Applicable Analysis and Discrete Mathematics, **1** (2007), 403–414.
Available electronically at **http://pefmath.etf.bg.ac.yu**

Presented at the conference: *Topics in Mathematical Analysis and Graph Theory*, Belgrade, September 1–4, 2006.

POLYNOMIAL INTERPOLATION PROBLEM FOR SKEW POLYNOMIALS

Aleksandra Lj. Erić

Let $R = K[x;\sigma]$ be a skew polynomial ring over a division ring K. We introduce the notion of derivatives of skew polynomial at scalars. An analogous definition of derivatives of commutative polynomials from $K[x]$ as a function of $K[x] \to K[x]$ is not possible in a non-commutative case. This is the reason why we have to define the derivative of a skew polynomial at a scalar. Our definition is based on properties of skew polynomial rings, and it makes possible some useful theorems about them. The main result of this paper is a generalization of polynomial interpolation problem for skew polynomials. We present conditions under which there exists a unique polynomial of a degree less then n which takes prescribed values at given points $x_i \in K$ $(1 \leq n)$. We also discuss some kind of Silvester-Lagrange skew polynomial.

1. INTRODUCTION

Let K be a division ring, and let σ be a monomorphism of K. For an indeterminate x over K, we write $K[x;\sigma]$ for the ring of skew polynomials over K. By this, we mean that $K[x;\sigma]$ is the set of all left polynomials $\sum_i c_i x^i$ which are added in the usual way, and multiplied by using the distributive law together with the rule that $xc = c^\sigma x$ for any $c \in K$ (by c^σ we will denote σ-image of c). Thus, the coefficients need not commute with the variable x. The fact that $(ab)^\sigma = a^\sigma b^\sigma$ guarantees the associative law for polynomial multiplications, so $K[x;\sigma]$ is a ring. This so-called skew polynomial ring is a basic object of study in noncommutative ring theory [**1**]. As it is easily seen,the usual division algorithm stays in $R = K[x;\sigma]$: For $f(x) \in R$ and $g(x) \in R \setminus \{0\}$, we can uniquely define $f(x) = h(x)g(x) + r(x)$, where $r(x) = 0$

2000 Mathematics Subject Classification. 16S36,16U30,15A03.
Key Words and Phrases. Interpolation, skew polynomials.

or $\deg r(x) < \deg g(x)$. In particular, R is a left PID (principal ideal domain) i.e. any nonzero left ideal I has the form Rg; here, g is any polynomial in I of the smallest degree [**2**].

To define evaluation of the left polynomials at scalar, it suffices to recall some of its main properties as follows.

- The remainder Theorem [**3**]: $f(x) = q(x)(x-a)+f(a)$ where $q(x)$ is uniquely determined by f and by a. From this it follows that f is divisible by $x-a$ iff $f(a) = 0$. In this case, we say that a is right root of f.

- The Product Formula [**3**] for evaluating $f = gh$ at any $d \in K$:

$$f(d) = \begin{cases} 0 & \text{if } h(d) = 0, \\ g(d^{h(d)})h(d) & \text{if } h(d) \neq 0. \end{cases}$$

  Here, a^c is the σ-conjugate of a by c, and it is defined by $a^c = \sigma(c)ac^{-1}$, for any $c \in K^*$.

- The evaluating formula [**3**]: if $f(x) = \sum_i a_i x^i$, then $f(a) = \sum_i a_i N_i(a)$ for all $a \in K$ where $N_0(a) = 1$, and $N_n(a) = \sigma^{n-1}(a) \dots \sigma(a)a$.

2. EVALUATING DERIVATIVES OF SKEW POLYNOMIALS AT SCALAR

Let $f(x) \in R = K[x;\sigma]$. By dividing $f(x)$ by polynomial $(x-d)^2 = x^2 - (d+d^\sigma)x + d^2$ we get the remainder $cx + r$.

We can define the first derivative of polynomial $f(x)$ at scalar d : $f'(d)$ to be c. We will denote by $M_n(d)$ the first derivative of polynomial x^n at scalar d. For example:

$$x^2 = (x-d)^2 + (d+d^\sigma)x - d^2.$$

So, $M_2(d) = d + d^\sigma$. Also from

$$x^3 = (x + d^\sigma + d^{\sigma^2})(x-d)^2 + (d^{\sigma^2}d^\sigma + d^{\sigma^2}d + d^\sigma d)x - (d^\sigma + d^{\sigma^2})d^2$$

we get

$$M_3(d) = \ d^{\sigma^2}d^\sigma + \ d^{\sigma^2}d + d^\sigma d.$$

Definition 1. *Let* $f(x) = \sum_i c_i x^i \in R$. *Then* $f'(d) = \sum_i c_i M_i(d)$, *where* $M_0(d) = 0$, $M_1(d) = 1$ *and*

$$M_i(d) = \sum_{i-1 \geq k_1 > k_2 > \dots > k_{i-1} \geq 0} d^{\sigma^{k_1}} \cdots \ d^{\sigma^{k_{i-1}}}.$$

Note that, if $\sigma = 1$, then $M_i(d) = id^{i-1}$. So $f'(d)$ is the usual evaluation of derivative of f.

