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 $\mathbb{Z}$:

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

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

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

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:

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

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 $\mathbb{Z}[X]$.

We want to give another interpretation of the fixed divisor of a polynomial $f \in \mathbb{Z}[X]$ by considering the maximal ideals of $\mathrm{Int}(\mathbb{Z})$ containing $f(X)$ and looking at their contraction to $\mathbb{Z}[X]$. We recall first the definition of unitary ideal given in [12].

Definition 1.2. An ideal $I \subseteq \mathrm{Int}(\mathbb{Z})$ is *unitary* if $I \cap \mathbb{Z} \neq 0$.

That is, an ideal I of $\mathrm{Int}(\mathbb{Z})$ is unitary if it contains a non-zero integer, or, equivalently, $I\mathbb{Q}[X] = \mathbb{Q}[X]$ (where $I\mathbb{Q}[X]$ denotes the extension ideal in $\mathbb{Q}[X]$). The whole ring $\mathrm{Int}(\mathbb{Z})$ is clearly a principal unitary ideal generated by 1.

The next results are probably well-known, but for the ease of the reader we report them. The first lemma says that a principal unitary ideal I is generated by a non-zero integer, which generates the contraction of I to $\mathbb{Z}$. In particular, this lemma establishes a bijective correspondence between the nonzero ideals of $\mathbb{Z}$ and the set of principal unitary ideals of $\mathrm{Int}(\mathbb{Z})$.

Lemma 1.2. *Let $I \subseteq \mathrm{Int}(\mathbb{Z})$ be a principal unitary ideal. If $I \cap \mathbb{Z} = n\mathbb{Z}$ with $n \neq 0$ then $I = n\,\mathrm{Int}(\mathbb{Z})$. In particular, $n\,\mathrm{Int}(\mathbb{Z}) \cap \mathbb{Z} = n\mathbb{Z}$. Moreover, $n_1\,\mathrm{Int}(\mathbb{Z}) = n_2\,\mathrm{Int}(\mathbb{Z})$ with $n_1, n_2 \in \mathbb{Z}$ if and only if $n_1 = \pm n_2$.*

Proof. If $I = (f)$ for some $f \in \mathrm{Int}(\mathbb{Z})$ then $\deg(f) = 0$ since a non-zero integer n is in I. Since $f(X)$ is integer-valued it must be equal to an integer and so it is contained in $I \cap \mathbb{Z} = n\mathbb{Z}$. Hence we get the first statement of the lemma. If $n_1\,\mathrm{Int}(\mathbb{Z}) = n_2\,\mathrm{Int}(\mathbb{Z})$ then $n_1 = n_2 f$ with $f \in \mathrm{Int}(\mathbb{Z})$; this forces f to be a non-zero integer, so that n_1 divides n_2. Similarly, we get that n_2 divides n_1. □

Lemma 1.3. *Let $I_1, I_2 \subseteq \mathrm{Int}(\mathbb{Z})$ be principal unitary ideals. Then $I_1 \cap I_2$ is a principal unitary ideal too.*

Proof. Suppose $I_i = n_i\,\mathrm{Int}(\mathbb{Z})$, where $n_i \in \mathbb{Z}$, $n_i\mathbb{Z} = I_i \cap \mathbb{Z}$, for $i = 1, 2$. We have $n_1\mathbb{Z} \cap n_2\mathbb{Z} = n\mathbb{Z}$, where $n = \mathrm{lcm}\{n_1, n_2\}$. The ideal $I_1 \cap I_2$ is unitary since $n \in I_1 \cap I_2$. In particular, we have $I_1 \cap I_2 \supseteq n\,\mathrm{Int}(\mathbb{Z})$. We have to prove that $I_1 \cap I_2 \subseteq n\,\mathrm{Int}(\mathbb{Z})$. Let $f \in I_1 \cap I_2$. Then $f(\mathbb{Z}) \subset n_1\mathbb{Z} \cap n_2\mathbb{Z} = n\mathbb{Z}$, so that $\frac{f(X)}{n} \in \mathrm{Int}(\mathbb{Z})$. □

The previous lemma implies the following decomposition for a principal unitary ideal generated by an integer n, with prime factorization $n = \prod_i p_i^{a_i}$. We have

$$n\,\mathrm{Int}(\mathbb{Z}) = \bigcap_i p_i^{a_i}\,\mathrm{Int}(\mathbb{Z}) = \prod_i p_i^{a_i}\,\mathrm{Int}(\mathbb{Z})$$

where the last equality holds because the ideals $p_i^{a_i}\mathbb{Z}$ are coprime in $\mathbb{Z}$, hence they are coprime in $\mathrm{Int}(\mathbb{Z})$.

We are now ready to give the following definition.

Definition 1.3. Let $f \in \mathrm{Int}(\mathbb{Z})$. The *extended fixed divisor* of $f(X)$ is the minimal ideal of the set $\{n\,\mathrm{Int}(\mathbb{Z}) \mid n \in \mathbb{Z},\ f \in n\,\mathrm{Int}(\mathbb{Z})\}$. We denote this ideal by $D(f)$.

Equivalently, in the above definition, we require that $n\,\mathrm{Int}(\mathbb{Z})$ contains the principal ideal in $\mathrm{Int}(\mathbb{Z})$ generated by the polynomial $f(X)$. Lemmas 1.2 and 1.3 show that the minimal ideal in the above definition does exist: it is equal to the intersection of all the principal unitary ideals containing $f(X)$. Notice that the extended fixed divisor is an ideal of $\mathrm{Int}(\mathbb{Z})$, while the fixed divisor is an ideal of $\mathbb{Z}$. The polynomial $f(X)$ is image primitive if and only if its extended fixed divisor is the whole ring $\mathrm{Int}(\mathbb{Z})$. In the next sections we will study the extended fixed divisor by considering the p-part of it, namely the principal unitary ideals of the form $p^n\,\mathrm{Int}(\mathbb{Z})$, $p \in \mathbb{Z}$ being prime and n a positive integer.

The following proposition gives a link between the fixed divisor and the extended fixed divisor: the latter is the extension of the former and conversely. So each of them gives information about the other one.

Proposition 1.1. *Let $f \in \mathrm{Int}(\mathbb{Z})$. Then we have*:

a) $D(f) \cap \mathbb{Z} = d(f)$,
b) $d(f)\,\mathrm{Int}(\mathbb{Z}) = D(f)$.

Proof. Let $d, D \in \mathbb{Z}$ be such that $d(f) = d\mathbb{Z}$ and $D(f) = D\,\mathrm{Int}(\mathbb{Z})$. Since $d(f)\,\mathrm{Int}(\mathbb{Z}) = d\,\mathrm{Int}(\mathbb{Z})$ is a principal unitary ideal containing $f(X)$, from the definition of extended fixed divisor, we have $D(f) \subseteq d\,\mathrm{Int}(\mathbb{Z})$. In particular, $D \geqslant d$. We also have $f(X)/D \in \mathrm{Int}(\mathbb{Z})$ and so $d \geqslant D$, by characterization 1) of Lemma 1.1. Hence we get a). From that we deduce that $d(f) \subseteq D(f)$, so statement b) follows. $\square$

As already remarked in [5], the rings $\mathbb{Z}$ and $\mathrm{Int}(\mathbb{Z})$ share the same units, namely $\{\pm 1\}$. Then [5, Proposition 2.1] can be restated as follows.

Proposition 1.2 *(Cahen–Chabert). Let $f \in \mathrm{Int}(\mathbb{Z})$ be irreducible in $\mathbb{Q}[X]$. Then $f(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ if and only if $f(X)$ is not contained in any proper principal unitary ideal of $\mathrm{Int}(\mathbb{Z})$.*

The next lemma has been given in [6] and is analogous to the Gauss Lemma for polynomials in $\mathbb{Z}[X]$ which are irreducible in $\mathrm{Int}(\mathbb{Z})$.

