Comm. Algebra, 43 (1), 197-211, 2015, http://dx.doi.org/10.1080/00927872.2014.897563.

Factorization of integer-valued polynomials with square-free denominator

Giulio Peruginelli

Dedicated to Marco Fontana on the occasion of his 65th birthday

Abstract

We describe an algorithm to compute the different factorizations of a given image primitive integer-valued polynomial $f(X) = g(X)/d \in \mathbb{Q}[X]$, where $g \in \mathbb{Z}[X]$ and $d \in \mathbb{N}$ is square-free, assuming that the factorizations of $g(X)$ in $\mathbb{Z}[X]$ and d in $\mathbb{Z}$ are known. We translate this problem into a combinatorial one.

Keywords: Integer-valued polynomial, Factorization, Fixed divisor, Primary components. MSC Classification codes: 13B25, 13F20, 13P05.

1 Introduction

It is well known that the ring of integer-valued polynomials $\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subset \mathbb{Z}\}$ is far from being a unique factorization domain. We know that the ring $\mathrm{Int}(\mathbb{Z})$ is atomic (every non-zero non-unit of $\mathrm{Int}(\mathbb{Z})$ admits a factorization into irreducibles) and every non-zero non-unit has only has only finitely many factorizations into irreducibles (see [7]). In particular, this implies that $\mathrm{Int}(\mathbb{Z})$ is a bounded factorization domain (the length of the different factorizations of a given element is bounded, see [2, Prop. VI.3.2]). Moreover, in [3] it is shown that the ring has infinite elasticity, where the elasticity of a domain is defined as the supremum of the set of ratios between length of factorizations of non-zero non-units. We recall that the length of a factorization is the number of irreducible elements which appear in the factorization itself. Two factorizations into irreducibles of an element x in a commutative ring R, say $x = r_1 \cdot \ldots \cdot r_n$ and $x = s_1 \cdot \ldots \cdot s_m$, are essentially the same if $n = m$ and after possibly re-indexing, r_i is associated to s_i, for $i = 1, \ldots, n$ (that is, there exists a unit $u_i \in R$ such that $r_i = u_i s_i$). Otherwise the two factorizations are essentially different (see [7]).

More recently, in [7] the following result is proved. Given a finite set $S = \{n_1, \ldots, n_r\}$ of (non necessarily distinct) positive integers greater than 1, there exists an integer-valued polynomial $f(X)$ with r essentially distinct factorizations into irreducibles of length $n_1, \ldots, n_r$, respectively. Hence, there are elements in the ring of integer-valued polynomials which admit distinct factorizations into irreducibles of arbitrary lengths.

We propose here a new method to describe the essentially different factorizations into irreducibles of a given integer-valued polynomial, under the assumption that the denominator is square-free (we will treat the general case in a future work). We remark that in all the examples produced in [7] to exhibit polynomials with prescribed sets of lengths, only polynomials with square-free denominator appear (in [7, Thm. 10] there is a polynomial with more than one prime in the denominator, in all the other results there is just one prime factor in the denominator). So, a treatment of this case has a certain interest. We begin by recalling some classical definitions.

Definition 1.1. The **content** of a polynomial $g(X) = \sum_{k=0,\ldots,n} a_k X^k \in \mathbb{Z}[X]$ is defined as the g.c.d. of its coefficients a_k. We denote the content of $g(X)$ by $\mathrm{c}(g)$. A polynomial $g \in \mathbb{Z}[X]$ is called **primitive** if its content is equal to 1. Given $f \in \mathrm{Int}(\mathbb{Z})$, we denote by $\mathrm{d}(f)$ the **fixed divisor** of f, that is the g.c.d. of the set of values $\{f(n) \mid n \in \mathbb{Z}\}$. An integer-valued polynomial $f(X)$ is said to be **image primitive** if its fixed divisor is equal to 1. Let $p \in \mathbb{Z}$ be a prime. If $g \in \mathbb{Z}[X]$ we say that $g(X)$ is p-primitive if p does not divide $\mathrm{c}(g)$, that is, at least one of the coefficient of $g(X)$ is not divisible by p. If $f \in \mathrm{Int}(\mathbb{Z})$, we say that $f(X)$ is p-image primitive if p does not divide $\mathrm{d}(f)$.

Given a polynomial $g \in \mathbb{Z}[X]$, the content of $g(X)$ is in general a proper divisor of the fixed divisor of $g(X)$: consider for example $g(X) = X(X-1)$ which is primitive but its fixed divisor is equal to 2. Already in [4] it is shown the important role played by the fixed divisor in the study of the factorizations of an integer-valued polynomial (see the results that we recall below). For example, the polynomial $g(X) = X^2 + X + 2$, which is irreducible in $\mathbb{Z}[X]$ (and consequently in $\mathbb{Q}[X]$ by Gauss Lemma), has fixed divisor equal to 2, so that in $\mathrm{Int}(\mathbb{Z})$ we have the non trivial factorization $g(X) = 2 \cdot \frac{g(X)}{2}$.

We recall the following facts:

- $\mathrm{Int}(\mathbb{Z})$, $\mathbb{Z}[X]$ and $\mathbb{Z}$ share the same group of units, $\{\pm 1\}$ ([3, Lemma 1.1]).
- An irreducible integer p stays irreducible in $\mathrm{Int}(\mathbb{Z})$ ([2, Lemma VI.3.1]).
- $\mathrm{Int}(\mathbb{Z})$ has no prime elements ([1, Prop. 3.2]).
- If $g \in \mathbb{Z}[X]$ is p-primitive for some prime p and p divides the fixed divisor of $g(X)$, then $p \le \deg(g)$ (this is due to Polya, see [8, Thm. 3.1] for a modern treatment).
- Let $g \in \mathbb{Z}[X]$ be primitive. Then $g(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ if and only if it is image primitive and irreducible in $\mathbb{Z}[X]$ (Chapman-McClain [4, Thm. 2.6]). Hence,

an irreducible factor in $\mathrm{Int}(\mathbb{Z})$ of an irreducible polynomial $g \in \mathbb{Z}[X]$ is either a constant c which is a divisor of $d(g)$ or $\frac{g(X)}{d(g)}$.

- Given two integer-valued polynomials f and g, we have $d(fg) \subset d(f)d(g)$ and in general we may not have an equality (see the above example $X(X-1)$). This is the main difference between fixed divisor and content: in fact, the content of the product of two polynomials $g_1(X)$ and $g_2(X)$ is equal to the product of the contents of $g_1(X)$ and $g_2(X)$ by Gauss Lemma. This is equivalent to the fact that a primitive polynomial $g \in \mathbb{Z}[X]$ is irreducible if and only if it is irreducible in $\mathbb{Q}[X]$; this sentence is no more true if we substitute the ring $\mathbb{Q}[X]$ with $\mathrm{Int}(\mathbb{Z})$ (see the above example $g(X) = X^2 + X + 2$). By the above cited theorem of Chapman-McClain, we have to add the assumption that $g(X)$ is also image primitive. We notice that a factor of an image primitive polynomial is image primitive ([4]).

