DECOMPOSITION OF POLYNOMIALS AND APPROXIMATE ROOTS

ARNAUD BODIN

Abstract. We state a kind of Euclidian division theorem: given a polynomial $P(x)$ and a divisor d of the degree of P, there exist polynomials $h(x), Q(x), R(x)$ such that $P(x) = h \circ Q(x) + R(x)$, with $\deg h = d$. Under some conditions h, Q, R are unique, and Q is the approximate d-root of P. Moreover we give an algorithm to compute such a decomposition. We apply these results to decide whether a polynomial in one or several variables is decomposable or not.

1. Introduction

Let A be an integral domain (i.e. a unitary commutative ring without zero divisors). Our main result is:

Theorem 1. *Let $P \in A[x]$ be a monic polynomial. Let $d \geqslant 2$ such that d is a divisor of $\deg P$ and d is invertible in A. There exist $h, Q, R \in A[x]$ such that*

$$P(x) = h \circ Q(x) + R(x)$$

with the conditions that

(i) *h, Q are monic;*
(ii) *$\deg h = d$, $\operatorname{coeff}(h, x^{d-1}) = 0$, $\deg R < \deg P - \frac{\deg P}{d}$;*
(iii) *$R(x) = \sum_i r_i x^i$ with $(\deg Q | i \Rightarrow r_i = 0)$.*

Moreover such h, Q, R are unique.

The previous theorem has a formulation similar to the Euclidian division; but here Q is not given (only its degree is fixed); there is a natural Q (that we will compute, see Corollary 2) associated to P and d. Notice also that the decomposition $P(x) = h \circ Q(x) + R(x)$ is *not* the Q-adic decomposition, since the coefficients before the powers $Q^i(x)$ belong to A and not to $A[x]$.

Date: October 16, 2009.
2000 *Mathematics Subject Classification.* 13B25.
Key words and phrases. Decomposable and indecomposable polynomials in one or several variables.

Example. Let $P(x) = x^6 + 6x^5 + 6x + 1 \in \mathbb{Q}[x]$. If $d = 6$ we find the following decomposition $P(x) = h \circ Q(x) + R(x)$ with $h(x) = x^6 - 15x^4 + 40x^3 - 45x^2 + 30x - 10$, $Q(x) = x + 1$ and $R(x) = 0$. If $d = 3$ we have $h(x) = x^3 + 65$, $Q(x) = x^2 + 2x - 4$ and $R(x) = 40x^3 - 90x$. If $d = 2$ we get $h(x) = x^2 - \frac{725}{4}$, $Q(x) = x^3 + 3x^2 - \frac{9}{2}x + \frac{27}{2}$ and $R(x) = -\frac{405}{4}x^2 + \frac{255}{2}x$.

Theorem 1 will be of special interest when then ring A is itself a polynomial ring. For instance at the end of the paper we give an example of a decomposition of a polynomial in two variables $P(x, y) \in A[x]$ for $A = K[y]$.

The polynomial Q that appears in the decomposition has already been introduced in a rather different context. We denote by $\sqrt[d]{P}$ the approximate d-root of P. It is the polynomial such that $(\sqrt[d]{P})^d$ approximate P in a best way, that is to say $P - (\sqrt[d]{P})^d$ has smallest possible degree. The precise definition will be given in section 2, but we already notice the following:

Corollary 2.

$$Q = \sqrt[d]{P}$$

We apply these results to another situation. Let $A = K$ be a field and $d \geqslant 2$. $P \in K[x]$ is said to be *d-decomposable* in $K[x]$ if there exist $h, Q \in K[x]$, with $\deg h = d$ such that

$$P(x) = h \circ Q(x).$$

Corollary 3. *Let $A = K$ be a field. Suppose that* $\operatorname{char} K$ *does not divide d. P is d-decomposable in $K[x]$ if and only if $R = 0$ in the decomposition of Theorem 1.*

In particular, if P is d-decomposable, then $P = h \circ Q$ with $Q = \sqrt[d]{P}$.