Lemma 1.4 *(Chapman–McClain). Let $f \in \mathbb{Z}[X]$ be a primitive polynomial. Then $f(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ if and only if it is irreducible in $\mathbb{Z}[X]$ and image primitive.*

For example, the polynomial $f(X) = X^2 + X + 2$ is irreducible in $\mathbb{Q}[X]$ and also in $\mathbb{Z}[X]$ since it is primitive (because of Gauss Lemma). But it is reducible in $\mathrm{Int}(\mathbb{Z})$ since its extended fixed divisor is not trivial, namely it is the ideal $2\,\mathrm{Int}(\mathbb{Z})$. So in $\mathrm{Int}(\mathbb{Z})$ we have the following factorization:

$$f(X) = 2 \cdot \frac{X^2 + X + 2}{2}$$

and indeed this is a factorization into irreducibles in $\mathrm{Int}(\mathbb{Z})$, since the latter polynomial is image primitive and irreducible in $\mathbb{Q}[X]$, and by [5, Lemma 1.1], the irreducible elements in $\mathbb{Z}$ remain irreducible in $\mathrm{Int}(\mathbb{Z})$. So the study of the extended fixed divisor of the elements in $\mathrm{Int}(\mathbb{Z})$ is a first step toward studying the factorization of the elements in this ring (which is not a unique factorization domain).

Here is an overview of the content of the paper. At the beginning of the next section we recall the structure of the prime spectrum of $\mathrm{Int}(\mathbb{Z})$. Then, for a fixed prime p, we describe the contractions to $\mathbb{Z}[X]$ of the maximal unitary ideals of $\mathrm{Int}(\mathbb{Z})$ containing p (Lemma 2.1). In Theorem 2.1 we describe the ideal I_p of $\mathbb{Z}[X]$ of those polynomials whose fixed divisor is divisible by p, namely the contraction to $\mathbb{Z}[X]$ of the principal unitary ideal $p\,\mathrm{Int}(\mathbb{Z})$, which is the ideal of integer-valued polynomials whose extended fixed divisor is contained in $p\,\mathrm{Int}(\mathbb{Z})$. It turns out that I_p is the intersection of the aforementioned contractions. In the third section we generalize the result of the second section to prime powers, by means of a structure theorem of Loper regarding unitary ideals of $\mathrm{Int}(\mathbb{Z})$. We consider the contractions to $\mathbb{Z}[X]$ of the powers of the prime unitary ideals of $\mathrm{Int}(\mathbb{Z})$ (Lemma 3.1). In Remark 2 we give a description of the structure of the set of these contractions; that allows us to give the primary decomposition of the ideal $I_{p^n} = p^n\,\mathrm{Int}(\mathbb{Z}) \cap \mathbb{Z}[X]$, made up of those polynomials whose fixed divisor is divisible by a prime power p^n. We shall see that we have to distinguish two cases: $p \leqslant n$ and $p > n$ (see also the examples in Remark 3). In Theorem 3.1 we describe I_{p^n} in the case $p \leqslant n$. This result was already known in a slightly different context by Dickson (see [7, p. 22, Theorem 27]), but our different proof uses the primary decomposition of I_{p^n} and that gives an insight to generalize the result to the second case. In Proposition 3.2 we give a set of generators for the primary components of I_{p^n}, in the case $p > n$. Finally in the last section, as an application, we explicitly compute the ideal $I_{p^{p+1}}$.

2. Fixed divisor via Spec(Int($\mathbb{Z}$))

The study of the prime spectrum of the ring Int($\mathbb{Z}$) began in [3]. We recall that the prime ideals of Int($\mathbb{Z}$) are divided into two different categories, unitary and non-unitary. Let P be a prime ideal of Int($\mathbb{Z}$). If it is unitary then its intersection with the ring of integers is a principal ideal generated by a prime p.

Non-unitary prime ideals: $P \cap \mathbb{Z} = \{0\}$.
In this case P is a prime (non-maximal) ideal and it is of the form

$$\mathfrak{P}_q = q\mathbb{Q}[X] \cap \mathrm{Int}(\mathbb{Z})$$

for some $q \in \mathbb{Q}[X]$ irreducible. By Gauss Lemma we may suppose that $q \in \mathbb{Z}[X]$ is irreducible and primitive.

Unitary prime ideals: $P \cap \mathbb{Z} = p\mathbb{Z}$.
In this case P is maximal and is of the form

$$\mathfrak{M}_{p,\alpha} = \{f \in \mathrm{Int}(\mathbb{Z}) \mid f(\alpha) \in p\mathbb{Z}_p\}$$

for some p prime in $\mathbb{Z}$ and some $\alpha \in \mathbb{Z}_p$, the ring of p-adic integers. We have $\mathfrak{M}_{p,\alpha} = \mathfrak{M}_{q,\beta}$ if and only if $(p,\alpha) = (q,\beta)$. So if we fix the prime p, the elements of $\mathbb{Z}_p$ are in bijection with the unitary prime ideals of Int($\mathbb{Z}$) above the prime p. Moreover, $\mathfrak{M}_{p,\alpha}$ is height 1 if and only if α is transcendental over $\mathbb{Q}$. If α is algebraic over $\mathbb{Q}$ and $q(X)$ is its minimal polynomial then $\mathfrak{M}_{p,\alpha} \supset \mathfrak{P}_q$. We have $\mathfrak{P}_q \subset \mathfrak{M}_{p,\alpha}$ if and only if $q(\alpha) = 0$. Every prime ideal of Int($\mathbb{Z}$) is not finitely generated.

For a detailed study of Spec(Int($\mathbb{Z}$)) see [4].

If we denote by $d(f,\mathbb{Z}_p)$ the fixed divisor of $f \in \mathrm{Int}(\mathbb{Z})$ viewed as a polynomial over the ring of p-adic integers $\mathbb{Z}_p$ (that is, $d(f,\mathbb{Z}_p)$ is the ideal $(f(\alpha) \mid \alpha \in \mathbb{Z}_p)$), Gunji and McQuillan in [8] observed that

$$d(f) = \bigcap_p d(f,\mathbb{Z}_p)$$

where the intersection is taken over the set of primes in $\mathbb{Z}$. Moreover, $d(f,\mathbb{Z}_p) = d(f)\mathbb{Z}_p \subset \mathbb{Z}_p$. Remember that given an ideal $I \subset \mathbb{Z}$ and a prime p we have $I\mathbb{Z}_p = \mathbb{Z}_p$ if and only if $I \not\subset (p)$, so that in the previous equation we have a finite intersection. Since $\mathbb{Z}_p$ is a DVR we have $d(f,\mathbb{Z}_p) = p^n\mathbb{Z}_p$, for some integer n (which of course depends on p), so that the exact power of p which divides $f(\mathbb{Z})$ is the same as the power of p dividing $f(\mathbb{Z}_p)$. Without loss of generality, we can restrict our attention to the p-part of the fixed divisor of a polynomial $f \in \mathbb{Z}[X]$. We begin our research by finding those polynomials in $\mathbb{Z}[X]$ whose fixed divisor is divisible by a fixed prime p, namely the ideal $p\,\mathrm{Int}(\mathbb{Z}) \cap \mathbb{Z}[X]$.