Given a polynomial $f \in \mathbb{Q}[X]$, we have $f(X) = g(X)/d$, for some uniquely determined $g \in \mathbb{Z}[X]$ and $d \in \mathbb{N}$ such that $(d, \mathrm{c}(g)) = 1$ (we essentially use the fact that $\mathbb{Z}$ is UFD). For short, we call d the denominator of $f(X)$ and $g(X)$ the numerator of $f(X)$.

We can further express $f(X)$ in the following way:

$$f(X) = \frac{g(X)}{d} = \frac{\prod_{i \in I} g_i(X)^{e_i}}{\prod_{k \in K} p_k^{e_k}} \tag{1}$$

where $g(X) = \prod_{i \in I} g_i(X)^{e_i}$ is the unique irreducible factorization in $\mathbb{Z}[X]$ (the $g_i(X)$ may be possibly constant) and $d = \prod_{k \in K} p_k^{f_k}$ is the factorization of d in $\mathbb{Z}$. Obviously, $f(X)$ is integer-valued if and only if d divides the fixed divisor of $g(X)$, that is, for each $k = 1, \ldots, m$, $p_k^{e_k}$ divides $\mathrm{d}(g)$. Since $\mathrm{Int}(\mathbb{Z}) \subset \mathbb{Q}[X]$ and $\mathbb{Q}[X]$ is a UFD, any irreducible factor $h(X)$ of $f(X)$ in $\mathrm{Int}(\mathbb{Z})$ is a rearrangement of the irreducible factors $g_i(X)$ of $g(X)$ and the prime factors p_k of d, in such a way that we still have an integer-valued polynomial, that is:

$$h(X) = \frac{g_1(X)}{d_1} = \frac{\prod_{i \in J} g_i(X)^{e'_i}}{\prod_{k \in T} p_k^{f'_k}}$$

where $J \subseteq I$, $T \subseteq K$, $e'_i \leq e_i, f'_k \leq f_k$ for each $i \in J$ and $k \in T$ and $h(X)$ is in $\mathrm{Int}(\mathbb{Z})$, that is d_1 divides $\mathrm{d}(g_1)$. It is already not clear how a general irreducible polynomial in $\mathrm{Int}(\mathbb{Z})$ looks like (for polynomials $g \in \mathbb{Z}[X]$ which are irreducible in $\mathrm{Int}(\mathbb{Z})$ see the above Theorem of Chapman-McClain). To our knowledge, the only characterization of such irreducibles is given by [4, Cor. 2.9], which largely relies on the problem of establishing the fixed divisor of a polynomial with integer coefficients. We will give a new characterization of the irreducible elements of $\mathrm{Int}(\mathbb{Z})$ in the case of square-free denominator.

As we observed above, being image primitive is a necessary condition for an integer-valued polynomial to be irreducible. We will give a chacterization of image primitive polynomials. In particular, being image primitive implies that the numerator $g(X)$ is primitive (since we assume that the denominator d is coprime with the content of $g(X)$). Notice that the converse of the previous statement does not hold, namely, if an integer-valued $f(X)$ is image primitive then it is not true in general that $f(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$. Consider for example $f(X) = X(X-1)^2/2$ which has the irreducible factor $X-1$ (by [3, Cor. 2.2 & Example 2.3], monic linear polynomials are irreducible in $\mathrm{Int}(\mathbb{Z})$).

Let $p \in \mathbb{Z}$ be a fixed prime. We set

$$I_p \doteqdot p\mathrm{Int}(\mathbb{Z}) \cap \mathbb{Z}[X] = \{g \in \mathbb{Z}[X] \mid p|d(g)\},$$

which is the ideal of polynomials in $\mathbb{Z}[X]$ whose fixed divisor is divisible by p. From [9] (but see also [5, Chapt. 2, **18**, p. 22]) we know that

$$I_p = (p, X^p - X) = \Big(p, \prod_{i=0,\dots,p-1}(X-i)\Big) = \bigcap_{j=0}^{p-1}(p, X-j).$$

The last intersection is precisely the primary decomposition of the ideal I_p (see [9, Lemma 2.2]). For $j = 0, \dots, p-1$, we set

$$\mathcal{M}_{p,j} \doteqdot (p, X-j) = \{g \in \mathbb{Z}[X] \mid p|g(j)\}.$$

The above intersection is actually equal to a product of ideals, since $\mathcal{M}_{p,j}$, for $j = 0, \dots, p-1$, are p distinct maximal ideals in $\mathbb{Z}[X]$. More in general, if n is a positive integer, we set

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

which is the ideal of polynomials whose fixed divisor is divisible by p^n. Clearly, a polynomial $f \in \mathbb{Q}[X]$ like in (1) is in $\mathrm{Int}(\mathbb{Z})$ if and only if for every prime factor p_k of the denominator d, the numerator $g(X)$ is in $I_{p_k^{e_k}}$.

In the next section we will introduce the notion of prime covering for the set of irreducible factors of the numerator of an integer-valued polynomial $f(X)$. For each prime p which appears in the denominator and for each irreducible polynomial $g \in \mathbb{Z}[X]$ which appears in the numerator, we look for the primary components of I_p which contain $g(X)$. A subset of the irreducible factors $\{g_i(X)\}_{i\in I}$ of the numerator of $f(X)$ whose elements are contained in all the primary components of I_p is called a p-covering. A p-covering is minimal if, whenever we remove an element, one of the primary components of I_p is not covered by any of the polynomials left in the p-covering itself. In the case of prime denominator, say $f(X) = \frac{g(X)}{p} = \frac{\prod_{i\in I} g_i(X)}{p}$, $f(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ if and only if $\{g_i(X)\}_{i\in I}$ form a minimal p-covering. In the same way, if for a subset $J \subsetneq I$ we have $\prod_{i\in J} g_i(X)$ in I_p, then $f(X)$ is reducible in $\mathrm{Int}(\mathbb{Z})$. If that choice is minimal in the above sense, then that factor is irreducible.

In the subsequent section, we generalize the previous results to the case of an integer-valued polynomial with square-free denominator. Finally, as an explicit example, we consider the case of an integer-valued polynomial with denominator equal to the product of two distinct primes.

