BINOMIAL IDEALS AND CONGRUENCES ON $\mathbb{N}^n$

DEDICATED TO PROFESSOR ANTONIO CAMPILLO ON THE OCCASION OF HIS 65TH BIRTHDAY.

LAURA FELICIA MATUSEVICH AND IGNACIO OJEDA

ABSTRACT. A *congruence* on $\mathbb{N}^n$ is an equivalence relation on $\mathbb{N}^n$ that is compatible with the additive structure. If $\Bbbk$ is a field, and I is a *binomial ideal* in $\Bbbk[X_1,\ldots,X_n]$ (that is, an ideal generated by polynomials with at most two terms), then I induces a congruence on $\mathbb{N}^n$ by declaring $\mathbf{u}$ and $\mathbf{v}$ to be equivalent if there is a linear combination with nonzero coefficients of $\mathbf{X}^{\mathbf{u}}$ and $\mathbf{X}^{\mathbf{v}}$ that belongs to I. While every congruence on $\mathbb{N}^n$ arises this way, this is not a one-to-one correspondence, as many binomial ideals may induce the same congruence. Nevertheless, the link between a binomial ideal and its corresponding congruence is strong, and one may think of congruences as the underlying combinatorial structures of binomial ideals. In the current literature, the theories of binomial ideals and congruences on $\mathbb{N}^n$ are developed separately. The aim of this survey paper is to provide a detailed parallel exposition, that provides algebraic intuition for the combinatorial analysis of congruences. For the elaboration of this survey paper, we followed mainly [10] with an eye on [5] and [13].

1. Preliminaries

In this section we introduce our main objects of study: binomial ideals and monoid congruences, and recall some basic results.

Throughout this article, $\Bbbk[\mathbf{X}] := \Bbbk[X_1,\ldots,X_n]$ is the commutative polynomial ring in n variables over a field $\Bbbk$. In what follows we write $\mathbf{X}^{\mathbf{u}}$ for $X_1^{u_1}X_2^{u_2}\cdots X_n^{u_n}$, where $\mathbf{u}=(u_1,u_2,\ldots,u_n)\in\mathbb{N}^n$, where here and henceforth, $\mathbb{N}$ denotes the set of nonnegative integers.

1.1. Binomial ideals.

In this section we begin our study of binomial ideals. First of all, we recall that a **binomial** in $\Bbbk[\mathbf{X}]$ is a polynomial with at most two terms, say $\lambda\mathbf{X}^{\mathbf{u}}+\mu\mathbf{X}^{\mathbf{v}}$, where $\lambda,\mu\in\Bbbk$ and $\mathbf{u},\mathbf{v}\in\mathbb{N}^n$. We emphasize that, according to this definition, monomials are binomials.

Definition 1. *A* ***binomial ideal*** *of* $\Bbbk[\mathbf{X}]$ *is an ideal of* $\Bbbk[\mathbf{X}]$ *generated by binomials.*

Throughout this article, we assume that the base field $\Bbbk$ is algebraically closed. The reason for this is that some desirable results are not valid over an arbitrary field. These include the characterization of binomial prime ideals (Theorem 34), and the fact that associated primes of binomial ideals are binomial (see, e.g. Proposition 50). This failure can be seen even in one variable: the ideal $\langle X^2+1\rangle\subset\mathbb{R}[X]$ is prime, but does not conform to the description in Theorem 34; the ideal $\langle X^3-1\rangle\subset\mathbb{R}[X]$ has the associated prime $\langle X^2+X+1\rangle$, which is not binomial. It is also worth noting that the characteristic of $\Bbbk$ plays a role when studying binomial ideals, as can be seen by the different behaviors presented by $\langle X^p-1\rangle\subset\Bbbk[X]$ depending on whether the characteristic of $\Bbbk$ is p.

Key words and phrases. Binomial ideals. Graded Algebras. Congruences. Semigroup ideals. Toric ideals. Primary decomposition.

The first author was partially supported by NSF grant DMS-1500832.

The second author was partially supported by the project MTM2015-65764-C3-1, National Plan I+D+I, and by Junta de Extremadura (FEDER funds) - FQM-024.

The following result is an invaluable tool when studying binomial ideals.

Proposition 2. *Let $I \subset \Bbbk[\mathbf{X}]$ be an ideal. The following are equivalent:*

(1) I is a binomial ideal.
(2) The reduced Gröbner basis of I with respect to any monomial order on $\Bbbk[\mathbf{X}]$ consists of binomials.
(3) A universal Gröbner basis of I consists of binomials.

Proof. If I has a binomial generating set, the S-polynomials produced by a step in the Buchberger algorithm are necessarily binomials. □

Since the Buchberger algorithm for computing Gröbner bases respects the binomial condition, Gröbner techniques are particularly effective when working with these objects. In particular, it can be shown that some important ideal theoretic operations preserve binomiality. For instance, it is easy to show that eliminating variables from binomial ideals results in binomial ideals.

Corollary 3. *Let I be a binomial ideal of $\Bbbk[\mathbf{X}]$. The elimination ideal $I \cap \Bbbk[X_i \mid i \in \sigma]$ is a binomial ideal for every nonempty subset $\sigma \subset \{1, \ldots, n\}$.*

Proof. The intersection is generated by a subset of the reduced Gröbner basis of I with respect to a suitable lexicographic order. □

Example 4. Let $\varphi : \Bbbk[X, Y, Z] \to \Bbbk[T]$ be the $\Bbbk-$algebra morphism such that

$$X \to T^3, Y \to T^4 \text{ and } Z \to T^5.$$

It is known that $\ker(\varphi) = \langle X - T^3, Y - T^4, Z - T^5\rangle \cap \Bbbk[X, Y, Z]$. As a consequence of Corollary 3, $\ker(\varphi)$ is a binomial ideal. In fact, $\ker(\varphi)$ is the ideal generated by $\{Y^2 - XZ, X^2Y - Z^2, X^3 - YZ\}$, as can be checked by executing the following code in Macaulay2 ([8]):

```
R = QQ[X,Y,Z,T]
I = ideal(X-T^3,Y-T^4,Z-T^5)
eliminate(T,I)
```

Taking ideal quotients is a fundamental operation in commutative algebra. We can now show that some ideal quotients of binomial ideals are binomial.

Corollary 5. *If I is a binomial ideal of $\Bbbk[\mathbf{X}]$, and $\mathbf{X}^\mathbf{u}$ is a monomial, then $(I : \mathbf{X}^\mathbf{u})$ is a binomial ideal.*

Proof. Recall that if $\{f_1, \ldots, f_\ell\}$ is a system of generators for $I \cap \langle \mathbf{X}^\mathbf{u}\rangle$, then $\{f_1/\mathbf{X}^\mathbf{u}, \ldots, f_\ell/\mathbf{X}^\mathbf{u}\}$ is a system of generators for $(I : \mathbf{X}^\mathbf{u})$. Thus, the binomiality of $(I : \mathbf{X}^\mathbf{u})$ follows if we show that $I \cap \langle \mathbf{X}^\mathbf{u}\rangle$ is binomial.

