ON PURELY-TRANSCENDENCY OF A CERTAIN FIELD

HIDEO KUNIYOSHI

(Received June 20, 1954)

Let k be a field of characteristic $p > 0$, and $K = k(s_1, \cdots, s_{p^n})$ a purely transcendental extension field over k. We denote by σ the automorphism of K induced by a cyclic permutation $\sigma: s_i \to s_{i-1}$ (i mod. p^n). The object of this note lies in proving the fact that *the fixed field L of σ is also a purely transcendental extension field over k*[1].

We prove it by construc ing a system of generators of L/k which are algebraically independent over k. In the construction we take several systems of generators of K/k and obtain, finally, a system $(V_0, \ldots, V_{n-1}, v_1, \ldots, v_{p^n-n})$ which is transformed by σ in the following manner:

$$\begin{aligned} \sigma V_j &= V_j + f_j(V_0, \ldots, V_{j-1}), \qquad & j &= 0, \ldots, n-1, \\ \sigma v_i &= v_i, & i &= 1, \ldots, p^n - n, \end{aligned} \tag{1}$$

where $f_j(x_0, \ldots, x_{j-1})$ means a polynomial which arises in the j-th principal component by the computation of Witt's vectors (E. Witt [3])

$$\begin{aligned} &(x_0, \ldots, x_{n-1}) + \mathbf{1} \\ &= (x_0 + f_0, x_1 + f_1(x_0), \ldots, x_{n-1} + f_{n-1}(x_0, \ldots, x_{n-2})). \end{aligned} \tag{2}$$

When we have proved the existence of such generators (1), the seeking generators for L/k are constructed as follows: Since

$$\sigma(V_0, \ldots, V_{n-1}) = (V_0, \ldots, V_{n-1}) + \mathbf{1},$$

the component F_i of the right side of a relation

$$(V_0, \ldots, V_{n-1})^p - (V_0, \ldots, V_{n-1}) = (F_0, F_1, \ldots, F_{n-1})$$

belongs to L. Hence,

$$L' = k(F_0, \ldots, F_{n-1}, v_1, \ldots, v_{p^n-n}) \subset L,$$
$$(K : L') \geqq (K : L).$$

$V_0, \ldots, V_{n-1}$ are algebraic over L' and $L'(V_0, \ldots, V_{n-1}) = K$ is a cyclic extension field over L' of degree at most p^n (E. Witt [3]),

$$(K : L') \leqq p^n = (K : L).$$

Therefore, $L = L' = k(F_0, \ldots, F_{n-1}, v_1, \ldots, v_{p^n-n})$. As L is a field with degree of transcendency p^n over k, the p^n generators

$$F_0, \ldots, F_{n-1}, v_1, \ldots, v_{p^n-n}$$

are algebraically independent over k. Furthermore, in the following construction we may take a system of polynomials in $s_1, \ldots, s_{p^n}$ as the seeking generators of L/k.

1) The original problem which we have heard of from Prof. C. Chevalley, was the case for any field k of arbitrary characteristic and $K = k(x_1, \ldots\ldots, x_p)$ with $p = 5$, and was already established in [1] and [2]. It is not yet solved for p which is not equal to the characteristic of k.

Thus the problem is reduced to the proof of the existence of generators with (1). In order to construct them, we take, at first, a new system of generators[2)] $(t_1, \ldots t_{p^n})$ of K/k which are transformed by σ as follows:

$$\sigma t_i = \begin{cases} t_i, & i = 1, \\ t_i + t_{i-1}, & i = 2, \ldots, p^n. \end{cases} \tag{4}$$