Lemma 2.1. *Let p be a prime and $\alpha \in \mathbb{Z}_p$. Then $\mathfrak{M}_{p,\alpha} \cap \mathbb{Z}[X] = (p, X - a)$, where $a \in \mathbb{Z}$ is such that $\alpha \equiv a \pmod p$. Moreover, if $\beta \in \mathbb{Z}_p$ is another p-adic integer, we have $\mathfrak{M}_{p,\alpha} \cap \mathbb{Z}[X] = \mathfrak{M}_{p,\beta} \cap \mathbb{Z}[X]$ if and only if $\alpha \equiv \beta \pmod p$.*

Proof. Let a be an integer as in the statement of the lemma; it exists since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ for the p-adic topology. We immediately see that p and $X - a$ are in $\mathfrak{M}_{p,\alpha}$. Then the conclusion follows since $(p, X - a)$ is a maximal ideal of $\mathbb{Z}[X]$ and $\mathfrak{M}_{p,\alpha} \cap \mathbb{Z}[X]$ is not equal to the whole ring $\mathbb{Z}[X]$. The second statement follows from the fact that $(p, X - a) = (p, X - b)$ if and only if $a \equiv b \pmod p$. □

We have just seen that the contraction of $\mathfrak{M}_{p,\alpha}$ to $\mathbb{Z}[X]$ depends only on the residue class modulo p of α. So, if p is a fixed prime, the contractions of $\mathfrak{M}_{p,\alpha}$ to $\mathbb{Z}[X]$ as α ranges through $\mathbb{Z}_p$ are made up of p distinct maximal ideals, namely

$$\{\mathfrak{M}_{p,\alpha}\cap\mathbb{Z}[X]\mid \alpha\in\mathbb{Z}_p\}=\{(p,X-j)\mid j\in\{0,\dots,p-1\}\}.$$

Conversely, the set of prime ideals of $\mathrm{Int}(\mathbb{Z})$ above a fixed maximal ideal of the form $(p, X-j)$ is $\{\mathfrak{M}_{p,\alpha}\mid \alpha\in\mathbb{Z}_p,\ \alpha\equiv j \pmod p\}$, since $\mathfrak{P}_q$ are non-unitary ideals and p is the only prime integer in $\mathfrak{M}_{p,\alpha}$.

For a prime p and an integer $j\in\{0,\dots,p-1\}$, we set:

$$\mathcal{M}_{p,j}=\mathcal{M}_j \doteqdot (p, X-j).$$

Whenever the notation $\mathcal{M}_{p,j}$ is used, it will be implicit that $j\in\{0,\dots,p-1\}$.

The next lemma computes the intersection of the ideals $\mathcal{M}_{p,j}$, for a fixed prime p, by finding an ideal whose primary decomposition is given by this intersection (and its primary components are precisely the p ideals $\mathcal{M}_{p,j}$). From now on we will omit the index p.

Lemma 2.2. *Let $p\in\mathbb{Z}$ be a prime. Then we have*

$$\bigcap_{j=0,\dots,p-1}\mathcal{M}_j=\Bigl(p,\prod_{j=0,\dots,p-1}(X-j)\Bigr).$$

Proof. Let J be the ideal on the right-hand side. If P is a prime minimal over J, then we see immediately that $P=\mathcal{M}_j$ for some $j\in\{0,\dots,p-1\}$, since $\mathcal{M}_j$ is a maximal ideal. Conversely, every such a maximal ideal contains J and is minimal over it. Then the minimal primary decomposition of J is of the form

$$J=\bigcap_{j=0,\dots,p-1}Q_j$$

where Q_j is an $\mathcal{M}_j$-primary ideal. Since $X-i\notin\mathcal{M}_j$ for all $i\in\{0,\dots,p-1\}\setminus\{j\}$, we have $(X-j)\in Q_j$, so indeed $Q_j=(p,X-j)$ for each $j=0,\dots,p-1$. $\square$

The next proposition characterizes the principal unitary ideals in $\mathrm{Int}(\mathbb{Z})$ generated by a prime p.

Proposition 2.1. *Let $p\in\mathbb{Z}$ be a prime. Then the principal unitary ideal $p\,\mathrm{Int}(\mathbb{Z})$ is equal to*

$$p\,\mathrm{Int}(\mathbb{Z})=\bigcap_{\alpha\in\mathbb{Z}_p}\mathfrak{M}_{p,\alpha}.$$

Proof. We trivially have that $p\,\mathrm{Int}(\mathbb{Z})$ is contained in the above intersection, since p is in every ideal of the form $\mathfrak{M}_{p,\alpha}$. On the other hand, this intersection is equal to $\{f\in\mathrm{Int}(\mathbb{Z})\mid f(\mathbb{Z}_p)\subset p\mathbb{Z}_p\}$. If $f(X)$ is in this intersection, since $f(X)$ is integer-valued and $p\mathbb{Z}_p\cap\mathbb{Z}=p\mathbb{Z}$, we have $f(\mathbb{Z})\subset p\mathbb{Z}$. This is equivalent to saying that $f(X)/p\in\mathrm{Int}(\mathbb{Z})$, that is, $f\in p\,\mathrm{Int}(\mathbb{Z})$. $\square$

In particular, the previous proposition implies that $\mathrm{Int}(\mathbb{Z})$ does not have the finite character property (we recall that a ring has this property if every non-zero element is contained in a finite number of maximal ideals).

From the above results we get the following theorem, which characterizes the ideal of polynomials with integer coefficients whose fixed divisor is divisible by a prime p, that is, the ideal $p\,\mathrm{Int}(\mathbb{Z})\cap\mathbb{Z}[X]$.

Theorem 2.1. *Let p be a prime. Then*

$$p\,\mathrm{Int}(\mathbb{Z})\cap\mathbb{Z}[X]=\Bigl(p,\prod_{j=0,\dots,p-1}(X-j)\Bigr).$$

Notice that Lemma 2.2 gives the primary decomposition of $p\,\mathrm{Int}(\mathbb{Z})\cap\mathbb{Z}[X]$, so $\mathcal{M}_j$ for $j=0,\dots,p-1$ are exactly the prime ideals belonging to it. As a consequence of this theorem we get the following well-known result: if $f\in\mathbb{Z}[X]$ is primitive and p is a prime such that $d(f)\subseteq p$ then $p\leqslant\deg(f)$. This immediately follows from the theorem, since the degree of $\prod_{j=0,\dots,p-1}(X-j)$ is p.

We remark that by Fermat's little theorem the ideal on the right-hand side of the statement of Theorem 2.1 is equal to (p, X^p-X). This amounts to saying that the two polynomials $X\cdot\dots\cdot(X-(p-1))$ and X^p-X induce the same polynomial function on $\mathbb{Z}/p\mathbb{Z}$.

3. Contraction of primary ideals

We remark that Proposition 2.1 also follows from a general result contained in [11]: every unitary ideal in $\mathrm{Int}(\mathbb{Z})$ is an intersection of powers of unitary prime ideals (namely the maximal ideals $\mathfrak{M}_{p,\alpha}$). In particular, every $\mathfrak{M}_{p,\alpha}$-primary ideal is a power of $\mathfrak{M}_{p,\alpha}$ itself, since $\mathfrak{M}_{p,\alpha}$ is maximal. From the same result we also have the following characterization of the powers of $\mathfrak{M}_{p,\alpha}$, for any positive integer n:

$$\mathfrak{M}_{p,\alpha}^n=\{f\in\mathrm{Int}(\mathbb{Z})\mid f(\alpha)\in p^n\mathbb{Z}_p\}.$$

This fact implies the following expression for the principal unitary ideal generated by p^n:

$$p^n\,\mathrm{Int}(\mathbb{Z})=\bigcap_{\alpha\in\mathbb{Z}_p}\mathfrak{M}_{p,\alpha}^n. \tag{1}$$

We remark again that the previous ideal is made up of those integer-valued polynomials whose extended fixed divisor is contained in $p^n\,\mathrm{Int}(\mathbb{Z})$. Similarly to the previous case $n=1$ (see Theorem 2.1) we want to find the contraction of this ideal to $\mathbb{Z}[X]$, in order to find the polynomials in $\mathbb{Z}[X]$ whose fixed divisor is divisible by p^n. We set:

$$I_{p^n}\doteqdot p^n\,\mathrm{Int}(\mathbb{Z})\cap\mathbb{Z}[X]. \tag{2}$$

Notice that by (1) we have $I_{p^n}=\bigcap_{\alpha\in\mathbb{Z}_p}(\mathfrak{M}_{p,\alpha}^n\cap\mathbb{Z}[X])$.