EXAMPLE. Let $R = \mathbb{C}[x;\ ^-]$. Then

$$M_2(d) = d + \overline{d}, \quad M_3(d) = d^2 + 2|d|^2, \quad M_4(d) = 2|d|^2(d + \overline{d}).$$

If $f(x) = ix^2 + (2+i)x - 3$, then $f'(2-i) = 2 + 5i$.

If $f(x) = x^3 - (1+i)x^2 - x + 1 + i = (x - 1 - i)(x - i)^2$, then, $f'(i) = 0,\ f(i) = 0$.

If $f(x) = x^4 - 20x$, then $f'(1+2i) = 0$ and $f(1+2i) = 5 - 40i$.

EXAMPLE. Let $R = \mathbb{R}(t)[x;\sigma]$, $\sigma : f(t) \mapsto f(t^2)$. Then

$$M_2(f(t)) = f(t) + f(t^2), \quad M_3(f(t)) = f(t^4)f(t^2) + f(t^4)f(t) + f(t^2)f(t).$$

If $p(x) = (x+t)(x-t)^2 = x^3 + (t - t^2 - t^4)x^2 + (t^4 - t^3 - t^2)x + t^3$, then

$$\begin{aligned} p(t) &= t^7 + (t - t^2 - t^4)t^3 + (t^4 - t^3 - t^2)t + t^3 = 0, \\ p'(t) &= (t^6 + t^5 + t^3) + (t - t^2 - t^4)(t + t^2) + (t^4 - t^3 - t^2) = 0. \end{aligned}$$

Proposition 2.1. *Let $f(x),\ g(x) \in R = K[x;\sigma]$ and $d \in K$. Then*

$$(f+g)'(d) = f'(d) + g'(d).$$

Proof. For $f(x) = \sum\limits_i a_i x^i$ and $g(x) = \sum\limits_i b_i x^i$ (we can assume that the polynomials are of the same degree) $(f+g)(x) = \sum\limits_i (a_i + b_i)x^i$, so

$$(f+g)'(d) = \sum_i (a_i + b_i)M_i(d) = \sum_i a_i M_i(d) + \sum_i b_i M_i(d) = f'(d) + g'(d).$$

Proposition 2.2. $M_{i+j}(d) = N_j(d)^{\sigma^i} M_i(d) + M_j(d)^{\sigma^i} N_i(d)$.

Proof. $M_{i+1}(d) = d^{\sigma^i} M_i(d) + N_i(d)$ because of

$$\begin{aligned} M_{i+1}(d) &= \sum_{i \geq k_1 > k_2 > \cdots > k_i \geq 0} d^{\sigma^{k_1}} \cdots d^{\sigma^{k_i}} \\ &= d^{\sigma^i} \sum_{i-1 \geq k_2 > k_3 > \cdots > k_i \geq 0} d^{\sigma^{k_2}} \cdots d^{\sigma^{k_i}} + \sum_{i-1 \geq k_1 > k_2 > \cdots > k_i \geq 0} d^{\sigma^{k_1}} \cdots d^{\sigma^{k_i}} \\ &= d^{\sigma^i} M_i(d) + d^{\sigma^{i-1}} \ldots d = d^{\sigma^i} M_i(d) + N_i(d). \end{aligned}$$

We proceed by induction on j. The case $j = 1$ follows from the first expression. Now, suppose that the proposition is true for some j, i. e.

$$M_{i+j+1}(d) = d^{\sigma^{i+j}} M_{i+j}(d) + N_{i+j}(d).$$

Then

$$M_{i+j+1}(d) = d^{\sigma^{i+j}} N_j(d)^{\sigma^i} M_i(d) + d^{\sigma^{i+j}} M_j(d)^{\sigma^i} N_i(d) + N_{i+j}(d).$$

Applying

$$\begin{aligned}(d^{\sigma^j} N_j(d))^{\sigma^i} &= (N_{j+1}(d))^{\sigma^i},\\ N_{i+j}(d) &= N_j(d)^{\sigma^i} N_i(d),\\ d^{\sigma^{i+j}} M_j(d)^{\sigma^i} + N_j(d)^{\sigma^i} &= M_{j+1}(d)^{\sigma^i},\end{aligned}$$

we get

$$M_{i+j+1}(d) = N_{j+1}(d)^{\sigma^i} M_i(d) + M_{j+1}(d)^{\sigma^i} N_i(d). \qquad \square$$

Proposition 2.3. *Let* $f(x) = g(x)h(x) \in R = K[x;\sigma]$, $g(x) = \sum_i b_i x^i$ *and* $h(x) = \sum_j c_j x^j$. *Then*

$$f'(d) = \sum_i b_i a^{\sigma^i} M_i(d) + g(e^\sigma d e^{-1})e,$$

where $a = h(d)$, $e = h'(d)$ *and* $e \neq 0$.