CONSTRUCTION OF GENERATORS WITH (4). The elements

$$t_i = \sum_{\mu=0}^{p^n-1} \binom{i+\mu-1}{i-1} s_{i+\mu} \quad \left(\begin{matrix}\text{the index of } s_{i+\mu} \text{ is to be} \\ \text{considered modulo } p^n\end{matrix}\right) \tag{5}$$

$$i = 1, \ldots, p^n,$$

satisfy (4). In fact,

$$\begin{aligned}
\sigma t_1 &= t_1 \\
\sigma t_i - t_i &= \sum_{\mu=0}^{p^n-1} \binom{i-1+\mu}{i-1} s_{i+\mu-1} - \sum_{\mu=0}^{p^n-1} \binom{i-1+\mu}{i-1} s_{i+\mu} \\
&= \left[\binom{i-1}{i-1} - \binom{i-1+p^n-1}{i-1}\right] s_{i-1} \\
&\quad + \sum_{\mu=1}^{p^n-1} \left[\binom{i-1+\mu}{i-1} - \binom{i-1+\mu-1}{i-1}\right] s_{i+\mu-1} \\
&= \binom{i-2}{i-2} s_{i-1} + \sum_{\mu=1}^{p^n-1} \binom{i-2+\mu}{i-2} s_{i-1+\mu} \\
&= t_{i-1}, \qquad\qquad i \geqq 2.
\end{aligned}$$

As the determinant of right side of (5) is 1, s_i are also linear forms in t_i. Therefore $k(s_1, \ldots, s_{pn}) = k(t_1, \ldots, t_{pn})$, so that t_i are seeking generators (4).

From these t_i, we now construct a new set of generators (u_i) on which the automorphism σ operates as follows:

$$\sigma u_i = \begin{cases} u_i, & i \neq p^j + 1, \\ u_i + 1, & i = p^0 + 1 = 2, \\ u_i + (u_{p^0+1} u_{p+1} \cdots u_{p^{j-1}+1})^{p-1}, & i = p^j + 1 \\ & (1 \leqq j < n). \end{cases} \tag{6}$$

In the following, for convenience' sake, we distinguish two kinds of letters capital letter U_j means u_i with $i = p^j + 1$, and small letter u_i means always u_i with index $i \neq p^j + 1, 0 \leqq j < n$ (which is invariant uuder σ):

$$\begin{aligned}
&\left.\begin{array}{ll} u_i & i = 1, \ldots, p^n,\ i \neq p^j + 1,\ 0 \leqq j < n \\ U_j = u_{p^j+1}, & j = 0, \ldots, n-1 \end{array}\right\} p^n \text{ in number,} \\
&\sigma u_i = u_i, \\
&\sigma U_j = \begin{cases} U_j + 1, & j = 0, \\ U_j + (U_1 \cdots U_{j-1})^{p-1}, & j \neq 0. \end{cases}
\end{aligned} \tag{6'}$$

CONSTRUCTION OF GENERATORS WITH (6'). Putting U_j into its own place

2) The existence of such generators are informed by Prof. T. Tannaka and Mr. S. Takahashi, independently. Mr. S. Takahashi has proved it employing the Jordan's normal form of linear transformation without giving the concrete form of t_i.

in the series $\{u_i\}$ with $i = p^j + 1$, and arranging u_i in the order $i = 1, 2, 3$, ... we shall construct them by induction on i. By the construction we do more precisely

(7) $$\left.\begin{matrix} u_i \\ U_{j+1} \end{matrix}\right\} = a_i t_i + B_i(U_0, \dots, U_j), \qquad p^j + 1 < i \leqq p^{j+1} + 1$$

where $a_i \in k(u_1, \dots, u_{i-1})$[3] $\subset L$,

(8) B_i is a polynomial in $U_0, \dots, U_j$ over $k(u_1, \dots, u_{i-1})$[3] $\subset L$ of grade $i-1$,[4]

and

(9) for $i \neq p^j + 1$ the coefficient of the term $U_0^{\alpha_0} \dots U_j^{\alpha_j}$ $(0 \leqq \alpha_k < p)$ of grade $i-1$ is not zero.

Firstly we put

$$u_1 = t_1,\ U_0 = \frac{1}{u_1} t_2,$$

and assume that we have already succeeded to construct the generators up to u_i, U_{j+1} with, $p^j + 1 \leqq i \leqq p^{j+1}$. We shall prove a lemma concerning the terms in B_i.