Introducing an auxiliary variable T, we have that

$$I \cap \langle \mathbf{X}^\mathbf{u}\rangle = (TI + (1 - T)\langle \mathbf{X}^\mathbf{u}\rangle) \cap \Bbbk[\mathbf{X}].$$

Since $TI + (1 - T)\langle \mathbf{X}^\mathbf{u}\rangle$ is a binomial ideal, Corollary 3 implies that $I \cap \langle \mathbf{X}^\mathbf{u}\rangle$ is also binomial, as we wanted. □

We remark that the ideal quotient of a binomial ideal by a binomial is not necessarily binomial, and neither is the ideal quotient of a binomial ideal by a monomial ideal. When taking colon with a single binomial, the above proof breaks because the product of two binomials is not a binomial in general; indeed,

$$\big(\langle X^3 - 1\rangle : \langle X - 1\rangle\big) = \langle X^2 + X + 1\rangle \subset \Bbbk[X].$$

In the case of taking ideal quotient by a monomial ideal, say $J = \langle \mathbf{X}^{\mathbf{u}_1}, \ldots \mathbf{X}^{\mathbf{u}_r}\rangle$, instead of a single monomial, what makes the argument invalid is that the ideal $(I : J)$ is equal to

$\cap_{i=1}^r (I : \langle \mathbf{X}^{\mathbf{u}_i} \rangle)$, and the intersection of binomial ideals is not necessarily binomial, as the following shows: $\langle X-1 \rangle \cap \langle X-2 \rangle = \langle X^2 - 3X + 2 \rangle \subset \Bbbk[X]$.

1.2. Graded algebras.

Gradings play a big role when studying binomial ideals. The main result of this section is that a ring is a quotient of a polynomial ring by a binomial ideal if and only if it has a special kind of grading (Theorem 8).

Recall that a $\Bbbk-$algebra of finite type R is *graded* by a finitely generated commutative monoid S if R is a direct sum

$$R = \bigoplus_{\mathbf{a} \in S} R_{\mathbf{a}}$$

of $\Bbbk-$vector spaces and the multiplication of R satisfies the rule $R_{\mathbf{a}} R_{\mathbf{a}'} = R_{\mathbf{a}+\mathbf{a}'}$.

Example 6. Observe that $\Bbbk[\mathbf{X}] = \bigoplus_{\mathbf{u} \in \mathbb{N}^n} \mathrm{Span}_{\Bbbk}\{\mathbf{X}^{\mathbf{u}}\}$.

Remark 7. Let I be *any* ideal of $\Bbbk[\mathbf{X}]$ and let π be the canonical projection of $\Bbbk[\mathbf{X}]$ onto $R := \Bbbk[\mathbf{X}]/I$. Let S be the set of all one-dimensional subspaces $\mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{u}})\}$ of R; if the kernel of π contains monomials, we adjoin to S the symbol ∞ associated to the monomials in $\ker(\pi)$. The set S is a commutative monoid with the operation

$$\mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{u}})\} + \mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{v}})\} = \mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{u}}\mathbf{X}^{\mathbf{v}})\} = \mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{u}+\mathbf{v}})\}$$

and identity element $\mathrm{Span}_{\Bbbk}\{1\} = \mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{0}})\}$. Note that if $\mathbf{X}^{\mathbf{v}} \in \ker(\pi)$, then for any other monomial $\mathbf{X}^{\mathbf{u}}$, $\mathbf{X}^{\mathbf{u}}\mathbf{X}^{\mathbf{v}} \in \ker(\pi)$. In other words,

$$\mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{u}})\} + \infty = \infty.$$

We point out that the set $\{\mathrm{Span}_{\Bbbk}\{\pi(X_1)\}, \ldots, \mathrm{Span}_{\Bbbk}\{\pi(X_n)\}\}$ generates S as a monoid. There is a natural $\Bbbk-$vector space surjection

$$\bigoplus_{\substack{\mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{u}})\} \in S \\ \mathbf{X}^{\mathbf{u}} \notin \ker \pi}} \mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{u}})\} \to R. \tag{1}$$

We observe that if (1) is an isomorphism of $\Bbbk-$vector spaces, then R is **finely graded** by S, meaning that R is $S-$graded and every graded piece has dimension at most 1.

The following result provides the first link between binomial ideals and monoids.

Theorem 8. *A $\Bbbk-$algebra R of finite type admits a presentation of the form $\Bbbk[\mathbf{X}]/I$, where I is a binomial ideal, if and only if R can be finely graded by a finitely generated commutative monoid.*

Proof. First assume that R admits a grading of the given type by a finitely generated commutative monoid S. Let $f_1, \ldots, f_n$ be $\Bbbk-$algebra generators of R. Without loss of generality, we may assume that $f_1, \ldots, f_n$ are homogeneous. Denote $\mathbf{a}_i$ the degree of f_i, for $i = 1, \ldots, n$. Since R is (finely) graded by the monoid generated by $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$, we may assume that S is generated by $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$.

Give $\Bbbk[\mathbf{X}]$ an $S-$grading by setting the degree of X_i to be $\mathbf{a}_i$, and consider the surjection $\Bbbk[\mathbf{X}] \to R$ given by $X_i \mapsto f_i$, which is a graded ring homomorphism. The kernel of this map is a homogeneous ideal of $\Bbbk[\mathbf{X}]$, and is therefore generated by homogeneous elements. On the other hand, by the fine grading condition, for any two monomials $\mathbf{X}^{\mathbf{u}}, \mathbf{X}^{\mathbf{v}} \in \Bbbk[\mathbf{X}]$ with the same $S-$degree, neither of which maps to zero in R, there is a scalar $\lambda \in \Bbbk^*$ such that the binomial $\mathbf{X}^{\mathbf{u}} - \lambda \mathbf{X}^{\mathbf{v}} \in \Bbbk[\mathbf{X}]$ maps to zero in R. Thus, the kernel of the above surjection is generated by binomials.

Conversely, by Remark 7, it suffices to show that the map (1) is injective. We need to prove that if Σ is a nonempty subset of $\{\mathrm{Span}_{\Bbbk}\{\pi(\mathbf{X}^{\mathbf{u}})\} \in S \mid \mathbf{X}^{\mathbf{u}} \notin \ker \pi\}$, then the image of Σ in R

is linearly independent. This follows if we show that if $f = \sum_{i=1}^{r} \lambda_i \mathbf{X}^{\mathbf{u}_i} \in I$ with $\lambda_1, \ldots, \lambda_r \in \Bbbk^*$ and $\mathbf{X}^{\mathbf{u}_i} \notin I$ for all $1 \leq i \leq r$, then there exist $1 \leq j \leq r$ and $\lambda \in \Bbbk^*$ such that $\mathbf{X}^{\mathbf{u}_1} - \lambda \mathbf{X}^{\mathbf{u}_j} \in I$ (in other words, $\pi(\mathbf{X}^{\mathbf{u}_1}) = \pi(\mathbf{X}^{\mathbf{u}_j})$). To see this, note that since I is a binomial ideal, it has a $\Bbbk-$vector space basis consisting of binomials, and therefore we can write $f = \sum_{i=1}^{\ell} \mu_i B_i$, where $\mu_1, \ldots, \mu_\ell \in \Bbbk^*$ and each B_i is a binomial in I with two terms, neither of which is in I (the latter by the assumption on f). The monomial $\mathbf{X}^{\mathbf{u}_1}$ must appear in at least one of the binomials $B_1, \ldots, B_\ell$, say B_{i_1}. Of course, the second monomial appearing in B_{i_1} has the same image under π as $\mathbf{X}^{\mathbf{u}_1}$. If this second monomial in B_{i_1} is one of the $\mathbf{X}^{\mathbf{u}_2}, \ldots, \mathbf{X}^{\mathbf{u}_r}$, we are done. Otherwise, the second term of B_{i_1} must appear in another of the binomials B_i, say B_{i_2}. Note that both monomials in B_{i_2} have the same image under π as $\mathbf{X}^{\mathbf{u}_1}$. If the second monomial of B_{i_2} is one of the $\mathbf{X}^{\mathbf{u}_2}, \ldots, \mathbf{X}^{\mathbf{u}_r}$, again, we are done. Otherwise, continue in the same manner. Since we only have finitely many binomials to consider, this process must stop, and produce a monomial $\mathbf{X}^{\mathbf{u}_j}$ such that $\pi(\mathbf{X}^{\mathbf{u}_1}) = \pi(\mathbf{X}^{\mathbf{u}_j})$. □

2. Congruences on monoids and binomial ideals

We now start our study of monoid congruences, and their relationship to binomial ideals. We show how binomial ideals induce congruences, and how any congruence can arise this way. We also address the question of when two different binomial ideals give rise to the same congruence.