Proof. Since $f(x) = \sum_{i,j} b_i c_j^{\sigma^i} x^{i+j}$, we have

$$\begin{aligned}f'(d) &= \sum b_i c_j^{\sigma^i} M_{i+j}(d)\\ &= \sum_{i,j} b_i c_j^{\sigma^i} N_j(d)^{\sigma^i} M_i(d) \ + \sum_{i,j} b_i c_j^{\sigma_i} M_j(d^{\sigma^i}) N_i(d)\\ &= \sum_{i,j} b_i (c_j N_j(d))^{\sigma^i} M_i(d) + \sum_{i,j} b_i (c_j M_j(d))^{\sigma^i} N_i(d)\\ &= \sum_i b_i a^{\sigma^i} M_i(d) + \sum_i b_i e^{\sigma^i} N_i(d).\end{aligned}$$

Therefore,

$$\sum_{i,j} b_i e^{\sigma^i} N_i(d) = \sum_{i,j} b_i N_i(e^\sigma d e^{-1}) e = g(e^\sigma d e^{-1}) e. \qquad \square$$

If $\sigma = 1$, then $f'(d) = g'(d)h(d) + g(d)h'(d)$, which is the usual formula for a derivative of product.

Theorem 2.4. *Let* $f(x) \in R = K[x;\sigma]$ *and* $d \in K$. *Then*

$$f(x) = g(x)(x-d)^2$$

for some $g(x) \in R = K[x;\sigma]$ *iff* $f(d) = f'(d) = 0$.

The proof is easy and thus omitted.

3. EVALUATING DERIVATIVES OF THE HIGHER ORDER OF SKEW POLYNOMIALS AT SCALAR

The derivative of order n of polynomial x^i at $d \in K$ for $1 < i < n$ is $M_i^n(d) = n! \sum\limits_{i-1 \geq k_1 > k_2 > \cdots > k_{i-n} \geq 0} d^{\sigma^{k_1}} \cdots d^{\sigma^{k_{i-n}}}$, $M_n^n(d) = n!$ and $M_i^n(d) = 0$ for $n > i$.

We get it as $n!A_n$ where A_n is from

$$x^i = q(x)(x-d)^{n+1} + A_n x^n + \ldots + A_0.$$

For example,

$$(x-d)^3 = x^3 - (d^{\sigma^2} + d^\sigma + d)x^2 + ((d^\sigma)^2 + d^2 + dd^\sigma)x - d^3,$$
$$x^3 = (x-d)^3 + (d^{\sigma^2} + d^\sigma + d)x^2 - ((d^\sigma)^2 + d^2 + dd^\sigma)x + d^3.$$

and so, $M_3^2(d) = 2(d^{\sigma^2} + d^\sigma + d)$.

EXAMPLE. Let $R = \mathbb{C}[x; {}^-]$ and $f(x) = x^3 + (1+i)x^2 - x - (1+i)$ from R. Then $M_3^2(d) = 2(d + \overline{d} + d) = 2(2d + \overline{d})$. Here we have $f(1+i) = 0$, $f'(1+i) = 5 + 3i$, $f''(1+i) = 8 + 4i$. For $f(x) = x^3 - ix^2 - x + i = (x-i)^3$ we have $f(i) = f'(i) = f''(i) = 0$.

Definition 2. *The n-th derivative of polynomial $f(x) \in R = K[x;\sigma]$, $f(x) = \sum\limits_i c_i x^i$ at $d \in K$ is*

$$f^{(n)}(d) = \sum_i c_i M_i^n(d).$$

Note that $M_i^n(d) = 0$ if $n > i$.

Proposition 3.1. *For $d \in K$, $n > 1$, we have*

(1) $M_{i+1}^n(d) = d^{\sigma^i} M_i^n(d) + n M_i^{n-1}(d)$.

(2) $M_{i+j}^n(d) = \sum\limits_{k=0}^{n} \binom{n}{k} M_j^k(d^{\sigma^i}) M_i^{n-k}(d)$.

Proof. (1)

$$M_{i+1}^n(d) = n! \sum_{i \geq k_1 > k_2 > \cdots > k_{i-n+1} \geq 0} d^{\sigma^{k_1}} \cdots d^{\sigma^{k_{i-n+1}}}$$
$$= n! \left(d^{\sigma^i} \frac{M_i^n(d)}{n!} + \frac{M_i^{n-1}(d)}{(n-1)!} \right) = d^{\sigma^i} M_i^n(d) + n M_i^{n-1}(d).$$

(2) We proceed by induction. In case $j = 1$ it is (1).

$$M_{i+j+1}^n(d) = d^{\sigma^{i+j}} M_{i+j}^n(d) + n M_{i+j}^{n-1}(d)$$
$$= \sum_{k=0}^{n} \binom{n}{k} d^{\sigma^{i+j}} M_j^k(d^{\sigma^i}) M_i^{n-k}(d)$$
$$+ n \sum_{k=0}^{n-1} \binom{n-1}{k} M_j^k(d^{\sigma^i}) M_i^{n-k-1}(d).$$