After the first version of this paper, M. Ayad and G. Chèze communicated us some references so that we can picture a part of history of the subject. Approximate roots appeared (for $d = 2$) in some work of E.D. Rainville [9] to find polynomial solutions of some Riccati type differential equations. An approximate root was seen as the polynomial part of the expansion of $P(x)^{\frac{1}{d}}$ into decreasing powers of x. The use of approximate roots culminated with S.S. Abhyankar and T.T. Moh who proved the so-called Abhyankar-Moh-Suzuki theorem in [1] and [2]. For the latest subject we refer the reader to an excellent expository article of P. Popescu-Pampu [8]. On the other hand Ritt's decompostion theorems (see [10] for example) have led to several practical algorithms to decompose polynomials in one variable into the form $P(x) = h \circ Q(x)$: for example D. Kozen and S. Landau in [6] give an algorithm (refined in [5]) that computes a decomposition in polynomial time. Unification of both subjects starts with P.R. Lazov and A.F. Beardon ([7], [3]) for polynomials in one variable over complex numbers: they notice that the polynomial Q is in fact the approximate d-root of P.

We define approximate roots in section 2 and prove uniqueness of the decomposition of Theorem 1. Then in section 3 we prove the existence of such decomposition and give an algorithm to compute it. Finally in section 4 we apply these results to decomposable polynomials in one variable and in section 5 to decomposable polynomials in several variables.

2. Approximate roots and proof of the uniqueness

The approximate roots of a polynomial are defined by the following property, [1], [8, Proposition 3.1].

Proposition 4. *Let $P \in A[x]$ a monic polynomial and $d \geqslant 2$ such that d is a divisor of $\deg P$ and d is invertible in A. There exists a unique monic polynomial $Q \in A[x]$ such that:*

$$\deg(P - Q^d) < \deg P - \frac{\deg P}{d}.$$

We call Q the *approximate d-root* of P and denote it by $\sqrt[d]{P}$.

Let us recall the proof from [8].

Proof. Write $P(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n$ and we search an equation for $Q(x) = x^{\frac{n}{d}} + b_1 x^{\frac{n}{d}-1} + b_2 x^{\frac{n}{d}-2} + \cdots + b_{\frac{n}{d}}$. We want $\deg(P - Q^d) < \deg P - \frac{\deg P}{d}$, that is to say, the coefficients of $x^n, x^{n-1}, \ldots, x^{n-\frac{n}{d}}$ in $P - Q^d$ equal zero. By expanding Q^d we get the following system of equations:

$$(\mathcal{S}) \quad \begin{cases} a_1 = db_1 \\ a_2 = db_2 + \binom{d}{2} b_1^2 \\ \vdots \\ a_k = db_k + \displaystyle\sum_{i_1 + 2i_2 + \cdots + (k-1)i_{k-1} = k} c_{i_1 \ldots i_{k-1}} b_1^{i_1} \cdots b_{k-1}^{i_{k-1}}, \qquad 1 \leqslant k \leqslant \frac{n}{d} \end{cases}$$

where the coefficients $c_{i_1 \ldots i_{k-1}}$ are the multinomial coefficients defined by the following formula:

$$c_{i_1 \ldots i_{k-1}} = \binom{d}{i_1, \ldots, i_{k-1}} = \frac{d!}{i_1! \cdots i_{k-1}!(d - i_1 - \cdots - i_{k-1})!}.$$

The system $(\mathcal{S})$ being a triangular system, we can inductively compute the b_i for $i = 1, 2, \ldots, \frac{n}{d}$: $b_1 = \frac{a_1}{d}$, $b_2 = \frac{a_2 - \binom{d}{2} b_1^2}{d}$, ... Hence the system $(\mathcal{S})$ admits one and only one solution $b_1, b_2, \ldots, b_{\frac{n}{d}}$.