Definition 9. *Let S be a commutative monoid. A* ***congruence*** $\sim$ *on S is an equivalence relation on S which is additively closed:* $\mathbf{a} \sim \mathbf{b} \Rightarrow \mathbf{a} + \mathbf{c} \sim \mathbf{b} + \mathbf{c}$ *for* $\mathbf{a}, \mathbf{b}$ *and* $\mathbf{c} \in S$.

The following result, which follows directly from the definition, gives a first indication that congruences on commutative monoids are analogous to ideals in commutative rings.

Proposition 10. *If $\sim$ is a congruence on a commutative monoid S, then $S/\sim$ is a commutative monoid.* □

Let $\phi : S \to S'$ be a monoid morphism.The **kernel of** ϕ is defined as

$$\ker \phi := \big\{(\mathbf{a}, \mathbf{b}) \in S \times S \mid \phi(\mathbf{a}) = \phi(\mathbf{b})\big\}.$$

Note that if ϕ is a monoid morphism, the relation on S determined by $\ker \phi \subset S \times S$ is actually a congruence. Moreover, every congruence on S arises in this way: if $\sim$ is a congruence on S, then $\sim$ can be recovered as the congruence induced by the kernel of the natural surjection $S \to S/\sim$.

We write $\mathrm{cong}(S) \subset \mathcal{P}(S \times S)$ for the set of congruences on S ordered by inclusion. (Here $\mathcal{P}$ indicates the power set.) We say that S is **Noetherian** if every nonempty subset of $\mathrm{cong}(S)$ has a maximal element (equivalently, $\mathrm{cong}(S)$ satisfies the ascending chain condition). The following is an important result in monoid theory.

Theorem 11. *A commutative monoid S is Noetherian if and only if S is finitely generated.*

The fact that a Noetherian monoid is finitely generated is the hard part of the proof. It is due to Budach [4], and is the main result in Chapter 5 in Gilmer's book [7], where it appears as Theorem 5.10. Brookfield has given a short and self contained proof in [2]. We will just provide a proof of the converse, namely, that finitely generated monoids are Noetherian (see [7, Theorem 7.4]), after Theorem 13.

Set S be a commutative monoid finitely generated by $\mathcal{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$. The monoid morphism

$$\pi : \mathbb{N}^n \longrightarrow S;\ \mathbf{e}_i \longmapsto \mathbf{a}_i,\ i = 1, \ldots, n, \tag{2}$$

where $\mathbf{e}_i$ denotes the element in $\mathbb{N}^n$ whose $i-$th coordinate is 1 with all other coordinates 0, is surjective and gives a **presentation**

$$S = \mathbb{N}^n/\sim$$

by simply taking $\sim = \ker \pi$. Unless stated otherwise, we write $[\mathbf{u}]$ for the class of $\mathbf{u} \in \mathbb{N}^n$ modulo $\sim$.

Remark 12. In what follows, all monoids considered are commutative and finitely generated.

Given a monoid S, the **semigroup algebra** $\mathbb{k}[S] := \bigoplus_{\mathbf{a}\in S} \operatorname{Span}_{\mathbb{k}}\{\chi^{\mathbf{a}}\}$ is the direct sum with multiplication $\chi^{\mathbf{a}}\chi^{\mathbf{b}} = \chi^{\mathbf{a}+\mathbf{b}}$. (This terminology is in wide use, even though the algebra $\mathbb{k}[S]$ would be more precisely named a "monoid algebra".)

Theorem 13. *Let $\mathcal{A} = \{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ be a generating set of a monoid S, and consider the presentation map $\pi : \mathbb{N}^n \to S$ induced by $\mathcal{A}$. We define a map of semigroup algebras*

$$\hat{\pi} : \mathbb{k}[\mathbb{N}^n] = \mathbb{k}[\mathbf{X}] \to \mathbb{k}[S] \; ; \quad \mathbf{X}^{\mathbf{u}} \mapsto \chi^{\pi(\mathbf{u})}. \tag{3}$$

Let

$$I_{\mathcal{A}} := \langle \mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \mid \pi(\mathbf{u}) = \pi(\mathbf{v})\rangle \subseteq \mathbb{k}[\mathbf{X}]. \tag{4}$$

Then $\ker \hat{\pi} = I_{\mathcal{A}}$*, so that* $\mathbb{k}[S] \cong \mathbb{k}[\mathbf{X}]/I_{\mathcal{A}}$*. Moreover,* $I_{\mathcal{A}}$ *is spanned as a* $\mathbb{k}-$*vector space by* $\{\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \mid \pi(\mathbf{u}) = \pi(\mathbf{v})\}$.

Proof. By construction, $I_{\mathcal{A}} \subseteq \ker \hat{\pi}$. To prove the other inclusion, give $\mathbb{k}[\mathbf{X}]$ an $S-$grading by setting $\deg(X_i) = \pi(\mathbf{e}_i) = \mathbf{a}_i$. Then the map $\hat{\pi}$ is graded (considering $\mathbb{k}[S]$ with its natural $S-$grading), and therefore its kernel is a homogeneous ideal of $\mathbb{k}[\mathbf{X}]$. Note that $\mathbf{X}^{\mathbf{u}}$ and $\mathbf{X}^{\mathbf{v}}$ have the same $S-$degree if and only if $\pi(\mathbf{u}) = \pi(\mathbf{v})$.

We observe that $\ker \hat{\pi}$ contains no monomials, so any polynomial in $\ker \hat{\pi}$ has at least two terms. Let f be a homogeneous element of $\ker \hat{\pi}$. Then there are $\lambda, \mu \in \mathbb{k}^*$ and $\mathbf{u}, \mathbf{v} \in \mathbb{N}^n$ such that $f = \lambda \mathbf{X}^{\mathbf{u}} + \mu \mathbf{X}^{\mathbf{v}} + g$, with g a homogeneous polynomial with two fewer terms than f. Since f is homogeneous, we have that $\pi(\mathbf{u}) = \pi(\mathbf{v})$, and therefore $\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \in I_{\mathcal{A}} \subset \ker \hat{\pi}$. Then $f - \lambda(\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}})$ is a homogeneous element of $\ker \hat{\pi}$, and has fewer terms than f. Continuing in this manner, we conclude that $f \in I_{\mathcal{A}}$. Since $\ker \hat{\pi}$ is a homogeneous ideal, we see that $I_{\mathcal{A}} \supseteq \ker \hat{\pi}$, and therefore $I_{\mathcal{A}} = \ker \hat{\pi}$.