Like before, we begin by finding the contraction to $\mathbb{Z}[X]$ of $\mathfrak{M}_{p,\alpha}^n$, for each $\alpha\in\mathbb{Z}_p$. The next lemma is a generalization of Lemma 2.1.

Lemma 3.1. *Let p be a prime, n a positive integer and $\alpha\in\mathbb{Z}_p$. Then $\mathfrak{M}_{p,\alpha}^n\cap\mathbb{Z}[X]=(p^n, X-a)$, where $a\in\mathbb{Z}$ is such that $\alpha\equiv a\pmod{p^n}$. The ideal $\mathfrak{M}_{p,\alpha}^n\cap\mathbb{Z}[X]$ is $\mathcal{M}_{p,j}$-primary, where $j\equiv\alpha\pmod p$. Moreover, if $\beta\in\mathbb{Z}_p$ is another p-adic integer, we have $\mathfrak{M}_{p,\alpha}^n\cap\mathbb{Z}[X]=\mathfrak{M}_{p,\beta}^n\cap\mathbb{Z}[X]$ if and only if $\alpha\equiv\beta\pmod{p^n}$.*

Proof. The case $n=1$ has been done in Lemma 2.1. For the general case, let $a\in\mathbb{Z}$ be such that $a\equiv\alpha\pmod{p^n}$ (again, such an integer exists since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ for the p-adic topology). We have $(p^n, X-a)\subset\mathfrak{M}_{p,\alpha}^n\cap\mathbb{Z}[X]$ (notice that if $n>1$ then $(p^n, X-a)$ is not a prime ideal). To prove the other inclusion let $f\in\mathfrak{M}_{p,\alpha}^n\cap\mathbb{Z}[X]$. By the Euclidean algorithm in $\mathbb{Z}[X]$ (the leading coefficient of $X-a$ is a unit) we have

$$f(X)=q(X)(X-a)+f(a).$$

Since $f(\alpha)\in p^n\mathbb{Z}_p$ and $p^n|a-\alpha$ we have $p^n|f(a)$. Hence, $f\in(p^n, X-a)$ as we wanted. Since $\mathfrak{M}_{p,\alpha}^n$ is an $\mathfrak{M}_{p,\alpha}$-primary ideal in $\mathrm{Int}(\mathbb{Z})$ and the contraction of a primary ideal is a primary ideal, by Lemma 2.1 we get the second statement. Finally, like in the proof of Lemma 2.1, we immediately see that $(p^n, X-a)=(p^n, X-b)$ if and only if $a\equiv b\pmod{p^n}$, which gives the last statement of the lemma. $\square$

Remark 1. It is worth to write down the fact that we used in the above proof: given a polynomial $f \in \mathbb{Z}[X]$, we have

$$f \in \left(p^n, X - a\right) \iff f(a) \equiv 0 \pmod{p^n}. \tag{3}$$

Remark 2. If p is a fixed prime and n is a positive integer, Lemma 3.1 implies

$$\mathcal{I}_{p,n} \doteqdot \left\{\mathfrak{M}^n_{p,\alpha} \cap \mathbb{Z}[X] \;\middle|\; \alpha \in \mathbb{Z}_p\right\} = \left\{\left(p^n, X - i\right) \;\middle|\; i = 0, \ldots, p^n - 1\right\}.$$

Let us consider an ideal $I = \mathfrak{M}^n_{p,\alpha} \cap \mathbb{Z}[X] = (p^n, X - i)$ in $\mathcal{I}_{p,n}$, with $i \in \mathbb{Z}$, $i \equiv \alpha \pmod{p^n}$. It is quite easy to see that I contains $(\mathfrak{M}_{p,\alpha} \cap \mathbb{Z}[X])^n = \mathcal{M}^n_{p,j} = (p, X - j)^n$, where $j \in \{0, \ldots, p - 1\}$, $j \equiv \alpha \pmod p$ (notice that $j \equiv i \pmod p$). If $n > 1$ this containment is strict, since $X - i \notin (p, X - j)^n$. We can group the ideals of $\mathcal{I}_{p,n}$ according to their radical: there are p radicals of these p^n ideals, namely the maximal ideals $\mathcal{M}_{p,j}$, $j = 0, \ldots, p - 1$. This amounts to making a partition of the residue classes modulo p^n into p different sets of elements congruent to j modulo p, for $j = 0, \ldots, p - 1$; each of these sets has cardinality p^{n-1}. Correspondingly we have:

$$\mathcal{I}_{p,n} = \bigcup_{j=0,\ldots,p-1} \mathcal{I}_{p,n,j}$$

where $\mathcal{I}_{p,n,j} \doteqdot \{(p^n, X - i) \mid i = 0, \ldots, p^n - 1,\ i \equiv j \pmod p\}$, for $j = 0, \ldots, p - 1$. Every ideal in $\mathcal{I}_{p,n,j}$ is $\mathcal{M}_{p,j}$-primary and it contains the n-th power of its radical, namely $\mathcal{M}^n_{p,j}$.

Now we want to compute the intersection of the ideals in $\mathcal{I}_{p,n}$, which is equal to the ideal I_{p^n} in $\mathbb{Z}[X]$ (see (1) and (2)). We can express this intersection as an intersection of $\mathcal{M}_{p,j}$-primary ideals as we have said above, in the following way (in the first equality we make use of Eq. (1) and Lemma 3.1):

$$I_{p^n} = \bigcap_{i=0,\ldots,p^n-1} \left(p^n, X - i\right) = \bigcap_{j=0,\ldots,p-1} \mathcal{Q}_{p,n,j} \tag{4}$$

where

$$\mathcal{Q}_{p,n,j} \doteqdot \bigcap_{i \equiv j \pmod p} \left(p^n, X - i\right)$$

(notice that the intersection is taken over the set $\{i \in \{0, \ldots, p^n - 1\} \mid i \equiv j \pmod p\}$). The ideal $\mathcal{Q}_{p,n,j}$ is an $\mathcal{M}_{p,j}$-primary ideal, for $j = 0, \ldots, p - 1$, since the intersection of M-primary ideals is an M-primary ideal. We will omit the index p in $\mathcal{Q}_{p,n,j}$ and in $\mathcal{M}_{p,j}$ if that will be clear from the context. The $\mathcal{M}_{p,j}$-primary ideal $\mathcal{Q}_{n,j}$ is just the intersection of the ideals in $\mathcal{I}_{p,n,j}$, according to the partition we made. It is equal to the set of polynomials in $\mathbb{Z}[X]$ which modulo p^n are zero at the residue classes congruent to j modulo p (see (3) of Remark 1). We remark that (4) is the minimal primary decomposition of I_{p^n}. Notice that there are no embedded components in this primary decomposition, since the prime ideals belonging to it (the minimal primes containing I_{p^n}) are $\{\mathcal{M}_j \mid j = 0, \ldots, p - 1\}$, which are maximal ideals.

We recall that if I and J are two coprime ideals in a ring R, that is $I + J = R$, then $IJ = I \cap J$ (in general only the inclusion $IJ \subset I \cap J$ holds). The condition for two ideals I and J to be coprime amounts to saying that I and J are not contained in a same maximal ideal M, that is, $I + J$ is not contained in any maximal ideal M. If M_1 and M_2 are two distinct maximal ideals then they are coprime, and the same holds for any of their respective powers. If R is Noetherian, then every primary ideal Q contains a power of its radical and moreover if the radical of Q is maximal then also the converse holds (see [14]). So if Q_i is an M_i-primary ideal for $i = 1, 2$ and M_1, M_2 are distinct maximal ideals, then Q_1 and Q_2 are coprime.

