МАТЕМАТИЧКИ ВЕСНИК
60 (2008), 3–8

UDK 517.984
оригинални научни рад
research paper

THE RESULTANT OF NON-COMMUTATIVE POLYNOMIALS

Aleksandra Lj. Erić

Abstract. Let $R = K[x;\sigma]$ be a skew polynomial ring over a division ring K. Necessary and sufficient condition under which common right factor of two skew polynomials exists is established. It is shown that the existence of common factor depends on the value of non-commutative (Dieudonné) determinant built on coefficients of polynomials and their σ^l-images.

1. Introduction

The main purpose of this paper is to extend the well known criterion for existence of common factor of two polynomials. Our basic tool is the notion of resultant of polynomials in non-commutative sense which we will introduce in Section 2. Several examples are discussed in Section 3.

In Ore extension $R = K[x;\sigma]$, one can "right divide" a polynomial f by another polynomial $h \neq 0$ via an Euclidean algorithm: $f = gh + r$ where either $r = 0$ or $\deg r < \deg h$. From this, it follows easily that R is a PLID (principal left ideal domain). However, it is also widely known that, if $\sigma(K) \neq K$ (i.e. when σ fails to be an automorphism of K), then left division does not work, and R is not a PRID (principal right ideal domain).

Let us recall some basic facts. The first is the *Remainder Theorem* [2]: $f(x) = q(x)(x-a) + f(a)$ where $q(x)$ is uniquely determined by f and by a. It follows that f is divisible by $x - a$ iff $f(a) = 0$. In this case, we say that a is a right root of f. The second is the *Product Formula* [2] (Theorem 8.6.4) for evaluating $f = gh$ at any $a \in K$:

$$f(a) = \begin{cases} 0 & \text{if} \quad h(a) = 0 \\ g(a^{h(a)})h(a) & \text{if} \quad h(a) \neq 0 \end{cases}$$

where, for any $c \in K^*$, a^c denotes $a^c = \sigma(c)ac^{-1} + \delta(c)c^{-1}$, which is called the (σ,δ)-conjugate of a by c. We will denote $\sigma(a)$ by a^σ.

The third is the *Evaluating formula*: for $f(x) = \sum_i a_i x^i$ we have

$$f(a) = \sum_i a_i N_i(a) \quad (a \in K)$$

AMS Subject Classification: 12E15
Keywords and phrases: Polynomial ring, skew polynomial, resultant.

where $N_0(a) = 1$ and inductively

$$N_{n+1}(a) = \sigma(N_n(a))a + \delta(N_n(a)) \ \ (n \in N_0).$$

In the case when $\delta = 0$, $N_n(a) = \sigma^{n-1}(a)\sigma^{n-2}(a)\cdots\sigma(a)a$.

2. The resultant of non-commutative polynomials

First let us recall the well known criterion for existence of a common factor of two ordinary polynomials in the ring $F[x]$, where F is a field:

Let $f, g \in F[x]$, F be a field and $\deg f = m$, $\deg g = n$. Polynomials f, g have a common right factor iff there exists polynomials $c, d \in F[x]$ such that:

$$cf = dg$$

where $\deg c < \deg g$ and $\deg d < \deg f$.

In this section, we are going to extend this criterion to the skew polynomials with $\delta = 0$. Although the ring $R := K[x; \sigma, \delta]$ is non-commutative, it is still a UFD (unique factorization domain) in the sense of [3] (page 28). Let us mention some more advanced facts about the skew polynomials.

Proposition 2.1. ([6], Theorem 2.2) (1) *Let $f \in K[x, \sigma]$. Then R/Rf is a left K-vector space and $\dim R/Rf = \deg f$.*

(2) *Let $f, g \in K[x, \sigma]$. Then Rf/Rg is a left K-vector space and $\dim Rf/Rg = \deg g - \deg f$.*

Proposition 2.2. ([6], Theorem 2.2) *Let E_1 and E_2 be submoduls of an R-modul E, when R is a ring. Then the sequence*

$$0 \ \longrightarrow E_1 \cap E_2 \ \longrightarrow E_1 + E_2 \ \longrightarrow (E_1 + E_2)/E_1 \oplus (E_1 + E_2)/E_2 \ \longrightarrow 0$$

is exact.