For the final statement, we note that any binomial ideal in $\mathbb{k}[\mathbf{X}]$ is spanned as a $\mathbb{k}-$vector space by the set of all of its binomials. Since $I_{\mathcal{A}}$ contains no monomials and is $S-$graded, any binomial in $I_{\mathcal{A}}$ is of the form $\mathbf{X}^{\mathbf{u}} - \lambda \mathbf{X}^{\mathbf{v}}$, where $\lambda \in \mathbb{k}^*$ and $\pi(\mathbf{u}) = \pi(\mathbf{v})$. But then $\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \in I_{\mathcal{A}}$, and again using that $I_{\mathcal{A}}$ contains no monomials, we see that $\lambda = 1$. This implies that $\{\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \mid \pi(\mathbf{u}) = \pi(\mathbf{v})\}$ is the set of all binomials of $I_{\mathcal{A}}$, which implies that it is a $\mathbb{k}-$spanning set for this ideal. □

We are now ready to prove that finitely generated monoids are Noetherian.

Proof of Theorem 11, reverse implication. Let S be a finitely generated monoid, and consider a presentation $S = \mathbb{N}^n/\sim$, where $\sim$ is a congruence on $\mathbb{N}^n$. In this proof, for $\mathbf{u} \in \mathbb{N}^n$, we denote by $[\mathbf{u}]$ the equivalence class of $\mathbf{u}$ with respect to $\sim$.

Let $\approx$ be a congruence on S, and let $\simeq$ be the congruence on $\mathbb{N}^n$ given by setting the equivalence class of $\mathbf{u} \in \mathbb{N}^n$ with respect to $\simeq$ to be the set $\bigcup_{\{\mathbf{v}\in\mathbb{N}^n \mid [\mathbf{u}]\approx[\mathbf{v}]\}}[\mathbf{v}]$. Then the congruence $\simeq$ is such that $S/\approx \, = \mathbb{N}^n/\simeq$.

Now let $\approx_1$ and $\approx_2$ be two congruences on S and consider the natural surjections $\pi_i : \mathbb{N}^n \to \mathbb{N}^n/\simeq_i$ for $i = 1, 2$. Then if $\approx_1 \subseteq \approx_2$ (as subsets of $S \times S$), we have that $I_{\mathcal{A}_1} \subseteq I_{\mathcal{A}_2}$, where these ideals are defined as in (4) by considering the generating sets $\mathcal{A}_i = \{\pi_i(\mathbf{e}_j) \mid j = 1, \dots, n\}$, $i = 1, 2$, respectively. We conclude that Noetherianity of the monoid S follows from the fact that $\mathbb{k}[\mathbf{X}]$ is a Noetherian ring. □

In order to continue to explore the correspondence between congruences and binomial ideals, we introduce some terminology.

Definition 14. *A binomial ideal is said to be* ***unital*** *if it is generated by binomials of the form* $\mathbf{X}^{\mathbf{u}} - \lambda \mathbf{X}^{\mathbf{v}}$ *with* λ *equal to either* 0 *or* 1*. A binomial ideal is said to be* ***pure*** *if does not contain any monomial.*

Corollary 15. *A relation* $\sim$ *on* $\mathbb{N}^n$ *is a congruence if and only if there exists a pure unital ideal* $I \subset \Bbbk[\mathbf{X}]$ *such that* $\mathbf{u} \sim \mathbf{v} \Longleftrightarrow \mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \in I$*.*

Proof. If $\sim$ is a congruence on $\mathbb{N}^n$, then $\mathbb{N}^n/\sim$ is a (finitely generated) monoid. Consider the natural surjection $\pi : \mathbb{N}^n \to \mathbb{N}^n/\sim$, and let $\mathcal{A} = \{\pi(\mathbf{e}_1), \ldots, \pi(\mathbf{e}_n)\}$. Use this information to construct $I_{\mathcal{A}}$ as in (4). By Theorem 13 and its proof, the ideal $I_{\mathcal{A}}$ satisfies the required conditions.

For the converse, let I a pure unital ideal of $\Bbbk[\mathbf{X}]$ such that $\mathbf{u} \sim \mathbf{v} \Longleftrightarrow \mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \in I$. Clearly, $\sim$ is reflexive and symmetric. For transitivity, it suffices to observe that $\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{w}} = (\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}}) + (\mathbf{X}^{\mathbf{v}} - \mathbf{X}^{\mathbf{w}}) \in I$, for every $\mathbf{u}, \mathbf{v}$ and $\mathbf{w}$ such that $\mathbf{u} \sim \mathbf{v}$ and $\mathbf{v} \sim \mathbf{w}$. Finally, as I is an ideal, it follows that $\mathbf{X}^{\mathbf{w}}(\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}}) = \mathbf{X}^{\mathbf{u}+\mathbf{w}} - \mathbf{X}^{\mathbf{v}+\mathbf{w}} \in I$, for every $\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \in I$ and $\mathbf{X}^{\mathbf{w}} \in \Bbbk[\mathbf{X}]$. We conclude that $\sim$ is a congruence. □

We review some examples of pure unital binomial ideals and their associated congruences. We remark in particular that different binomial ideals may give rise to the same congruence.

Example 16.

(i) The ideal $I = \langle X - Y \rangle \subset \Bbbk[X, Y]$ defines a congruence $\sim$ on $\mathbb{N}^2$ with $\mathbb{N}^2/\sim = \mathbb{N}$.
(1) The ideal $I = \langle X - Y, Y^2 - 1 \rangle \subset \Bbbk[X, Y]$ defines a congruence $\sim$ on $\mathbb{N}^2$ such that $\mathbb{N}^2/\sim = \mathbb{Z}/2\mathbb{Z}$.
(2) The ideal $I = \langle X^2 - Y^2 \rangle \subset \Bbbk[X, Y]$ defines a congruence $\sim$ on $\mathbb{N}^2$ such that $\mathbb{N}^2/\sim$ is isomorphic to the submonoid S of $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ generated by $(1, 0)$ and $(1, 1)$.
(3) Consider the monoid $S = \{0, a, b\}$ where the sum is defined as follows:

$+$	0	a	b
0	0	a	b
a	a	b	b
b	b	b	b

The ideal $I = \langle X - Y, Y^3 - Y^2 \rangle \subset \Bbbk[X, Y]$ determines a congruence $\sim$ on $\mathbb{N}^2$ such that $S \cong \mathbb{N}^2/\sim$.

An arbitrary binomial ideal J of $\Bbbk[\mathbf{X}]$ induces a congruence $\sim_J$ on $\mathbb{N}^n$ defined as

$$\mathbf{u} \sim_J \mathbf{v} \Longleftrightarrow \text{there exists } \lambda \in \Bbbk^* \text{ such that } \mathbf{X}^{\mathbf{u}} - \lambda \mathbf{X}^{\mathbf{v}} \in J. \tag{5}$$

Note that this ideal defines the same congruence as the pure unital binomial ideal

$$I = \langle \mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \mid \text{there exists } \lambda \in \Bbbk^* \text{ such that } \mathbf{X}^{\mathbf{u}} - \lambda \mathbf{X}^{\mathbf{v}} \in J \rangle.$$

Example 17.

(1) Let $J = \langle X - Y, Y^2 \rangle \subset \Bbbk[X, Y]$. The congruence $\sim_J$ induced by J on $\mathbb{N}^2$ is exactly the same that one in Example 16 3.
(2) The congruence $\sim_{\langle X,Y \rangle}$ on $\mathbb{N}^2$ is the same as the induced by $I = \langle X - Y, X - X^2 \rangle$ on $\mathbb{N}^2$. Note that $\langle X, Y \rangle$ is a monomial ideal, while I contains no monomials.