2 Integer-valued polynomials with prime denominator

2.1 Prime covering

Definition 2.1. Let $g \in \mathbb{Z}[X]$ and $p \in \mathbb{Z}$ be a prime. We set

$$C_{p,g} \doteqdot \{j \in \{0, \ldots, p-1\} \mid p|g(j)\}.$$

Notice that the elements of $C_{p,g}$ correspond precisely to the primary components $\mathcal{M}_{p,j} = (p, X-j)$ of I_p which contain $g(X)$. Observe that the set $C_{p,g}$ can be empty: for instance, take $g(X) = X^2 + 1$ and $p = 3$. Obviously, $\#C_{p,g} \leq p$. Equivalently, we may consider the polynomial $\overline{g} \in (\mathbb{Z}/p\mathbb{Z})[X]$ obtained by reducing the coefficients of g modulo p. A residue class $j \in \mathbb{Z}/p\mathbb{Z}$ is a root of $\overline{g}(X)$ if and only if the primary component $\mathcal{M}_{p,j}$ of I_p contains $g(X)$.

We have the following result, which involves the family of sets $\{C_i\}_{i\in I}$ just defined. We omit the proof, which follows directly from the definitions.

Lemma 2.1. *Let $g(X) = \prod_{i\in I} g_i(X)$ be a product of polynomials in $\mathbb{Z}[X]$ and let p be a prime. For each $i \in I$, let $C_i = C_{p,g_i}$. Then*

$$g \in I_p \Leftrightarrow \bigcup_{i\in I} C_i = \{0, \ldots, p-1\}.$$

In particular, $g(X)$ is p-image primitive if and only if there exists $j \in \{0, \ldots, p-1\}$ such that no C_i contains j.

Notice that the condition $g(X)$ is p-image primitive is equivalent to $g \notin I_p$. Obviously we don't need to factor a given integer coefficient polynomial $g(X)$ in $\mathbb{Z}[X]$ in order to establish whether it is p-image primitive or not (just consider it modulo p as we said above). By Polya's Theorem we cited in the introduction, it is sufficient to consider only those primes p which are less or equal to the degree of $g(X)$. Anyway, for the study of the problem of the factorization in the ring $\mathrm{Int}(\mathbb{Z})$ it is useful to write the statement as it is.

We give now the following definition.

Definition 2.2. Let $\mathcal{G} = \{g_i(X)\}_{i\in I}$ be a set of polynomials in $\mathbb{Z}[X]$. Let p be a prime. For each $i \in I$ we set $C_i = C_{p,g_i}$. A p-**covering** for $\mathcal{G}$ (or just **prime covering**, if the prime p is understood) is a subset J of I such that

$$\bigcup_{i\in J} C_i = \{0, \ldots, p-1\}.$$

We say that J is **minimal** if no proper subset J' of J has the same property. We will always assume that a given prime covering J is *proper*, that is, for each $i \in J$ we have $C_i \neq \emptyset$.

Two p-covering $J_1, J_2 \subset I$ for $\mathcal{G}$ are disjoint if $J_1 \cap J_2 = \emptyset$.

Notice that from a prime covering we can always extract a minimal prime covering, by discarding the redundant sets C_i. We may rephrase Lemma 2.1 by saying that $f(X) = g(X)/p = \prod_{i\in I} g_i(X)/p$ belongs to $\mathrm{Int}(\mathbb{Z})$ if and only if I contains a p-covering for $\{g_i\}_{i\in I}$. A minimal p-covering can have 1 element, for example consider the irreducible polynomial $X^p - X + p$. It has at most p elements. The problem to find such p-coverings has a combinatorial flavour.

The next example shows that given a minimal p-covering J, it does not follow that $\{C_i\}_{i\in J}$ forms a family of disjoint subsets of the residue classes modulo p. In fact, a polynomial $g_i(X)$ may belong to different primary components of I_p. If this is the case the degree of $g_i(X)$ has to be greater than one.

Example 2.1.

$$f(X) = \frac{(X^2 - X + 3)(X^2 + 2)}{3} \tag{2}$$

if we set $g_1(X) = X^2 - X + 3, g_2(X) = X^2 + 2$ we immediately see that

- $C_{3,g_1} = \{0, 1\}, C_{3,g_2} = \{1, 2\}$
- $C_{2,g_1} = \emptyset, C_{2,g_2} = \{0\}$

the second line implies that 2 does not divide the fixed divisor of the numerator, that is $f(X)$ is 2-image primitive (by Polya's Theorem, we check only those primes p which are less or equal to the degree of $f(X)$). We have that C_{3,g_1} and C_{3,g_2} covers the residue classes modulo 3 and they have non trivial intersection. In particular, $I = \{1, 2\}$ is a minimal 3-covering.

2.2 Integer-valued polynomials which are p-image primitive

We characterize now p-image primitive integer-valued polynomials, when the denominator is exactly divisible by a prime p (we denote this by $p \parallel d$).

Suppose that for a polynomial $f(X)$ as in (1) the denominator d is equal to a prime p. If $f(X)$ is p-image primitive, then there exists $i \in I$ such that $e_i = 1$, otherwise the fixed divisor of the numerator $g(X)$ is divisible by p^n, for some $n > 1$. For example, $\frac{X(X-1)^2}{2}$ is 2-image primitive, while $\frac{X^2(X-1)^2}{2}$ is not (the numerator has fixed divisor equal to 4). However, this condition on the exponents of the irreducible factors $g_i(X)$ is not sufficient to ensure that $f(X)$ is p-image primitive, as the next example shows:

$$f(X) = \frac{(X^2 + 4)(X^2 + 3)}{2} \tag{3}$$

The polynomial $f(X)$ is not 2-image primitive since the numerator has fixed divisor equal to 4 (modulo 2, each factor at the numerator has a double root in 0 and 1, respectively).

Moreover, under the above assumption, the next lemma shows that all the minimal p-coverings must intersect in one spot. For $g(X) = \prod_{i \in I} g_i(X) \in \mathbb{Z}[X]$ and $J \subseteq I$, we set

$$g_J(X) \doteqdot \prod_{i \in J} g_i(X).$$

For each $i \in I$ we set $C_i = C_{p,g_i}$. By Lemma 2.1, for any subset $J \subseteq I$ we have $g_J \in I_p \Leftrightarrow J$ is a p-covering.

Lemma 2.2. *Let*

$$f(X) = \frac{\prod_{i \in I} g_i(X)}{d}$$

be in $\mathrm{Int}(\mathbb{Z})$. *Let p be a prime factor of d such that $p \parallel d$. Then $f(X)$ is p-image primitive if and only if the following condition holds: there exists a primary component $\mathcal{M}_{p,\bar{j}}$ of I_p, for some $\bar{j} \in \{0, \ldots, p-1\}$, such that $g_{\bar{i}} \in \mathcal{M}_{p,\bar{j}} \setminus \mathcal{M}^2_{p,\bar{j}}$ for some $\bar{i} \in I$ and for all $i \in I$, $i \neq \bar{i}$, we have $g_i \notin \mathcal{M}_{p,\bar{j}}$.*

If that condition holds, then for every minimal p-covering $J \subseteq I$, we have $\bar{i} \in J$.

