m-applications over finite fields

by

A. Prószyński (Toruń)

Abstract. The main results proved in this paper are the following:

(1) Theorem 1.4 shows that any m-application over a finite field is a polynomial mapping.

(2) Theorem 2.4 gives a basis of m-applications over a finite field.

(3) Theorems 2.7 and 4.1 show when any m-application over an algebraic extension of a finite field is obtained from a form of degree m in the polynomial ring.

(4) Theorem 4.4 shows that any 3-application over a field is obtained from a form of degree 3.

0. Preliminaries. Let K be a field and let $m>0$ be a natural number. A mapping $f\colon X\to Y$, where X, Y are K-modules, is called an *m-application* (see [1]) iff the following conditions are satisfied:

(A1) $f(rx) = r^m f(x)$ for any $r\in K$, $x\in X$.

(A2) $\Delta^m f\colon X\times\ldots\times X\to Y$ is m-linear, where

$$(\Delta^m f)(x_1,\ldots,x_m) = \sum_{H\subset[1,m]} (-1)^{m-\operatorname{card}(H)} f\Big(\sum_{i\in H} x_i\Big).$$

m-applications from X to Y form a K-module denoted by $\operatorname{Appl}^m_K(X, Y)$, and in a natural way we get the functor Appl^m_K. $\operatorname{Appl}^m_K(X, -)$ is represented by $\Gamma_m(X)$ (see [1]) and it is easy to prove that Γ_m commutes with direct limits. Therefore the investigation of Appl^m_K can be reduced to the study of $\operatorname{Appl}^m_K(K^n, K)$.

We have the following K-homomorphism (see [1], [2]):

$$\nu^m\colon K[T_1,\ldots,T_n]_m \to \operatorname{Appl}^m_K(K^n, K), \qquad \nu^m(F) = \bar{F},$$

where $\bar{F}(x_1,\ldots,x_n) = F(x_1,\ldots,x_n)$. Denote $\operatorname{Im}(\nu^m) = \operatorname{Hom}^m_K(K^n, K)$. The following question arises: when $\operatorname{Hom}^m_K(K^n, K) = \operatorname{Appl}^m_K(K^n, K)$? It is known from [1] that the answer is positive if $m\leqslant 2$ or $n = 1$ or $m!\neq 0$ in K. The aim of this paper is to give some more detailed information concerned with that problem.

It will be assumed in the next three sections that:

1) K is a fixed finite field, $\operatorname{char}(K) = p$, $\operatorname{card}(K) = q = p^s$.

2) $m>0$ is the degree and $n>0$ is the dimension.

3) $a\equiv b$ means $a\equiv b \pmod{q-1}$.

4) If $I = (i_1,\ldots,i_n)\in N^n$ (N contains 0) then $|I| = i_1+\ldots+i_n$ and $I<a$ ($I>a$) means that $i_1,\ldots,i_n<a$ ($i_1,\ldots,i_n>a$).

1. Polynomial mappings. The K-module $P(K^n, K)$ of all polynomial mappings from K^n to K is generated by elements $\exp(I)$, $I \in N^n$, defined in the following way:

$$\exp(I)(x_1, \ldots, x_n) = x_1^{i_1} \ldots x_n^{i_n} \quad \text{for} \quad I = (i_1, \ldots, i_n).$$

LEMMA 1.1. *The elements* $\exp(I)$, $I \in N^n$, $I<q$, *form a basis of* $P(K^n, K)$.

Proof. For any $J = (j_1, \ldots, j_n)$ define $\operatorname{red}(J) = (i_1, \ldots, i_n) < q$ as follows:

$$i_k \equiv j_k,\ 1 \leqslant i_k \leqslant q-1, \text{ if } j_k > 0 \quad \text{and} \quad i_k = 0 \text{ for } j_k = 0.$$

Since $\exp(i) = \exp(j)$ for $i \equiv j$, $i, j > 0$, it follows that $\exp(J) = \exp(\operatorname{red}(J))$. The linear independence of the above elements can easily be proved by induction on n.

LEMMA 1.2. (1) *The elements* $\exp(I)$, $I \in N^n$, $I<q$, $0<|I| \leqslant m$, $|I| \equiv m$, *form a basis of* $\operatorname{Hom}_K^m(K^n, K)$.

(2) $\dim_K \operatorname{Hom}_K^m(K^n, K) = \operatorname{card}(B_n)$ *where*

$$B_n = \{H \in N^k \mid H<q, |H|<m, 0 \leqslant k \leqslant n-1\}.$$

Proof. (1) If $J \in N^n$ and $|J| = m > 0$, then $I = \operatorname{red}(J)$ satisfies the above conditions. Using the converse procedure, we infer that all the above elements belong to $\operatorname{Hom}_K^m(K^n, K)$.

