Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 56 (2001)

Artikel: Derivates and irreducible polynomials
Autor: Gologan, Radu-Nicolae
DOI: https://doi.org/10.5169/seals-6684

Elem. Math. 56 (2001) 170 – 172
0013-6018/01/040170-3 $ 1.50+0.20/0

Elemente der Mathematik

Derivatives and irreducible polynomials

Radu-Nicolae Gologan

Radu-Nicolae Gologan received his Ph.D. from the University of Bucharest in 1981. He is now a professor at the Polytechnical University of Bucharest. His main mathematical interests are ergodic theorems, operator theory and operator algebras, ergodic theoretical methods in number theory. In addition, he is involved in the Romanian Olympiad for high-school mathematics.

1 Introduction

It is well-known that formal derivatives provide useful techniques, not only in analysis but in various other domains of mathematics such as algebra of polynomials. The aim of this note is to present a simple technique, based mainly on the use of formal derivatives, that provides simple results with amazing proofs on irreducibility properties for some classes of polynomials with integer coefficients. Although derivatives can be replaced by algebraic calculations, their use gives more elegance and sometimes, significance, in proofs.

2 Main results

By $\mathbb{Z}[X]$ we shall denote, as usual, the ring of polynomials with integer coefficients in the variable X. For $f \in \mathbb{Z}[X]$, $\deg f$ will stand for the degree of f. A polynomial f with $\deg f = n$, is called monic, if the coefficient of X^n is 1. Recall also that $f \in \mathbb{Z}[X]$ is called irreducible (over $\mathbb{Z}$) if it cannot be written as the product of two polynomials

Die Untersuchung von Polynomen, welche über dem Ring der ganzen Zahlen irreduzibel sind, hat eine lange Geschichte. Zum Beispiel führt die Frage nach der Irreduzibilität quadratischer Polynome über den ganzen Zahlen auf das Studium quadratischer Irrationalitäten, welches bereits in der Antike eine prominente Rolle spielte. Ein weiteres Beispiel ist das Eisensteinsche Irreduzibilitätskriterium für Polynome über einem Integritätsbereich, das vielen Lesern bekannt sein dürfte. Im nachfolgenden Beitrag werden mit Hilfe formaler Ableitungen auf elementare Weise einige Klassen irreduzibler Polynome gefunden. Es wird zum Beispiel für ein Polynom f über den ganzen Zahlen mit n verschiedenen ganzzahligen Nullstellen gezeigt, dass das Polynom $f^2 + 1$ einen irreduziblen Faktor vom Grad grösser oder gleich n besitzt.

in $\mathbb{Z}[X]$, each with positive degree. The multiplicity of an integer root a of $f \in \mathbb{Z}[X]$ is the largest positive n such that $(X-a)^n$ divides f.

The first result we consider is the following:

Theorem 1 *Suppose $f \in \mathbb{Z}[X]$ has n distinct integer roots, each of order at least two. Then each of the polynomials $f \pm 1$ has an irreducible factor of degree $\geq n$.*

Proof. Consider the case for $f+1$. The other case will be similar. Suppose that $f+1 = f_1 f_2 \cdots f_p$ is the decomposition in irreducible factors over $\mathbb{Z}$, and let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ be the n distinct multiple roots (of order ≥ 2) of f. We thus have $f_1(a_i) \cdots f_p(a_i) = 1$ for all $i = 1, 2, \ldots, n$. As $f_j(a_i) \in \mathbb{Z}$ for all $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, p$, the last relation can be written

$$f_1(a_i) \cdots \check{f}_k(a_i) \cdots f_p(a_i) = f_k(a_i), \quad i = 1, 2, \ldots, n, \ \ k = 1, 2, \ldots, p, \tag{1}$$

where the symbol $\check{}$ stands for the fact that the respective factor is missing.