Proof : Suppose $f(X)$ is p-image primitive. If for every $j \in \{0, \ldots, p-1\}$ there exist $i_1(j) \neq i_2(j)$ in I such that $g_{i_1}, g_{i_2} \in \mathcal{M}_{p,j}$, then we can form two disjoint p-coverings $J_t = \{i_t(j)\}_{j=0,\ldots,p-1}$, for $t = 1, 2$. By Lemma 2.1 the polynomials g_{J_1} and g_{J_2} belong to I_p, thus their fixed divisor is divisible by p; since g_I is divisible by $g_{J_1} \cdot g_{J_2}$, it has fixed divisor divisible by p^2, contradiction. So there exists $j' \in \{0, \ldots, p-1\}$ for which only one irreducible factor $g_{i'}(X)$ is in $\mathcal{M}_{p,j'}$. If $g_{i'} \notin \mathcal{M}^2_{p,j'}$ we are done. Suppose that is not the case. If for all the other j's we have either more than one factor $g_i(X)$ in $\mathcal{M}_{p,j}$ or a factor $g_i(X)$ which belongs to $\mathcal{M}^2_{p,j}$ we get again to the same contradiction as before. Hence, there must be some $\bar{j} \in \{0, \ldots, p-1\}$ for which the corresponding primary component $\mathcal{M}_{p,\bar{j}}$ of I_p contains only one factor $g_{\bar{i}}(X)$. Moreover, $g_{\bar{i}} \notin \mathcal{M}^2_{p,\bar{j}}$.

Conversely, suppose there exists $\bar{j} \in \{0, \ldots, p-1\}$ as in the statement. If, for each $i \in I$, we set $C_i = C_{p,g_i}$ we have that $\bar{j} \notin C_i$ for all $i \neq \bar{i}$. Let $J \subseteq I$ be a minimal p-covering for $\{g_i\}_{i \in I}$ (we know that such a prime covering exists by Lemma 2.1). Since by definition $\bigcup_{i \in J} C_i = \{0, \ldots, p-1\}$, and for all $i \in I$, $i \neq \bar{i}$, we have $C_i \not\ni \bar{j}$, it follows that $\bar{i}$ is contained in J. Notice that this proves the last statement of the Lemma. So there are no two disjoint p-coverings. Since $g_{\bar{i}} \notin \mathcal{M}^2_{p,\bar{j}}$ and $g_{\bar{i}}$ is the only factor of the numerator of $f(X)$ in $\mathcal{M}_{p,\bar{j}}$ we have that $g_J \notin I_{p^2}$. Since this holds for every minimal p-covering J, this concludes the proof of the lemma. $\square$

Remark 2.1. Under the assumptions of Lemma 2.2, $f(X)$ is p-image primitive if and only if there exists a primary component $\mathcal{M}_{p,\bar{j}}$ of I_p which contains one and only one irreducible factor $g_{\bar{i}}(X)$ of the numerator of $f(X)$ and $g_{\bar{i}} \notin \mathcal{M}^2_{p,\bar{j}}$. In particular, this means that only $C_{\bar{i}}$ contains $\bar{j}$.

The last statement of Lemma 2.2 cannot be reversed, see for example (3). We have to add the hypothesis that for each minimal p-covering $J \subseteq I$ there exists at least one $i \in J$ such that $g_i \in \mathcal{M}_{p,j} \setminus \mathcal{M}_{p,j}^2$ for some $j \in J$. Equivalently, by the remarks after Definition 2.1, we can say that for at least one residue classes j modulo p, there is one and only one irreducible factor $g_i(X)$ which has a simple root modulo p in j.

We can have more than one minimal p-covering, say $J_1, J_2 \subseteq I$, provided they are not disjoint, as Lemma 2.2 says. For instance, consider the polynomial:

$$f(X) = \frac{X(X-1)(X-2)}{2 \cdot 3} \tag{4}$$

which is known to be irreducible ([3, Example 2.8]; in particular, $f(X)$ is image primitive). We set $g_{i+1}(X) = X - i$, for $i = 0, 1, 2$. Then $J_1 = \{1, 2\}$ and $J_2 = \{2, 3\}$ are different minimal 2-coverings, which are not disjoint.

Example 2.2.

$$f(X) = \frac{X^2 \cdot (X-1) \cdot (X^2+4)}{2}$$

in this example only $X - 1$ belongs to $\mathcal{M}_{2,1}$ and moreover it does not belong to $\mathcal{M}_{2,1}^2$. Hence, the polynomial is 2-image primitive.

Example 2.3.

$$f(X) = \frac{X \cdot (X^2 - 2X + 5) \cdot (X+6)}{2}$$

in this example, only $g(X) = X^2 - 2X + 5$ belongs to $\mathcal{M}_{2,1}$. Moreover, $g \in \mathcal{M}_{2,1}^2$. No irreducible polynomial in the numerator belongs to $\mathcal{M}_{2,0}^2$, but there are two distinct factors, namely X and $X + 6$, which belong to $\mathcal{M}_{2,0}$. Hence, $f(X)$ is not 2-image primitive, since the fixed divisor of the numerator is 4. So it is not sufficient to have a unique $\bar{i} \in I$ such that $g_{\bar{i}} \in \mathcal{M}_{p,\bar{j}}$. We must also take care of the exact power of the maximal ideal $\mathcal{M}_{p,j}$ to which each polynomial $g_i(X)$ belongs to.

2.3 Irreducible integer-valued polynomials

Suppose that an integer-valued polynomial $f(X)$ is of the form

$$f(X) = \frac{g(X)}{p} = \frac{\prod_{i \in I} g_i(X)}{p} \tag{5}$$

where, for $i \in I$, $g_i \in \mathbb{Z}[X]$ is irreducible. The fact that $f \in \mathrm{Int}(\mathbb{Z})$ is image primitive amounts to saying that $d(g)$ is equal to p. Since $f \in \mathrm{Int}(\mathbb{Z})$, by Lemma 2.1 there exists a p-covering $J \subseteq I$ for $\{g_i(X)\}_{i \in I}$. The next lemma establishes that $f(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ if and only if I is a minimal p-covering.