From (1), $M^k_{j+1}(d^{\sigma^i}) = d^{\sigma^{i+j}} M^k_j(d^{\sigma^i}) + kM^{k-1}_j(d^{\sigma^i})$, so

$$M^n_{i+j+1}(d) = \sum_{k=0}^{n} \binom{n}{k} M^k_{j+1}(d^{\sigma^i}) M^{n-k}_i(d) - \sum_{k=0}^{n} \binom{n}{k} kM^{k-1}_j(d^{\sigma^i}) M^{n-k}_i(d) + n\sum_{k=0}^{n-1} \binom{n-1}{k} M^k_j(d^{\sigma^i}) M^{n-k-1}_i(d)$$

$$n\sum_{k=0}^{n-1} \binom{n-1}{k} M^k_j(d^{\sigma^i}) M^{n-k-1}_i(d) = n\sum_{k=1}^{n} \binom{n-1}{k-1} M^{k-1}_j(d^{\sigma^i}) M^{n-k}_i(d) = \sum_{k=1}^{n} \binom{n}{k} kM^{k-1}_j(d^{\sigma^i}) M^{n-k}_i(d).$$

So, $M^n_{i+j+1}(d) = \sum_{k=0}^{n} \binom{n}{k} M^k_{j+1}(d^{\sigma^i}) M^{n-k}_i(d)$. If $f(x) = g(x)h(x) = \sum_{i,j} b_i c_j^{\sigma^i} x^{i+j}$, then

$$f^{(n)}(d) = \sum_{i,j} b_i c_j^{\sigma^i} M^n_{i+j}(d) = \sum_{i,j,k} \binom{n}{k} b_i c_j^{\sigma^i} M^k_j(d^{\sigma^i}) M^{n-k}_i(d)$$

$$= \sum_{i,j,k} \binom{n}{k} b_i (c_j M^k_j(d))^{\sigma^i} M^{n-k}_i(d) = \sum_{i,k} nk b_i a_k^{\sigma^i} M^{n-k}_i(d),$$

where $a_k = g^{(k)}(d)$. □

Proposition 3.2. *Let $g(x) = (x-d)^n$. Then $g(d) = \cdots = g^{(n-1)}(d) = 0$.*

Proof. We prove the proposition by induction. In case $n = 1$ it is easy verified. Suppose that Proposition is true for any $k < n$. Let $g(x) = (x-d)^{n+1} = p(x)q(x)$, where $p(x) = (x-d)$ and $q(x) = (x-d)^n$. Then, for $0 \le \ell \le n-1$

$$g^{(\ell)}(d) = \sum \binom{\ell}{k} b_i a_k^{\sigma^i} M^{\ell-k}_i(d),$$

where $a_k = q^k(d)$, so $a_k = 0$ for $0 \le k \le n-1$.

Then $g^{(i)}(d) = 0$ for $0 \le i \le n-1$. We still need to prove $g^{(n)}(d) = 0$.

$$\begin{aligned} g(x) &= (x-d)^{n+1} = x^{n+1} - (d + d^{\sigma} + \cdots + d^{\sigma^n})x^n + \cdots, \\ g^{(n)}(d) &= M^n_{n+1} - (d + d^{\sigma} + \cdots + d^{\sigma^n}) M^n_n(d), \\ M^n_n(d) &= n!, \\ M^n_{n+1}(d) &= n!(d + d^{\sigma} + \cdots + d^{\sigma^n}). \end{aligned}$$

So, $g^n(d) = 0$. □

Theorem 3.3. *Let $f(x) \in K[x;\sigma]$ and $d \in K$. Then*

$$f(x) = g(x)(x-d)^n \quad \textit{for some} \quad g(x)$$

iff $f(d) = f'(d) = \cdots = f^{n-1}(d) = 0$.

Proof. Assume $f(d) = f'(d) = \cdots = f^{n-1}(d) = 0$.Then

$$f(x) = g(x)(x-d)^n + \ a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \qquad (a_i \in K)$$

For $G(x) = g(x)(x-d)^n$ we have

$$G^k(d) = \sum_i b_i a_k^{\sigma^i} M_i^{n-1}(d),$$

where b_i are coefficients of polynomial $g(x)$ and a_k is the k-th derivative of polynomial $(x-d)^n$. So $a_k = 0$, then $G^k(d) = 0 \quad 0 \le k \le n-1$

$$\begin{aligned}
0 &= f(d) = a_{n-1}N_{n-1}(d) + \ldots + a_1N_1(d) + a_0,\\
0 &= f'(d) = a_{n-1}M_{n-1}(d) + \ldots + \ a_1M_1(d),\\
0 &= f''(d) = a_{n-1}M_{n-1}^2(d) + \ldots + a_2M_2^2(d),\\
&\ \ \vdots\\
0 &= f^n(d) = a_{n-1}M_{n-1}^{n-1}(d),
\end{aligned}$$