Since $\{\mathcal{M}_j\}_{j=0,\dots,p-1}$ are p distinct maximal ideals, for what we have just said above we have

$$\bigcap_{j=0,\dots,p-1} \mathcal{Q}_{n,j} = \prod_{j=0,\dots,p-1} \mathcal{Q}_{n,j}.$$

Now we want to describe the $\mathcal{M}_j$-primary ideals $\mathcal{Q}_{n,j}$, for $j = 0, \dots, p-1$. The next lemma gives a relation of containment between these ideals and the n-th powers of their radicals.

Lemma 3.2. *Let p be a fixed prime and n a positive integer. For each $j = 0, \dots, p-1$, we have*

$$\mathcal{Q}_{n,j} \supseteq \mathcal{M}_j^n.$$

Proof. The statement follows from Remark 2. □

As a consequence of this lemma, we get the following result:

Corollary 3.1. *Let p be a fixed prime and n a positive integer. Then we have*:

$$I_{p^n} \supseteq \left(p, \prod_{j=0,\dots,p-1} (X - j)\right)^n.$$

Proof. By (4) and Lemma 3.2 we have

$$I_{p^n} = \prod_{j=0,\dots,p-1} \mathcal{Q}_{n,j} \supseteq \prod_{j=0,\dots,p-1} \mathcal{M}_j^n$$

where the last containment follows from Lemma 3.2. Finally, by Lemma 2.2, the product of the ideals $\mathcal{M}_j^n$ is equal to

$$\prod_{j=0,\dots,p-1} \mathcal{M}_j^n = \left(p, \prod_{j=0,\dots,p-1} (X - j)\right)^n.$$

Notice that the product of the $\mathcal{M}_j$'s is actually equal to their intersection, since they are maximal coprime ideals. □

The last formula of the previous proof gives the primary decomposition of the ideal $(p, \prod_{j=0,\dots,p-1}(X-j))^n$.

Remark 3. In general, for a fixed $j \in \{0, \dots, p-1\}$, the reverse containment of Lemma 3.2 does not hold, that is, the n-th power of $\mathcal{M}_j$ can be strictly contained in the $\mathcal{M}_j$-primary ideal $\mathcal{Q}_{n,j}$. For example (again, we use (3) to prove the containment):

$$X(X-2) \in \left(\bigcap_{k=0,\dots,3} (2^3, X - 2k)\right) \setminus (2, X)^3.$$

Because of that, in general we do not have an equality in Corollary 3.1. For example, let $p = 2$ and $n = 3$. We have

$$X(X-1)(X-2)(X-3) \in I_{2^3} \setminus \big(2, X(X-1)\big)^3.$$

It is also false that

$$\bigcap_{i=0,\dots,p^n-1}(p^n, X-i)=\Bigl(p^n,\prod_{i=0,\dots,p^n-1}(X-i)\Bigr).$$

See for example: $p=2$, $n=2$: $2X(X-1)\in\bigcap_{i=0,\dots,3}(4, X-i)\setminus(4,\prod_{i=0,\dots,3}(X-i))$.

We want to study under which conditions the ideal $\mathcal{Q}_{n,j}$ is equal to $\mathcal{M}_j^n$. Our aim is to find a set of generators for $\mathcal{Q}_{n,j}$. For $f\in\mathcal{Q}_{n,j}$, we have $f\in(p^n, X-i)$ for each $i\equiv j \pmod p$, $i\in\{0,\dots,p^n-1\}$. By (3) that means $p^n|f(i)$ for each such an i. Equivalently, such a polynomial has the property that modulo p^n it is zero at the p^{n-1} residue classes of $\mathbb{Z}/p^n\mathbb{Z}$ which are congruent to j modulo p.

Without loss of generality, we proceed by considering the case $j=0$. We set $\mathcal{M}=\mathcal{M}_0=(p,X)$ and $\mathcal{Q}_n=\mathcal{Q}_{n,0}=\bigcap_{i\equiv 0 \pmod p}(p^n, X-i)$. Let $f\in\mathcal{Q}_n$, of degree m. We have

$$f(X)=q_1(X)X+f(0) \tag{5}$$

where $q_1\in\mathbb{Z}[X]$ has degree equal to $m-1$. Since $f\in(p^n,X)$ we have $p^n|f(0)$.

Since $f\in(p^n, X-p)$, we have $p^n|f(p)=q_1(p)p+f(0)$, so $p^{n-1}|q_1(p)$. By the Euclidean algorithm,

$$q_1(X)=q_2(X)(X-p)+q_1(p) \tag{6}$$

for some polynomial $q_2\in\mathbb{Z}[X]$ of degree $m-2$. So

$$f(X)=q_2(X)(X-p)X+q_1(p)X+f(0).$$

We set $R_1(X)=q_1(p)X+f(0)$. Then $R_1\in\mathcal{M}^n$, since $p^{n-1}|q_1(p)$ and $p^n|f(0)$. Since $f\in(p^n, X-2p)$, we have $p^n|f(2p)=q_2(2p)2p^2+q_1(p)2p+f(0)$. If $p>2$ then $p^{n-2}|q_2(2p)$, because $p^n|q_1(p)2p+f(0)$. If $p=2$ then we can just say $p^{n-3}|q_2(2p)$. By the Euclidean algorithm again, we have

$$q_2(X)=q_3(X)(X-2p)+q_2(2p)$$

for some $q_3\in\mathbb{Z}[X]$. So we have

$$f(X)=q_3(X)(X-2p)(X-p)X+q_2(2p)(X-p)X+q_1(p)X+f(0).$$

Like before, if we set $R_2(X)=q_2(2p)(X-p)X+q_1(p)X+f(0)$, we have $R_2\in\mathcal{M}^n$ if $p>2$, or $R_2\in\mathcal{Q}_n$ if $p=2$.

We define now the following family of polynomials:

Definition 3.1. For each $k\in\mathbb{N}$, $k\geqslant 1$, we set

$$G_{p,0,k}(X)=G_k(X)\doteqdot\prod_{h=0,\dots,k-1}(X-hp).$$

We also set $G_0(X)\doteqdot 1$.

From now on, we will omit the index p in the above notation.

Notice that the polynomials $G_k(X)$, whose degree for each k is k, enjoy these properties:

i) For every $t\in\mathbb{Z}$, $G_k(tp)=p^k t(t-1)\cdots(t-(k-1))$. Hence, the highest power of p which divides all the integers in the set $\{G_k(tp)\mid t\in\mathbb{Z}\}$ is $p^{k+v_p(k!)}$. It is easy to see that $k+v_p(k!)=v_p((pk)!)$.
ii) $G_k(X)=(X-kp)G_{k-1}(X)$.

iii) since for every integer h, $X-hp\in\mathcal{M}$, we have $G_k(X)\in\mathcal{M}^k$. We remark that k is the maximal integer with this property, since $\deg(G_k)=k$ and $G_k(X)$ is primitive (since monic).

Recall that, by Lemma 3.2, for every integer n we have $\mathcal{Q}_n\supseteq\mathcal{M}^n$. By property iii) above $G_k\in\mathcal{M}^n$ if and only if $n\leqslant k$. By property i) we have $G_k\in\mathcal{Q}_n$ if and only if $k+v_p(k!)\geqslant n$. From these remarks, it is very easy to deduce that, in the case $p\geqslant n$, if $G_k\in\mathcal{Q}_n$ then $G_k\in\mathcal{M}^n$. In fact, if that is not the case, it follows from above that $k<n$. Since $n\leqslant p$ we get $k+v_p(k!)=k$. Since $G_k\in\mathcal{Q}_n$, we have $n\leqslant k$, contradiction.

The next lemma gives a sort of division algorithm between an element of $\mathcal{Q}_n$ and the polynomials $\{G_k(X)\}_{k\in\mathbb{N}}$. In particular, we will deduce that $\mathcal{Q}_n=\mathcal{M}^n$, if $p\geqslant n$.