Proposition 2.3. ([6], Theorem 2.2) *Let $f, g \in R = K[x; \sigma]$ and $\deg f > 0$, $\deg g > 0$. If $k, h \in R$ so that $Rf \cap Rg = Rh$ and $Rf + Rg = Rh$, then*

$$\deg f + \deg g = \deg h + \deg k.$$

Here is the main result of this section.

Theorem 2.4. *Let $f, g \in R = K[x; \sigma]$ and $\deg f = n$, $\deg g = m$. Polynomials f and g have a common right (nonunit) factor if and only if there exist polynomials $c, d \in R$ such that $cf = dg$ and $\deg c < m$ and $\deg d < n$.*

Proof. Since R is a PLID, we have $Rf \cap Rg = Rh$, and $Rf + Rg = Rk$. From $h \in Rf$, it follows that $h = cf$ for some $c \in R$, and similarly $h \in Rg$ implies that $h = dg$ for some $d \in R$.

Assume that polynomials f and g have common right (nonunit) factor k_1. Then k_1 is a right factor of k and $\deg k \geq \deg k_1 > 0$. According to the Proposition 2.3., we have

$$\deg k + \deg h = \deg f + \deg g. \tag{1}$$

It follows that $\deg h < \deg f + \deg g$ which means that $\deg c < \deg g$, and $\deg d < \deg f$.

Conversely, suppose that there exist $c, d \in R$, $\deg c < m$, $\deg d < n$ such that $cf = dg = h_1$. Then $h_1 \in Rh$, so $\deg h \leq \deg h_1 < m + n \leq \deg f + \deg g$. Thus it follows from equation (1) that $\deg k > 0$. It means that k is nonunit and also a right factor of the polynomials f, g (according to the fact $Rf + Rg = Rk$). ■

Now, we are going to introduce a notion of resultant in non-commutative setting. If

$$f = \sum_{i=0}^{m} a_i x^i, \quad g = \sum_{i=0}^{n} b_i x^i$$

and

$$c = \sum_{i=0}^{n-1} c_i x^i, \quad d = \sum_{i=0}^{m-1} d_i x^i$$

are the polynomials from Theorem 2.4., then

$$cf = \sum_{k} \sum_{i=0}^{k} c_i a_{k-i}^{\sigma^i} x^k, \quad dg = \sum_{k} \sum_{i=0}^{k} d_i b_{k-i}^{\sigma^i} x^k.$$

So the equality $cf = dg$ means $\sum_{i=0}^{k} c_i a_{k-i}^{\sigma^i} = \sum_{i=0}^{k} d_i b_{k-i}^{\sigma^i}$ for all $0 \leq k < m + n$.

For example, for $m = n = 2$ we get the system of linear equations with unknowns $c_0, c_1, -d_0, -d_1$:

$$\begin{aligned}
c_0 a_0 \qquad\qquad &- d_0 b_0 \qquad\qquad = 0\\
c_0 a_1 + c_1 a_0^{\sigma} &- d_0 b_1 - d_1 b_0^{\sigma} = 0\\
c_0 a_2 + c_1 a_1^{\sigma} &- d_0 b_2 - d_1 b_1^{\sigma} = 0\\
c_1 a_2^{\sigma} \qquad &\qquad\quad - d_1 b_2^{\sigma} = 0
\end{aligned}$$

The determinant of this system is

$$\begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0^{\sigma} & a_1^{\sigma} & a_2^{\sigma} \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0^{\sigma} & b_1^{\sigma} & b_2^{\sigma} \end{vmatrix}.$$

In general, we get a system of $m + n$ linear equations with $m + n$ unknowns $c_0, \ldots, c_{m-1}, -d_0, \ldots, -d_{n-1}$ with coefficients in division ring K ([4]). The determinant of the system is

$$\begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_n & 0 & \dots & 0 \\ 0 & a_0^\sigma & a_1^\sigma & \dots & a_{n-1}^\sigma & a_n^\sigma & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & 0 & \dots & a_0^{\sigma^{n-1}} & a_1^{\sigma^{n-1}} & \dots & a_n^{\sigma^{n-1}} \\ b_0 & b_1 & b_2 & \dots & b_m & 0 & \dots & 0 \\ 0 & b_0^\sigma & b_1^\sigma & \dots & b_{m-1}^\sigma & b_m^\sigma & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & 0 & \dots & b_0^{\sigma^{m-1}} & b_1^{\sigma^{m-1}} & \dots & b_m^{\sigma^{m-1}} \end{vmatrix}.$$