Lemma 2.3. *An image primitive polynomial* $f(X) = g(X)/p$ *in* $\mathrm{Int}(\mathbb{Z})$ *as in (5) is irreducible in* $\mathrm{Int}(\mathbb{Z})$ *if and only if there is no proper subset* J *of* I *such that* $\bigcup_{j\in J} C_j = \{0,\dots,p-1\}$ *(that is,* I *is a minimal* p*-covering).*

Proof : Suppose there exists $J \subsetneq I$ such that J is a p-covering. Then

$$f(X) = \frac{g_J(X)}{p} \cdot g_{I\setminus J}(X)$$

is a non-trivial factorization of $f(X)$ in $\mathrm{Int}(\mathbb{Z})$, because the first factor is integer-valued by Lemma 2.1 and the second one is in $\mathbb{Z}[X] \subset \mathrm{Int}(\mathbb{Z})$.

Conversely, if $f(X)$ is reducible in $\mathrm{Int}(\mathbb{Z})$, then there exist non-constant $g, h \in \mathrm{Int}(\mathbb{Z})$ such that $f(X) = h_1(X)h_2(X)$ (because we are assuming $f(X)$ to be image primitive). Since p must appear in the denominator of one of the two factors, say $h_1(X)$, then for some $\emptyset \neq J \subsetneq I$ we have $h_1(X) = g_J(X)/p$ and consequently $h_2 = g_{I\setminus J} \in \mathbb{Z}[X]$. Since $h_1 \in \mathrm{Int}(\mathbb{Z})$, by Lemma 2.1 J is a p-covering (notice that $h_1 \in \mathrm{Int}(\mathbb{Z}) \Leftrightarrow g_J \in I_p$). $\square$

Notice that Lemma 2.3 does not hold without assuming $f(X)$ to be image primitive, as example (3) shows. By the arguments we have just given, we deduce that every factorization of an image primitive integer-valued polynomial with prime denominator $f(X) = \frac{g(X)}{p}$ is of the form $f(X) = \frac{g_J(X)}{p} \cdot g_{I\setminus J}(X)$, for some $J \subseteq I$ minimal p-covering. Notice that the number of irreducible factors of the previous factorization in $\mathrm{Int}(\mathbb{Z})$ is $1 + \#(I \setminus J)$. The assumption that $f(X)$ is image primitive implies that for each such a minimal p-covering J, the set $I \setminus J$ does not contain a p-covering.

3 Integer-valued polynomials with square-free denominator

The main problem in the general case of more than one prime factor in the denominator d of an integer-valued polynomial $f(X)$ is that each irreducible factor $g_i(X)$ of the numerator of $f(X)$ may belong to different primary components $\mathcal{M}_{p_k,j}$ of I_{p_k}, where $\{p_k\}_{k\in K}$ are the different prime factors of d.

As already remarked in [6], this phenomenon has the effect that if p,q are two distinct primes, then it does not follow that $I_p \cdot I_q = I_{pq}$: for example, $g(X) = X(X-1)(X-2)$ belongs to $I_{2\cdot 3}$ (see (4)), but it cannot be expressed as a product of a polynomial in I_2 and a polynomial in I_3. This is due to the fact that the only minimal 3-covering $J = \{1, 2, 3\}$ is equal to the set I itself, so in particular it has non-zero intersection with any possible 2-covering (we saw that there are only two of them). Hence, in the next subsection, we are lead to give this globalizing definition.

3.1 Family of minimal $\mathcal{P}$-coverings

Definition 3.1. Let $\mathcal{G} = \{g_i(X)\}_{i\in I}$ be a set of polynomials in $\mathbb{Z}[X]$ and let $\mathcal{P} = \{p_k\}_{k\in K}$ be a set of distinct prime integers. A **family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$** is a family of sets $\{J_k\}_{k\in K}$ such that for each $k \in K$, $J_k \subseteq I$ is a minimal p_k-covering for $\mathcal{G}$.

Let $f \in \mathbb{Q}[X]$ be as in (1). If $f(X)$ is an integer-valued polynomial, then by Lemma 2.1 there exists a family of minimal $\mathcal{P} = \{p_k\}_{k\in K}$-coverings for $\mathcal{G} = \{g_i(X)\}_{i\in I}$.

We can now formulate a proposition, which gives a criterion for an integer-valued polynomial to be irreducible, in the case that the denominator is square-free. This is a first step to determine explicitly all the factorizations of a given element in the ring $\mathrm{Int}(\mathbb{Z})$.

Firstly we set some notations. Let

$$f(X) = \frac{g(X)}{d} = \frac{\prod_{i\in I} g_i(X)}{\prod_{k\in K} p_k} \tag{6}$$

be a polynomial in $\mathbb{Q}[X]$, with p_k distinct prime integers, $g_i \in \mathbb{Z}[X]$ irreducible polynomials. Notice that the condition that $f(X)$ is integer-valued is equivalent to $g_I(X) = \prod_{i\in I} g_i(X) \in \bigcap_{k\in K} I_{p_k}$. We set $\mathcal{G} = \{g_i(X)\}_{i\in I}$ and $\mathcal{P} = \{p_k\}_{k\in K}$. As in the previous section, given $J \subseteq I$ we set $g_J(X) \doteqdot \prod_{i\in J} g_i(X)$. Notice that if $J_1 \subseteq J_2 \subseteq I$ we have that $g_{J_1}(X)$ divides $g_{J_2}(X)$ in $\mathbb{Z}[X]$ (and so in $\mathrm{Int}(\mathbb{Z})$). Similarly, for a subset $T \subseteq K$ we set

$$d_T \doteqdot \prod_{k\in T} p_k$$

($d_K = d$). With these notations, a factor of $f(X)$ is of the form:

$$h(X) = \frac{g_J(X)}{d_T}$$

for some $J \subseteq I$ and $T \subseteq K$.

Finally, if $T \subseteq K$ and $\mathcal{J} = \{J_k\}_{k\in K}$ is a family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$, we set

$$I_{\mathcal{J},T} \doteqdot \bigcup_{k\in T} J_k.$$

Notice that, if $T_1, T_2 \subseteq K$ are two disjoint subsets, then $I_{\mathcal{J},T_1\cup T_2} = I_{\mathcal{J},T_1} \cup I_{\mathcal{J},T_2}$.