(2) Induction on n. The case $n = 1$ is evident. Let $n>1$. Then

$$B_n = B_{n-1} \cup \{H \in N^{n-1} \mid H<q, |H|<m\}.$$

There is a one-to-one correspondence between B_{n-1} and the set of the base elements $\exp(I)$ with $I = (I', 0)$. For $I = (I', i)$ with $i>0$ the mapping $I \mapsto I'$ gives us a one-to-one correspondence between the rest of the base elements $\exp(I)$ and the second part of B_n. In fact, the last integer i is uniquely determined by the conditions $1 \leqslant i \leqslant q-1$ and $i \equiv m-|I'|$. (Another proof of (2) is given in [2], Corollary 8.5).

Let us consider the K-module $\overline{\operatorname{Appl}}_K^m(K^n, K)$ of all mappings $f\colon K^n \to K$ satisfying the condition (A1). We want to prove that all such mappings are polynomial mappings and to find a basis of $\overline{\operatorname{Appl}}_K^m(K^n, K)$. The first step is the following:

PROPOSITION 1.3. *If* $m-1 \geqslant (n-1)(q-1)$ *then* $\operatorname{Hom}_K^m(K^n, K) = \operatorname{Appl}_K^m(K^n, K) = \overline{\operatorname{Appl}}_K^m(K^n, K)$.

Proof. Since $m-1 \geqslant (n-1)(q-1)$, it follows that $B_n = \{B \in N^k \mid B<q, 0 \leqslant k \leqslant n-1\}$ and hence

$$\dim_K \operatorname{Hom}_K^m(K^n, K) = 1+q+\ldots+q^{n-1} = \frac{q^n-1}{q-1} = t.$$

On the other hand, the projective space $\boldsymbol{P}^{n-1}(K)$ has t elements. This means that there exist elements $x_1, \ldots, x_t \in K^n - \{0\}$ such that any $x \in K^n$ is a multiple of some x_i. Therefore any $f \in \overline{\operatorname{Appl}}_K^m(K^n, K)$ is uniquely determined by $f(x_1), \ldots, f(x_t)$, and

hence $\dim \overline{\operatorname{Appl}}_K^m(K^n, K) \leqslant t$. (Compare also [1], Section 7.) This completes the proof.

THEOREM 1.4. $\overline{\operatorname{Appl}}_K^m(K^n, K)$ *is contained in* $P(K^n, K)$ *and has the following basis:* $\exp(I)$, $I \in N^n$, $I<q$, $0<|I| \equiv m$.

Proof. Let $m+k-1 \geqslant n(q-1)$ for a suitable natural number k. Any $f \in \overline{\operatorname{Appl}}_K^m(K^n, K)$ gives us the mapping $g\colon K^{n+1} \to K$ defined as follows:

$$g(x_1, \ldots, x_{n+1}) = f(x_1, \ldots, x_n) x_{n+1}^k.$$

Observe that $g \in \overline{\operatorname{Appl}}_K^{m+k}(K^{n+1}, K) = \operatorname{Hom}_K^{m+k}(K^{m+1}, K) \subset P(K^{n+1}, K)$ by Proposition 1.3. Putting $x_{n+1} = 1$, we obtain $f \in P(K^n, K)$. Let $f = \sum_i \overline{F}_i$ where $F_i \in K[T_1, \ldots, T_n]_i$. Condition (A1) for f means that

$$r^m f(x) = \sum_i r^i \overline{F}_i(x)$$

for any $r \in K$ and any fixed $x \in K^n$. Observe that $F = \Sigma a_i T^i \in K[T]$ vanishes as a polynomial mapping iff $T^q - T | F$ iff $a_0 = 0$ and $\sum_{i \equiv k} a_i = 0$ for any k. Hence it follows that $f = \sum_{0<i \equiv m} \overline{F}_i$.

Lemma 1.2 gives us now the basis of $\overline{\operatorname{Appl}}_K^m(K^n, K)$.

2. m-applications over finite fields. To study condition (A2) we must compute $\Delta^m \exp(I)$. Let $I = (i_1, \ldots, i_n)$. Consider $m \times n$-matrices $A = (a_{ij})$ with rows $A_1, \ldots, A_m$ (we write $(A = A_1, \ldots, A_m)$) satisfying the following conditions: $|A_1|, \ldots, |A_m| > 0$, $A_1 + \ldots + A_m = I$.

The set of those matrices will be denoted by $M(m, I)$.