Notice that we need d to be invertible in A to compute b_i. Moreover b_i depends only on the first coefficients $a_1, a_2, \ldots, a_{\frac{n}{d}}$ of P. $\square$

Proposition 4 enables us to prove Corollary 2: by condition (ii) of Theorem 1 we know that $\deg(P - Q^d) < \deg P - \frac{\deg P}{d}$ so that Q is the approximate d-root of P. Another way to compute $\sqrt[d]{P}$ is to use iterations of Tschirnhausen transformation, see [1] or [8, Proposition 6.3]. We end this section by proving uniqueness of the decomposition of Theorem 1.

Proof. Q is the approximate d-root of P so is unique (see Proposition 4 above). In order to prove the uniqueness of h and R, we argue by contradiction. Suppose $h \circ Q + R = h' \circ Q + R'$ with $R \neq R'$; set $r_i x^i$ to be the highest monomial of $R(x) - R'(x)$. From one hand x^i is a monomial of R or R', hence $\deg Q \nmid i$ by condition (iii) of Theorem 1. From the equality $(h' - h) \circ Q = R - R'$ we deduce that $i = \deg(R - R')$ is a multiple of $\deg Q$; that yields a contradiction. Therefore $R = R'$, hence $h = h'$. $\square$

3. Algorithm and proof of the existence

Here is an algorithm to compute the decomposition of Theorem 1.

Algorithm 5.

- ***Input.*** *$P \in A[x]$, $d | \deg P$.*
- ***Output.*** *$h, Q, R \in A[x]$ such that $P = h \circ Q + R$.*
- ***1st step.*** *Compute $Q = \sqrt[d]{P}$ by solving the triangular system $(\mathcal{S})$ of Proposition 4. Set $h_1(x) = x^d$, $R_1(x) = 0$.*
- ***2nd step.*** *Compute $P_2 = P - Q^d = P - h_1(Q) - R_1$. Look for its highest monomial $a_i x^i$. If $\deg Q | i$ then set $h_2(x) = h_1(x) + a_i x^{\frac{i}{\deg Q}}$, $R_2 = R_1$. If $\deg Q \nmid i$ then $R_2(x) = R_1(x) + a_i x^i$, $h_2 = h_1$.*
- ***3thd step.*** *Set $P_3 = P - h_2(Q) - R_2$, look for its highest monomial $a_i x^i$,...*
- ...
- ***Final step.*** *$P_n = P - h_{n-1}(Q) - R_{n-1} = 0$ yields the decomposition $P = h \circ Q + R$ with $h = h_{n-1}$ and $R = R_{n-1}$.*

The algorithm terminates because the degree of the P_i decreases at each step. It yields a decomposition $P = h \circ Q + R$ that verifies all the conditions of Theorem 1: in the second step of the algorithm, and due to Proposition 4 we know that $i < \deg P - \frac{\deg P}{d}$. That implies $\mathrm{coeff}(h_2, x^{d-1}) = 0$ and $\deg R_2 < \deg P - \frac{\deg P}{d}$. Therefore at the end $\mathrm{coeff}(h, x^{d-1}) = 0$. Of course the algorithm proves the existence of the decomposition in Theorem 1.

4. Decomposable polynomials in one variable

Let K be a field and $d \geqslant 2$. $P \in K[x]$ is said to be *d-decomposable* in $K[x]$ if there exist $h, Q \in K[x]$, with $\deg h = d$ such that

$$P(x) = h \circ Q(x).$$

We refer to [4] for references and recent results on decomposable polynomials in one and several variables.

Proposition 6. *Let $A = K$ be a field whose characteristic does not divide d. A monic polynomial P is d-decomposable in $K[x]$ if and only if $R = 0$ in the decomposition $P = h \circ Q + R$.*

In view of Algorithm 5 we also get an algorithm to decide whether a polynomial is decomposable or not and in the positive case give its decomposition.

