+1) & \\ 1 & & j(a)\end{pmatrix}.$$

For fixed k and i, let $\Pi\binom{k}{i}$ be an automorphism of $\boldsymbol{Z}[x, u]$ over $\boldsymbol{Z}$ such that

$$\Pi\binom{k}{i}(x(a)) = x(a')$$

$$\Pi\binom{k}{i}(u((a\,;b))) = u((a'\,;b))$$

$$\Pi\binom{k}{i}(x(a')) = x(a)$$

$$\Pi\binom{k}{i}(u((a'\,;b))) = u((a\,;b))$$

where $k(a)=k$, $i(a)=i$ and $1 \leqq j(a) \leqq m-k(a)-1$ and the other variables are left fixed.

LEMMA 1. *The notations are as above. Then we have*

$$\varphi_a(x, u) = \Pi\binom{k(a)}{i(a)}\varphi_{a'}(x, u) \qquad \text{for } a \text{ with } 0 \leqq j(a) \leqq m-k(a)-1 \tag{3}$$

and

$$\varphi_b(x, u) = \Pi\binom{k}{i}\varphi_b(x, u) \qquad \text{for } b \in R \text{ with } k(b) > k+1\,. \tag{4}$$

PROOF. Since $\varphi_b(x, u)$ for $k(b) > k+1$ does not contain the variables $x(a)$, $x(a')$, $u((a\,;b))$ and $u((a'\,;b))$ with $k(a)=k$, (4) is clear. For $j(a)=0$, (3) is trivial. To prove (3) by induction on $j(a)$ we may assume that (3) is true for $a-1$, i.e., $\Pi\binom{k(a)}{i(a)}\varphi_{(a-1)'}(x, u) = \varphi_{a-1}(x, u)$. By the definition of φ we have

$$\varphi_a(x, u) = p^{j(a)}x(a) + \varphi_{a-1}(x^p, u^p) + \sum_{\substack{b \in R \\ j(b)=m-k(b) \\ j(b)<j(a)}} p^{j(a)-j(b)-1}t((a\,;b))\varphi_b(x^p, u^p)$$

and

$$\varphi_{a'}(x, u) = p^{j(a)}x(a') + \varphi_{(a-1)'}(x^p, u^p) + \sum_{\substack{b \in R \\ j(b)=m-k(b) \\ j(b)<j(a')}} p^{j(a')-j(b)-1}t((a'\,;b))\varphi_b(x^p, u^p)\,.$$

Since $\Pi\binom{k(a)}{i(a)}\varphi_{(a-1)'}(x^p, u^p) = \varphi_{a-1}(x^p, u^p)$, the result is clear for a by (4).

Next we define a family of polynomials $\Phi_a(x, u) \in \boldsymbol{Z}[x, u]$ for each $a \in R$ by induction on $k(a)$, as follows:

$$\Phi_a(x, u) = \varphi_a(x, u) \qquad \text{for } a \text{ with } a = a^* \tag{5}$$

and if $j(a) < m-k(a)$

$$\Phi_a(x, u) = \Pi\binom{k(a)}{i(a)}\Phi_{a'}(x, u) + \sum_{\substack{b \in R \\ j(b)<r \\ j(b)=m-k(b)}} p^{r-j(b)-1}t((a^*\,;b))^{p^{j(a)-r}}\Phi_{b-r+j(a)+1}(x, u) \tag{5'}$$

where we put $\Phi_{b-\nu}=0$ if $b-\nu \notin R$ and where $r=m-k(a)$.

LEMMA 2. (i) *For each* $a \in R$, $\Phi_a(x, u)-\varphi_a(x, u)$ *is a linear combination of* $\{\varphi_c(x, u); j(c) \leqq j(a), k(c)>k(a)\}$ *over* $\boldsymbol{Z}[u]$.

(ii) $p^{-j(a)}(\Phi_a(x, u)-\Phi_{a-1}(x^p, u^p))-x(a)$ *belongs to* $\boldsymbol{Z}[x, u]$ *and is a linear combination of* $\{x(c); j(c) \leqq j(a), k(c)>k(a)\}$ *over* $\boldsymbol{Z}[u]$.