If a binomial ideal I contains monomials, then the exponents of all monomials in I form a single equivalence class in the congruence $\sim_I$. This equivalence class satisfies an absorption property, as in the definition below.

Definition 18. *A non-identity element* ∞ *in a monoid* S *is* ***nil*** *if* $\mathbf{a} + \infty = \infty$*, for all* $\mathbf{a} \in S$*.*

For example, the "formal" element ∞ introduced in Remark 7 is nil, since it corresponds to the monomial class. Note that a monoid S can have at most one nil element: if $\infty, \infty' \in S$ are both nil, then $\infty + \infty' = \infty'$ because ∞' is nil, and $\infty' + \infty = \infty$ because ∞ is nil. Since S is commutative, $\infty = \infty'$.

As we have noted above, if I is a binomial ideal that contains monomials, then the class of monomial exponents is a nil element for the congruence $\sim_I$. The converse of this assertion is false: if J is a binomial ideal containing monomials, then the ideal I produced by Corollary 15 for the congruence $\sim_J$ has no monomials and has a nil element (since J contains monomials, and therefore $\sim_J$ does). On the other hand, if $\sim$ is a congruence on $\mathbb{N}^n$ with a nil element ∞, then there exists a binomial ideal J in $\Bbbk[\mathbf{X}]$ that contains monomials, and such that $\sim = \sim_J$. To see this, let I be the ideal produced by Corollary 15 for $\sim$, and consider $J = I + \langle \mathbf{X}^\mathbf{e} \mid [\mathbf{e}] = \infty \rangle$, noting that adding this particular monomial ideal does not change the underlying congruence. We make this more precise in Proposition 19.

Proposition 19. *Let $I \subset \Bbbk[\mathbf{X}]$ be a binomial ideal. If J is a binomial ideal of $\Bbbk[\mathbf{X}]$ such that $I \subset J$ and $\sim_J = \sim_I$, then $\mathbb{N}^n/\sim_I$ has a nil ∞ and $J = I + \langle \mathbf{X}^\mathbf{e} \mid [\mathbf{e}] = \infty \rangle$.*

Proof. As $I \subset J$, there is a binomial $\mathbf{X}^\mathbf{u} - \lambda \mathbf{X}^\mathbf{v} \in J \setminus I$. Since $\sim_I = \sim_J$, necessarily $\mathbf{X}^\mathbf{u}, \mathbf{X}^\mathbf{v} \in J$; in particular $\mathbb{N}^n/\sim_J = \mathbb{N}^n/\sim_I$ has a nil ∞. We claim that the ideal J is equal to $I + \langle \mathbf{X}^\mathbf{e} \mid [\mathbf{e}] = \infty \rangle$. To see that J contains $I + \langle \mathbf{X}^\mathbf{e} \mid [\mathbf{e}] = \infty \rangle$, we note that $I \subset J$. Also, we know that J contains a monomial $\mathbf{X}^\mathbf{u}$, and so $[\mathbf{u}] = \infty$. If $\mathbf{e} \in \mathbb{N}^n$ is such that $[\mathbf{e}] = \infty = [\mathbf{u}]$, then $\mathbf{X}^\mathbf{u} - \mu \mathbf{X}^\mathbf{e} \in J$ for some $\mu \in \Bbbk^*$, and since $\mathbf{X}^\mathbf{u} \in J$, we see that $\mathbf{X}^\mathbf{e} \in J$. For the reverse inclusion, it is enough to see that any binomial in J belongs to $I + \langle \mathbf{X}^\mathbf{e} \mid [\mathbf{e}] = \infty \rangle$. But as before, if $\mathbf{X}^\mathbf{u} - \lambda \mathbf{X}^\mathbf{v} \in J \setminus I$, then $\mathbf{X}^\mathbf{u}, \mathbf{X}^\mathbf{v} \in J$, and therefore $[\mathbf{u}] = [\mathbf{v}] = \infty$, because a monoid can have at most one nil element. □

A **monoid ideal** E of $\mathbb{N}^n$ is a proper subset such that $E + \mathbb{N}^n \subseteq E$; Figure 1 shows a typical example.

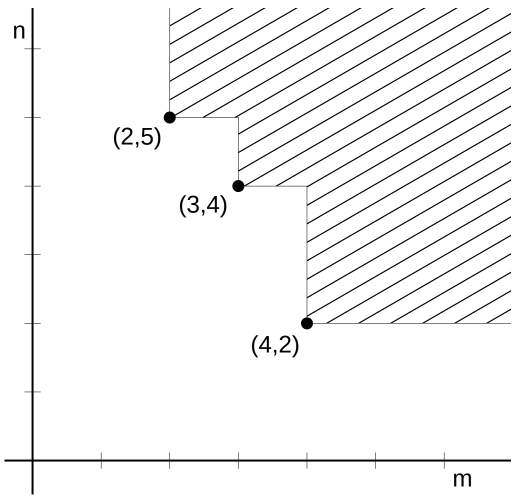

FIGURE 1. The integer points in shaded area form a monoid ideal of $\mathbb{N}^2$.

Let $E \subseteq \mathbb{N}^n$ be a monoid ideal of $\mathbb{N}^n$. The **Rees congruence** on $\mathbb{N}^n$ modulo E is the correspondence $\sim$ on $\mathbb{N}^n$ defined by $\mathbf{u} \sim \mathbf{v} \iff \mathbf{u} = \mathbf{v}$ or both $\mathbf{u}$ and $\mathbf{v} \in E$. Notice that the Rees congruence on $\mathbb{N}^n$ modulo E is the same as the induced by $\sim_{M_E}$ with $M_E = \langle \mathbf{X}^\mathbf{e} \mid \mathbf{e} \in E \rangle$.

Monoid ideals and nil elements are related as follows.

Lemma 20. *Let S be a monoid. Then S has a nil element if and only if for any presentation $\mathbb{N}^n/\sim$ of S there exists a monoid ideal E of $\mathbb{N}^n$ such that $\sim$ contains the Rees congruence on $\mathbb{N}^n$ modulo E. In this case, $[\mathbf{e}] = \infty$, for any $\mathbf{e} \in E$.*

Proof. Let $\mathbb{N}^n/\sim$ be a presentation of S given by a monoid surjection $\pi : \mathbb{N}^n \to S$.

For the direct implication, assume that $\infty \in S$ is a nil. Then $E := \pi^{-1}(\infty)$ is a monoid ideal of $\mathbb{N}^n$. Indeed, given $\mathbf{u} \in \mathbb{N}^n$ and $\mathbf{e} \in E$ we have that

$$\pi(\mathbf{e} + \mathbf{u}) = \pi(\mathbf{e}) + \pi(\mathbf{u}) = \infty + \pi(\mathbf{u}) = \infty,$$

so that $\mathbf{e}+\mathbf{u} \in E$. Note that $E \neq \mathbb{N}^n$ since nil elements are nonzero. Moreover, by construction, if $\mathbf{e}, \mathbf{e}' \in E$, then $\mathbf{e} \sim \mathbf{e}'$, which means that $\sim$ contains the Rees congruence on $\mathbb{N}^n$ modulo E.