$M_n^n(d) = (n-1)!$ implies $a_{n-1} = 0$ and by solving the system, we get $a_i = 0$ for all i i.e. $f(x) = g(x)(x-d)^n$. The converse is easy to verify from Proposition 3.2 and properties of derivatives. □

Theorem 3.4. *Let* $f(x) \in K[x;\sigma]$ *and* $\deg f = n$. *Then*

$$(*) \qquad f(x) = f(d) + \frac{f'(d)}{1!}(x-d) + \frac{f''(d)}{2!}(x-d)^2 + \cdots + \frac{f^{(n)}(d)}{n!}(x-d)^n.$$

Proof. We proceed by induction on the degree of f. Let $\deg f = 1$. Then $f(x) = A(x-d) + f(d)$ and $f'(d) = A$, so

$$f(x) = f(d) + \frac{f'(d)}{1!}(x-d).$$

Assume that $(*)$ holds, for any polynomial f with $\deg f = n$.

Let $f(x)$ be a polynomial with $\deg f = n+1$. Then $f(x) = g(x)(x-d) + f(d)$ for some $g(x)$ and $\deg g = n$. Then

$$f^{(m)}(d) = (g(x)(x-d))^{(m)}(d).$$

Using the product formula, we obtain

$$(g(x)(x-d))^{(m+1)}(d) = \sum_{i,k} \binom{m+1}{k} b_i a_k^{\sigma^i} M_i^{m+1-k}(d),$$

where b_i are coefficients of g and a_k value of k-th derivative of polynomial $(x-d)$ at d. So $a_1 = 1$ and $a_i = 0$ for $i > 1$, which implies: $\big(g(x)(x-d)\big)^{(m+1)}(d) =$

$(m+1)\sum_i b_i M_i^m(d) = (m+1)g^{(m)}(d)$. So, $(m+1)g^{(m+1)}(d) = f^{(m+1)}(d)$ and finally, we get $(*)$ for n replace with $n+1$. □

4. POLYNOMIAL INTERPOLATION FOR SKEW POLYNOMIALS

For a field K, it is well known that for $x_0, \ldots, x_{n-1}, x_n$ being different elements of K and $y_0, \ldots, y_{n-1}, y_n \in K$, there exists the unique polynomial $f \in K[x]$ such that $f(x_i) = y_i$ and $\deg f \leq n$. However, the condition $x_i \neq x_j$ is not sufficient for existence of such a polynomial in a non-commutative case.

Let us first mention some facts about skew polynomials.

Proposition 4.1. *Let $\Delta = \{x_0, \ldots, x_n\}$ and $x_i \in K$, where K is a division ring. Then*

(1) *There exists the nonzero polynomial $f \in K[x;\sigma]$ such that $f(x_i) = 0$.*

(2) *The set I of polynomials vanishing on Δ form a left ideal in $K[x;\sigma]$.*

(3) *If f_Δ is monic polynomial of the smallest degree in I, then $I = Rf_\Delta$, where $R = K[x;\sigma]$. We will call f_Δ minimal polynomial of Δ.*

Proof. (1) Let Δ be doubleton i.e. $\Delta = \{a, b\}$. Then, a polynomial f vanishing on Δ is

$$f(x) = \big(x - \sigma(b-a)b(b-a)^{-1}\big)\big(x - a\big),$$

which follows from Product and Remainder Theorem.

If g is a polynomial vanishing on $\Gamma = \{x_0, \ldots, x_{n-1}\}$, then a polynomial f vanishing on $\Delta = \Gamma \cup \{x_n\}$ is

$$f(x) = \big(x - \sigma(g(x_n)\big)x_n g(x_n)^{-1})g(x).$$

(2) If $f, g \in I$, then $f(d) = g(d) = 0$ for all $d \in \Delta$. So, $(f+g)(d) = f(d) + g(d) = 0$. Also, for $\alpha \in R$ $(\alpha f)(d) = \alpha\big(\sigma(f(d))df(d)^{-1}\big)f(d) = 0$ (from Product formula). Then I is the left ideal in left PID, so it is principal.

(3) If $f \in I$, then $f(x_i) = 0$ for all $x_i \in \Delta$. $f = qf_\Delta + r$ where f_Δ is a polynomial of minimal degree in I, $q, r \in K[x;\sigma]$ and $\deg r < \deg f_\Delta$. From $f(x_i) = r(x_i) = 0$ it follows $r \equiv 0$. The conclusion is that $f \in Rf_\Delta$. □

Theorem 4.2. *Let $\Delta = \{x_0, \ldots, x_n\}$ and $x_i \in K$ where K is a division ring. For any $y_0, \ldots, y_n \in K$ there exists a unique polynomial $f \in R$ such that $f(x_i) = y_i$ and $\deg f \leq n$ if and only if $\deg f_\Delta = n+1$ where f_Δ is the minimal polynomial of the set Δ.*

Proof. Let $\Phi : R = K[x;\sigma] \to K^{n+1}$ be a K-linear function of the left K-spaces such that

$$f \mapsto \big(f(x_0), \ldots, f(x_n)\big).$$

The kernel of the homomorphism Φ consists of all polynomials f such that $f(x_i) = 0$ for all i. So, $\operatorname{Ker}\Phi = Rf_\Delta$, where f_Δ is the minimal polynomial of the set Δ. Then