LEMMA *For any term $U_0^{\alpha_0} \dots U_j^{\alpha_j}$ of grade $G \leqq i-1$, not equal to $(U_0 \dots U_j)^{p-1}$, there exists a polynomial $P(U_0, \dots, U_j)$ of grade $\leqq G+1$ with coefficients in the prime field such that*

(10) $$U_0^{\alpha_0} \dots U_j^{\alpha_j} = (\sigma - 1) P(U_0, \dots, U_j).$$

Furthermore the term $U_0^{\bar\beta_0} \dots U_j^{\bar\beta_j}$ $(0 \leqq \bar\beta_k < p, \sum \bar\beta_k p^k = G+1)$ appears in the polynomial $P(U_0, \dots, U_j)$ with a non zero coefficient, when $U_0^{\alpha_0} \dots U_j^{\alpha_j} = U_0^{\bar\alpha_0} \dots U_j^{\bar\alpha_j}$ $(0 \leqq \bar\alpha_k < p)$.

PROOF. Induction in the grade. Since $1 = (\sigma - 1) U_0$, we assume that the lemma is true for terms of grade less than m. Then we define an ordering among terms of grade m:

(0) $$U_0^{\alpha_0} \dots U_j^{\alpha_j} < U_0^{\beta_0} \dots U_j^{\beta_j} \text{ if } \alpha_j = \beta_j, \dots, \alpha_{k+1} = \beta_{k+1}, \alpha_k < \beta_k.$$

Next, we use induction in this ordering. The first step of induction is devided in two cases. The first term in the ordering is U_0^m.

1. When $m \not\equiv -1 \bmod. p$,

$$\sigma U_0^{m+1} = U_0^{m+1} + \binom{m+1}{1} U_0^m + \binom{m+1}{2} U_0^{m-1} + \dots.$$

Hence, collecting terms after the third in a polynomial C,

$$U_0^m = (\sigma - 1) \frac{1}{m+1} U_0^{m+1} + C$$

3) Strictly speaking, this means $k(\dots, u_k, \dots)$, $k \leqq i-1$, $k \neq p^l + 1$, $l < j + 1$. By distinguishing the capital letters U_j and the small letters u_k, these restrictions $k \neq p^l + 1$ can be carried out automatically.

4) We define the grade of $V_0^{\alpha_0} \dots V_j^{\alpha_j}$ by the number $\alpha_0 + \alpha_1 p + \dots + \alpha_j p^j$ and the grade of a polynomial by the highest grade of its terms.

where C is a polynomial in U_0 of grades less than $m-1$. By the assumption of induction for m, $C=(\sigma-1)C'$, C' is a polynomial of grade less than m. Therefore

$$U_0^m=(\sigma-1)\left[\frac{1}{m+1}U_0^{m+1}+C'\right]. \tag{11}$$

The polynomial in the right side is of grade at most $m+1$.

2. When $m\equiv -1 \bmod. p$, we put $m=pq-1$. Then,

$$\begin{aligned}\sigma[U_0^{p(q-1)}U_1]^{5)} &= (U_0^p+1)^{q-1}(U_1+U_0^{p-1})\\ &= U_0^{p(q-1)}U_1+\binom{q-1}{1}U_0^{p(q-2)}U_1+\cdots\\ &\quad + U_0^{pq-1}+\binom{q-1}{1}U_0^{p(q-1)-1}+\cdots\cdots\end{aligned}$$

From the same reason as in the case 1,

$$U_0^m=(\sigma-1)[U_0^{p(q-1)}U_1+D'] \tag{12}$$

where the polynomial in the right side is of grade at most $m+1$.

Now, we assume that the lemma is already proved to be true for terms of grade m which are placed before $U_0^{\alpha_0}\cdots U_j^{\alpha_j}$ in the ordering (0), and prove the lemma for $U_0^{\alpha_0}\cdots U_j^{\alpha_j}$.