LEMMA 2.1. *Let* $I = (i_1, \ldots, i_n)$ *and* $|I|>0$. *Then*

$$(\Delta^m \exp(I))(x_{11}, \ldots, x_{1n}; \ldots; x_{m1}, \ldots, x_{mn}) = \sum_{A \in M(m,I)} ((a_{11}, \ldots, a_{m1})) \ldots ((a_{1n}, \ldots, a_{mn})) x_{11}^{a_{11}} \ldots x_{mn}^{a_{mn}}.$$

In other words:

$$\Delta^m \exp(I) = \sum_{A \in M(m,I)} ((a_{11}, \ldots, a_{m1})) \ldots ((a_{1n}, \ldots, a_{mn})) \exp(A).$$

Proof. Induction on m. The case $m = 1$ is evident since $\Delta^1 f = f$. Let $m>1$. Observe that

$$(\Delta^m f)(x_1, \ldots, x_m) = (\Delta^{m-1} f)(x_1, \ldots, x_{m-2}, x_{m-1}+x_m) - (\Delta^{m-1} f)(x_1, \ldots, x_{m-1}) - (\Delta^{m-1} f)(x_1, \ldots, x_{m-2}, x_m).$$

Hence by the inductive assumption and the binomial formula we get:

$$\Delta^m \exp(I) = \sum_{B \in M(m-1,I)} ((b_{11}, \dots, b_{m-1,1})) \dots ((b_{1n}, \dots, b_{m-1,n})) \times$$
$$\times \sum_{\substack{J+K=B_{m-1} \\ |J|,|K|>0}} ((j_1, k_1)) \dots ((j_n, k_n)) \exp(B_1, \dots, B_{m-2}, J, K)$$
$$= \sum_{A \in M(m,I)} ((a_{11}, \dots, a_{m1})) \dots ((a_{1n}, \dots, a_{mn})) \exp(A) .$$

Now we answer the question when $\Delta^m \exp(I) = 0$. We need the following

LEMMA 2.2. *Let* $a = a_1 + \dots + a_m$, $a = \sum_{k=0}^{t} a^{(k)} p^k$, $a_j = \sum_{k=0}^{t} a_j^{(k)} p^k$, $j = 1, \dots, m$, *where* $0 \leqslant a^{(k)}, a_j^{(k)} < p$. *Then*

$$((a_1, \dots, a_m)) \neq 0 \text{ in } Z_p \quad \text{iff} \quad \sum_{j=1}^{m} a_j^{(k)} = a^{(k)} \text{ for any } k = 0, 1, \dots, t .$$

Proof. Induction on m reduces the lemma to the case $m = 2$. The following computation in $Z_p[T]$:

$$(T+1)^a = (T+1)^{a^{(0)}} \dots (T^{p^t}+1)^{a^{(t)}} = \sum_{b_0=0}^{a^{(0)}} \dots \sum_{b_t=0}^{a^{(t)}} \binom{a^{(0)}}{b_0} \dots \binom{a^{(t)}}{b_t} T^b$$

where $b = b_0 + \dots + b_t p^t$, shows that

$$\binom{a}{b} = \binom{a^{(0)}}{b_0} \dots \binom{a^{(t)}}{b_t} \neq 0 \quad \text{iff} \quad b_k \leqslant a^{(k)} \text{ for any } k.$$

This completes the proof.

Let $I = (i_1, \dots, i_n)$ and $i_l = \sum_k i_l^{(k)} p^k$ where $0 \leqslant i_l^{(k)} < p$. Then we put $\Sigma_p(I) = \sum_{k,l} i_l^{(k)}$.

COROLLARY 2.3. *Let* $|I| > 0$ *and* $I < q$. *Then* $\Delta^m \exp(I) = 0$ *iff* $\Sigma_p(I) < m$.

Proof. Since $I < q$, it follows that $A < q$ for any $A \in M(m, I)$, and hence the presentation in Lemma 2.1 is unique. Therefore $\Delta^m \exp(I) = 0$ iff all coefficients are zero. This means that any $m \times n$-matrix A satisfying the conditions

$$A_1 + \dots + A_m = I, \quad ((a_{11}, \dots, a_{m1})) \dots ((a_{1n}, \dots, a_{mn})) \neq 0 ,$$

must have a zero row. By Lemma 2.2 this is equivalent to the following implication:

$$\forall_{k,l} \sum_{j=1}^{m} a_{jl}^{(k)} = i_l^{(k)} \Rightarrow \exists_j \forall_{k,l} a_{jl}^{(k)} = 0 .$$

The above is true if $\Sigma_p(I) < m$ since $1 \leqslant j \leqslant m$ and there are at most $m-1$ non-zero $a_{jl}^{(k)}$. Conversely, let $\Sigma_p(I) \geqslant m$. If $i_l^{(k)} \geqslant m$ for some k, l; then $i_l^{(k)}$ is a sum of m positive integers, and hence there exists such an A that $a_{jl}^{(k)} > 0$ for any j. If $i_l^{(k)} < m$ for any k, l,

then we can put $a_{jl}^{(k)} = 0$ or 1 in such a way that for any j some $a_{jl}^{(k)}$ is 1. This completes the proof.

