HAL open science

On powers of polynomials

Rodney Coleman, Laurent Zwald

To cite this version:

Rodney Coleman, Laurent Zwald. On powers of polynomials. 2014. hal-01001707

HAL Id: hal-01001707

https://hal.science/hal-01001707v1

Preprint submitted on 4 Jun 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On Powers of Polynomials

Rodney Coleman, Laurent Zwald
Laboratoire Jean Kuntzmann
Domaine Universitaire de Saint-Martin-d'Hères, France.

Abstract

The aim of this short note is to show that, under certain conditions, when the coefficients of a power of a polynomial over a field lie in a subfield, then the coefficients of the polynomial itself lie in the subfield.

Let K be a field and k a subfield of K. If $P(X) \in K[X]$, $m \in N^*$ and $P^m(X) \in k[X]$, then in general we cannot say that $P(X) \in k[X]$. For example, if $P(X) = iX \in \mathbb{C}[X]$, then $P^2(X) = -X^2 \in \mathbb{Q}[X]$, or if $P(X) = \sqrt{2} + \frac{1}{\sqrt{2}}X \in \mathbb{R}[X]$, then $P^2(X) = 2 + 2X + \frac{1}{2}X^2 \in \mathbb{Q}[X]$. In both cases the square of the polynomial P lies in a subfield of a field and the polynomial itself does not lie in this subfield. In this note we will show that this cannot occur if the coefficients of the polynomial $P(X)$ satisfy a certain simple condition. To fix our ideas we will initially suppose that $K = \mathbb{C}$ and $k = \mathbb{Q}$. Of course, if $m = 1$ there is nothing to prove, so we will suppose that this is not the case.

Let us write $P(X) = \sum_{i=0}^{n} a_i X^i$, with the $a_i \in \mathbb{C}$. Using the multinomial theorem we obtain

$$P^m(X) = \sum_{k_0+k_1+\cdots+k_n=m} \binom{m}{k_0, k_1, \ldots, k_n} \prod_{0\le t\le n} (a_t X^t)^{k_t},$$

where

$$\binom{m}{k_0, k_1, \ldots, k_n} = \frac{m!}{k_0! k_1! \cdots k_n!}.$$

We will write $Q(X) = P^m(X) = \sum_{j=0}^{mn} b_j X^j$ and at first suppose that $a_0 \neq 0$. Then the coefficient b_s of $X^s \in Q(X)$ may be written

$$b_s = \sum a_0^{k_0} a_1^{k_1} \cdots a_n^{k_n} \binom{m}{k_0, k_1, \ldots, k_n},$$

where

$$k_1 + 2k_2 + \cdots + nk_n = s \tag{1}$$
$$k_0 + k_1 + k_2 + \cdots + k_n = m. \tag{2}$$

If $s = 0$, then from the above equations we obtain $k_0 = m$ and $k_i = 0$ for $i \neq 0$, thus $b_0 = a_0^m$.

If $s = 1$, then, from equation (1) , $k_1 = 1$ and $k_i = 0$ if $i > 1$. Now, using equation (2), we obtain $k_0 = m - 1$ and so $b_1 = m a_0^{m-1} a_1$.

Now let us consider the case $s = 2$. From (1) $k_i = 0$ if $i > 2$ and for (k_1, k_2) we have $(0, 1)$ or $(2, 0)$. From (2) the corresponding values of k_0 are $m - 1$ and $m - 2$. Hence we have

$$b_2 = m a_0^{m-1} a_2 + a_0^{m-2} a_1^2 \binom{m}{m-2, 2}.$$

Continuing, we now consider the case $s = 3$. From (1) we see that $k_i = 0$ if $i > 3$ and for (k_1, k_2, k_3) we have $(0, 0, 1)$, $(1, 1, 0)$ or $(3, 0, 0)$. Using (2) we obtain the corresponding values of k_0, namely $m - 1$, $m - 2$ or $m - 3$. Therefore

$$b_3 = ma_0^{m-1}a_3 + a_0^{m-2}a_1a_2\binom{m}{m-2,1,1} + a_0^{m-3}a_1^3\binom{m}{m-3,3}.$$

We now turn to the general case. One possibility for the k_i's is $k_0 = m - 1$, $k_s = 1$ and $k_i = 0$ for $i \neq 0, s$. This gives us the term $ma_0^{m-1}a_s$. All other possibilities have $k_s = 0$ which from (1) and (2) above gives us

$$\begin{aligned} k_1 + 2k_2 + \cdots + (s-1)k_{s-1} &= s && (3)\\ k_0 + k_1 + k_2 + \cdots + k_{s-1} &= m. && (4) \end{aligned}$$

We thus obtain

$$b_s = ma_0^{m-1}a_s + \sum a_0^{k_0}a_1^{k_1}\cdots a_{s-1}^{k_{s-1}}\binom{m}{k_0, k_1, \ldots, k_{s-1}},$$

where the sum is over the s-tuples $(k_0, k_1, \ldots, k_{s-1})$ satisifying equations (3) and (4) above. (In passing, notice that in all the terms in the sum the power of a_0 is strictly less than $m - 1$.)