When $\alpha_0\equiv\cdots\equiv\alpha_j\equiv -1 \bmod. p$, we have $\alpha_0=\cdots=\alpha_j=p-1$, because $\sum\alpha_k p^k=i-1\leqq p^{j+1}-1$. This term arises only when $i=p^{j+1}$, and it is the exceptional term of the lemma. We may put accordingly

$$\begin{aligned}&\alpha_0\equiv\cdots\equiv\alpha_{k-1}\equiv -1\\ &\qquad\qquad \alpha_k\not\equiv -1 \bmod. p, && 0\leqq k\leqq j,\\ &\alpha_l=p(q_l+1)-1, && 0\leqq l\leqq k-1.\end{aligned}$$

Then,

$$\begin{aligned}&\sigma[U_0^{pq_0}\cdots U_{k-1}^{pq_{k-1}}U_k^{\alpha_k+1}U_{k+1}^{\alpha_{k+1}}\cdots U_j^{\alpha_j}]\\ &=(U_0^p+1)^{q_0}(U_1^p+U_0^{p(p-1)})^{q_1}\cdots(U_{k-1}^p+(U_0\cdots U_{k-2})^{p(p-1)})^{q_{k-1}}\\ &\times(U_k+(U_0\cdots U_{k-1})^{p-1})^{\alpha_k+1}\\ &\times(U_{k+1}+(U_0\cdots U_k)^{p-1})^{\alpha_{k+1}}\cdots(U_j+(U_0\cdots U_{j-1})^{p-1})^{\alpha_j}\\ &=U_0^{pq_0}\cdots U_{k-1}^{pq_{k-1}}U_k^{\alpha_k+1}U_{k+1}^{\alpha_{k+1}}\cdots U_j^{\alpha_j}+(\alpha_k+1)U_0^{\alpha_0}\cdots U_j^{\alpha_j}+E,\end{aligned} \tag{13}$$

where E means the sum of remainder terms and they are of grade at most m and placed before $(\alpha_0,\ldots,\alpha_j)$ if grade are m. Therefore, from the assumption

$$U_0^{\alpha_0}\cdots U_j^{\alpha_j}=(\sigma-1)\left[\frac{1}{\alpha_k+1}U_0^{pq_0}\cdots U_{k-1}^{pq_{k-1}}U_k^{\alpha_k+1}U_{k+1}^{\alpha_{k+1}}\cdots U_j^{\alpha_j}+E'\right]. \tag{14}$$

In the right side, the polynomial is of grade at most $m+1$.

In the above deformation of $U_0^{\alpha_0}\cdots U_j^{\alpha_j}$ into the form (10), if any one of exponents in $U_0^{\alpha_0}\cdots U_j^{\alpha_j}$ is greater than p, each term of grade $m+1$ in

5) Since $i-1\geqq m=pq-1, q\geqq 1$, we see $i\geqq p$. When $i=p$, then $m=p-1$, and it is the exceptional case of the lemma. When $i>p$, the $(p+1)$-th term U_1 was already constructed.

the polynomial P in (10) contains an exponent greater than p. In fact, it is obvious for U_0^m by (11), (12). As, in the right side of (13), each term of grade m in E contains an exponent greater than p, the assertion is proved by induction in the ordering (0).

When we deform $U_0^{\overline{\alpha}_0}\cdots U_j^{\overline{\alpha}_j}$, $0 \leqq \overline{\alpha}_k < p$, into a form (14), each term of grade $m+1$ in E' contains an exponent greater than p, because each term of grade m in E in (13) also contains such exponents. Therefore, in the relation (14), any term in E' cannot cancel with the first one.

Thus we proved the lemma.

Now, we continue the construction of (6′).
From (4) and (7)

$$(15)\qquad (\sigma-1)t_{i+1} = \begin{cases} \dfrac{1}{a_i}u_i - \dfrac{1}{a_i}B_i(U_0, \ldots, U_j), & i \neq p^j+1, \\ \dfrac{1}{a_i}U_j - \dfrac{1}{a_i}B_i(U_0, \ldots, U_{j-1}), & i = p^j+1. \end{cases}$$

In both cases the right side is polynomial in $U_0, \ldots, U_j$ of grade $i-1$ over $k(u_1, \ldots, u_k, \ldots)$[4], $k \leqq i$, with non-zero coefficient for $U_0^{\overline{\alpha}_0}\cdots U_j^{\overline{\alpha}_j}, 0 \leqq \overline{\alpha}_k < p$, $\sum \alpha_k p^k = i-1$[6]. In particular, when $i = p^{j+1}$ the coefficient b_i of $(U_0\cdots U_j)^{p-1}$ is not zero. Since all coefficients are invariant under σ, applying the previous lemma, we may deform the right side of (15) into the form $(\sigma-1)B_{i+1}(U_0, \ldots, U_j)$, except for the term $(U_0\cdots U_j)^{p-1}$ for $i = p^{j+1}$, i.e.

