Journal of Algebra 398 (2014) 227–242

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Primary decomposition of the ideal of polynomials whose fixed divisor is divisible by a prime power

Giulio Peruginelli

Institut für Analysis und Comput. Number Theory, Technische Universität, Steyrergasse 30, A-8010 Graz, Austria

ARTICLE INFO

Article history:
Received 10 May 2012
Available online 17 October 2013
Communicated by Bernd Ulrich

MSC:
13B25
13F20

Keywords:
Integer-valued polynomial
Image of a polynomial
Fixed divisor
Factorization of integer-valued polynomials
Primary components
Primary decomposition

ABSTRACT

We characterize the fixed divisor of a polynomial $f(X)$ in $\mathbb{Z}[X]$ by looking at the contraction of the powers of the maximal ideals of the overring $\mathrm{Int}(\mathbb{Z})$ containing $f(X)$. Given a prime p and a positive integer n, we also obtain a complete description of the ideal of polynomials in $\mathbb{Z}[X]$ whose fixed divisor is divisible by p^n in terms of its primary components.

To Sergio Paolini, whose teachings and memory I deeply preserve.

1. Introduction

In this work we investigate the image set of integer-valued polynomials over $\mathbb{Z}$. The set of these polynomials is a ring usually denoted by:

$$\mathrm{Int}(\mathbb{Z}) \doteqdot \{ f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subset \mathbb{Z} \}.$$

Since an integer-valued polynomial $f(X)$ maps the integers in a subset of the integers, it is natural to consider the subset of the integers formed by the values of $f(X)$ over the integers and the ideal

E-mail address: peruginelli@math.tugraz.at.

0021-8693
http://dx.doi.org/10.1016/j.jalgebra.2013.09.016

generated by this subset. This ideal is usually called the fixed divisor of $f(X)$. Here is the classical definition.

Definition 1.1. Let $f \in \mathrm{Int}(\mathbb{Z})$. The *fixed divisor* of $f(X)$ is the ideal of $\mathbb{Z}$ generated by the values of $f(n)$, as n ranges in $\mathbb{Z}$:

$$d(f) = d(f, \mathbb{Z}) = \bigl(f(n) \bigm| n \in \mathbb{Z}\bigr).$$

We say that a polynomial $f \in \mathrm{Int}(\mathbb{Z})$ is *image primitive* if $d(f) = \mathbb{Z}$.

It is well-known that for every integer $n \geqslant 1$ we have

$$d\bigl(X(X-1)\cdots\bigl(X-(n-1)\bigr)\bigr) = n!$$

so that the so-called binomial polynomials $B_n(X) \doteqdot X(X-1)\cdots(X-(n-1))/n!$ are integer-valued (indeed, they form a free basis of $\mathrm{Int}(\mathbb{Z})$ as a $\mathbb{Z}$-module; see [4]).

Notice that, given two integer-valued polynomials f and g, we have $d(fg) \subset d(f)d(g)$ and we may not have an equality. For instance, consider $f(X) = X$ and $g(X) = X - 1$; then we have $d(f) = d(g) = \mathbb{Z}$ and $d(fg) = 2\mathbb{Z}$. If $f \in \mathrm{Int}(\mathbb{Z})$ and $n \in \mathbb{Z}$, then directly from the definition we have $d(nf) = nd(f)$. If $\mathrm{cont}(F)$ denotes the content of a polynomial $F \in \mathbb{Z}[X]$, that is, the greatest common divisor of the coefficients of F, we have $F(X) = \mathrm{cont}(F)G(X)$, where $G \in \mathbb{Z}[X]$ is a primitive polynomial (that is, $\mathrm{cont}(G) = 1$). We have the relation:

$$d(F) = \mathrm{cont}(F)d(G).$$

In particular, the fixed divisor is contained in the ideal generated by the content. Hence, given a polynomial with integer coefficients, we can assume it to be primitive. In the same way, if we have an integer-valued polynomial $f(X) = F(X)/N$, with $f \in \mathbb{Z}[X]$ and $N \in \mathbb{N}$, we can assume that $(\mathrm{cont}(F), N) = 1$ and $F(X)$ to be primitive.

The next lemma gives a well-known characterization of a generator of the above ideal (see [1, Lemma 2.7]).

Lemma 1.1. *Let $f \in \mathrm{Int}(\mathbb{Z})$ be of degree d and set*

1) $d_1 = \sup\{n \in \mathbb{Z} \mid \frac{f(X)}{n} \in \mathrm{Int}(\mathbb{Z})\}$,
2) $d_2 = GCD\{f(n) \mid n \in \mathbb{Z}\}$,
3) $d_3 = GCD\{f(0), \ldots, f(d)\}$,

then $d_1 = d_2 = d_3$.

Let $f \in \mathrm{Int}(\mathbb{Z})$. We remark that the value d_1 of Lemma 1.1 is plainly equal to:

$$d_1 = \sup\bigl\{n \in \mathbb{Z} \bigm| f \in n\,\mathrm{Int}(\mathbb{Z})\bigr\}.$$

Moreover, given an integer n, we have this equivalence that we will use throughout the paper, a sort of ideal-theoretic characterization of the arithmetical property that all the values attained by $f(X)$ are divisible by n:

$$f(\mathbb{Z}) \subset n\mathbb{Z} \quad \Longleftrightarrow \quad f \in n\,\mathrm{Int}(\mathbb{Z})$$

($n\,\mathrm{Int}(\mathbb{Z})$ is the principal ideal of $\mathrm{Int}(\mathbb{Z})$ generated by n). From 1) of Lemma 1.1 we see immediately that if $f(X) = F(X)/N$ is an integer-valued polynomial, where $F \in \mathbb{Z}[X]$ and $N \in \mathbb{N}$ coprime with the content of $F(X)$, then $d(f) = d(F)/N$, so we can just focus our attention on the fixed divisor of a primitive polynomial in $\mathbb{Z}[X]$.