CREATIVE MATH.
13 (2004), 5 - 10

A Theorem of Division with a Remainder in a Set of Polynomials with Several Variables

Marcel Migdalovici

Abstract. The set of polynomials of several variables with coefficients in factorial ring (such as the integers ring) has not provided a structure of Euclidean ring and implicitly do not permit Euclid algorithm to perform the greatest common divisor of two or more polynomials.

In this work is performed a division theorem with a remainder in the set of polynomials of several variables with coefficients in a factorial ring.

This theorem underline the possibility to do a new definition of Euclidean ring and a new algorithm to perform the greatest common divisor of two or more polynomials of several variables.

The algorithm for performing the greatest common divisor of polynomials with several variables may be used to determine an analytical inverse matrix for a matrix of such polynomials that intervene in a mathematical modeling of mechanical phenomena.

1. Introductional notions

A unitary and commutative ring K without divisors of zero is named an integral domain. We write briefly K i.d.

Let K a factorial ring, therefore an integral domain with the property that every non zero and non invertible element of K is a product of prime elements of K. We write K f.r.

If $a, b \in K$ we say that a divide b if $b = ac$ with $c \in$K and will write $a \mid b$.

A non zero and non invertible element $p \in K$ is named “prime” if for any $a, b \in K$ with $p \mid ab$ it results $p \mid a$ or $p \mid b$.

An element $c \in K$ (if exist) is named a greatest common divisor of a and b if $c \mid a$, $c \mid b$ and if $d \mid a$, $d \mid b$ then $d \mid c$. Is denoted $c = (a, b)$.

If $d_1 = (a, b)$, $d_2 = (a, b)$ then exists $u \in K$, invertible such that $d_1 = ud_2$.

Two elements d_1, $d_2 \in K$ such that exists $u \in K$ invertible, with $d_1 = ud_2$ are named adjoints in divisibility.

The elements $a, b \in K$ such that $(a, b) = 1$ are named relatively prime.

The ring of polynomials of one variable with coefficients in K is denoted by $K[X]$ and the ring of polynomials of several variable $X_1, \ldots, X_n$ with coefficients in K is denoted by $K[X_1, ..., X_n]$.

If K i.d. and f$\in$K[X] of the form

$$f = a_o + a_1 X + \ldots + a_n X^n \tag{1.1}$$

is denoted by $c(f) \in K$ the greatest common divisor (g.c.d.) for the coefficients $a_i \in K$, $(i = 1, \ldots, n)$ of polynomial f.

If $f \in K[X]$ is of the form (1.1) and $a \in K$ with $a \mid f$ then $a \mid a_i$, $i = 1, \ldots, n$ where $a_i \in K$.

Received: 13.09.2004. In revised form: 29.11.2004

2000 *Mathematics Subject Classification.* 11C08, 13B25, 13P05.

Key words and phrases. *Polynomials, division with a remainder, Euclidean ring.*

If $g \in K[X]$ and $c(g) = 1$ we say that g is primal polynomial.

Is denoted by $K_0[X_m]$ the ring of polynomials in indeterminate X_m over ring $K_0 = K[X_1, ..., X_{m-1}, X_{m+1}, ..., X_n]$ where $m \leq n$. A polynomial $g \in K_0[X_m]$ is of the form

$$g = b_0 + b_1 X_m + \cdots + b_n X_m^n \tag{1.2}$$

where $b_0, b_1, \ldots, b_n \in K_0$ are polynomials from the ring $K[X_1, \ldots, X_{m-1}, X_{m+1}, \ldots, X_n]$.

If K is i.d. then $K[X]$ is i.d. and if K is f.r. then $K[X]$ is f.r.

If K is f.r., $f, g, h \in K[X]$ and f, g are relatively prime such that $f \mid gh$ then $f \mid h$.

We will use the following property [1]:

Theorem 1. *Let f and $g \neq 0$ be polynomials in $R[X]$, R a ring, and let p be degree and b_p the leading coefficient of g. Then there exists a $k \in N$ and polynomials q and $r \in R[X]$ with deg $r <$ deg g such that*

$$b_p^k f = qg + r \tag{1.3}$$

where $k = \max(0, deg\, f - deg\, g + 1)$.

2. A division with a remainder theorem for $K[X_1, \ldots, X_n]$

Let K factorial ring and $0 < m \leq n$, with $m, n \in \mathbb{N}$.

We formulate bellow the following:

Theorem 2. *If a polynomials $p_1, p_2 \in K[X_1, \ldots, X_n]$, $p_1 \neq 0$, $p_2 \neq 0$, for fixed m exists a polynomials $q_1, q_2, r \in K[X_1, \ldots, X_n]$, uniques without a adjointly in divisibility, such that*

$$p_1 q_1 = p_2 q_2 + r \tag{2.4}$$

where $r = 0$ or $deg\, r < deg\, p_2$, with degree refereed to variable m.