Lemma 3.3. *Let p be a prime and n a positive integer. Let $f\in\mathcal{Q}_{p,n,0}=\mathcal{Q}_n$ be of degree m. Then for each $1\leqslant k\leqslant m$ there exists $q_k\in\mathbb{Z}[X]$ of degree $m-k$ such that*

$$f(X)=q_k(X)G_k(X)+R_{k-1}(X)$$

where $R_{k-1}(X)\doteqdot\sum_{h=1,\dots,k-1}q_h(hp)G_h(X)$ for $k\geqslant 2$ and $R_0(X)\doteqdot f(0)$.
We also have $q_k(X)=q_{k+1}(X)(X-kp)+q_k(kp)$ for $k=1,\dots,m-1$. Moreover, for each such a k the following hold:

i) *$p^{n-v_p((pk)!)}|q_k(kp)$, if $v_p((pk)!)<n$.*
ii) *$q_k(kp)G_k(X)\in\mathcal{Q}_n$ and if $k<p$ then $q_k(kp)G_k(X)\in\mathcal{M}^n$.*
iii) *If $m\leqslant p$ then $R_{k-1}\in\mathcal{M}^n$ for $k=1,\dots,m$.*
If $m>p$ then $R_{k-1}\in\mathcal{M}^n$ for $k=1,\dots,p$ and $R_{k-1}\in\mathcal{Q}_n$ for $k=p+1,\dots,m$.

Proof. We proceed by induction on k. The case $k=1$ follows from (5), and by (6) we have the last statement regarding the relation between $q_1(X)$ and $q_2(X)$. Suppose now the statement is true for $k-1$, so that

$$f(X)=q_{k-1}(X)G_{k-1}(X)+R_{k-2}(X)$$

with $R_{k-2}(X)\doteqdot\sum_{h=1,\dots,k-2}q_h(hp)G_h(X)$ and

- $p^{n-v_p((p(k-1))!)}|q_{k-1}((k-1)p)$, if $v_p((p(k-1)!))<n$,
- $q_{k-1}((k-1)p)G_{k-1}(X)$ belongs to $\mathcal{Q}_n$ and if $k-1<p$ it belongs to $\mathcal{M}^n$,
- $R_{k-2}\in\mathcal{Q}_n$ and if $k-2<p$ then $R_{k-2}\in\mathcal{M}^n$.

We divide $q_{k-1}(X)$ by $(X-(k-1)p)$ and we get

$$q_{k-1}(X)=q_k(X)\bigl(X-(k-1)p\bigr)+q_{k-1}\bigl((k-1)p\bigr)$$

for some polynomial $q_k\in\mathbb{Z}[X]$ of degree $m-k$. We substitute this expression of $q_{k-1}(X)$ in the equation of $f(X)$ at the step $k-1$ and we get:

$$f(X)=q_k(X)\bigl(X-(k-1)p\bigr)G_{k-1}(X)+R_{k-1}(X),\tag{7}$$

where $R_{k-1}(X)\doteqdot q_{k-1}((k-1)p)G_{k-1}(X)+R_{k-2}(X)$. This is the expression of $f(X)$ at step k, since $(X-(k-1)p)G_{k-1}(X)$ is equal to $G_k(X)$. By the inductive assumption, $R_{k-1}\in\mathcal{Q}_n$ and if $k-1<p$ we also have $R_{k-1}\in\mathcal{M}^n$. We still have to verify i) and ii).

We evaluate the expression (7) in $X=kp$ and we get

$$f(kp)=q_k(kp)G_k(kp)+R_{k-1}(kp)=q_k(kp)p^kk!+R_{k-1}(kp).$$

Since p^n divides both $f(kp)$ and $R_{k-1}(kp)$ (by definition of $\mathcal{Q}_n$), if $v_p((pk)!) < n$ we get that $q_k(kp)$ is divisible by $p^{n-v_p((pk)!)}$, which is statement i) at the step k. Notice that $q_k(kp)G_k(X)$ is zero modulo p^n on every integer congruent to zero modulo p; hence, $q_k(kp)G_k(X) \in \mathcal{Q}_n$. Moreover, $k < p \Leftrightarrow v_p(k!) = 0$, so in that case $q_k(kp)G_k(X) \in \mathcal{M}^n$. So ii) follows. $\square$

Notice that by formula (3) of Remark 1, under the assumptions of Lemma 3.3 we have for each $k \in \{1, \dots, p-1\}$ that

$$q_k \in \left(p^{n-k}, X - kp\right)$$

(see i) of Lemma 3.3: in this case $v_p((pk)!) = k$). If $k = m = \deg(f)$ then $q_k \in \mathbb{Z}$. Hence, we get the following expression for a polynomial $f \in \mathcal{Q}_n$ in the case $p \geqslant n > m$ (this assumption is not restrictive, since $X^n \in \mathcal{Q}_n$):

$$f(X) = q_m G_m(X) + R_{m-1}(X) = q_m G_m(X) + \sum_{k=1,\dots,m-1} q_k(kp) G_k(X) \tag{8}$$

where $q_m \in \mathbb{Z}$ is divisible by p^{n-m} and $R_{m-1}(X)$ is in $\mathcal{M}^n$.

The next proposition determines the primary components $\mathcal{Q}_{n,j}$ of I_{p^n} of (4) in the case $p \geqslant n$. It shows that in this case the containment of Lemma 3.2 is indeed an equality.

Proposition 3.1. *Let $p \in \mathbb{Z}$ be a prime and n a positive integer such that $p \geqslant n$. Then for each $j = 0, \dots, p-1$ we have*

$$\mathcal{Q}_{n,j} = \mathcal{M}_j^n.$$

Proof. It is sufficient to prove the statement for $j = 0$: for the other cases we consider the $\mathbb{Z}[X]$-automorphisms $\pi_j(X) = X - j$, for $j = 1, \dots, p-1$, which permute the ideals $\mathcal{Q}_{n,j}$ and $\mathcal{M}_j$. Let $\mathcal{Q}_n = \mathcal{Q}_{n,0}$ and $\mathcal{M} = \mathcal{M}_0$.

The inclusion ($\supseteq$) follows from Lemma 3.2. For the other inclusion ($\subseteq$), let $f(X)$ be in $\mathcal{Q}_n$. We can assume that the degree m of $f(X)$ is less than n, since X^n is the smallest monic monomial in $\mathcal{Q}_n$. By Eq. (8) above, $f(X)$ is in $\mathcal{M}^n$, since p^{n-m} divides q_m, $G_m \in \mathcal{M}^m$ and $R_{m-1} \in \mathcal{M}^n$ by Lemma 3.3 (notice that $m - 1 < p$). $\square$

Remark 4. In the case $p \geqslant n$, Lemma 3.3 implies that $\mathcal{Q}_n$ is generated by $\{p^{n-m}G_m(X)\}_{0 \leqslant m \leqslant n}$: it is easy to verify that these polynomials are in $\mathcal{Q}_n$ (using (3) again) and (8) implies that every polynomial $f \in \mathcal{Q}_n$ is a $\mathbb{Z}$-linear combination of $\{p^{n-m}G_m(X)\}_{0 \leqslant m \leqslant n}$, since $q_m(mp)$ is divisible by p^{n-m}, for each of the relevant m.

The following theorem gives a description of the ideal I_{p^n} in the case $p \geqslant n$. In this case the containment of Corollary 3.1 becomes an equality.