Taking derivatives in $f+1 = f_1 f_2 \cdots f_p$, the fact that $x = a_i$, $i = 1, 2, \ldots, n$ are multiple zeros of f, implies

$$\sum_{k=1}^{n} f_1(a_i) \cdots f_k'(a_i) \cdots f_p(a_i) = 0, \quad i = 1, 2, \ldots, n.$$

By (1), the last equality can be written

$$\sum_{k=1}^{p} f_k(a_i) f_k'(a_i) = 0 \quad \text{for all} \ \ i = 1, 2, \ldots, n. \tag{2}$$

As $f_k^2(a_j) = 1$ for all $k = 1, 2, \ldots, p$, $j = 1, 2, \ldots, n$, equation (2) simply says that the polynomial

$$\sum_{k=1}^{n} f_k^2 - n$$

has $a_1, a_2, \ldots, a_n$ as roots of multiplicity at least two. As $\sum_{k=1}^{p} f_k^2 - n$ cannot be null, we must have $\deg \sum_{k=1}^{p} f_k^2 \geq 2n$, implying that one of the f_k has degree at least n. □

A simple argument on the parity of n has as consequence the following:

Corollary *Suppose that $f \in \mathbb{Z}[X]$ has $n > 1$ distinct integer roots. Then, the polynomial $f^2 + 1$ has at least one irreducible factor of degree $\geq 2\left[\frac{n+1}{2}\right]$, where $[\,\cdot\,]$ represents the integer part.*

Proof. Look at the case when n is odd. As f^2+1 has no real roots, the irreducible factors must have even degree, that is, one of them must have degree $\geq n+1$. □

The idea used in the proof of Theorem 1 can be used to describe a class of irreducible polynomials that extends Problem 123, Ch. VIII from [1].

Theorem 2 *Suppose that* $f \in \mathbb{Z}[X]$ *has* n *distinct multiple roots and* $\deg f \leq 3n-1$. *If* $f+1$ *has no real roots, then it is irreducible. Moreover, if* f *is monic, the result remains true for* $\deg f = 3n$.

Proof. We may assume without loss of generality that $f(x)+1$ is positive for all real x. Suppose that $f+1 = pq$, where $p, q \in \mathbb{Z}[X]$ are positive on $\mathbb{R}$ and non-constant. We have $p(a_i) = q(a_i) = 1$, $i = 1, 2, \ldots, n$; in particular $\deg p \geq n$, $\deg q \geq n$. Considering the derivative, we infer $p'(a_i) + q'(a_i) = 0$, $i = 1, 2, \ldots, n$. Thus $p+q-2$ has $a_1, a_2, \ldots, a_n$ as roots of multiplicity at least two, that is, it is the null polynomial, or one of the polynomials p or q has degree $\geq 2n$. In the first case we conclude $f+1+q^2 = 2p$ which contradicts $\deg p < 2n$. In the later case, as $n \leq \deg p$, $\deg q < 3n$ we conclude that one of the factors must be a constant, a contradiction.

In the case when f is monic of degree $3n$, then the degrees of p and q are, in some order, n and $2n$ respectively. This would imply $p+q-2 = (X-a_1)^2(X-a_2)^2 \cdots (X-a_n)^2$ and $p = (X-a_1)(X-a_2)\cdots(X-a_n)$. As $f = (X-a_1)^2(X-a_2)^2\cdots(X-a_n)^2 s(X)$ where s is a monic positive polynomial in $\mathbb{Z}[X]$, we conclude from the previous form of p and q, that s is divisible by $X-a_i$ for $i = 1, 2, \ldots, n$, a contradiction. □

References

[1] G. Polya and G. Szegö: *Aufgaben und Lehrsätze aus der Analysis*, Third edition, Springer, Berlin 1964.

[2] S. Lang: *Algebra*, Addison-Wesley, 1965.

Radu-Nicolae Gologan
Institute of Mathematics of the Romanian Academy
and
University "Politehnica" Bucharest
P.O. Box 1-764
70700 Bucharest, Romania
e-mail: rgologan@theta.ro