The polynomials q_1, q_2, r are relatively prime and $q_1 \neq 0$.

Proof. In the following all polynomials are considered as polynomials in the variable X_m. If $\deg p_1 < \deg p_2$ the relation (2.4) is determined by considering $q_1 = 1$, $q_2 = 0$, $r = p_1$.

For $\deg p_1 \geq \deg p_2$ we use the relation (1.3) of the theorem 1, where $R[X]$ is $K_0(X_m)$ is the ring of polynomials with variable X_m with coefficients from K_0 in the variables X_i, $i = 1, \ldots, n$, $i \neq m$,

$$b_p^k p_1 = q p_2 + r^* \tag{2.5}$$

where b_p is the leading coefficient of p_2 refereed to variable X_m, that is b_p is polynomial from the ring $K[X_1, \ldots, X_{m-1}, X_{m+1}, \ldots, X_n]$, and where $k = \max(0, \deg p_1 - \deg p_2 + 1)$.

Let d be the greatest common divisor of polynomials b_p^k and q as the polynomials of ring K[X$_1$,..., X$_n$]. Because b_p^k is a polynomial no more than $n-1$ variables then d is a polynomial no more than $n-1$ variables. Polynomial d is also divisor of polynomial r^* because

$$b_p^k p_1 - q p_2 = r^*. \tag{2.6}$$

We simplify the relation (2.5) with polynomial d and it follows:

$$q_1 p_1 = q_2 p_2 + r \tag{2.7}$$

where are denoted by q_1 , q_2 and r the polynomials $b_p^k\ q$, respectively r^* divided by d.

The polynomials q_1, q_2, r are relatively prime from your deduction and $q_1 \neq 0$ because $p_2 \neq 0$.

We study the uniqueness of the relationship (2.4). Suppose the existence of the second division relationship of the polynomials p_1 and p_2 such that

$$p_1 q_1' = p_2 q_2' + r' \tag{2.8}$$

where the polynomials q_1', q_2', r' are relatively prime and $q_1' \neq 0$.

From (2.4) and (2.8) it follows that

$$p_2(q_1' q_2 - q_1 q_2') = r' q_1 - r q_1' \tag{2.9}$$

If $q_1' q_2 - q_1 q_2' \neq 0$ then $\deg(r' q_1 - r q_1') \geq \deg p_2$ as polynomials in X_m.

But $\deg r < \deg p_2$ and $\deg r' < \deg p_2$ then $\deg(r' q_1 - r q_1') < \deg p_2$. Contradiction. It follows $q_1' q_2 - q_1 q_2' = 0$ and $r' q_1 - r q_1' = 0$.

Because $q_1 \mid q_1' q_2$ and q_1, q_2 are relatively prime it follows that $q_1 \mid q_1'$. Analogue, from $r' q_1 = r q_1'$ and $q_1' \mid r' q_1$ with q_1', r' relatively prime, we deduce that $q_1' \mid q_1$ such that q_1 and q_1' are adjointly in divisibility.

From $r' q_1 = r q_1'$ and q_1, q_1' adjointly in divisibility, it follows that r, r' are adjointly in divisibility. □

3. The Euclid's type algorithm in the factorial ring $K[X_1, \ldots X_n]$

We suppose that K is factorial ring and $0 < m \leq n$, with $m, n \in N$.

Let $p_1, p_2 \in K[X_1, \ldots, X_n]$, $p_1 \neq 0$, $p_2 \neq 0$. From the second theorem, for fixed m exists a polynomials $q_1, q_2, r \in K[X_1, \ldots, X_n]$, uniques without a adjointly in divisibility, such that

$$p_1 q_1 = p_2 q_2 + r \tag{3.10}$$

where $r = 0$ or $\deg r < \deg p_2$, with degree refereed to variable m.

The polynomials q_1, q_2, r are relatively prime and $q_1 \neq 0$.

There is the following property:

Theorem 3. *In the conditions of second theorem, is true the equality* $D(p_1, p_2)$=$D(p_2, r)$*, where* r *is the remainder of the division of the polynomials* p_1 *and* p_2*, and where* $D(f, g)$ *is the set of polynomials greatest common divisors of* f *and* g*.*

Proof. We suppose, for beginning, that p_1 and p_2 are primal polynomials. It is sufficiently to provide the property for the set of prime divisors.

Let $d \in D(p_1, p_2)$, d prime polynomial and $d \mid p_1$, $d \mid p_2$. But $r = p_1 q_1 - p_2 q_2$. Then $d \mid r$ and thus $d \in D(p_2, r)$, such that $D(p_1, p_2) \subseteq D(p_2, r)$.