3.2 Irreducible integer-valued polynomials

Theorem 3.1. *Let*

$$f(X) = \frac{g(X)}{d} = \frac{\prod_{i\in I} g_i(X)}{\prod_{k\in K} p_k}$$

be an image primitive integer-valued polynomial. Let $\mathcal{P} = \{g_i(X)\}_{i\in I}$ *and* $\mathcal{G} = \{p_k\}_{k\in K}$*. We suppose that the polynomials* $g_i(X)$ *are irreducible in* $\mathbb{Z}[X]$ *and that the* p_k *are distinct prime integers. Then* $f(X)$ *is irreducible in* $\mathrm{Int}(\mathbb{Z})$ *if and only if the following holds: for every family* $\mathcal{J} = \{J_k\}_{k\in K}$ *of minimal* $\mathcal{P}$*-coverings for* $\mathcal{G}$ *we have*

i) $I = I_{\mathcal{J},K}$*.*

ii) there is no non-trivial partition $K = K_1 \dot\cup K_2$ *such that* $I_{\mathcal{J},K_1} \cap I_{\mathcal{J},K_2} = \emptyset$*.*

Notice that condition i) implies that for each $i \in I$ there exists $k \in K$ such that $C_{p_k,g_i} \neq \emptyset$, so that each of the g_i's belongs to at least one of the primary components $\mathcal{M}_{p_k,j}$ of some of the ideals I_{p_k}. Moreover, condition ii) says that the union of the elements J_k of the family $\mathcal{J}$ cannot be partitioned (in a sense we will make precise soon). We will treat the case $\mathcal{P} = \{p_1, p_2\}$ as an example in section 3.4.

Proof : Suppose $f \in \mathrm{Int}(\mathbb{Z})$ irreducible. Let $\mathcal{J} = \{J_k\}_{k\in K}$ be a family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$ (it exists because of Lemma 2.1). If I strictly contains $I_{\mathcal{J},K}$ then there exists $t \in I$ which is not contained in any J_k (equivalently, $J_k \subseteq I \setminus \{t\}$ for every $k \in K$). This means that $g_t(X)$ divides $f(X)$ in $\mathrm{Int}(\mathbb{Z})$, because we have

$$f(X) = g_t(X) \cdot \frac{g_{I\setminus\{t\}}(X)}{d}$$

and the second factor is integer-valued, since for each $k \in K$ we have $g_{J_k}(X) \in I_{p_k}$ (see Lemma 2.1). Hence, for all such k's, we have $g_{I\setminus\{t\}}(X) \in I_{p_k}$, since $J_k \subseteq I \setminus \{t\}$. This is a contradiction, hence condition i) holds.

If we have a non-trivial partition $K = K_1 \dot\cup K_2$ such that $I_1 \doteqdot I_{\mathcal{J},K_1}$ and $I_2 \doteqdot I_{\mathcal{J},K_2}$ are disjoint, then

$$f(X) = \frac{g_{I_1}(X)}{d_{K_1}} \cdot \frac{g_{I_2}(X)}{d_{K_2}}.$$

Notice that for every $k_1 \in K_1$ we have $g_{J_{k_1}}(X) \in I_{p_{k_1}}$ (again by Lemma 2.1) and $g_{J_{k_1}}(X)$ divides $g_{I_1}(X)$ in $\mathbb{Z}[X]$, since $J_{k_1} \subset I_1$. This implies that $g_{I_1}(X)/d_{K_1}$ is integer-valued. Similarly, the second factor is integer-valued, too. That would be a non-trivial factorization of $f(X)$, which is a contradiction.

Conversely, suppose that for every family $\mathcal{J} = \{J_k\}_{k\in K}$ of minimal $\mathcal{P}$-coverings for $\mathcal{G}$ conditions i) and ii) hold. Since $f(X)$ is image primitive, there is no non-unit in $\mathbb{Z}$ which divides $f(X)$ in $\mathrm{Int}(\mathbb{Z})$. If $f(X)$ is reducible in $\mathrm{Int}(\mathbb{Z})$ we have $f(X) = h_1(X)h_2(X)$, where $h_1, h_2 \in \mathrm{Int}(\mathbb{Z})$ are not constant. Since $\mathrm{Int}(\mathbb{Z}) \subset \mathbb{Q}[X]$ we have

$$h_i(X) = \frac{g_{I_i}(X)}{d_{K_i}}$$

for some $I_i \subseteq I$ and $K_i \subseteq K$, for $i = 1, 2$. Necessarily, I_1, I_2 are disjoint and $I_1 \cup I_2 = I$. Similarly, K_1 and K_2 are disjoint and $K_1 \cup K_2 = K$. Suppose that one of the K_i, say K_2, is empty. Then, by Lemma 2.1 for each $k \in K_1 = K$ there exists a minimal p_k-covering $J_k \subseteq I_1$. We set $\mathcal{J} = \{J_k\}_{k \in K}$. By definition, the family $\mathcal{J}$ is a minimal $\mathcal{P}$-coverings for $\mathcal{G}$. In particular, $I_{\mathcal{J},K} \subseteq I_1$, because each of the J_k's is a subset of I_1. Because of i) we have that $I = I_{\mathcal{J},K}$, so that $I = I_1$ and consequently $I_2 = \emptyset$, since I_1 and I_2 are disjoint. This means that $h_2(X)$ is a unit.

Suppose now that $K_i \neq \emptyset$, for $i = 1, 2$. This fact also leads us to a contradiction. In fact, by Lemma 2.1, for each $i = 1, 2$ and for each $k_i \in K_i$ there exists a minimal p_{k_i}-covering $J_{k_i} \subseteq I_i$. We set $\mathcal{J} = \{J_k\}_{k \in K}$, which is a family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$. In particular, $I_{\mathcal{J},K_i} \subseteq I_i$. By condition i) on $\mathcal{J}$ we have that

$$I = I_{\mathcal{J},K} = I_{\mathcal{J},K_1} \dot{\cup} I_{\mathcal{J},K_2}.$$

Since $I_1 \cup I_2 = I$, we get $I_{\mathcal{J},K_i} = I_i$ for $i = 1, 2$, which is in contradiction with condition ii). $\square$

Example 3.1. It is not sufficient that conditions i) and ii) of Theorem 3.1 hold only for one family $\{J_k\}_{k \in K}$ of minimal $\mathcal{P}$-coverings. For instance, let us consider

$$f(X) = \frac{(X-1) \cdot (X-2) \cdot (X-3) \cdot (X-9)}{2 \cdot 3}$$

then if $g_i(X) = X - i$, for $i = 1, 2, 3$, $g_4(X) = X - 9$ and $I = \{1, 2, 3, 4\}$, we have that

- $J_2 = \{2, 1\}$, $J_2' = \{2, 3\}$ and $J_2'' = \{2, 4\}$ are the minimal 2-coverings.
- $J_3 = \{1, 2, 3\}$ and $J_3' = \{1, 2, 4\}$ are the minimal 3-coverings.

We have that $\mathcal{J} = \{J_2'', J_3\}$ is a family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$ which satisfies both conditions i) and ii) but the polynomial is not irreducible, since $X - 9$ divides $f(X)$ in $\mathrm{Int}(\mathbb{Z})$. In fact, the family $\mathcal{J}' = \{J_2', J_3\}$ of $\mathcal{P}$-coverings for $\mathcal{G}$ does not satisfy condition i) of the proposition.