$Im\Phi \cong R/\mathrm{Ker}\,\Phi$ ([**4**], Th. 2.1).

$$\dim Im\Phi = \dim R/\mathrm{Ker}\,\Phi = \dim R/Rf_\Delta = \deg f_\Delta$$

$\dim R/Rf_\Delta = \deg f_\Delta$ because for $m = \deg f_\Delta$, $\{1, x, \ldots, x^{m-1}\}$ is a base of the left K-space R/Rf_Δ. Indeed, $g = qf_\Delta + r$ and $\deg r < m$.

The homomorphism Φ is surjective iff $\dim Im\Phi = n+1$, which means that $\deg f_\Delta = n+1$. Then, the interpolation polynomial for such a set Δ is

$$f(x) = \sum_{i=0}^{n} y_i L_i(x_i)^{-1} L_i(x),$$

where $L_i(x)$ is the monic polynomial such that $L_i(x_j) = 0$ for $i \neq j$. The degree of the polynomial f is $\leq n$. If there is another polynomial g, $\deg g \leq n$ and $g(x_i) = y_i$, then $(f-g)(x_i) = 0$ implies $f - g \in Rf_\Delta$, so $\deg \geq n+1$ and this is impossible.□

Example. Let $R = \mathbb{C}[x;\ ^-]$ and $\Delta = \{1, i, -1\}$. Then, the minimal polynomial of Δ is $f_\Delta = x^2 - 1$ of degree 2. It means that for this set, Theorem 4.2 does not hold. For example, there is no polynomial f such that $f(1) = 1$, $f(i) = 0$ and $f(-1) = -1$. Also, there are many polynomials such that $f(1) = 1$, $f(i) = 0$ and $f(-1) = i$.

$$f(x) = ax^2 + \frac{1+i}{2}\,x + \left(\frac{1-i}{2} - a\right).$$

Example. Let $R = \mathbb{C}[x;\ ^-]$ and $\Delta = \{1, i, 2i\}$. Then, the minimal polynomial of Δ is $f_\Delta = x^3 - 2ix^2 - x + 2i$. (We get it from $\big(x - \overline{g(2i)}\,2i(g(2i))^{-1}\big)g(x)$ where $g(x) = x^2 - 1$). The degree of minimal polynomial is 3 so, there is a unique polynomial f of degree ≤ 2 such that $f(1) = A$, $f(2i) = B$ and $f(-1) = C$ for any A, B, C.

$$\begin{aligned}
L_0(x) &= \big(x - \overline{i}\,2i\,i^{-1}\big)(x-i) = (x+2i)(x-i) = x^2 + 3ix + 2,\\
L_1(x) &= \big(x - \overline{(2i-1)}\,2i\,(2i-1)^{-1}\big)(x-1) = x^2 + \frac{1}{5}\,(3+6i)x - \frac{2}{5}\,(4+3i),\\
L_2(x) &= \big(x - \overline{(i-1)}\,i(i-1)^{-1}\big)(x-1) = (x+1)(x-1) = x^2 - 1.
\end{aligned}$$

Then,

$$f(x) = \Big(\frac{1-i}{6}\,A + \frac{i-3}{6}\,B + \frac{1}{3}\,C\Big)x^2 + \Big(\frac{1+i}{2}\,A - \frac{1+i}{2}\,B\Big)x + \Big(\frac{1-i}{3}\,A + \frac{3+i}{3}\,B - \frac{1}{3}\,C\Big).$$

Example. Let $R = D[x]$ where D is a division field of real quaternions. If $\Delta = \{i, j, k\}$, then $f_\Delta = x^2 + 1$ is a polynomial of degree 2. There is no polynomial of degree ≤ 2 such that $f(i) = 1$, $f(j) = 0$ and $f(k) = 0$.

If $\Delta = \{1, i, j\}$, then $f_\Delta = (x-1)(x^2+1) = x^3 - x^2 + x - 1$ is a polynomial of degree 3. Then, there exists a unique polynomial of degree ≤ 3 such that $f(1) = A$, $f(i) = B$ and $f(j) = C$.

There is a relation between the interpolation polynomial problem and the

σ-VANDERMONDE matrix. We define σ-VANDERMONDE matrix to be

$$V_n^\sigma(x_0,\dots,x_{n-1}) = \begin{bmatrix} 1 & 1 & \dots & 1 \\ N_1(x_0) & N_1(x_1) & \dots & N_1(x_{n-1}) \\ N_2(x_0) & N_2(x_1) & \dots & N_2(x_{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ N_{n-1}(x_0) & N_{n-1}(x_1) & \dots & N_{n-1}(x_{n-1}) \end{bmatrix}.$$

T. Y. LAM [**3**] proves that the rank of this matrix is same as the degree of a minimal polynomial of the set $\Delta = \{x_0,\dots,x_{n-1}\}$, and also gives the following useful formulae for computing it:

(1) For any generalized quaternion division algebra D over a field F of characteristics $\neq 2$, then rank V$= \sum_i \min\{2, |\Delta_i|\}$ where $\Delta = \Delta_1 \cup \dots \cup \Delta_m$ is the partition of Δ into σ-conjugacy classes.