PROOF. We are going to prove (i) and (ii) by induction on $k(a)$. They are true for $k(a)=m$. Let $k(a)<m$ and $r=m-k(a)$. (i) is clear for $a \in R$ with $j(a)=m-k(a)$ by (5). For $j(a)<m-k(a)$, by (5′) it suffices only to note that $\Pi\binom{k(a)}{i(a)}\Phi_{a'}(x, u)-\varphi_a(x, u)$ is a linear combination of $\{\varphi_c(x, u); j(c) \leqq j(a), k(c)>k(a)\}$ over $\boldsymbol{Z}[u]$. By the induction assumption $\Phi_{a'}(x, u)-\varphi_{a'}(x, u)$ is a linear combination of $\{\varphi_c(x, u); j(c) \leqq j(a), k(c)>k(a)+1\}$ over $\boldsymbol{Z}[u]$. Hence (i) is true for $j(a)<m-k(a)$ by using Lemma 1. This proves (i).

Next for $j(a)<m-k(a)$ we have by definition

$$
\begin{aligned}
\Phi_a(x, u)-\Phi_{a-1}(x^p, u^p)= & \Pi\binom{k(a)}{i(a)}\Phi_{a'}(x, u) \\
& +\sum_{\substack{b \in R \\ j(b)<r \\ j(b)=m-k(b)}} p^{r-j(b)-1} t((a^* ; b))^{p^{j(a)-r}} \Phi_{b-r+j(a)+1}(x, u) \\
& -\Big\{\Pi\binom{k(a)}{i(a)}\Phi_{(a-1)'}(x^p, u^p) \\
& \quad +\sum_{\substack{b \in R \\ j(b)<r \\ j(b)=m-k(b)}} p^{r-j(b)-1} t((a^* ; b))^{p^{j(a)-r}} \Phi_{b-r+j(a)}(x^p, u^p)\Big\} \\
= & \Pi\binom{k(a)}{i(a)}(\Phi_{a'}(x, u)-\Phi_{(a-1)'}(x^p, u^p)) \\
& +\sum_{\substack{b \in R \\ j(b)<r \\ j(b)=m-k(b)}} p^{r-j(b)-1} t((a^* ; b))^{p^{j(a)-r}}\{\Phi_{b-r+j(a)+1}(x, u) \\
& \quad -\Phi_{b-r+j(a)}(x^p, u^p)\}\,.
\end{aligned}
$$

Thus using Lemma 1 and induction on $k(a)$ and $j(a)$, (ii) is true for $j(a)<m-k(a)$. For $j(a)=m-k(a)$ (ii) is clear by the definition of φ and Φ using $\Pi\binom{k(a)}{i(a)}\Phi_{(a-1)'}(x, u)=\varphi_{a-1}(x, u)$ and $\Phi_b(x, u)=\varphi_b(x, u)$ for $b \in R$ with $j(b)<r$ and $j(b)=m-k(b)$.

We shall define a family of polynomials $X_a(x, u) \in \boldsymbol{Z}[x, u]$ for $a \in R$. They are defined by the following system of equations;

$$
\sum_{\nu=0}^{j(a)} p^{j(a)-\nu} X_{a-\nu}^{p^\nu}=\Phi_a(x, u)\,. \tag{6}
$$

Now we are going to prove that $X_a(x, u) \in \boldsymbol{Z}[x, u]$. Its proof is essentially the same as that of Satz 1 in [2]. For $(m+1)$ independent variables $\{z_j\}$ over

$\boldsymbol{Q}$, we put

$$(7) \qquad W_j(z_0, z_1, \cdots, z_j) = W_j(z) = \sum_{\nu=0}^{j} p z_\nu^{p^{j-\nu}}, \qquad (0 \leqq j \leqq m).$$

For $c, d \in \boldsymbol{Z}[x, u]$ we write $c \equiv d\ (p^\mu)$ if $c-d \in p^\mu \boldsymbol{Z}[x, u]$.

LEMMA 3. *Let $\xi_\mu, \eta_\mu \in \boldsymbol{Z}[x, u]$ $(\mu=0, 1, \cdots, m)$. Then for any positive integer e the system of congruences*

$$\xi_\mu \equiv \eta_\mu \qquad (p^e) \qquad 0<\mu<\nu$$

is equivalent to

$$W_\mu(\xi) \equiv W_\mu(\eta) \qquad (p^{e+\mu}) \qquad 0<\mu<\nu .$$

PROOF. This is Lemma in [2] (p. 129).