Theorem 3.1. *Let $p \in \mathbb{Z}$ be a prime and n a positive integer such that $p \geqslant n$. Then the ideal in $\mathbb{Z}[X]$ of those polynomials whose fixed divisor is divisible by p^n is equal to*

$$I_{p^n} = \left(p, \prod_{i=0,\dots,p-1} (X - i)\right)^n.$$

Proof. By Proposition 3.1, for each $j = 0, \dots, p-1$ the ideal $\mathcal{Q}_{n,j}$ is equal to $\mathcal{M}_j^n$. So, by the last formula of the proof of Corollary 3.1, we get the statement. $\square$

As a consequence, we have the following remark. Let p be a prime and n a positive integer less than or equal to p. Let $f \in I_{p^n}$ such that the content of $f(X)$ is not divisible by p. Then $\deg(f) \geqslant np$, since $np = \deg(\prod_{i=0,\dots,p-1}(X-i)^n)$. Another well-known result in this context is the following: if we fix the degree d of such a polynomial f, then the maximum n such that $f \in I_{p^n}$ is bounded by $n \leqslant \sum_{k \geqslant 1}[d/p^k] = v_p(d!)$.

If we drop the assumption $p \geqslant n$, the ideal $\mathcal{Q}_{n,j}$ may strictly contain $\mathcal{M}_j^n$, as we observed in Remark 3. The next proposition shows that this is always the case, if $p < n$. This result follows from Lemma 3.3 as Proposition 3.1 does, and it covers the remaining case $p < n$. It is stated for the case $j = 0$. Remember that $\mathcal{M} = (p, X)$ and $\mathcal{Q}_n = \bigcap_{i \equiv 0 \pmod p}(p^n, X-i)$.

Proposition 3.2. *Let $p \in \mathbb{Z}$ be a prime and n a positive integer such that $p < n$. Then we have*

$$\mathcal{Q}_n = \mathcal{M}^n + \bigl(q_{n,p}G_p(X), \dots, q_{n,n-1}G_{n-1}(X)\bigr)$$

where, for each $k = p, \dots, n-1$, $q_{n,k}$ is an integer defined as follows:

$$q_{n,k} \doteqdot \begin{cases} p^{n-v_p((pk)!)}, & \text{if } v_p((pk)!) < n, \\ 1, & \text{otherwise.} \end{cases}$$

In particular, $\mathcal{M}^n$ is strictly contained in $\mathcal{Q}_n$.

Proof. We begin by proving the containment $(\supseteq)$. Lemma 3.2 gives $\mathcal{M}^n \subseteq \mathcal{Q}_n$. We have to show that the polynomials $q_{n,k}G_k(X)$, for $k \in \{p, \dots, n-1\}$, lie in $\mathcal{Q}_n$. This follows from property i) of the polynomials $G_k(X)$ and the definition of $q_{n,m}$.

Now we prove the other containment $(\subseteq)$. Let $f \in \mathcal{Q}_n$ be of degree m. If $m < p$ then $f \in \mathcal{M}^n$ (see Lemma 3.3 and in particular (8)). So we suppose $p \leqslant m$. By Lemma 3.3 we have

$$f(X) = \sum_{k=p,\dots,m} q_h(hp)G_h(X) + R_{p-1}(X) \tag{9}$$

where $R_{p-1}(X) = \sum_{k=1,\dots,p-1} q_k(hp)G_h(X) \in \mathcal{M}^n$ and $q_m \in \mathbb{Z}$, so that $q_m(mp) = q_{n,m}$. Then, since $q_{n,k} = p^{n-v_p((pk)!)} | q_k(kp)$ if $v_p((pk)!) < n$, it follows that the first sum on the right-hand side of the previous equation belongs to the ideal $(q_{n,p}G_p(X), \dots, q_{n,n-1}G_{n-1}(X))$. For the last sentence of the proposition, we remark that the polynomials $\{q_{n,k}G_k(X)\}_{k=p,\dots,n-1}$ are not contained in $\mathcal{M}^n$: in fact, for each $k \in \{p, \dots, n-1\}$, by property iii) of the polynomials $G_k(X)$ we have that the minimal integer N such that $q_{n,k}G_k(X)$ is contained in $\mathcal{M}^N$ is $n - v_p(k!)$ if $v_p((pk)!) = k + v_p(k!) < n$ and it is k otherwise. In both cases it is strictly less than n (since $v_p(k!) \geqslant 1$, if $k \geqslant p$). $\square$

Remark 5. The following remark allows us to obtain another set of generators for $\mathcal{Q}_n$. We set

$$\overline{m} = \overline{m}(n, p) \doteqdot \min\bigl\{m \in \mathbb{N} \bigm| v_p\bigl((pm)!\bigr) \geqslant n\bigr\}. \tag{10}$$

Remember that $v_p((pm)!) = m + v_p(m!)$. If $p \geqslant n$ then $\overline{m} = n$ and if $p < n$ then $p \leqslant \overline{m} < n$.

Suppose $p < n$. Then for each $m \in \{\overline{m}, \dots, n\}$ we have $v_p((pm)!) \geqslant n$, since the function $e(m) = m + v_p(m!)$ is increasing. So for each such m we have $q_{n,m} = 1$, hence $G_m \in (G_{\overline{m}}(X))$. So we have the equalities:

$$\begin{aligned} \mathcal{Q}_n &= \mathcal{M}^n + \bigl(q_{n,m}G_m(X) \bigm| m = p, \dots, \overline{m}\bigr) \\ &= \bigl(q_{n,m}G_m(X) \bigm| m = 0, \dots, \overline{m}\bigr) \end{aligned} \tag{11}$$

where $q_{n,m} = p^{n-m}$, for $m = 0, \dots, p-1$, and for $m = p, \dots, \overline{m}$ is defined as in the statement of Proposition 3.2. The containment ($\supseteq$) is just an easy verification using the properties of the polynomials $G_m(X)$; the other containment follows by (9).

We can now group together Proposition 3.1 and 3.2 into the following one:

Proposition 3.3. *Let $p \in \mathbb{Z}$ be a prime and n a positive integer. Then we have*

$$\mathcal{Q}_n = \big(q_{n,0}G_0(X), \dots, q_{n,\overline{m}}G_{\overline{m}}(X)\big)$$

where $\overline{m} = \min\{m \in \mathbb{N} \mid v_p((pm)!) \geqslant n\}$ and for each $m = 0, \dots, \overline{m}$, $q_{n,m}$ is an integer defined as follows:

$$q_{n,m} \doteq \begin{cases} p^{n-v_p((pm)!)}, & m < \overline{m}, \\ 1, & m = \overline{m}. \end{cases}$$

It is clear what the primary ideals $\mathcal{Q}_j$, for $j = 1, \dots, p-1$, look like:

$$\begin{aligned} \mathcal{Q}_{n,j} &= \bigcap_{i \equiv j \ (\mathrm{mod}\ p)} \big(p^n, X - i\big) = \mathcal{M}_j^n + \big(q_{n,p}G_p(X-j), \dots, q_{n,\overline{m}}G_{\overline{m}}(X-j)\big) \\ &= \big(q_{n,0}G_0(X-j), \dots, q_{n,\overline{m}}G_{\overline{m}}(X-j)\big). \end{aligned}$$

In fact, for each $j = 1, \dots, p-1$, it is sufficient to consider the automorphisms of $\mathbb{Z}[X]$ given by $\pi_j(X) = X - j$. It is straightforward to check that $\pi_j(I_{p^n}) = I_{p^n}$. Moreover, $\pi(\mathcal{Q}_{n,0}) = \mathcal{Q}_{n,j}$ and $\pi(\mathcal{M}_0) = \mathcal{M}_j$ for each such a j, so that π_j permutes the primary components of the ideal I_{p^n}.

The ideal $I_{p^n} = p^n \operatorname{Int}(\mathbb{Z}) \cap \mathbb{Z}[X]$ was studied in [2] in a slightly different context, as the kernel of the natural map $\varphi_n : \mathbb{Z}[X] \to \Phi_n$, where the latter is the set of functions from $\mathbb{Z}/p^n\mathbb{Z}$ to itself. In that article a recursive formula is given for a set of generators of this ideal. Our approach gives a new point of view to describe this ideal.

For other works about the ideal I_{p^n} in a slightly different context, see [9,10,13]. This ideal is important in the study of the problem of the polynomial representation of a function from $\mathbb{Z}/p^n\mathbb{Z}$ to itself.