This is an $(m+n)$ determinant over division ring where m and n are degrees of polynomials f and g. It is also called the Dieudonné determinant ([5]) and it takes values in the factor group $K^*/[K^*,K^*]\cup\{0\}$ where $[K^*,K^*]$ is the commutator of the multiplicative group $K^* = K\setminus\{0\}$. We will denote this determinant by $R(f,g)$, and we will call it the *resultant of polynomials f and g*.

If the system has a nontrivial solution, determinant must be zero. Conversely, if determinant is zero, then system has a nontrivial solution. So, there exist polynomials $c,d\in R$ such that $cf = dg$ and $\deg c < \deg g$, $\deg d < \deg f$.

Theorem 2.5. *Polynomials f, g from $R = K[x,\sigma]$ have a common (nonunit) right factor iff $R(f,g) = 0$.*

Corollary 1. Let $f,g\in R = K[x;\sigma]$, $f(x) = a_nx^n + \dots + a_0$, $g(x) = x-d$. Then

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} & a_n \\ -d & 1 & 0 & \dots & 0 & 0 \\ 0 & -d^\sigma & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -d^{\sigma^{n-1}} & 1 \end{vmatrix}.$$

We switch the first and the last row and then move columns cyclically. We get

$$R(f,g) = \begin{vmatrix} 1 & -d^{\sigma^{n-1}} & 0 & \dots & 0 & 0 \\ 0 & 1 & -d^{\sigma^{n-2}} & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & -d^{\sigma^{n-3}} & \dots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \end{vmatrix}.$$

We continue the procedure until we get a determinant which differs from unit in the last place ($(n+1,n+1)$ entry). The last place will be

$$a_0 + \dots + a_{n-1}d^{\sigma^{n-2}}\cdots d^\sigma d + a_n d^{\sigma^{n-1}}\cdots d^\sigma d$$

and that is $f(d)$. So $R(f,g) = 0$ iff $f(d) = 0$. This means that f is divisible by $x-d$ iff $f(d) = 0$.

Example 1. Let $R = D[x]$ where D is the ring of real quaternions. First, we consider a pair of polynomials

$$f(x) = x^2 - (i+j)x - ij = (x-j)(x-i),$$
$$g(x) = x^2 - jx + (1-ij) = (x+i-j)(x-i).$$
$$R(f,g) = \begin{vmatrix} -ij & -(i+j) & 1 & 0 \\ 0 & -ij & -(i+j) & 1 \\ 1-ij & -j & 1 & 0 \\ 0 & 1-ij & -j & 1 \end{vmatrix}.$$

This is a Dieudonné determinant. We get a determinant which differs from unit in the last place by left multiplying its rows. The last place is $R(f,g) = 0$, so the polynomials f, g have a common right factor.

Next, let us consider

$$f(x) = (x-j)^2 = x^2 - 2jx - 1,$$
$$g(x) = (x+i-j)(x-i) = x^2 - jx + 1 - ij.$$

We get a determinant which differs from unit in the last place by left multiplying its rows. The last place is $R(f,g) = -2 + 4i + [D^*, D^*] \neq 0$, so the polynomials f, g have no common right factor.

Example 2. Let $R = K[x]$, where K is the field of fractions ([2]) of the skew polynomial ring $\mathbf{C}[t;^-]$, i.e. $K = \mathbf{C}(t;^-)$. For the pair of polynomials

$$f(x) = x^2 + t^{-1},$$
$$g(x) = (t-1)^{-1}x^3 + (t^2-1)(t-i)x^2 + (t^2-t)^{-1}x + (t^3-t)^{-1}(t-i),$$

$R(f,g)$ is

$$\begin{vmatrix} t^{-1} & 0 & 1 & 0 & 0 \\ 0 & t^{-1} & 0 & 1 & 0 \\ 0 & 0 & t^{-1} & 0 & 1 \\ (t^3-t)^{-1}(t-i) & (t^2-t)^{-1} & (t^2-1)(t-i) & (t-1)^{-1} & 0 \\ 0 & (t^3-t)^{-1}(t-i) & (t^2-t)^{-1} & (t^2-1)(t-i) & (t-1)^{-1} \end{vmatrix}.$$

This is a Dieudonné determinant and $R(f,g) = 0$, so the polynomials f and g have a common right factor. But polynomial f is irreducible, so f is a factor of the polynomial g. Really,

$$g(x) = ((t-1)^{-1}x + (t^2-1)(t+i))(x^2 + t^{-1}).$$

Note that $(t^2-1)^{-1}(t+i)t^{-1} = (t^3-t)^{-1}(t-i)$.