LEMMA 4. *Let $X_a(x, u)$ be defined as above. Then we have*

$$X_a(x, u) \in \boldsymbol{Z}[x, u].$$

PROOF. The proof is by induction on $j(a)$. If $j(a)=0$, then $X_a(x, u) = \Phi_a(x, u)$. Thus we may assume that $X_{a-\nu}(x, u) \in \boldsymbol{Z}[x, u]$ for $1 \leqq \nu \leqq j(a)-1$. Then we have $X_{a-\nu}(x, u)^p \equiv X_{a-\nu}(x^p, u^p)\ (p)$. By Lemma 3 we have

$$\begin{aligned} & W_{j(a)-1}(X_{a-j(a)}(x, u)^p, \cdots, X_{a-1}(x, u)^p) \\ & \quad \equiv W_{j(a)-1}(X_{a-j(a)}(x^p, u^p), \cdots, X_{a-1}(x^p, u^p)) \qquad (p^{j(a)}) \\ & \quad = \Phi_{a-1}(x^p, u^p). \end{aligned}$$

By Lemma 2 (ii) we have

$$\Phi_a(x, u) \equiv \Phi_{a-1}(x^p, u^p) \qquad (p^{j(a)})$$

and by (6)

$$\begin{aligned} p^{j(a)} X_a(x, u) &= \Phi_a(x, u) - W_{j(a)-1}(X_{a-j(a)}(x, u)^p, \cdots, X_{a-1}(x, u)^p) \\ &\equiv 0 \qquad (p^{j(a)}). \end{aligned}$$

Hence $X_a(x, u) \in \boldsymbol{Z}[x, u]$.

PROPOSITION 1. *Let $X_a(x, u)$ $(a \in R)$ be polynomials defined as above. Then we have $\boldsymbol{Z}[x, u] = \boldsymbol{Z}[X, u]$.*

PROOF. $\boldsymbol{Z}[x, u] \supset \boldsymbol{Z}[X, u]$ is clear by Lemma 4. Hence it suffices only to prove $\boldsymbol{Z}[X, u] \supset \boldsymbol{Z}[x, u]$. First we note that $X_a(x, u) - x(a)$ is a polynomial in $\boldsymbol{Z}[\{x(c)\,;\ c \neq a,\ k(c) \geqq k(a),\ j(c) \leqq j(a)\}, u]$. For by Lemma 2 (i) and by the form of $\varphi_a(x, u)$ we have

$$\begin{aligned} & p^{j(a)}(X_a(x, u) - x(a)) + p^{j(a)-1}(X_{a-1}(x, u)^p - x(a-1)^p) \\ & \qquad + \cdots + (X_{a-j(a)}(x, u)^{p^{j(a)}} - x(a-j(a))^{p^{j(a)}}) \\ & \quad \in \boldsymbol{Z}[\{x(c)\,;\ k(c) > k(a),\ j(c) \leqq j(a)\}, u]. \end{aligned}$$

Using induction on j and Lemma 4 we have the result. Now we put $x(a) =$

$X_a(x, u)+h(x, u)$, where $h(x, u) \in \boldsymbol{Z}[\{x(c)\,;\, c \neq a,\, k(c) \geqq k(a),\, j(c) \leqq j(a)\},\, u]$. For $a \in R$ with $k(a)=m$, we have $h(x, u)=0$. Hence the induction on k and j completes the proof of the proposition.

By the definition of $\varphi_a(x, u)$ we have

$$\Phi_a(x, u)=\varphi_a(X(x, u), 0) \tag{8}$$

and

$$\psi_a(\varphi(X(x, u), 0), 0)=X_a(x, u)\,. \tag{9}$$

By Lemma 2 (i) there are linear forms $L_a(x)$ over $\boldsymbol{Z}[u]$ $(a \in R)$ such that

$$\Phi_a(x, u)=L_a(\varphi(x, u))\,. \tag{10}$$

Hence we have

$$\varphi_a(X(x, u), 0)=L_a(\varphi(x, u))\,. \tag{11}$$

PROPOSITION 2. *We have the following identities;*

$$X_a(f(x, y, u), u)=f_a(X(x, u), X(y, u), 0) \qquad \textit{for all } a \in R\,.$$