Conversely, let d be prime polynomial, $d \in D(p_2, r)$. Then d_2 and $d \mid r$. Thus $d \mid p_1 q_1$ because $p_1 q_1 = p_2 q_2 + r$. But d is prime polynomial, therefore $d \mid p_1$ or $d \mid q_1$. Because $d \mid p_2$ and p_2 primal polynomial it follows d is primal polynomial. If $d \mid q_1$ than d is polynomial independent of X_m and because $d \mid p_2$ it follows d

divide the coefficients of p_2. Contradiction, because p_2 is primal polynomial. Then $d \mid p_1$, such that $d \in D(p_1, p_2)$. Thus $D(p_1, p_2) \supseteq D(p_2, r)$.

We denote by $D'(p_1, p_2)$ the set of polynomials common divisors of coefficients for p_1 and p_2.

If p_1, p_2 are not primal polynomials and d, prime polynomial, divide the coefficients of polynomials p_1 and p_2 then d divide the polynomial r and thus the coefficients of polynomial r, such that $D'(p_1, p_2) \subseteq D'(p_2, r)$. If d divide the coefficients of polynomials p_2 and r then d divide $p_1 q_1$. If $d \mid q_1$ then q_1 and r are not relative prime. It follows $d \mid p_1$, such that d divide the coefficients of p_1, thus $D'(p_1, p_2) \supseteq D'(p_2, r)$. □

This theorem permits to give an Euclid's type algorithm for performing the greatest common divisor of two polynomials of several variables with coefficients in factorial ring.

We suppose that $\deg p_1 \geq \deg p_2$. From the third theorem applied to polynomials p_1 and p_2 we obtain that $D(p_1, p_2) = D(p_2, r)$, where r is the remainder of division for p_1, p_2. If $r = 0$ then $(p_1, p_2) = p_2$. If $r \neq 0$ then $\deg r < \deg p_2$.

Apply the third theorem polynomials p_2 and r. We can write:

$$p_2 q_1' = r q_2' + r_1 \tag{3.11}$$

If $r_1 = 0$ then $(p_1, p_2) = (p_2, r) = r$. If $r_1 \neq 0$ then:

$$\deg p_1 \geq \deg p_2 > \deg r > \deg r_1 > \dots \tag{3.12}$$

and $(p_1, p_2) = (p_2, r) = (r, r_1) = \dots$ such that after a finite number of steps is obtained a zero remainder. The latest non zero divisor in the row (3.12) is the greatest common divisor of polynomials p_1 and p_2.

4. Applications

4.1. **The greatest common divisor of polynomials** $p_1 = X^3 + Y^3 + Z^3 - 3XYZ$**,** $p_2 = X + Y + Z$**.**

We choose the variable Z for division. Polynomials p_1 and p_2 ordered are of the form:

$$p_1 = Z^3 - 3XYZ + (X^3 + Y^3), \quad p_2 = Z + (X + Y) \tag{4.13}$$

The first relation of division is: $p_1 = p_2\big(Z^2 - (X + Y)Z + (X^2 + Y^2 - XY)\big)$.

Thus the greatest common divisor of p_1 and p_2 is p_2.

4.2. **The greatest common divisor of polynomials** $\mathbf{p_1 = 2X^2 + (2Z + 1)X + (-2Y^2 - 2YZ + Y + Z)}$**,** $\mathbf{p_2 = 2X^2 + (4Y + 2Z + 1)X + (2Y^2 + 2YZ + Y + Z)}$**.** The first relation of division is: $p_1 = p_2 - 4Y(X + Y + Z)$ or $p_1 = p_2 + r$.

The second relation of division is $(-4Y)p_2 = r(2X + 2Y + 1)$. But $-4Y \mid r$. Thus the second relation of division is $p_2 = r'(2X + 2Y + 1)$ with $r' = X + Y + Z$. The greatest common divisor is r'.

4.3. **Inversion of matrix of polynomials with several variables.**

In this subheading is described an inverse matrix of a matrix of several variable that intervene in the mechanical modeling of the plane shapes.