$$(\sigma-1)t_{i+1} = \begin{cases} (\sigma-1)B_{i+1}(U_0, \ldots, U_j), & i \neq p^{j+1}, \\ b_i(U_0, \ldots, U_j)^{p-1} + (\sigma-1)B_{i+1}(U_0, \ldots, U_j), & \\ \qquad\qquad b_i \neq 0, & i = p^{j+1}. \end{cases}$$

B_{i+1} is a polynomial of grade i with non zero coefficient for $U_0^{\overline{\beta}_0}\cdots U_j^{\overline{\beta}_j}$, $0 \leqq \overline{\beta}_k < p$, $\sum \overline{\beta}_k p^k = i$. Then

$$\begin{aligned} u_{i+1} &= t_{i+1} - B_{i+1}(U_0, \ldots, U_j), && i \neq p^{j+1}, \\ U_{j+1} &= \frac{1}{b_i}t_{i+1} - \frac{1}{b_i}B_{i+1}(U_0, \ldots, U_j), && i = p^{j+1} \end{aligned}$$

satisfy the conditions (6′), (8) and (9). Thus we have completed the construction of all u_i, U_j. Obviously, they generate K over k, $k(u, U) = k(t)$.

To construct (1), we utilize some properties of Witt's vectors over K. Let $x_0, x_1, \ldots, y_0, y_1, \ldots$ be variables over K. The addition of two vectors $(x_0, x_1, \ldots)$ and $(y_0, y_1, \ldots)$ is defined by polynomials:

$$(16)\qquad \begin{aligned} &(x_0, x_1, \ldots) + (y_0, y_1 \ldots) \\ &= (x_0+y_0, x_1+y_1+g_1(x,y), \ldots) \end{aligned}$$

where $g_1(x, y)$ *is a polynomial of equi-grade* p^i *in* $x_0, \ldots, x_{i-1}, y_0, \ldots,$

---

6) When $i \neq p^j+1$, it is obvious by the condition (9). For $i = p^j+1$, the term is U with non zero coefficient $1/a_i$.

y_{i-1}[7]) *over prime field* k_0. *Furthermore, the coefficient of* $(x_0, \cdots, x_{i-1})^{p-1} y_0$ *in* $g_i(x,y)$ *is* $(-1)^i$.

PROOF. We shall deal with vectors over prime field R of characteristic 0 and use "sub-components" $x^{(i)}$

$$x^{(i)} = x_0^{p^i} + px_1^{p^{i-1}} + \cdots + p^i x_i. \tag{17}$$

The addition (16) over K is induced by addition over R defined by sub-components (17),

$$\begin{aligned}(x_0, x_1, \cdots) &+ (y_0, y_1, \cdots) \\ &= (x_0 + y_0, x_1 + y_1 + h_1(x,y), \cdots \mid x^{(0)} + y^{(0)}, x^{(1)} + y^{(1)}, \cdots),\end{aligned} \tag{18}$$

$h_i(x,y)$ is a polynomial with integral coefficients and reduces into $g_i(x,y)$ modulo p. It is sufficient to prove the assertion for these $h_i(x,y)$. (17) (18) show

$$\begin{aligned}&x^{(i+1)} + y^{(i+1)} \\ &= (x+y)_0^{p^{i+1}} + p(x+y)_1^{p^i} + \cdots + p^i(x+y)_i^p + p^{i+1}(x+y)_{i+1} \\ &= (x_0 + y_0)^{p^{i+1}} + p(x_1 + y_1 + h_1)^{p^i} + \cdots + p^i(x_i + y_i + h_i)^p \\ &\qquad + p^{i+1}(x_{i+1} + y_{i+1} + h_{i+1}),\end{aligned}$$

so that,

$$\begin{aligned}h_{i+1} = \frac{-1}{p^{i+1}}\Big[&(x_0 + y_0)^{p^{i+1}} - x_0^{p^{i+1}} - y_0^{p^{i+1}} \\ &+ p(x_1 + y_1 + h_i)^{p^i} - px_1^p - py_1^{p^i} \\ &\cdots\cdots\cdots\cdots \\ &+ p^i(x_i + y_i + h_i)^p - p^i x_i^{p^i} - p^i y_i^{p^i}\Big].\end{aligned} \tag{19}$$