The above corollary allows us to find the basis of $\mathrm{Appl}_K^m(K^n, K)$ and then answer our fundamental question for finite fields.

THEOREM 2.4. $\mathrm{Appl}_K^m(K^n, K)$ *has a basis composed from elements of the following two types*:

(H) $\exp(I)$, $I \in N^n$, $I < q$, $0 < |I| \leqslant m$, $|I| \equiv m$ (*the basis of* $\mathrm{Hom}_K^m(K^n, K)$),

(P) $\exp(I)$, $I \in N^n$, $I < q$, $m < |I| \equiv m$, $\Sigma_p(I) < m$.

Proof. It follows from Lemma 1.2, Theorem 1.4 and Corollary 2.3 that the above elements belong to $\mathrm{Appl}_K^m(K^n, K)$ and are linearly independent. Let $f \in \mathrm{Appl}_K^m(K^n, K)$. Then

$$f = \sum_{\substack{q > I \in N^n \\ 0 < |I| \equiv m}} a_I \exp(I), \quad a_I \in K ,$$

by Theorem 1.4. By Lemma 1.2 we can assume that $|I| > m$. It remains to prove that $\Delta^m \exp(I) = 0$ if a_I is non-zero (cf. Corollary 2.3). By the above formula and Lemma 2.1 we get:

$$\Delta^m f = \sum_{\substack{q > I \in N^n \\ m < |I| \equiv m}} a_I \Delta^m \exp(I) = \sum_{\substack{q > I \in N^n \\ m < |I| \equiv m}} \sum_{A \in M(m,I)} a_I c_A \exp(A) .$$

Consider this equality as an equality of polynomial mappings in mn variables $x_{11}, \dots, x_{mn}$. Observe that the matrices A are all different (since $A_1 + \dots + A_m = I$) and $\exp(A)$ are linearly independent by Lemma 1.1 (since $A < q$). Moreover, $|A| > m$. On the other hand, $\Delta^m f$ is m-linear, and hence in the variables x_{kl}, $\Delta^m f \in \mathrm{Hom}_K^m(K^{mn}, K)$. Comparing the coefficients in the above equality, we conclude that $a_I c_A = 0$ for all $A \in M(m, I)$. Hence $\Delta^m \exp(I) = 0$ for $a_I \neq 0$ as we want.

COROLLARY 2.5. $\mathrm{Hom}_K^m(K^n, K) \neq \mathrm{Appl}_K^m(K^n, K)$ *iff there exists an* $I \in N^n$ *such that*

$$I < q, \quad \Sigma_p(I) < m \quad \text{and} \quad |I| = m + a(q-1) \text{ where } a > 0 .$$

For any such I *we have* (i) $q > p$ *and* (ii) $m > ap + 1$.

Proof. The first part is evident. Suppose that $q = p$. Then $I < p$ and hence $m < |I| = \Sigma_p(I) < m$, a contradiction. Suppose that $ap - m + 1 \geqslant 0$. Then:

$$m + a(p^s - 1) = |I| \leqslant \Sigma_p(I) p^{s-1} \leqslant (m-1)p^{s-1}, \quad ap - m + 1 \leqslant (ap - m + 1)p^{s-1} \leqslant a - m .$$

Hence $a(p-1) + 1 \leqslant 0$, a contradiction.

COROLLARY 2.6. $\mathrm{Hom}_K^m \neq \mathrm{Appl}_K^m$ *iff there exist* $n_0, \dots, n_{s-1} \in N$ *such that*:

1° $n_0 + n_1 p + \dots + n_{s-1} p^{s-1} = m + a(q-1)$, $a > 0$,

2° $n_0 + \dots + n_{s-1} < m$.

Proof. For any I satisfying the conditions of Corollary 2.5 define n_k ($k = 0, \dots, s-1$) as a partial sum of $\Sigma_p(I)$, n_k = the sum of coefficients at p^k. Conversely, for given $n_0, \dots, n_{s-1}$ define

$$I = (\underbrace{1, \dots, 1}_{n_0}, \underbrace{p, \dots, p}_{n_1}, \dots, \underbrace{p^{s-1}, \dots, p^{s-1}}_{n_{s-1}}).$$

Then I satisfies the conditions of Corollary 2.5 for $n = n_0+\dots+n_{s-1}$.

THEOREM 2.7. *If K is a finite field, then the following conditions are equivalent:*

(1) $\mathrm{Hom}_K^m = \mathrm{Appl}_K^m$,

(2) *K is a prime field or $m \leqslant 2p$.*

Proof. By Corollary 2.5(i) it can be assumed that K is not prime. Then it suffices to prove that the following conditions are equivalent:

(1)′ There exist $n_0, \dots, n_{s-1} \in N$ such that $n_0+\dots+n_{s-1} < m$ and

$$n_0+n_1p+\dots+n_{s-1}p^{s-1} = (m-1)+p^s.$$

(2)′ $m > 2p$.