The inverse matrix of the matrix $[p_{ij}]$, i, $j = 1, \ldots, 8$, is denoted by $[q_{ij} \mid q_i]$, i, $j = 1, \ldots, 8$, and is deduced by reduce the fractions of polynomials. The expression of the coefficients is:

$$\begin{aligned}
&p_{14} = -b, p_{16} = a, p_{25} = a, p_{26} = -b, p_{37} = 2ab, p_{48} = -2ab, p_{51} = 1,\\
&p_{53} = -b, p_{54} = -a, p_{55} = pa, p_{56} = b(1+p), p_{62} = 1, p_{63} = -a\\
&p_{64} = -bp, p_{66} = -a(1+p), p_{73} = b, p_{74} = -a, p_{75} = ap,\\
&p_{76} = -b(1+p), p_{77} = a^2+b^2, p_{83} = -a, p_{84} = bp, p_{85} = -b,\\
&p_{86} = -a(1+p), p_{88} = -(a^2+b^2).
\end{aligned}$$

In the rest, the values of p_{ij} are zero.

$$\begin{aligned}
&q_{11} = -4a^2b^2(1+p)(2a^2+b^2-b^2p), q_{12} = -4a^3b^3(1+p)^2,\\
&q_{13} = (a^2+b^2)(a^4-2a^2b^2-b^4-2a^2b^2p), q_{14} = 2ab(a^2+b^2)(a^2-b^2p),\\
&q_{15} = 2ab(a^2+b^2)^2, q_{17} = -2ab(a^4-2a^2b^2-b^4-2a^2b^2p),\\
&q_{18} = -4a^2b^2(a^2-b^2p), q_{21} = -4a^3b^3(1+p)^2,\\
&q_{22} = -4a^2b^2(1+p)(2b^2+a^2-a^2p), q_{23} = 2ab(a^2+b^2)(-b^2+a^2p),\\
&q_{24} = (a^2+b^2)(2b^2+a^2-a^2p), q_{26} = 2ab(a^2+b^2)^2, q_{27} = -4a^2b^2(a^2p-b^2),\\
&q_{28} = -2ab(a^4+2a^2b^2-b^4+2a^2b^2p), q_{31} = 2a^2b(1+p), q_{32} = 2ab^2(1+p),\\
&q_{33} = b(a^2+b^2), q_{34} = -a(a^2+b^2), q_{37} - 2ab^2, q_{38} = 2a^2b,\\
&q_{41} = -2b^2(2a^2+b^2+a^2p), q_{42} = -2ab(b^2-a^2p), q_{43} = a^2(a^2+b^2),\\
&q_{44} = ab(a^2+b^2), q_{47} = -2a^3b, q_{48} = -2a^2b^2, q_{51} = -2ab(a^2-b^2p),\\
&q_{52} = -2a^2(a^2+2b^2+b^2p), q_{53} = -ab(a^2+b^2), q_{54} = -b^2(a^2+b^2),\\
&q_{57} = 2a^2b^2, q_{58} = 2ab^3, q_{61} = -2a(a^2-b^2p), q_{62} = 2b(b^2-a^2p),\\
&q_{63} = -a(a^2+b^2), q_{64} = -b(a^2+b^2), q_{67} = 2a^2b, q_{68} = 2ab^2, q_{73} = 1, q_{84} = 1
\end{aligned}$$

In the rest the values of q_{ij} are zero.

$$\begin{aligned}
&q_1 = 2ab(a^2+b^2)^2,\ q_2 = 2ab(a^2+b^2)^2,\ q_1 = -2ab(a^2+b^2), q_4 = 2b(a^2+b^2)^2,\\
&q_5 = -2a(a^2+b^2)^2,\ q_6 = -2(a^2+b^2)^2,\ q_7 = 2ab, q_8 = -2ab.
\end{aligned}$$

5. A new definition of Euclidean ring

N. Jacobson, in the treatise "Basic Algebra" give the following definition of Euclidean ring:

A domain of integrity D is called Euclidean if there exists a map $\delta : D \to N$, of D into the set N of non-negative integers, such that if $a, b \neq 0 \in D$, then there exist $q, r \in D$ such that $a = bq + r$ where $\delta(r) < \delta(b)$.

We propose the following definition of Euclidean ring:

A factorial ring D is called Euclidean if there exists a map $\delta : D \to N$, of D into the set N of non-negative integers, such that if $a, b \neq 0 \in D$, then there exist $q_1, q_2, r \in D$ such that $aq_1 = bq_2 + r$ where $\delta(r) < \delta(b)$ and q_1, q_2, r are relatively prime.

6. Acknowledgements

Thanks to the CNCSIS-Bucharest for its financial support through the Grant nr.33344 | 2004, theme A3.

References

[1] Ion, D. Ion, Niţă, C., Năstăsescu, C., *Complemente de algebră,* Editura Ştiinţifică şi Enciclopedică, 1984
[2] Jacobson, N., *Basic Algebra*, vol.I, Editura FREEMAN, San Francisco, 1973
[3] Migdalovici, M., *Automatizarea calculului structurilor mecanice cu aplicaţii la C.N.E.*, Teză de doctorat, 1985
[4] Năstăsescu, C., Niţă, C., Vraciu, C., *Bazele Algebrei*, vol. **I**, Editura Academiei, Bucureşti, 1986

Institute of Solid Mechanics Bucharest
Romania
E-mail address: migdal@imsar.bu.edu.ro