It is obvious that h_{i+1} is equi-grade p^{i+1}, when all h_k are equi-grade p^k, $k \leq i$. Furthermore, as the term, which contains x_i exactly, arises only from $p^i(x_i + y_i + h_i)^p$, the coefficient of $(x_0 \cdots x_i)^{p-1} y_0$ in (19) is $-p^i\binom{p}{p-1}\Big/p^{i+1} = -1$ times multiple of that of $(x_0 \cdots x_{i-1})^{p-1} y_0$ in $h_i(x,y)$. Since the assertion is true for $h_1(x_0, y_0) = \dfrac{-1}{p}\sum_{\nu=1}^{p-1}\binom{p}{\nu} x_0^\nu y_0^{p-\nu}$, we may complete the proof by induction on i.

When we calculate about vectors of components in K, we may put them into (16). Therefore, we put $(y_0, y_1, \cdots) = (1, 0, \cdots) = \mathbf{1}$ into (16), then

$$\begin{aligned}&(x_0, x_1, \cdots) + \mathbf{1} \\ &= (x_0 + f_0, x_1 + f_1(x), \cdots)\end{aligned} \tag{20}$$

where $f_i(x)$ is a polynomial in $x_0, \cdots, x_{i-1}$ of grade $p^i - 1$ and contains the term $(x_0 \cdots x_{i-1})^{p-1}$ with coefficient $(-1)^i$.

CONSTRUCTION OF GENERATORS WITH (1). We take $p^n - n$ elements $u_1, \cdots$

7) This means that $g_i(x,y)$ is a polynomial with terms $x^{\alpha_0} \ldots\ldots x_{i-1}^{\alpha_{i-1}} y_0^{\beta_0} \ldots\ldots y_{i-1}^{\beta_{i-1}}$, $\sum_{k=0}^{i-1} \alpha_k p^k + \sum_{l=0}^{i-1} \beta_l p^l = p^i$.

$\cdots, u_{p^n}$ as $v_1, \cdots, v_{pn-n}$, with a suitable renewing of indices. As for V_j with

(1) $$\sigma V_j = V_j + f_j(V_0, \cdots, V_{j-1}), \qquad j = 0, \cdots, n-1,$$

we may define inductively as follows:

(21) $$\begin{aligned} &V_0 = U_0, \\ &V_j = \varepsilon_j U_j + H_j(U_0, \cdots, U_{j-1}), \qquad \varepsilon_j = \pm 1, \end{aligned}$$

when $H_j(U_0, \cdots, U_{j-1})$ is a polynomial over prime field k_0 of grade at most p^j. Assume that $V_k, k \leqq j$ are already defined, then

(22) $$\begin{aligned} (\sigma - 1)U_{j+1} &= (U_0 \cdots U_j)^{p-1} \\ &= \varepsilon_1 \cdots \varepsilon_j V_0^{p-1}(V_1 - H_1(U_0))^{p-1} \cdots (V_j - H_j(U_0, \cdots, U_{j-1}))^{p-1} \\ &= \varepsilon_1 \cdots \varepsilon_j[(V_0 V_1 \cdots V_j)^{p-1} + H'(U_0, \cdots, U_{j-1}, V_0, \cdots, V_j)]. \end{aligned}$$

Putting (21) into H', we deform it into a polynomial H'' in $U_0, \cdots, U_j$ of grade less than $p^{j+1} - 1$. As $(V_0 \cdots V_j)^{p-1}$ is not in H', the exceptional term $(U_0 \cdots U_j)^{p-1}$ of the previous lemma can not appear in H''. Indeed, a term in H' is

$$U_0^{\alpha_0} \cdots U_{k-1}^{\alpha_{k-1}} V_0^{\beta_0} \cdots V_j^{\beta_j}, \qquad \begin{aligned} &\beta_j = \cdots = \beta_{k+1} = p-1, \\ &\beta_k < p-1, \quad k = 0, \cdots, j. \end{aligned}$$