In fact, (1)′ implies $\mathrm{Hom}_K^m \neq \mathrm{Appl}_K^m$ by Corollary 2.6. Conversely, $\mathrm{Hom}_K^m \neq \mathrm{Appl}_K^m$ and $m \leqslant 2p$ imply $a = 1$ for any I in Corollary 2.5, which gives us (1)′, a contradiction.

Let $m-1 = c_0+c_1p+\dots+c_{s-2}p^{s-2}+cp^{s-1}$ where $0 \leqslant c_0, \dots, c_{s-2} < p$, $c \geqslant 0$. Then (1)′ means that:

(a) There exist $n_0, \dots, n_{s-1} \in N$ such that $n_0+\dots+n_{s-1} < m$ and

$$n_0+n_1p+\dots+n_{s-1}p^{s-1} = c_0+c_1p+\dots+c_{s-2}p^{s-2}+(c+p)p^{s-1}.$$

Observe that $c_0+\dots+c_{s-2}+(c+p) \leqslant n_0+\dots+n_{s-1}$. In fact, $c+p \geqslant n_{s-1}$ since $(c+p)p^{s-1}$ is the greatest multiple of p^{s-1} contained in $(m-1)+q$. Next we apply induction on s: from the equality $n_0+n_1p+\dots+(n_{s-2}+pn_{s-1})p^{s-2} = c_0+c_1p+\dots+(c_{s-2}+p(c+p))p^{s-2}$ we get $c_0+\dots+c_{s-2}+p(c+p) \leqslant n_0+\dots+n_{s-2}+pn_{s-1}$; then we add $-(p-1)(c+p) \leqslant -(p-1)n_{s-1}$. Hence (a) is equivalent to

(b) $c_0+\dots+c_{s-2}+c+p < m$,

and this is equivalent to the following conditions:

(c) $c_0+\dots+c_{s-2}+c+p \leqslant c_0+\dots+c_{s-2}p^{s-2}+cp^{s-1}$,

(d) $c_1(p-1)+c_2(p^2-1)+\dots+c_{s-2}(p^{s-2}-1)+c(p^{s-1}-1) \geqslant p$.

Then it suffices to prove that the condition $m \leqslant 2p$ is equivalent to

(d)′ $c_1(p-1)+\dots+c_{s-2}(p^{s-2}-1)+c(p^{s-1}-1) < p$.

Observe that $p^k-1 \geqslant p$ for $k \geqslant 2$ and $2(p-1) \geqslant p$. Hence (d)′ means that $c_1 \leqslant 1$ and $c_2 = \dots = c_{s-2} = c = 0$, i.e. $m-1 < 2p$. This completes the proof.

COROLLARY 2.8. *If $m \leqslant 4$ then $\mathrm{Hom}_K^m = \mathrm{Appl}_K^m$ for any finite field K.*

3. Some examples. We want to show how we can find all presentations from Corollary 2.6. Then the proof of Corollary 2.6 allow us to find the basis of $\mathrm{Appl}_K^m(K^n, K)$.

EXAMPLE 3.1. Let $m = 2p+1$. Observe that $a = 1$ by Corollary 2.5(ii). Hence we look for presentations:

$$n_0+\dots+n_{s-1}p^{s-1} = 2p+p^s, \quad n_0+\dots+n_{s-1} \leqslant 2p.$$

1) Let $p = 2$ and hence $m = 5$. It is easy to see that $4+2^s$ can be presented as the sum of $\leqslant 4$ powers of 2 less than 2^s in the following three ways:

$2+2+2^{s-1}+2^{s-1}$ for $s \geqslant 2$, $2^2+2^{s-1}+2^{s-1}$ and $2^2+2^{s-2}+2^{s-2}+2^{s-1}$ for $s \geqslant 3$.

Hence the positive and monotonic I of type (P) are the following:

$(2, 2, 2, 2)$ for $s = 2$, $(2, 2, 4, 4,)$, $(4, 4, 4)$, $(2, 4, 6)$, $(6, 6)$ for $s = 3$,

$(2, 2, 8, 8)$ $(4, 8, 8)$, $(4, 4, 4, 8)$, $(2, 8, 10)$, $(10, 10)$, $(8, 12)$, $(4, 4, 12)$ for $s = 4$,

$(2, 2, 2^{s-1}, 2^{s-1})$, $(4, 2^{s-1}, 2^{s-1})$, $(4, 2^{s-2}, 2^{s-2}, 2^{s-1})$, $(2, 2^{s-1}, 2+2^{s-1})$,

$(2+2^{s-1}, 2+2^{s-1})$, $(2^{s-1}, 4+2^{s-1})$, $(4, 2^{s-2}, 2^{s-2}+2^{s-1})$, $(2^{s-2}, 4+2^{s-2}, 2^{s-1})$,

$(2^{s-2}, 2^{s-2}, 4+2^{s-1})$, $(2^{s-2}, 4+2^{s-2}+2^{s-1})$ for $s \geqslant 5$.