Conversely, let E be a monoid ideal of $\mathbb{N}^n$ such that $\sim$ contains the Rees congruence on $\mathbb{N}^n$ modulo E. We claim that the class $[\mathbf{e}]$ (for any $\mathbf{e} \in E$) is a nil in $S = \mathbb{N}^n/\sim$. To see this, let $\mathbf{e} \in E$, $\mathbf{u} \in \mathbb{N}^n$. Then $\pi(\mathbf{e}) + \pi(\mathbf{u}) = \pi(\mathbf{e} + \mathbf{u})$. Since E is a monoid ideal, $\mathbf{e} + \mathbf{u} \in E$. This implies that $\mathbf{e} \sim \mathbf{e} + \mathbf{u}$ (or equivalently, $\pi(\mathbf{e}) = \pi(\mathbf{e} + \mathbf{u})$) because $\sim$ contains the Rees congruence modulo E. To complete the proof of our claim, we need to show that $[\mathbf{e}]$ ($\mathbf{e} \in E$) is not the zero class. This follows from the fact that $E \neq \mathbb{N}^n$. □

Our next goal is to prove Theorem 22, which is a more precise version of Proposition 19. With that result in hand, we will be able to introduce the binomial ideal associated to a congruence in Definition 25.

Definition 21. *An* ***augmentation ideal*** *for a given binomial ideal $I \subset \Bbbk[\mathbf{X}]$ is a maximal ideal of the form*

$$I_{\text{aug}} := \langle X_i - \lambda_i \ \mid \lambda_i \in \Bbbk^*,\ i = 1, \dots, n\rangle$$

such that $I \cap I_{\text{aug}}$ is a binomial ideal.

We point out that, given a binomial ideal I, an augmentation ideal for I may or may not exist (see [10, Example 9.13] for a binomial ideal without an augmentation ideal). The following result is the $\mathbb{N}^n$-version of [10, Theorem 9.12].

Theorem 22. *If $I_\ell \supset \ldots \supset I_0$ is a chain of distinct binomial ideals of $\Bbbk[\mathbf{X}]$ inducing the same congruence on $\mathbb{N}^n$, then $\ell \leq 1$. Moreover, if $\ell = 1$ then I_0 is pure and I_1 is not: $I_0 = I_1 \cap I_{\text{aug}}$ for an augmentation ideal for I_1.*

Proof. By Proposition 19, all we need to show is that if $\ell = 1$, then $I_0 = I_1 \cap I_{\text{aug}}$, where I_{aug} is an augmentation ideal for I_1. Denote by $\sim$ the congruence induced by I_0 (and I_1).

Assume $\ell = 1$, so that I_0 does not have monomials, and I_1 does. In particular, we may select a monomial $\mathbf{X}^{\mathbf{e}} \in I_1$, and its equivalence class $[\mathbf{e}]$ with respect to $\sim$ is a nil element, that we denote ∞. For each $1 \leq i \leq n$, consider the monomial $X_i = \mathbf{X}^{\mathbf{e}_i}$. Since $[\mathbf{e}_i] + \infty = \infty$, there exists $\lambda_i \in \Bbbk^*$ such that $X_i\mathbf{X}^{\mathbf{e}} - \lambda_i\mathbf{X}^{\mathbf{e}} \in I_0$ (because I_0 and I_1 induce the same congruence). We now define $I_{\text{aug}} = \langle X_i - \lambda_i \mid i = 1, \dots, n\rangle$, and claim that $I_1 \cap I_{\text{aug}} = I_0$, which in particular shows that I_{aug} is an augmentation ideal for I_1.

By construction, $(I_0 : \mathbf{X}^{\mathbf{e}}) \supseteq I_{\text{aug}}$. Note that $(I_0 : \mathbf{X}^{\mathbf{e}}) \neq \langle 1\rangle$, as I_0 contains no monomials. Thus, since I_{aug} is maximal, $(I_0 : \mathbf{X}^{\mathbf{e}}) = I_{\text{aug}}$, and we conclude that I_{aug} contains I_0. This, and $I_1 \supset I_0$, imply that $I_1 \cap I_{\text{aug}} \supseteq I_0$. Moreover, $I_{\text{aug}} \not\supseteq I_1$ because I_1 has monomials, while I_{aug} does not. Consequently $I_1 \supsetneq I_1 \cap I_{\text{aug}} \supseteq I_0$. Now the equality $I_1 \cap I_{\text{aug}} = I_0$ will follow from Proposition 19 if we show that $I_1 \cap I_{\text{aug}}$ is binomial (since the fact that I_1 and I_0 induce the same congruence $\sim$ implies that the congruence induced by $I_1 \cap I_{\text{aug}}$ is also $\sim$). To see that $I_1 \cap I_{\text{aug}}$ is binomial, we use the argument from [5, Corollary 1.5]. Introduce an auxiliary variable t, and consider the binomial ideal $J = I_0 + tI_{\text{aug}} + (1-t)\langle \mathbf{X}^{\mathbf{u}} \mid [\mathbf{u}] = [\mathbf{e}]\rangle \subset \Bbbk[\mathbf{X}, t]$. Since, by Proposition 19, $I_1 = I_0 + \langle \mathbf{X}^{\mathbf{u}} \mid [\mathbf{u}] = \infty = [\mathbf{e}]\rangle$, we have that $J \cap \Bbbk[\mathbf{X}] = I_1 \cap I_{\text{aug}}$. Now apply Corollary 3.

□

Example 23. If $I_1 = \langle X-Y, Y^2\rangle \subset \Bbbk[X,Y]$, then $I_0 = I_1 \cap \langle X-1, Y-1\rangle = \langle X-Y, Y^3-Y^2\rangle$. This can be verified as follows.

```
R = QQ[X,Y];
I1 = ideal(X-Y, Y^2);
Iaug = ideal(X-1,Y-1);
I0 = intersect(I1,Iaug);
mingens I0;
```

Note that these ideals already appeared in Examples 17 (i) and 16 3.

Remark 24. The previous results highlight one way in which two different binomial ideals in $\Bbbk[\mathbf{X}]$ induce the same congruence on $\mathbb{N}^n$, namely if one contains the other, the congruence has a nil element, and the larger ideal contains monomials corresponding to the nil class, while the smaller ideal has no monomials.

There is another way to produce binomial ideals inducing the same congruence. Let I be a binomial ideal in $\Bbbk[\mathbf{X}]$, and let $\mu_1, \dots, \mu_n \in \Bbbk^*$. Consider the ring isomorphism $\Bbbk[\mathbf{X}] \to \Bbbk[\mathbf{X}]$ given by $X_i \mapsto \mu_i X_i$ for $i = 1, \dots, n$. (This kind of isomorphism is known as **rescaling the variables**.) Then the image of I is a binomial ideal, which induces the same congruence as I. Indeed, the effect on I of rescaling the variables is to change the coefficients of the binomials in I by a nonzero multiple, which does not alter the exponents of those monomials.

In Theorem 22, the ideal I_0 can be made unital by rescaling the variables, by using that $\Bbbk$ is algebraically closed if necessary. The ideal obtained this way equals the ideal introduced in (4).

We are now ready to introduce the binomial ideal associated to a congruence in $\mathbb{N}^n$.

Definition 25. *Given a congruence $\sim$ on $\mathbb{N}^n$, denote by $I_\sim$ the unital binomial ideal of* $\Bbbk[\mathbf{X}]$ *which is maximal among all proper binomial ideals inducing $\sim$. We say that $I_\sim$ is the* ***binomial ideal associated*** *to $\sim$.*

To close this section, we introduce one final notion.