PROOF.

$$\begin{aligned} X_a(f(x, y, u), u) &= \psi_a(\varphi(X(f(x, y, u), u), 0), 0) && \text{(by (9))} \\ &= \psi_a(L(\varphi(f(x, y, u), u)), 0) && \text{(by (11))} \\ &= \psi_a(L(\varphi(x, u)+\varphi(y, u)), 0) && \text{(by (1))} \\ &= \psi_a(L(\varphi(x, u))+L(\varphi(y, u)), 0) && \\ &= \psi_a(\varphi(X(x, u), 0)+\varphi(X(y, u), 0), 0) && \text{(by (11))} \\ &= f_a(X(x, u), X(y, u), 0)\,. \end{aligned}$$

§ 2. The main theorem.

Let F be a field of prime characteristic p and $\alpha: S \rightarrow F$ any function and we put $\beta(s)=\alpha(s)^{p^{1-m}}$ for $s \in S$. Let $F_1=F\,(\beta(s)\,;\, s \in S)$. Then F_1 is a purely inseparable extension of F. The commutative unipotent group defined by Seligman is $|R|$-dimensional affine space $A^{|R|}$ defined over F with composition law $\bar{f}$ and inverse map $\bar{g}$ such that $\bar{f}(x, y)=f(x, y, \beta)$ for $(x, y) \in A^{|R|} \times A^{|R|}$ and $\bar{g}(x)=g(x, \beta)$ for $(x) \in A^{|R|}$. We denote this algebraic group by U_R^α. It is defined over F.

THEOREM. *Let U_R^α be defined as above and $W^{(k,i)}$ the $(m-k+1)$-dimensional Witt groups for $1 \leqq i \leqq d_k$. Then U_R^α is isomorphic to direct sum of Witt groups $V=\prod_{k=1}^{m} \prod_{i=1}^{d_k} W^{(k,i)}$ over F_1.*

PROOF. As varieties $W^{(k,i)}$ are $(m-k+1)$-dimensional affine spaces. Its

j-th co-ordinates are indexed by $a_j = \binom{(k)}{ij}$. Let V be direct sum of Witt groups $W^{(k,i)}$ for $1 \leqq k \leqq m$, $1 \leqq i \leqq d_k$. Then $f(x, y, 0)$ and $g(x, 0)$ are the composition law and the inverse map of V, respectively. Let ρ be a rational map from U_R^α to V defined by $\rho(x) = X(x, \beta)$. It is defined over F_1 and is an isomorphism as algebraic varieties by Proposition 1 and homomorphism of groups by Proposition 2. Thus ρ is an isomorphism over F_1. This proves the theorem.

REMARK. In the definition of the set R of the symbols we have assumed that all d_k are positive. In [1] it is allowed that some d_k $(k \neq 1)$ are zero. This does not disturb the construction of U_R^α. In this case let R' be the set of symbols such that all d_k are positive and S' be the corresponding set of symbols as S corresponds to R. Then S' contains S. We extend the function $\alpha : S \to F$ to $\alpha' : S' \to F$ by putting $\alpha'(s) = 0$ for $s \in S' - S$. Then U_R^α can be imbedded naturally in $U_{R'}^{\alpha'}$ and is a direct summand in $U_{R'}^{\alpha'}$ over F. $U_{R'}^{\alpha'}$ is direct sum of U_R^α and $\prod_{k'} \prod_{i=1}^{d_{k'}} W^{(k',i)}$ where k' are those such that $d_{k'} = 0$ in R. The isomorphism of Theorem maps $\prod_{k'} \prod_{i=1}^{d_{k'}} W^{(k,i)}$ onto $\prod_{k'} \prod_{i=1}^{d_{k'}} W^{(k,i)}$. Thus U_R^α is also isomorphic to direct sum of Witt groups over F_1.

Department of Mathematics,
Tokyo Institute of Technology

References

[1] G. B. Seligman, On some commutative unipotent groups, Invent. Math., 5 (1968), 129–137.

[2] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n, J. Reine Angew. Math., 176 (1937), 126–140.