2) Let $p > 2$. Observe that $n_0+\dots+n_{s-1} \equiv 2p+p^s \equiv p+2 \pmod{p-1}$. Moreover, it follows from the proof of Theorem 2.7 that

$$n_0+\dots+n_{s-1} \geqslant c_0+\dots+c_{s-2}+(c+p)$$

where

$c_0 = 0$, $c_1 = 2$, $c_2 = \dots = c_{s-2} = c = 0$ for $s > 2$ and $c_0 = 0$, $c = 2$ for $s = 2$.

Hence $n_0+\dots+n_{s-1} = p+2$.

For $s = 2$ we have $n_0+n_1p = 2p+p^2$, $n_0+n_1 = p+2$, and hence $n_0 = 0$, $n_1 = p+2$. Let $s > 2$. Then $n_{s-1} \leqslant c+p = p$. Suppose that $n_{s-1} \leqslant p-1$. It follows that

$$2p+p^s \leqslant (p+2)p^{s-2}+n_{s-1}(p^{s-1}-p^{s-2}) \leqslant (p+2)p^{s-2}+(p-1)(p^{s-1}-p^{s-2})$$
$$= (p-1)p^{s-1}+3p^{s-2} \leqslant p^s.$$

This contradiction shows that $n_{s-1} = p$. Next we look for $n_0, \dots, n_{s-2}$ such that $n_0+\dots+n_{s-2}p^{s-2} = 2p$, and obtain $n_0 = 0$, $n_1 = 2$, $n_2 = \dots = n_{s-2} = 0$, $n_{s-1} = p$. Then for any $s \geqslant 2$ we have the system $J = (p, p, \underbrace{p^{s-1}, \dots, p^{s-1}}_{p})$ which "generates" all I of the type (P).

Observe that the minimal n such that $\mathrm{Hom}_K^m(K^n, K) \neq \mathrm{Appl}_K^m(K^n, K)$ is the following:

$n = 2$ for $s>2$: $\exp(p+p^{s-1}, p+(p-1)p^{s-1})$,
$n = 2$ for $s = 2$, $p>3$: $\exp((p-1)p, 3p)$,
$n = 3$ for $s = 2$, $p = 3$: $\exp(3, 6, 6)$,
$n = 4$ for $s = 2$, $p = 2$: $\exp(2, 2, 2, 2)$.

EXAMPLE 3.2. Let $2p<m\leqslant p^{s-1}$. We prove that $\mathrm{Hom}_K^m(K^2, K) \neq \mathrm{Appl}_K^m(K^2, K)$ and hence $\mathrm{Hom}_K^m(K^n, K) \neq \mathrm{Appl}_K^m(K^n, K)$ for any $n\geqslant 2$. It suffices to show that $I = ((m-1)+p^{s-1}, (p-1)p^{s-1})$ is of the type (P). Let $m-1 = c_0+\ldots+c_{s-2}p^{s-2}$, $0\leqslant c_i<p$. Since $m>2p$, it follows from the proof of Theorem 2.7 (condition (b)) that $\Sigma_p(I) = c_0+\ldots+c_{s-2}+p<m$. The rest is evident, and hence $\exp(I) \notin \mathrm{Hom}_K^m(K^2, K)$.

Let $K\subset K'$. We define I for K and I' for K' as above. It is easy to see that $I = \mathrm{red}(I')$ (over K), and hence $\exp(I) = \exp(I')|_{K^2}$.

4. Some generalizations. We prove some results on m-applications over infinite fields. The first is following:

THEOREM 4.1. *Let K be an infinite algebraic extension of $\boldsymbol{Z}_p$. Then the following conditions are equivalent*:

(1) $\mathrm{Hom}_K^m = \mathrm{Appl}_K^m$,

(2) $\mathrm{Hom}_K^m(K^2, K) = \mathrm{Appl}_K^m(K^2, K)$,

(3) $m\leqslant 2p$.

Proof. Let $\{K_t\}_{t\in T}$ be the family of all finite subfields of K having at least pm elements. Since K is infinite and algebraic over $\boldsymbol{Z}_p$ it follows that $K = \bigcup_{t\in T} K_t$.