Let $R = K[x;1;\delta]$ where δ is a σ-derivation. R is a PLID and it has the algorithm of dividing. Thus we can apply the same argument as before.

For $f, g \in R$, where $\deg f = \deg g = 2$, $R(f,g)$ is

$$\begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ a_0^\delta & a_1^\delta + a_0 & a_2^\delta + a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ b_0^\delta & b_1^\delta + b_0 & b_2^\delta + b_1 & b_2 \end{vmatrix}.$$

In general, if $f(x)=\sum_0^n a_i x^i$ and $g(x)=\sum_0^m b_i x^i$, than $R(f,g)$ is a determinant of dimension $(m+n)$.

The first row is $(a_0, \dots, a_n, 0, \dots 0)$, and the $(i+1)$-th row is $A_{i+1,j}$ $(1<j\le m-1)$, where

$$A_{i+1,j}=\sum_0^{j-1}\binom{i}{i-k}a_{j-1-k}^{\delta^{i-k}}$$

where $\binom{i}{-l}=0$ for $l>0$ and $a_i=0$ for $i>n$ and the $m+1$-th row is $(b_0, \dots, b_m, 0, \dots, 0)$.

$$A_{i+1+m,j}=\sum_0^{j-1}\binom{i}{i-k}b_{j-1-k}^{\delta^{i-k}}$$

where $\binom{i}{-l}=0$ for $l>0$ and $b_i=0$ for $i>m$ and $0<i\le m-1$.

EXAMPLE 3. Let $K=\mathbf{R}(t)$, $R=K[x;1;']$ where $'$ is the standard derivation. Then

$$xr(t)=r(t)x+r'(t)$$

for $r(t)\in\mathbf{R}(t)$. For the polynomials

$$f(x)=(x-\frac{1}{t})(x-t)=x^2-(t+\frac{1}{t})\quad\text{and}\quad g(t)=x(x-t)=x^2-tx-1,$$

$$R(f,g)=\begin{vmatrix}0 & -(t+\frac{1}{t}) & 1 & 0\\ 0 & -(1-\frac{1}{t^2}) & -(t+\frac{1}{t}) & 1\\ -1 & -t & 1 & 0\\ 0 & -2 & -t & 1\end{vmatrix}=0,$$

so polynomials f,g have a common factor.

On the other hand, for

$$f(x)=(x-t)x=x^2-tx,\quad g(x)=x(x-t)=x^2-tx-1,$$

$R(f,g)=-1$, so the polynomials have no common factors.

REFERENCES

[**1**] O. Ore, *Theory of non-commutative polynomials*, Ann. Math. **34** (1933), 480–508.

[**2**] P. M. Cohn, *Free Rings and Their Relations*, 2nd Ed., London Math. Soc. Monograph No. **19**, Academic Press, London, 1985.

[**3**] P. M. Cohn, *Skew Fields. Theory of General Division Rings*, Encyclopedia in Math., Vol. **57**, Cambridge Univ. Press, Cambridge, 1995.

[**4**] E. Artin, *Geometric Algebra.* Interscience Publishers Ltd., London, 1957.

[**5**] J. Dieudonné, *Les déterminants sur un corps non commutatif*, Bull. Soc. Math. France **71** (1943), 27–45.

[**6**] J. B. Castillon, *These de doctorat d'etat sciences mathematiques a la faculte des science de Montpellier*, 1971.

(received 20.08.2006, in revised form 16.11.2007)

Faculty of Civil Engineering, University of Belgrade, Bulevar Kralja Aleksandra 73, 11000 Beograd, Serbia

E-mail: eric@grf.bg.ac.yu