Definition 26. *Let $\sim_1$ and $\sim_2$ be congruences on $\mathbb{N}^n$. The* ***intersection*** *$\sim$ of $\sim_1$ and $\sim_2$, denoted $\sim = \sim_1 \cap \sim_2$, is the congruence on $\mathbb{N}^n$ defined by $\mathbf{u} \sim \mathbf{v}$ if and only if $\mathbf{u} \sim_1 \mathbf{v}$ and $\mathbf{u} \sim_2 \mathbf{v}$.*

From the point of view of equivalence relations, the equivalence classes of $\sim_1 \cap \sim_2$ form a partition of $\mathbb{N}^n$ which is the common refinement of the partitions induced by $\sim_1$ and $\sim_2$. The following result motivates the use of the intersection notation and terminology: the intersection of congruences corresponds to the ideal generated by the binomials in the intersection of their associated binomial ideals.

Proposition 27. *Let $\sim, \sim_1$ and $\sim_2$ be congruences on $\mathbb{N}^n$ whose associated ideals in* $\Bbbk[\mathbf{X}]$ (Definition 25) *are $I_\sim, I_{\sim_1}$ and $I_{\sim_2}$, respectively. Then $\sim = \sim_1 \cap \sim_2$ if and only if $I_\sim \subseteq I_{\sim_1} \cap I_{\sim_2}$, and the equality holds if and only if $I_{\sim_1} \cap I_{\sim_2}$ is a binomial ideal.*

Proof. The statement $\mathbf{u} \sim \mathbf{v}$ if and only if $\mathbf{u} \sim_1 \mathbf{v}$ and $\mathbf{u} \sim_2 \mathbf{v}$ is exactly the same as $\mathbf{X}^\mathbf{u} - \mathbf{X}^\mathbf{v} \in I_\sim$ if and only if $\mathbf{X}^\mathbf{u} - \mathbf{X}^\mathbf{v} \in I_{\sim_1}$ and $\mathbf{X}^\mathbf{u} - \mathbf{X}^\mathbf{v} \in I_{\sim_2}$. The direct implication of the last statement follows from Theorem 22 and its converse is trivially true because $I_\sim$ is a binomial ideal. □

The following example illustrates the last statement above.

Example 28. Let $\sim_1$ and $\sim_2$ be the congruences on $\mathbb{N}^2$ such that $\mathbf{u} \sim_1 \mathbf{v}$ if $\mathbf{u} - \mathbf{v} \in \mathbb{Z}(2, -2)$ and $\mathbf{u} \sim_2 \mathbf{v}$ if $\mathbf{u} - \mathbf{v} \in \mathbb{Z}(3, -3)$, respectively. The binomial ideals of $\mathbb{Q}[X, Y]$ associated to $\sim_1$ and $\sim_2$ are $I_{\sim_1} = \langle X^2 - Y^2\rangle$ and $I_{\sim_2} = \langle X^3 - Y^3\rangle$, respectively. Clearly, the binomial ideal associated to $\sim = \sim_1 \cap \sim_2$ is $I_\sim = \langle X^6 - Y^6\rangle$. Whereas, $I_{\sim_1} \cap I_{\sim_2} = \langle X^4 + X^3Y - XY^3 - Y^4\rangle$:

```
R = QQ[X,Y];
I1 = ideal(X^2-Y^2);
I2 = ideal(X^3-Y^3);
intersect(I1,I2);
```

3. Toric, lattice and mesoprime ideals

This section is devoted to the (finitely generated abelian) monoids contained in a group.

Let $(G,+)$ be a finitely generated abelian group and let $\mathcal{A}=\{\mathbf{a}_1,\ldots,\mathbf{a}_n\}$ be a given subset of G, we consider the subsemigroup S of G generated by $\mathcal{A}$, that is to say,

$$S=\mathbb{N}\mathbf{a}_1+\ldots+\mathbb{N}\mathbf{a}_n.$$

Since $0\in\mathbb{N}$, the semigroup S is actually a monoid. We may define a surjective monoid map as follows

$$\deg_{\mathcal{A}}:\mathbb{N}^n\longrightarrow S;\quad \mathbf{u}=(u_1,\ldots,u_n)\longmapsto \deg_{\mathcal{A}}(\mathbf{u})=\sum_{i=1}^n u_i\mathbf{a}_i. \tag{6}$$

In the literature, this map is called the factorization map of S and accordingly, the fiber $\deg_{\mathcal{A}}^{-1}(\mathbf{a})$ is called the set of factorizations of $\mathbf{a}\in S$.

Clearly $\deg_{\mathcal{A}}(-)$ determines a congruence on $\mathbb{N}^n$; in fact, it is the congruence on $\mathbb{N}^n$ whose presentation map is precisely $\deg_{\mathcal{A}}(-)$ (cf. (2)). Therefore, if $\widehat{\deg_{\mathcal{A}}}$ is the map defined in (3), namely,

$$\widehat{\deg_{\mathcal{A}}}:\Bbbk[\mathbb{N}^n]=\Bbbk[\mathbf{X}]\to\Bbbk[S]\ ;\quad \mathbf{X}^{\mathbf{u}}\mapsto\chi^{\deg_{\mathcal{A}}(\mathbf{u})},$$

by Theorem 13, we have that $I_{\mathcal{A}}=\ker(\widehat{\deg_{\mathcal{A}}})$ is spanned as a $\Bbbk-$vector space by the set of binomials

$$\{\mathbf{X}^{\mathbf{u}}-\mathbf{X}^{\mathbf{v}}\mid \mathbf{u},\mathbf{v}\in\mathbb{N}^n \text{ with } \deg_{\mathcal{A}}(\mathbf{u})=\deg_{\mathcal{A}}(\mathbf{v})\}. \tag{7}$$

Observe that $\Bbbk[\mathbf{X}]$ is $S-$graded via $\deg(X_i)=\mathbf{a}_i,\ i=1,\ldots,n$. This grading is known as the $\mathcal{A}-$**grading** on $\Bbbk[\mathbf{X}]$. The semigroup algebra $\Bbbk[S]=\oplus_{\mathbf{a}\in S}\mathrm{Span}_{\Bbbk}\{\chi^{\mathbf{a}}\}$ also has a natural $S-$grading. Under these gradings, the map of semigroup algebras $\widehat{\deg_{\mathcal{A}}}$ is a graded map. Hence, the ideal $I_{\mathcal{A}}=\ker(\widehat{\deg_{\mathcal{A}}})$ is $S-$homogeneous.

Proposition 29. *Use the notation introduced above, and assume that $\mathbf{a}_1,\ldots,\mathbf{a}_n$ are nonzero. The following are equivalent:*

(1) The fibers of map $\deg_{\mathcal{A}}(-)$ are finite.
(2) $\deg_{\mathcal{A}}^{-1}(\mathbf{0})=\{(0,\ldots,0)\}$.
(3) $S\cap(-S)=\{0\}$, that is to say, $\mathbf{a}\in S$ and $-\mathbf{a}\in S\Rightarrow\mathbf{a}=\mathbf{0}$.
(4) The relation $\mathbf{a}'\preceq\mathbf{a}\iff\mathbf{a}'-\mathbf{a}\in S$ is a partial order on S.

Proof. Before we proceed with the proof, we note that if one of the $\mathbf{a}_i$ is zero, then this result is false. For example, let $G=\mathbb{Z}$, $\mathcal{A}=\{\mathbf{a}_1=0,\mathbf{a}_2=1\}$. Then $S=\mathbb{N}$, for which 3 and 4 hold, but $\deg_{\mathcal{A}}(-)$ does not satisfy either 1 or 2.