Remark 3.1. From Theorem 3.1 we see that each family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$ determines a (possibly trivial, like for $\mathcal{J}$ in Example 3.1) factorization for $f(X)$ in $\mathrm{Int}(\mathbb{Z})$. Conversely, every non-trivial factorization determines a family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$ which can be partitioned in the following sense:

Definition 3.2. We say that a family $\mathcal{J}$ of minimal $\mathcal{P}$-coverings for $\mathcal{G}$ is **partitionable** if there exist a partition for K, say $K = \dot{\bigcup}_{j \in \mathcal{I}} K_j$ such that the sets $\{I_{\mathcal{J},K_j} = \bigcup_{k \in K_j} J_k \mid j \in \mathcal{I}\}$ are disjoint.

However, notice that different families of minimal $\mathcal{P}$-coverings may give the same factorization for $f(X)$. For instance, in the Example 3.1, there are six possible such families (we have to pair each minimal 2-covering with a minimal 3-covering). The family $\mathcal{J}'' = \{J_2, J_3\}$ gives the same factorization as $\mathcal{J}'$. This depends on the fact that $I_{\mathcal{J}',K}$ and $I_{\mathcal{J}'',K}$ are equal.

Corollary 3.1. *Let $f(X)$ be as in the assumptions of Theorem 3.1. If there exists $\overline{k} \in K$ such that I is a minimal $p_{\overline{k}}$-covering, then $f(X)$ is irreducible in* $\mathrm{Int}(\mathbb{Z})$.

Proof : We retain the notations of Theorem 3.1. Let $\mathcal{J}$ be a family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$. Notice that I is the only minimal $p_{\overline{k}}$-covering, so $I \in \mathcal{J}$ and consequently $I = I_{\mathcal{J},K}$ and $\mathcal{J}$ is not a partitionable family. Hence, the conditions i) and ii) of Theorem 3.1 are satisfied for every family of minimal $\mathcal{P}$-coverings, so $f(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$. $\square$

In particular, this corollary shows again that the polynomial in (4) is irreducible. The condition of the previous corollary is not necessary, see (10) below for an example.

3.3 The algorithm of factorization in $\mathrm{Int}(\mathbb{Z})$

The next corollary shows explicitly how to obtain a non-trivial factorization of an integer-valued polynomial $f(X)$ as in (6) from a partitionable family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$. We know from the proof of Theorem 3.1 that every such factorization is obtained in this way.

We recall that we are assuming $f(X)$ to be image primitive and the denominator of $f(X)$ to be square-free.

Schematically we are doing the following steps:

i) For each $k \in K$ and for each $i \in I$ we determine the sets C_{p_k,g_i}.

ii) Afterwards for each $k \in K$ we find all the minimal p_k-coverings J_k, by grouping together the sets C_{p_k,g_i}.

iii) Then for each $k \in K$ we choose one of the minimal p_k-coverings we found at point ii) and we define the family $\mathcal{J} = \{J_k\}_{k \in K}$ of minimal $\mathcal{P}$-coverings for $\mathcal{G}$.

Corollary 3.2. *Let*

$$f(X) = \frac{\prod_{i \in I} g_i(X)}{\prod_{k \in K} p_k} = \frac{g_I(X)}{d_K}$$

be an image primitive, integer-valued polynomial, where p_k are distinct prime integers, $g_i \in \mathbb{Z}[X]$ distinct and irreducible.

Every factorization of $f(X)$ in $\mathrm{Int}(\mathbb{Z})$ is obtained in the following way:

let $\mathcal{J} = \{J_k\}_{k \in K}$ be a family of minimal $\mathcal{P}$-coverings for $\mathcal{G}$ which is partitionable, say $K = \dot{\bigcup}_{j \in \mathcal{I}} K_j$, so that the sets $I_j \doteqdot I_{\mathcal{J},K_j} = \bigcup_{k \in K_j} J_k$, for $j \in \mathcal{I}$, are disjoint and for each $j \in \mathcal{I}$ the integer-valued polynomial $g_{I_j}(X)/d_{K_j}$ satisfies the conditions of Theorem 3.1 (so that each of them is irreducible). We set $I' \doteqdot \bigcup_{j \in \mathcal{I}} I_j$. Then

$$f(X) = g_{I \setminus I'}(X) \cdot \prod_{j \in \mathcal{I}} \frac{g_{I_j}(X)}{d_{K_j}}$$

is a factorization of $f(X)$ in $\mathrm{Int}(\mathbb{Z})$ *and every one of them is obtained in that way. Notice that in the previous factorization we have $\#(I \setminus I') + \#\mathcal{I}$ irreducible factors.*

3.4 Case $d = p_1 \cdot p_2$

Let $p_1, p_2 \in \mathbb{Z}$ be distinct primes. We consider an image primitive integer-valued polynomial of the following form:

$$f(X) = \frac{g(X)}{p_1 p_2} = \frac{\prod_{i \in I} g_i(X)}{p_1 p_2} \tag{7}$$

This amounts to saying that the fixed divisor $d(g)$ is equal to $p_1 p_2$. By Lemma 2.1, for $k = 1, 2$, there exists a p_k-covering J_k for $\{g_i(X)\}_{i \in I}$. For each $i \in I$ and for each $k = 1, 2$ we consider the sets C_{p_k, g_i} as defined in section 2. With the notation we introduced so far, we can have two different kind of factorization of $f(X)$. One possible factorization is:

$$f(X) = \frac{g_{J_1}(X)}{p_1} \cdot \frac{g_{J_2}(X)}{p_2} \cdot \prod_{i \in I \setminus J_1 \cup J_2} g_i(X) \tag{8}$$

for some $J_1, J_2 \subseteq I$, where, for $k = 1, 2$, $g_{J_k}(X)/p_k \in \mathrm{Int}(\mathbb{Z})$ is irreducible. By Lemma 2.3, this corresponds to the fact that, for $k = 1, 2$, J_k is a minimal p_k-covering. Obviously, J_1 and J_2 are disjoint.

Another possible factorization is

$$f(X) = \frac{g_J(X)}{p_1 p_2} \cdot \prod_{i \in I \setminus J} g_i(X) \tag{9}$$

for some $J \subseteq I$. In this factorization $g_J(X)/(p_1 p_2) \in \mathrm{Int}(\mathbb{Z})$ is irreducible.

By Lemma 2.1, since $g_J(X)/(p_1 p_2)$ is integer-valued then for each $k = 1, 2$, J contains a minimal p_k-covering J_k. By Theorem 3.1, the fact that $g_J(X)/(p_1 p_2)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ is equivalent to saying that $J = J_1 \cup J_2$ (otherwise, we can factor out some $g_i(X)$ from it) and $J_1 \cap J_2 \neq \emptyset$ (otherwise we fall in the previous case (8)). It is not true that for some $k = 1, 2$ we must have $I = J_k$, like example (10) below shows.