4. Case $I_{p^{p+1}}$

As a corollary we give an explicit expression for the ideal I_{p^n} in the case $n = p+1$. By Proposition 3.2 the primary components of $I_{p^{p+1}}$ are

$$\mathcal{Q}_{p+1,j} = \mathcal{M}_j^{p+1} + \big(G_p(X-j)\big) \tag{12}$$

for $j = 0, \dots, p-1$.

Corollary 4.1.

$$I_{p^{p+1}} = \Bigg(p, \prod_{i=0,\dots,p-1}(X-i)\Bigg)^{p+1} + \big(H(X)\big)$$

where $H(X) = \prod_{i=0,\dots,p^2-1}(X-i)$.

We want to stress that the polynomial $H(X)$ is not contained in the first ideal of the right-hand side of the statement. In [2] a similar result is stated with another polynomial $H_2(X)$ instead of our $H(X)$. Indeed the two polynomials, as already remarked in [2], are congruent modulo the ideal $(p, \prod_{i=0,\dots,p-1}(X-i))^{p+1}$.

Proof of Corollary 4.1. Like before, we set $\mathcal{Q}_{p,p+1,j} = \mathcal{Q}_{p+1,j}$. The containment ($\supseteq$) follows from Corollary 3.1 and because the polynomial $H(X)$ is equal to $\prod_{j=0,\dots,p-1} G_p(X-j)$ and for each $j = 0,\dots,p-1$ the polynomial $G_p(X-j)$ is in $\mathcal{Q}_{p+1,j}$ by Proposition 3.2. Since $\mathcal{Q}_{p+1,j}$, for $j = 0,\dots,p-1$, are exactly the primary components of $I_{p^{p+1}}$ (see (4)), we get the claim.

Now we prove the other containment ($\subseteq$). Let $f \in I_{p^{p+1}} = \bigcap_{j=0,\dots,p-1} \mathcal{Q}_{p+1,j}$. By (12) we have:

$$f(X) \equiv C_{p,j}(X) G_p(X-j) \pmod{\mathcal{M}_j^{p+1}}$$

for some $C_{p,j} \in \mathbb{Z}[X]$, for $j = 0,\dots,p-1$.

Since the ideals $\{\mathcal{M}_j^{p+1} = (p, X-j)^{p+1} \mid j = 0,\dots,p-1\}$ are pairwise coprime (because they are powers of distinct maximal ideals, respectively), by the Chinese Remainder Theorem we have the following isomorphism:

$$\mathbb{Z}[X] \Big/ \left(\prod_{j=0}^{p-1} \mathcal{M}_j^{p+1} \right) \cong \mathbb{Z}[X]/\mathcal{M}_0^{p+1} \times \cdots \times \mathbb{Z}[X]/\mathcal{M}_{p-1}^{p+1}. \tag{13}$$

We need now the following lemma, which tells us what is the residue of the polynomial $H(X)$ modulo each ideal $\mathcal{M}_j^{p+1}$:

Lemma 4.1. *Let p be a prime and let $H(X) = \prod_{j=0,\dots,p-1} G_p(X-j)$. Then for each $k = 0,\dots,p-1$ we have*

$$H(X) \equiv -G_p(X-k) \pmod{\mathcal{M}_k^{p+1}}.$$

Proof. Let $k \in \{0,\dots,p-1\}$ and set $I_k = \{0,\dots,p-1\} \setminus \{k\}$. For each $j \in I_k$ we have $G_p(k-j) \equiv (k-j)^p \pmod{p}$. We have

$$H(X) + G_p(X-k) = G_p(X-k)\left[1 + \prod_{j \in I_k} G_p(X-j)\right].$$

Since $G_p(X-k) \in \mathcal{M}_k^p$ we have just to prove that $T_k(X) = 1 + \prod_{j \in I_k} G_p(X-j) \in \mathcal{M}_k$. By formula (3) in Remark 1 it is sufficient to prove that $T_k(k)$ is divisible by p. We have

$$\begin{aligned} T_k(k) &\equiv 1 + \prod_{j \in I_k} (k-j)^p \pmod{p} \\ &\equiv 1 + \left(\prod_{s=1,\dots,p-1} s \right)^p \pmod{p} \\ &\equiv 1 + (p-1)!^p \pmod{p} \\ &\equiv \bigl(1 + (p-1)!\bigr)^p \pmod{p} \end{aligned}$$

which is congruent to zero by Wilson's theorem. $\square$

We finish now the proof of the corollary.

By the Chinese Remainder Theorem, there exists a polynomial $P \in \mathbb{Z}[X]$ such that $P(X) \equiv -C_{p,j}(X) \pmod{\mathcal{M}_j^{p+1}}$, for each $j = 0, \ldots, p-1$. Then by the previous lemma $P(X)H(X) \equiv C_{p,j}(X)G_p(X-j) \pmod{\mathcal{M}_j^{p+1}}$ and so again by the isomorphism (13) above we have

$$f(X) \equiv P(X)H(X) \quad \left(\mathrm{mod} \prod_{j=0,\ldots,p-1} \mathcal{M}_j^{p+1}\right)$$

so we are done since $\prod_{j=0,\ldots,p-1} \mathcal{M}_j^{p+1} = (p, \prod_{i=0,\ldots,p-1}(X-i))^{p+1}$ (see the proof of Corollary 3.1). □

Acknowledgments

I want to thank the referee for his/her suggestions. I wish also to thank Sophie Frisch for the useful references. I deeply thank Elvira Carlotti for her continuous and strenuous help. The author was supported by the Austrian Science Foundation (FWF), Project Number P23245-N18.

References

[1] D.F. Anderson, P.-J. Cahen, S.T. Chapman, W. Smith, Some factorization properties of the ring of integer-valued polynomials, in: Zero-Dimensional Commutative Rings, Knoxville, TN, 1994, in: Lect. Notes Pure Appl. Math., vol. 171, Dekker, New York, 1995, pp. 125–142.
[2] A. Bandini, Functions $f: \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ induced by polynomials of $\mathbb{Z}[X]$, Ann. Mat. Pura Appl. (4) 181 (1) (2002) 95–104.
[3] J.-L. Chabert, Anneaux de polynômes à valeurs entières et anneaux de Fatou, Bull. Soc. Math. France 99 (1971) 273–283.
[4] P.-J. Cahen, J.-L. Chabert, Integer-Valued Polynomials, Math. Surv. Monogr., vol. 48, Amer. Math. Soc., Providence, 1997.
[5] P.-J. Cahen, J.-L. Chabert, Elasticity for integral-valued polynomials, J. Pure Appl. Algebra 103 (3) (1995) 303–311.
[6] S.T. Chapman, B. McClain, Irreducible polynomials and full elasticity in rings of integer-valued polynomials, J. Algebra 293 (2) (2005) 595–610.
[7] L.E. Dickson, Introduction to the Theory of Numbers, Univ. Chicago Press, Chicago, 1929.
[8] H. Gunji, D.L. McQuillan, On a class of ideals in an algebraic number field, J. Number Theory 2 (1970) 207–222.
[9] G. Keller, F.R. Olson, Counting polynomial functions $\pmod{p^n}$, Duke Math. J. 35 (1968) 835–838.
[10] D.J. Lewis, Ideals and polynomial functions, Amer. J. Math. 78 (1956) 71–77.
[11] K.A. Loper, Ideals of integer-valued polynomial rings, Comm. Algebra 25 (3) (1997) 833–845.
[12] D.L. McQuillan, On Prüfer domains of polynomials, J. Reine Angew. Math. 358 (1985) 162–178.
[13] I. Niven, L.J. Warren, A generalization of Fermat's theorem, Proc. Amer. Math. Soc. 8 (1957) 306–313.
[14] D.G. Northcott, Ideal Theory, Cambridge University Press, 1953.