Lemma 1 *If $b_j \in \mathbb{Q}$ for all j, then $ma_0^{m-1}a_i \in \mathbb{Q}$ for all $i \geq 1$.*

PROOF We use an induction argument. As $b_1 = ma_0^{m-1}a_1$, the statement is true for $s = 1$. We now suppose that the statement is true up to a given s and consider the case $s + 1$. We have

$$b_{s+1} = ma_0^{m-1}a_{s+1} + \sum a_0^{k_0}a_1^{k_1}\cdots a_s^{k_s}\binom{m}{k_0, k_1, \ldots, k_s},$$

where

$$\begin{aligned} k_1 + 2k_2 + \cdots + sk_s &= s + 1 && (5)\\ k_0 + k_1 + k_2 + \cdots + k_s &= m. && (6) \end{aligned}$$

We can write

$$\begin{aligned} a_0^{k_0}a_1^{k_1}\cdots a_s^{k_s} &= \frac{a_0^{k_0}(ma_0^{m-1}a_1)^{k_1}\cdots(ma_0^{m-1}a_s)^{k_s}}{m^{k_1+\cdots+k_s}a_0^{(m-1)(k_1+\cdots+k_s)}}\\ &= \frac{(ma_0^{m-1}a_1)^{k_1}\cdots(ma_0^{m-1}a_s)^{k_s}}{m^{k_1+\cdots+k_s}a_0^{(m-1)(k_1+\cdots+k_s-1)-k_0}}\\ &= \frac{(ma_0^{m-1}a_1)^{k_1}\cdots(ma_0^{m-1}a_s)^{k_s}}{m^{k_1+\cdots+k_s}a_0^{m(k_1+\cdots+k_s-1)}}. \end{aligned}$$

As $a_0^m = b_0 \in \mathbb{Q}$ and $ma_0^{m-1}a_i \in \mathbb{Q}$, for $i = 1, \ldots, s$, by hypothesis, we have $a_0^{k_0}a_1^{k_1}\cdots a_s^{k_s} \in \mathbb{Q}$. However, $b_{s+1} \in \mathbb{Q}$, so $ma_0^{m-1}a_{s+1} \in \mathbb{Q}$. This finishes the induction step. □

We can now prove our first result on powers of polynomials.

Theorem 1 *Let $P(X) \in \mathbb{C}[X]$ and $m \in \mathbb{N}^*$ and suppose that $Q(X) = P^m(X) \in \mathbb{Q}[X]$. If there is a coefficient a_s of $P(X)$ such that $a_s \in \mathbb{Q}^*$, then $P(X) \in \mathbb{Q}(X]$.*

PROOF Let us first suppose that $a_0 \neq 0$. We will show that $a_0 \in \mathbb{Q}^*$. If $s = 0$, then there is nothing to prove, so let us suppose that $s \neq 0$. From what we have just seen, if $P(X) = \sum_{i=0}^n a_iX^i$, then $a_0^m \in \mathbb{Q}$ and $ma_0^{m-1}a_i \in \mathbb{Q}$ for $i = 1, \ldots, n$. Now

$$\frac{a_0}{ma_s} = \frac{a_0^m}{ma_0^{m-1}a_s} \in \mathbb{Q} \Longrightarrow a_0 \in \mathbb{Q}^*,$$

because $a_s \in \mathbb{Q}^*$. Now suppose that $i \neq 0, s$. Then

$$ma_0^{m-1}a_i \in \mathbb{Q},\ a_0 \in \mathbb{Q}^* \Longrightarrow a_i \in \mathbb{Q}.$$

Thus $P(X) \in \mathbb{Q}[X]$.

To finish we consider the case where the coefficient $a_0 = 0$. If a_u is the first non-zero coefficient, then we may write $P(X) = X^u P_1(X)$, with $P_1(X) = \sum_{i=0}^{n-u} c_i X^i$ and $c_i = a_{i+u}$. Then $P^m(X) = X^{um} P_1^m(X)$ and applying the above argument to $P_1(X)$ gives us the desired result. □

It is not difficult to generalize the result we have proved to a more general situation.

Theorem 2 *Let k be a subfield of a field K and $m \in \mathbb{N}^*$. If the polynomial $P(X) \in K[X]$ is such that $Q(X) = P^m(X) \in k[X]$ and there is a coefficient of $P(X)$, which belongs to k^*, then $P(X) \in k[X]$.*

PROOF If k is of characteristic 0, or of characteristic $p > 0$ and m is not a multiple of p, then we may use an argument analogous to that used in the preceding theorem. Suppose now that k has characteristic $p > 0$ and $m = p^\alpha m'$, with $\alpha \geq 1$ and $(p, m') = 1$. First we notice that

$$P^m(X) = (P^{p^\alpha}(X))^{m'} = P^{m'}(X^{p^\alpha}).$$

Hence $P^{m'}(X^{p^\alpha}) \in k[X]$. However, if $P(X) = \sum_{i=0}^n a_i X^i$, then

$$P(X^{p^\alpha}) = \sum_{i=0}^{n} a_i X^{p^\alpha i} = \sum_{j=0}^{np^\alpha} c_j X^j,$$

with

$$c_j = \begin{cases} a_i & \text{for } j = p^\alpha i, i = 0, \ldots, n \\ 0 & \text{otherwise} \end{cases}.$$

If we write $P_1(X) = \sum_{j=0}^{np^\alpha} c_j X^j$, then $P_1^{m'}(X) \in k[X]$ and one of the coefficients c_j belongs to k^*; also, m' is not a multiple of p. We thus deduce that $P_1(X) \in k[X]$. This completes the proof. □

Corollary 1 *Let k be a subfield of a field K and $m \in \mathbb{N}^*$. If the polynomial $P(X) \in K[X]$ is monic and such that $Q(X) = P^m(X) \in k[X]$, then $P(X) \in k[X]$.*

We might be tempted to generalize Corollary 1 to products of distinct polynomials, i.e., if $P_1(X), \ldots, P_s(X) \in \mathbb{C}[X]$, each having a coefficient in $\mathbb{Q}$, and $P_1(X) \cdots P_s(X) \in \mathbb{Q}[X]$, then $P_i(X) \in \mathbb{Q}[X]$ for all i. However, it is easy to find a counterexample; for instance, if $P_1(X) = -i + X$ and $P_2(X) = i + X$, then $P_1(X)P_2(X) = 1 + X^2 \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$.