(2) For $\mathbb{C}[x;-]$ let $\delta_1,\dots,\delta_m$ be different values among $|d|, d \in \Delta$. Then rank V $= \sum_{i=1}^{m} r_i$ where $r_i = 1$ if exactly one element in Δ has modulus δ_i and $r_i = 2$ otherwise.

Using this, we can answer the question about a degree of minimal polynomial of given set. Now, we will give an exposition on generalization of polynomial interpolation problem.

Proposition 4.3. *Let $\Delta = \{x_1,\dots,x_k\}$ and $S = \{(r,s_r)|1 \le r \le k, 0 \le s_r \le n_r\}$, where $n_1,\dots,n_k \in \mathbf{N}$. Then*

(1) *There exists a nonzero polynomial f such that $f^{(s_r)}(x_r) = 0$ for all $(r,s_r) \in S$.*

(2) *The set I of polynomials such that $f^{(s_r)}(x_r) = 0$ for all $(r,s_r) \in S$ form a left ideal in R.*

(3) *If $f_{\Delta,S}$ is a monic polynomial of the smallest degree in I, then $I = Rf_\Delta$. We will call $f_{\Delta,S}$ the minimal polynomial for the pair (Δ,S).*

Proof. (1) For n_r, $1 \le r \le k$ the polynomial f has right factor $(x-x_r)^{n_r-1}$. It follows from Theorem 3.3. The left factor is determined by the Product Theorem.

(2) If $f,g \in I$, then $f+g \in I$. It follows from additive property of derivatives at scalar. Let $\alpha \in R$, and $f \in I$. Then (from Proposition 3.1.)

$$(\alpha f)^{(s_r)}(x_r) = \sum_{i,k} \binom{s_r}{k} b_i a_k^{\sigma^i} M_i^{s_r-k}(d),$$

where $a_k = f^{(k)}(x_r) = 0$ and $f(x) = \sum b_i x^i$, $b_i \in K$. So, $(\alpha f)^{(s_r)}(x_r) = 0$ for all s_r such that $(r,s_r) \in S$. Then $\alpha f \in I$.

(3) Let $f \in I$, $f = qf_{\Delta,S} + r$, where $q,r \in R$ and $\deg r < \deg f_{\Delta,S}$. Then, $0 = f^{(s_r)}(x_r) = r^{(s_r)}(x_r)$ implies $r \in I$. $f_{\Delta,S}$ is polynomial of the smallest degree in I, so $r \equiv 0$. The conclusion is: $f \in Rf_{\Delta,S}$. □

Theorem 4.4. *Let $\Delta = \{x_1, \ldots, x_k\}$ and $S = \{(r, s_r) | 1 \leq r \leq k, 0 \leq s_r \leq n_r\}$ where $n_1, \ldots, n_k \in \mathbb{N}$ and $y_r^{s_r} \in K$. Then, there exists the unique polynomial $f \in R$ of degree $\leq n-1$ where $n = \sum(n_r+1)$, such that $f^{(s_r)}(x_r) = y_r^{s_r}$ for all pairs (r, s_r), iff the minimal polynomial (in the sense of Proposition 4.3.) $f_{\Delta,S}$ is of degree n.*

Proof. Let $\Phi : K[x;\sigma] \to K^n$ be a K-linear function of left K-spaces given by

$$f \mapsto (f^{(s_r)}(x_r) : (r, s_r)) \in S.$$

It follows from properties of derivatives. The rest of the proof is same as the proof of Theorem 4.2. □

EXAMPLE. Let $R = \mathbb{C}[x;-]$ and $\Delta = \{1, i\}$, $S = \{(1,0), (2,0), (2,1)\}$. The minimal polynomial of the pair (Δ, S), i.e. the minimal polynomial such that $f_{\Delta,S}(1) = f_{\Delta,S}(i) = f'_{\Delta,S}(i) = 0$ is $f_{\Delta,S}(x) = x^2 - 1$. This is polynomial of degree 2. There is no polynomial f such that $f(1) = 1$, $f(i) = 1$ and $f'(i) = 1$.

Let $\Delta = \{1, i\}$, $S = \{(1,0), (1,1), (2,0)\}$. The minimal polynomial of the pair (Δ, S) is $f_{\Delta,S}(x) = \big(x - \overline{(2-2i)}\, i(2-2i)^{-2}\big)(x-1)^2 = (x+1)(x-1)^2 = x^3 + x^2 - x - 1$ ($2 - 2i$ is value of polynomial $(x-1)^2 = x^2 - 2x + 1$ at i). This polynomial is of degree 3, so there is a unique polynomial f of degree ≤ 2 such that $f(1) = A$, $f(i) = B$ and $f'(1) = C$.