(2) $\Rightarrow$ (3). Suppose that $m>2p$. For any K_t define I_t as in Example 3.2. Next define $f\colon K^2 \to K$ in the following way:

$$f(x, y) = \exp(I_t)(x, y) \quad \text{if} \quad x, y \in K_t .$$

It follows from Example 3.2 that f is properly defined. Moreover, f is an m-application since the both conditions are "locally finite". On the other hand, suppose that $f\in \mathrm{Hom}_K^m(K^2, K)$. Then $\exp(I_t) \in \mathrm{Hom}_{K_t}^m(K_t^2, K)$, which is false by Example 3.2.

(3) $\Rightarrow$ (1). Any m-application $f\colon K^n \to K$ gives us the family of restrictions $f_t\colon K_t^n \to K$, $t\in T$, being also m-applications. Since $m\leqslant 2p$ it follows that $f_t \in \mathrm{Hom}_{K_t}^m(K_t^n, K)$. This means that $f_t = \bar{F}_t$ where

$$F_t \in K_t[T_1, \ldots, T_n]_m \otimes_{K_t} K = K[T_1, \ldots, T_n]_m .$$

If $K_t\subset K_u$ then $f_t = f_u|K_t^n$ and hence $F_t(x_1, \ldots, x_n) = F_u(x_1, \ldots, x_n)$ for $x_1, \ldots, x_n \in K_t$. Since K has at least $pm>m$ elements it follows that $F_t = F_u$. (cf. Lemma 1.1 or [2], Lemma 6.3). Hence $F_t = F_u = F$ for any $t, u\in T$. Therefore $f = \bar{F} \in \mathrm{Hom}_K^m(K^n, K)$.

Remark 4.2. It is easy to see that any m-application over infinite K which is a polynomial mapping must be obtained from a (uniquely determined) form of degree m. For example, the mapping f defined in the first part of the above proof is not polynomial.

Remark 4.3. Let K be a proper algebraic extension of $\boldsymbol{Z}_p$. If v^m is epimorphic for any dimension n, then $m\leqslant 2p\leqslant q$ and hence v^m is monomorphic for any n. (Cf. [2], Lemma 6.3.)

Using other methods, we can prove the following

THEOREM 4.4. $\mathrm{Hom}_K^3 = \mathrm{Appl}_K^3$ *for any field K.*

Proof. 1) Let $f\colon K^n \to K$ be a 3-application and let $\{e_1, \ldots, e_n\}$ be the standard basis of K^n. It is easy to see that

$$f\Big(\sum_i x_i e_i\Big) = \sum_{1\leqslant j_1<\ldots<j_k\leqslant n} (\Delta^k f)(x_{j_1}e_{j_1}, \ldots, x_{j_k}e_{j_k})$$
$$= \sum_i f(e_i)x_i^3 + \sum_{i<j} (\Delta^2 f)(x_i e_i, x_j e_j) + \sum_{i<j<k} (\Delta^3 f)(e_i, e_j, e_k)x_i x_j x_k$$

(cf. [2], formula (3.1)). It suffices to prove that

$$(\Delta^2 f)(x_i e_i, x_j e_j) = a_{ij}x_i^2 x_j + b_{ij}x_i x_j^2 .$$

Then we can assume that $n = 2$.

2) Observe that

$$(\Delta^3 f)(x, x, y)+(\Delta^3 f)(x, y, y) = (\Delta^3 f)(x, x+y, y) = (\Delta^3 f)(-x, x+y, -y)$$
$$= f(0)-f(y)-f(x)-f(-x-y)+f(-x)+$$
$$+ f(x+y)+f(-y) = 2f(x+y)-2f(x)-2f(y)$$
$$= 2(\Delta^2 f)(x, y) .$$

If 2 is invertible in K then

$$(\Delta^2 f)(x_1 e_1, x_2 e_2) = \tfrac{1}{2}(\Delta^3 f)(e_1, e_1, e_2)x_1^2 x_2 + \tfrac{1}{2}(\Delta^3 f)(e_1, e_2, e_2)x_1 x_2^2 .$$

3) It remains to assume that $\mathrm{char}(K) = 2$. In this case

$$(\Delta^3 f)(x, x, y) = f(2x+y)-f(2x)-2f(x+y)+2f(x)+f(y) = 0 .$$

Since $n = 2$ and $\Delta^3 f$ is symmetric 3-linear, it follows that $\Delta^3 f = 0$. Hence $\Delta^2 f$ is Z-bilinear.