Proof. If $R = 0$ then P is d-decomposable. Conversly if P is d-decomposable, then there exist $h, Q \in K[x]$ such that $P = h(Q)$. As P is monic we can suppose h, Q monic. Moreover, up to a linear change of coordinates $x \mapsto x + \alpha$, we can suppose that $\mathrm{coeff}(h, x^{d-1}) = 0$. Therefore $P = h(Q)$ is a decomposition that verifies the conditions of Theorem 1. $\square$

Remark. Let $P(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, we first consider $a_1, \ldots, a_n$ as indeterminates (i.e. P is seen as an element of $K(a_1, \ldots, a_n)[x]$). The coefficients of $h(x), Q(x)$ and $R(x) = r_0 x^k + r_1 x^{k-1} + \cdots + r_k$ (computed by Proposition 4, the system $(\mathcal{S})$ and Algorithm 5) are polynomials in the a_i, in particular $r_i = r_i(a_1, \ldots, a_n) \in K[a_1, \ldots, a_n]$, $i = 0, \ldots, k$.

Now we consider $a_1^*, \ldots, a_n^* \in K$ as specializations of $a_1, \ldots, a_n$ and denote by P^* the specialization of P at $a_1^*, \ldots, a_n^*$. Then, by Proposition 6, P^* is d-decomposable in $K[x]$ if and only if $r_i(a_1^*, \ldots, a_n^*) = 0$ for all $i = 0, \ldots, k$. It expresses the set of d-decomposable monic polynomials of degree n as an affine algebraic variety. We give explicit equations in the following example.

Example. Let K be a field of characteristic different from 2. Let $P(x) = x^6 + a_1 x^5 + a_2 x^4 + a_3 x^3 + a_4 x^2 + a_5 x + a_6$ be a monic polynomial of degree 6 in $K[x]$ (the $a_i \in K$ being indeterminates). Let $d = 2$. We first look for the approximate 2-root of $P(x)$. $\sqrt[2]{P(x)} = Q(x) = x^3 + b_1 x^2 + b_2 x + b_3$. In view of the triangular system $(\mathcal{S})$ we get

$$b_1 = \frac{a_1}{2}, \quad b_2 = \frac{a_2 - b_1^2}{2}, \quad b_3 = \frac{a_3 - 2b_1 b_2}{2}.$$

Once we have computed Q, we get $h(x) = x^2 + a_6 - b_3^2$. Therefore

$$R(x) = (a_4 - 2b_1 b_3 - b_2^2)x^2 + (a_5 - 2b_2 b_3)x.$$

Now $P(x)$ is 2-decomposable in $K[x]$ if and only if $R(x) = 0$ in $K[x]$ that is to say if and only if $(a_1, \ldots, a_6)$ satifies the polynomial system of equations in $a_1, \ldots, a_5$:

$$\begin{cases} a_4 - 2b_1 b_3 - b_2^2 = 0, \\ a_5 - 2b_2 b_3 = 0. \end{cases}$$

5. Decomposable polynomials in several variables

Again K is a field and $d \geqslant 2$. Set $n \geqslant 2$. $P \in K[x_1, \ldots, x_n]$ is said to be *d-decomposable* in $K[x_1, \ldots, x_n]$ if there exist $Q \in K[x_1, \ldots, x_n]$, and $h \in K[t]$ with $\deg h = d$, such that

$$P(x_1, \ldots, x_n) = h \circ Q(x_1, \ldots, x_n).$$

Proposition 7. *Let $A = K[x_2, \ldots, x_n]$, $P \in A[x_1] = K[x_1, \ldots, x_n]$ monic in x_1. Fix d that divides $\deg_{x_1} P$, such that $\operatorname{char} K$ does not divide d. P is d-decomposable in $K[x_1, \ldots, x_n]$ if and only if the decomposition $P = h \circ Q + R$ of Theorem 1 in $A[x_1]$ verifies $R = 0$ and $h \in K[t]$ (instead of $h \in K[t, x_2, \ldots, x_n]$).*

Proof. If P admits a decomposition as in Theorem 1 with $R = 0$ and $h \in K[t]$ then $P = h \circ Q$ is d-decomposable.