Putting (21) into it, it is reduced into

$$U_0^{\alpha_0} \cdots U_{k-1}^{\alpha_{k-1}} U_0^{\beta_0} (\varepsilon_1 U_1 + H_1 U_0))^{\beta_1} \cdots (\varepsilon_j V_j + H_j(U, \cdots U_{j-1}))^{\beta_j}$$

in which each term has an exponent less than $p - 1$ for one of $U_k, \cdots, U_j$. So that, $(U_0 \cdots U_j)^{p-1}$ does not exist in H''. Hence, applying the previous lemma we have

$$H'' = (\sigma - 1)H'''(U_0, \cdots, U_j)$$

where H''' is of grade at most p^{j+1}, and collecting it to the left side,

(23) $$(\sigma - 1)[U_{j+1} + H'''(U_0, \cdots, U_j)] = \varepsilon_1 \cdots \varepsilon_j(V_0, \cdots, V_j)^{p-1}.$$

On the other hand, in the polynomial

$$f_{j+1}(V_0, \cdots, V_j) = (-1)^{j+1}(V_0, \cdots, V_j)^{p-1} + J(V_0, \cdots, V_j),$$

there is no $(V_0, \cdots, V_j)^{p-1}$ in the remainder $J(V_0, \cdots, V_j)$. We put then (21) into J and reduce it into a form $(\sigma - 1)J''(U_0, \cdots, U_j)$, where J'' is of grade at most $p^{j+1} - 1$. It is really possible from the same reason as above. Transfering J to the left side

(24) $$(\sigma - 1)J''(U_0, \cdots, U_j) = f_{j+1}(V_0, \cdots, V_j) + (-1)^j(V_0, \cdots, V_j)^{p-1}.$$

From (23) and (24) it follows,

$$(\sigma - 1)[\varepsilon_1 \cdots \varepsilon_j V_{j+1} + \varepsilon_1 \cdots \varepsilon_j H''' + (-1)^{j+1}J''] = (-1)^{j+1} f_{j+1}(V_0, \cdots, V_j).$$

So that we may define

$$V_{j+1} = \varepsilon_1 \cdots \varepsilon_j(-1)^{j+1}U_{j+1} + \varepsilon_1 \cdots \varepsilon_j(-1)^{j+1}H''' + J''$$

where H''', J''' are of grade at most p^{j+1}.

Thus we completed the construction of (21). Obviously $k(V_0, \cdots V_{n-1}) = k(U_0, \cdots, U_{n-1})$, and v_i, V_j are generators of K/k.

In the above construction, (4) are linear forms in s, (6′) are rational functions in (4), (1) are polynomials in (6′), and the seeking generators of L/k are polynomials in (1). If we insert a new set of generators (4′) of K/k

$$(4') \qquad t'_i = \begin{cases} t_i, & i = 1, \\ t_i/t_1, & i = 2, \cdots, p^n, \end{cases}$$

between (4) and (6′), then (6′) may be defined from (4′) by

$$(7') \qquad \left.\begin{matrix} u_i \\ U_j \end{matrix}\right\} = a'_i t'_i + B'_1(U_0, \cdots, U_{j-1})$$

where a'_i lies in prime field k_0, and B'_i is a polynomial over $k_0(u_1, \cdots, u_{i-1})$. The final generators of L/k are, then, rational functions in s_i in which denominators are powers of $\sum_i s_i = v_1$. Therefore, multiplying a suitable powers of v_1, to $v_2, \cdots, v_{p^n-n}, F_0, \cdots : F_j$, we may take polynomials of $s_1, \cdots, s_p$, as seeking generators for L/k.

REFERENCES

[1] H. KUNIYOSHI, On a problem of Chevalley, Nagoya Journ.
[2] K. MASUDA, On a problem of Chevalley, Nagoya Journ.
[3] E. WITT, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charkteristik p. Journ. für Math., 176(1936), 126-140.

MATHEMATICAL INSTITUTE, TÔHOKU UNIVERSITY, SENDAI.