Consider the system of linear equations with unknows a, b:

$$x_1^2 x_2 a + x_1 x_2^2 b = (\Delta^2 f)(x_1 e_1, x_2 e_2), \quad x_1, x_2 \in K .$$

We must prove that it is solvable. We can assume that $x_1, x_2 \neq 0$. Since $(\Delta^2 f)(sx, sy) = s^3(\Delta^2 f)(x, y)$, it suffices to consider the system

$$ra+r^2 b = (\Delta^2 f)(e_1, re_2), \quad r \in K-\{0\} .$$

We can assume that $K \neq \boldsymbol{Z}_2$ (the case of $\boldsymbol{Z}_2$ is evident). Then the rank of the coefficient matrix is 2, and we must prove that the rank of the augmented matrix is also 2. In other words, it remains to prove that

$$\det \begin{pmatrix} r & r^2 & (\Delta^2 f)(e_1, re_2) \\ s & s^2 & (\Delta^2 f)(e_1, se_2) \\ t & t^2 & (\Delta^2 f)(e_1, te_2) \end{pmatrix} = 0$$

for any $r, s, t \in K$. Denote $(u, v) = (\Delta^2 f)(ue_1, ve_2)$. Since (u, v) is Z-bilinear and $2 = 0$ in K, it follows that the above determinant is equal to

$$\begin{aligned}&((s+t)^3+s^3+t^3)(1,r)+((r+t)^3+r^3+t^3)(1,s)+((r+s)^3+r^3+s^3)(1,t)\\ &\quad=(s+t, r(s+t))+(s, rs)+(t, rt)+(r+t, s(r+t))+(r, rs)+(t, st)+\\ &\quad+(r+s, t(r+s))+(r, rt)+(s, st)=(s, rt)+(t, rs)+(r, st)+(t, rs)+\\ &\quad+(r, st)+(s, rt)=0.\end{aligned}$$

This completes the proof.

It should be interesting to explain the situation for arbitrary fields. In particular, is the above theorem also true for $m = 4$?

References

[1] M. Ferrero and A. Micali, *Sur les n-applications*, Bull. Soc. Math. France Mém. 59 (1979), pp. 33–53.

[2] A. Prószyński, *Some functors related to polynomial theory*, Fund. Math. 98 (1978), pp. 219–229.

INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES

Accepté par la Rédaction le 16. 2. 1979

Indécidabilité de la théorie des anneaux de séries formelles à plusieurs indéterminées

par

Françoise Delon (Paris)

Abstract. We precise the degree of indecidability of rings of power series with several variables over a field: We define the second order arithmetic in power series ring $k[[\overline{X}]]$, in convergent series ring $k\{\overline{X}\}$, and algebraic series ring $Nk(\overline{X})$; we prove that each arithmetical serie is definable and that none of the inclusions $Nk(\overline{X}) \subset k\{\overline{X}\} \subset k[[\overline{X}]]$ is elementary; we give criteria of non elementary equivalence between power series rings over equivalent fields.

Les anneaux de séries formelles à une indéterminée sur un corps k de caractéristique nulle sont bien connus depuis les travaux d'Ax et Kochen [3] [4] et d'Ershov [9] [10]. On sait ainsi que $k[[X]]$ est décidable ssi k l'est, que $k_1[[X]] \equiv k_2[[X]]$ ssi $k_1 \equiv k_2$ et que l'inclusion $\boldsymbol{C}\{X\} \subset \boldsymbol{C}[[X]]$, où $\boldsymbol{C}\{X\}$ est l'ensemble des séries convergentes, est élémentaire. Le cas de plusieurs indéterminées est entièrement différent: Ershov [11] a montré l'indécidabilité des anneaux $A[[X_1, \ldots, X_m]]$, où A est un anneau commutatif et $m \geqslant 2$. Plus récemment Becker et Lipshitz [5] ont établi la définissabilité de N dans $k[[X_1, \ldots, X_m]]$, si carac $(k) = 0$, et donné des exemples de corps $k_1 \equiv k_2$, $k_1[[X_1, \ldots, X_m]] \not\equiv k_2[[X_1, \ldots, X_m]]$.

En 1951 R. M. Robinson [12] définissait N dans $k[X]$, grâce à la propriété qu'a cet anneau d'être factoriel. *A priori*, la même idée ne permet dans $k[[X_1, \ldots, X_m]]$ que de définir l'ensemble des séries dont le terme constant est un entier. Un raffinement de la méthode, déjà remarqué par Becker et Lipshitz, conduit au résultat. Les techniques utilisées ici sont plus précises en ce sens qu'elles permettent de définir autre chose que des séries constantes; on montre par exemple, que $Z[X_1]$ ou $k_0[X_1]$ (k_0 est constitué par les éléments de k algébriques sur Q) sont définissables dans $k[[X_1, \ldots, X_m]]$; plus généralement, est définissable tout anneau $A[X_1]$ ou $A[[X_1]]$, où A est lui-même définissable dans $k[[X_1, \ldots, X_m]]$. Cela permet de renforcer considérablement les résultats antérieurs:

(i) On définit dans $k[[X_1, \ldots, X_m]]$ le modèle standard de l'arithmétique du second ordre.