Conversly if P is d-decomposable in $K[x_1, \ldots, x_n]$ then $P = h \circ Q$ with $h \in K[t]$, $Q \in K[x_1, \ldots, x_n]$. As P is monic in x_1 we may suppose that h is monic and Q is monic in x_1. We can also suppose $\operatorname{coeff}(h, t^{d-1}) = 0$. Therefore h, Q and $R := 0$ verify the conditions of Theorem 1 in $A[x]$. As such a decomposition is unique, it ends the proof. $\square$

Example. Set $A = K[y]$ and let $P(x) = x^6 + a_1 x^5 + a_2 x^4 + a_3 x^3 + a_4 x^2 + a_5 x + a_6$ be a monic polynomial of degree 6 in $A[x] = K[x, y]$, with coefficients $a_i = a_i(y) \in A = K[y]$. In the example of section 4 we have computed the decomposition $P = h \circ Q + R$ for $d = 2$ and set $b_1 = \frac{a_1}{2}$, $b_2 = \frac{a_2 - b_1^2}{2}$, $b_3 = \frac{a_3 - 2b_1 b_2}{2}$. We found $h(t) = t^2 + a_6 - b_3^2 \in A[t]$

and $R(x) = (a_4 - 2b_1b_3 - b_2^2)x^2 + (a_5 - 2b_2b_3)x \in A[x]$. By Proposition 7 above, we get that P is 2-decomposable in $K[x,y]$ if and only

$$\begin{cases} a_6 - b_3^2 \in K, \\ a_4 - 2b_1b_3 - b_2^2 = 0 \quad \text{in } K[y], \\ a_5 - 2b_2b_3 = 0 \quad \text{in } K[y]. \end{cases}$$

Each line yields a system of polynomial equations in the coefficients $a_{ij} \in K$ of $P(x,y) = \sum a_{ij}x^iy^j \in K[x,y]$. In particular the set of 2-decomposable monic polynomials of degree 6 in $K[x,y]$ is an affine algebraic variety.

References

[1] S.S. Abhyankar, T.T. Moh, *Newton-Puiseux expansion and generalized Tschirnhausen transformation.* J. Reine Angew. Math. 260 (1973), 47–83 and 261 (1973), 29–54.

[2] S.S. Abhyankar, T.T. Moh, *Embeddings of the line in the plane.* J. Reine Angew. Math. 276 (1975), 148–166.

[3] A.F. Beardon, *Composition factors of polynomials.* The Chuang special issue. Complex Variables Theory Appl. 43 (2001), 225–239.

[4] A. Bodin, P. Dèbes, S. Najib, *Indecomposable polynomials and their spectrum.* Acta Arith. 139 (2009), 79–100.

[5] J.v.z. Gathen, *Functional decomposition of polynomials: the tame case.* J. Symb. Comp. 9 (1990), 281–299.

[6] D. Kozen, S. Landau, *Polynomial decomposition algorithms.* J. Symb. Comp. 7 (1989), 445–456.

[7] P.R. Lazov, *A criterion for polynomial decomposition.* Mat. Bilten 45 (1995), 43–52.

[8] P. Popescu-Pampu, *Approximate roots.* Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999), Fields Inst. Commun. 33, Amer. Math. Soc. (2003), 285–321.

[9] E.D. Rainville, *Necessary conditions for polynomial solutions of certain Riccati equations.* Amer. Math. Monthly 43 (1936), 473–476.

[10] A. Schinzel, *Polynomials with special regard to reducibility.* Encyclopedia of Mathematics and its Applications, 77. Cambridge University Press, Cambridge, 2000.

Laboratoire Paul Painlevé, Mathématiques, Université de Lille 1, 59655 Villeneuve d'Ascq, France.

E-mail address: `Arnaud.Bodin@math.univ-lille1.fr`