In [4, Example 3.6] the authors construct an integer-valued polynomial which has two distinct factorizations as in (8) and (9). Now we give other two explicit examples: in the first one only the factorization as in (8) occurs, in the second one we give an irreducible polynomial in $\mathrm{Int}(\mathbb{Z})$ of the form $g(X)/(p_1 p_2)$.

Example 3.2.

$$\begin{aligned} f(X) &= \frac{(X^2+12)(X^2+2)(X^2+10)(X^2+16)(X^2+4)}{3 \cdot 5} \\ &= \frac{(X^2+12)(X^2+2)}{3} \cdot \frac{(X^2+10)(X^2+16)(X^2+4)}{5} \end{aligned}$$

the second line is the only factorization in $\mathrm{Int}(\mathbb{Z})$ that $f(X)$ can have, since if we put $g_1(X) = X^2 + 12, g_2(X) = X^2 + 2, g_3(X) = X^2 + 10, g_4(X) = X^2 + 16, g_5(X) = X^2 + 4$ we have:

$$\begin{array}{lllll} C_{3,g_1} = \{0\}, & C_{3,g_2} = \{1,2\}, & C_{3,g_3} = \emptyset, & C_{3,g_4} = \emptyset, & C_{3,g_5} = \emptyset \\ C_{5,g_1} = \emptyset, & C_{5,g_2} = \emptyset, & C_{5,g_3} = \{0\}, & C_{5,g_4} = \{2,3\}, & C_{5,g_5} = \{1,4\} \end{array}$$

so in $I = \{1, \ldots, 5\}$ we only have one 3-covering $J_3 = \{1, 2\}$ and only one 5-covering $J_5 = \{3, 4, 5\}$, and they are disjoint. It is easy to check that 2 and 7 do not divide the fixed divisor of the numerator of $f(X)$.

Example 3.3.

$$f(X) = \frac{X(X^2 + 2)(X^2 + 16)(X^2 + 4)}{3 \cdot 5} \tag{10}$$

so if $g_1(X) = X, g_2(X) = X^2 + 2, g_3(X) = X^2 + 16, g_4(X) = X^2 + 4$ we have:

$$\begin{array}{llll} C_{3,g_1} = \{0\}, & C_{3,g_2} = \{1,2\}, & C_{3,g_3} = \emptyset, & C_{3,g_4} = \emptyset \\ C_{5,g_1} = \{0\}, & C_{5,g_2} = \emptyset, & C_{5,g_3} = \{2,3\}, & C_{5,g_4} = \{1,4\} \end{array}$$

Then by Theorem 3.1 $f(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ since $J_3 = \{1, 2\}$ is the only minimal 3-covering, $J_5 = \{1, 3, 4\}$ is the only minimal 5-covering, $I = J_3 \cup J_5$ and $J_3 \cap J_5 \neq \emptyset$. Notice that $J_3 \subsetneq I, J_5 \subsetneq I$. It is easy to check that 2 and 7 do not divide the fixed divisor of the numerator $g(X)$ of $f(X)$. In particular, $f(X)$ is image primitive, that is $d(g) = 3 \cdot 5$.

Example 3.4. As another application of Theorem 3.1 we consider the polynomial:

$$f(X) = \frac{X \cdot (X^2 + 1) \cdot (X^2 + X + 1) \cdot (X^2 + 2X + 4)}{2 \cdot 3}$$

and let $g_1(X) = X$, $g_2(X) = X^2 + 1$, $g_3(X) = X^2 + X + 1$, $g_4(X) = X^2 + 2X + 4$. Then

- $J_2 = \{1, 2\}$ and $J_2' = \{2, 4\}$ are the minimal 2-coverings.
- $J_3 = \{1, 3, 4\}$ is the only minimal 3-covering.

So $\mathcal{J} = \{J_2, J_3\}$ is a family of minimal $\mathcal{P}$-coverings of $\mathcal{G}$ such that $J_2 \subsetneq I$, $J_3 \subsetneq I$. The same holds for $\mathcal{J}' = \{J_2', J_3\}$. The polynomial is irreducible by Theorem 3.1: if we consider $\mathcal{J}$ we have $I = J_2 \cup J_3$ and $J_2 \cap J_3 \neq \emptyset$. The same holds for $\mathcal{J}'$.

Our method can be easily generalized to the case of denominator divisible by prime powers p^n such that $n \leq p$, since in this case, by [9, Proposition 3.1], the primary components of the ideal I_{p^n} are just the n-th power of the maximal ideals $\mathcal{M}_{p,j}$, for $j = 0, \ldots, p-1$. In general, a further study of the primary components of the ideal I_{p^n} is needed.

Acknowledgments

I would like to thank the referee for his/her valuable suggestions. The author was supported by the Austrian Science Foundation (FWF), Project Number P23245-N18 and also by INDAM - GNSAGA.

References

[1] D. F. Anderson, P.-J. Cahen, S.T. Chapman and W. Smith, *Some factorization properties of the ring of integer-valued polynomials*, Zero-dimensional commutative rings (Knoxville, TN, 1994), 125-142, Lecture Notes in Pure and Appl. Math., 171, Dekker, New York, 1995.

[2] J.-P. Cahen, J.-L. Chabert, *Integer-valued polynomials*, Amer. Math. Soc. Surveys and Monographs, 48, Providence, 1997.

[3] J.-P. Cahen, J.-L. Chabert, *Elasticity for integral-valued polynomials.*, J. Pure Appl. Algebra 103 (1995), no. 3, 303-311.

[4] S.T.Chapman, B. McClain. *Irreducible polynomials and full elasticity in rings of integer-valued polynomials*, J. Algebra 293 (2005), no. 2, 595-610.

[5] L. E. Dickson. *Introduction to the theory of numbers.* Chicago 1929.

[6] D. J. Lewis. *Ideals and Polynomial Functions*, Amer. J. Math. 78 (1956), 71-77.

[7] S. Frisch. *A construction of integer-valued polynomials with prescribed sets of lengths of factorizations*, Monatsh. Math. 171 (2013), 341-350.

[8] W. Narkiewicz. *Polynomial mappings*, Lecture Notes in Mathematics, 1600. Springer-Verlag, Berlin, 1995. viii+130 pp. ISBN: 3-540-59435-3.

[9] G. Peruginelli. *Primary decomposition of the ideal of polynomials whose fixed divisor is divisible by a prime power.* Accepted for publication by Journal of Algebra.