$L_0(x)$ is the monic polynomial such that $L_0(i) = L'_0(1) = 0$, then $L_0(x) = x^2 - 2x - 1 + 2i$. $L_1(x)$ is the monic polynomial such that $L_1(1) = L_1(i) = 0$. Then $L_1(x) = x^2 - 1$. $L_2(x)$ is the monic polynomial such that $L_2(1) = L'_2(1) = 0$. Then $L_2(x) = (x-1)^2$. We find that

$$f(x) = \Big(-\frac{1+i}{4}A + \frac{B}{2} + \frac{1+i}{4}C\Big)x^2 + \frac{1+i}{2}(A-C)x + \Big(\frac{3-i}{4}A - \frac{B}{2} + \frac{1+i}{4}C\Big).$$

Let $\Delta = \{1, i\}$ and $S = \{(1,0), (1,1), (1,2), (2,0)\}$. Then

$$f_{\Delta,S}(x) = \big(x - \overline{(4i-4)}\, i(4i-4)^{-1}\big)(x-1)^3 = (x+1)(x-1)^3$$

($4i - 4$ is the value of polynomial $(x-1)^3$ at i) is minimal polynomial of degree 4, so there is unique polynomial of degree ≤ 3 such that $f(1) = A$, $f'(1) = B$, $f''(1) = C$ and $f(i) = D$. The monic polynomial $L_0(x)$ such that $L'_0(1) = L''_0(1) = L_0(i) = 0$ is

$$L_0(x) = x^3 - 3x^2 + 3x - 4i + 3.$$

The monic polynomial $L_1(x)$ such that $L_1(1) = L''_1(1) = L_1(i) = 0$ is

$$L_1(x) = x^3 - 3x^2 - x + 3.$$

The monic polynomial $L_2(x)$ such that $L_2(1) = L'_2(1) = L_2(i) = 0$ is

$$L_2(x) = (x+1)(x-1)^2 = x^3 - x^2 - x + 1.$$

The monic polynomial $L_3(x)$ such that $L_3(1) = L'_3(1) = L''_3(1) = 0$ is

$$L_3(x) = (x-1)^3 = x^3 - 3x^2 + 3x - 1,$$

So, desired interpolation polynomial is

$$f(x) = AL_0(1)^{-1}L_0(x) + BL'_1(1)^{-1}L_1(x) + CL''_2(1)^{-1}L_2(x) + DL''_3(1)^{-1}L_3(x).$$

In general, we can find the interpolation polynomial for condition from Theorem 4.4

$$f(x) = \sum a_{\Gamma,S} f_{\Gamma,S},$$

where $a_{\Gamma,S} \in K$ are coefficients which we will find from condition $f^{(r_s)}(x_i) = y_i^{r^s}$ and $f_{\Gamma,S}$ is the minimal polynomial of the pair (Γ, S) where

$$\Gamma = \{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k\}$$

and

$$S = \{(r, s_r) | 1 \leq r \leq k, r \neq i, 0 \leq s_r \leq n_k\}$$

or $\Gamma = \Delta$ and

$$S = S_{m,\ell} = \{(r, s_r) | 1 \leq r \leq k, 0 \leq s_r \leq n_k, 0 \leq s_\ell \leq n_\ell - m\},$$

where $1 \leq \ell \leq k$ and $1 \leq m \leq n_\ell$.

For example: if $\Delta = \{x_1, x_2\}$ and $S = \{(1,0), (1,1), (2,0), (2,1)\}$

$$f(x) = a_1 f_{\{x_1\},\{(1,0),(1,1)\}} + a_2 f_{\{x_2\},\{(2,0),(2,1)\}} + a_3 f_{\{x_1,x_2\},\{(1,0),(1,1),(2,0)\}} + a_4 f_{\{x_1,x_2\},\{(1,0),(2,0),(2,1)\}}.$$

If $\Delta = \{x_1, x_2\}$ and $S = \{(1,0), \ldots, (1,n-1), (2,0)\}$, then

$$f(x) = A(x - x_1)^n + B(x - x_2) + \sum_{i=0}^{n-2} a_i f_{\{x_1,x_2\},S_i},$$

where $S_i = \{(2,0)\} \cup \{(1,s) | 0 \leq s \leq i\}$.

REFERENCES

1. N. Jacobson: *Theory of Rings.* Amer. Math. Soc., Providence, 1943.
2. P. M. Cohn: *Skew Fields. Theory of General Division Rings.* Encyclopedia in Math., Vol. **57**, Cabridge Univ. Press, Cambridge, 1995.
3. T. Y. Lam: *A general theory of Vandermonde matrices.* Expositions Math., **4** (1986), 193–215.
4. E. Artin: *Geometric Algebra.* Interscience Publishers, Inc., 1957.

Faculty of Civil Engineering,
University of Belgrade,
Bulevar Kralja Aleksandra 73
11000 Beograd, Serbia
E–mail: eric@grf.bg.ac.yu

Received October 24, 2006.