1$\Rightarrow$2 If $\mathbf{u}\in\deg_{\mathcal{A}}^{-1}(\mathbf{0})$, then for every $\ell\in\mathbb{N}$, $\ell\mathbf{u}\in\deg_{\mathcal{A}}^{-1}(\mathbf{0})$. If $\mathbf{u}\neq(0,\ldots,0)$, then $\deg_{\mathcal{A}}^{-1}(\mathbf{0})$ is infinite.

1$\Leftarrow$2 Dickson's Lemma states that any nonempty subset of $\mathbb{N}^n$ has finitely many minimal elements with respect to the partial order given by coordinatewise $\leq$. Suppose that $\deg_{\mathcal{A}}^{-1}(\mathbf{a})$ is infinite. Then by Dickson's Lemma there exists $\mathbf{u}\in\deg_{\mathcal{A}}^{-1}(\mathbf{a})$ which is not minimal, and therefore there is also $\mathbf{v}\in\deg_{\mathcal{A}}^{-1}(\mathbf{a})$ such that $\mathbf{v}\leq\mathbf{u}$ coordinatewise. We conclude that $\mathbf{u}-\mathbf{v}\in\mathbb{N}^n$ is a nonzero element of $\deg_{\mathcal{A}}^{-1}(\mathbf{0})$.

2⇒3 Let $\mathbf{u}, \mathbf{v} \in \mathbb{N}^n$ be such that $\deg_{\mathcal{A}}(\mathbf{u}) = \mathbf{a}$ and $\deg_{\mathcal{A}}(\mathbf{v}) = -\mathbf{a}$. Then $\deg_{\mathcal{A}}(\mathbf{u} + \mathbf{v}) = \mathbf{0}$, so that $\mathbf{u} + \mathbf{v} = (0, \ldots, 0)$, and therefore $\mathbf{u} = \mathbf{v} = (0, \ldots, 0)$, which implies that $\mathbf{a} = \mathbf{0}$.

2⇐3 Let $\mathbf{u} \in \deg_{\mathcal{A}}^{-1}(\mathbf{0})$. If $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{N}^n$ are such that $\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2$, then by 3 $\deg_{\mathcal{A}}(\mathbf{u}_1) = \deg_{\mathcal{A}}(\mathbf{u}_2) = \mathbf{0}$. Repeatedly applying this argument, we conclude that if $\mathbf{u} \neq 0$, so in particular it has a nonzero coordinate, then there exists $1 \leq i \leq n$ such that $\mathbf{a}_i = \deg_{\mathcal{A}}(\mathbf{e}_i) = \mathbf{0}$, a contradiction.

3⇔4 The relation $\preceq$ is always reflexive and transitive. The fact that $\preceq$ is antisymmetric is equivalent to 3. □

Remark 30. If the conditions of Proposition 29 hold, the monoid S generated by $\mathcal{A}$ is said to be **positive**. When S is positive, $\mathfrak{m} = \langle X_1, \ldots, X_n \rangle$ is the only $S-$homogeneous maximal ideal in $\Bbbk[\mathbf{X}]$. Recall that a graded ideal $\mathfrak{m}$ in a graded ring R is a **graded maximal ideal** or ***maximal ideal** if the only graded ideal properly containing $\mathfrak{m}$ is R itself. Graded rings with a unique graded maximal ideal are known as **graded local rings** or ***local rings**. Many results valid for local rings are also valid for graded local rings, starting with Nakayama's Lemma. In particular, the *minimal free resolution* of any finitely generated $\mathcal{A}-$graded $\Bbbk[\mathbf{X}]-$module is well-defined (see [3, Section 1.5] and [1]).

All the monoids in this section are contained in a group. The next result characterize the condition for a monoid to be contained in a group. To state it we need to introduce the following concepts.

Definition 31. *Let $\sim$ be a congruence on $\mathbb{N}^n$. We will say that $\mathbf{a} \in \mathbb{N}^n/\sim$ is **cancellable** if $\mathbf{b} + \mathbf{a} = \mathbf{c} + \mathbf{a} \Rightarrow \mathbf{b} = \mathbf{c}$, for all $\mathbf{b}, \mathbf{c} \in \mathbb{N}^n/\sim$. A monoid is said to be **cancellative** if all its elements are cancellable. A congruence $\sim$ on $\mathbb{N}^n$ is cancellative if the monoid $\mathbb{N}^n/\sim$ is cancellative.*

In the part 3 of Example 16, an example of non-cancellative monoid is exhibited.

Proposition 32. *A (finitely generated commutative) monoid is contained in a group if and only if it is cancellative.*

Proof. The direct implication is clear. Conversely, if $S = \mathbb{N}^n/\sim$ is a cancellative finitely generated commutative monoid, then $\sim$ can be extended on $\mathbb{Z}^n$ as follows: $\mathbf{u} \sim \mathbf{v}$ if $\mathbf{u}+\mathbf{e} \sim \mathbf{v}+\mathbf{e}$ for some (any) $\mathbf{e} \in \mathbb{N}^n$ such that $\mathbf{u} + \mathbf{e}$ and $\mathbf{v} + \mathbf{e} \in \mathbb{N}^n$. Since $G = \mathbb{Z}^n/\sim$ has a natural group structure and $S \subseteq G$, we are done. □

The above result shows that our definition of cancellative congruence is equivalent to the usual one (see [7, p. 44]).

3.1. **Toric ideals and toric congruences.**

Suppose now that G is torsion-free and let $G(\mathcal{A})$ denote the subgroup of G generated by $\mathcal{A}$. Since G is torsion-free, then $G \cong \mathbb{Z}^m$, for some m. Thus, the semigroup S is isomorphic to a subsemigroup of $\mathbb{Z}^m$. In this case, S is said to be an **affine semigroup** and the ideal $I_{\mathcal{A}}$ is called the **toric ideal** associated to $\mathcal{A}$.

Without loss of generality, we may assume that $\mathbf{a}_i \in \mathbb{Z}^d$, for every $i = 1, \ldots, n$, with $d = \mathrm{rank}(G(\mathcal{A})) \leq m$. Moreover, one can prove that, if $\mathcal{A}$ generates a positive monoid (see Remark 30), there exists a monoid isomorphism under which $\mathbf{a}_i$ is mapped to an element of $\mathbb{N}^n$, $i = 1, \ldots, n$ (see, e.g. [3, Proposition 6.1.5]), which justifies the use of the term "positive".

Lemma 33. *If $\mathcal{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbb{Z}^d$, then $I_{\mathcal{A}}$ is prime.*

Proof. By hypothesis, we have that $\Bbbk[S]$ is isomorphic to the subring $\Bbbk[\mathbf{t}^{\mathbf{a}_1}, \ldots, \mathbf{t}^{\mathbf{a}_n}]$ of the Laurent polynomial ring $\Bbbk[\mathbb{Z}^d] = \Bbbk[t_1^{\pm}, \ldots, t_d^{\pm}]$; in particular, $\Bbbk[S] \cong \Bbbk[\mathbf{X}]/I_{\mathcal{A}}$ is a domain. Therefore $I_{\mathcal{A}}$ is prime. $\square$

Theorem 34. *Let I be a binomial ideal of $\Bbbk[\mathbf{X}]$. The ideal I is prime if and only if there exists $\mathcal{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_r\} \subset \mathbb{Z}^d$ such that*

$$I = I_{\mathcal{A}}\, \Bbbk[\mathbf{X}] + \langle X_{r+1}, \ldots, X_n \rangle,$$

up to permutation and rescaling of variables.

Proof. Suppose that I is prime. If I contains monomials, there exists a set of variables, say $X_{r+1}, \ldots, X_n$ (by permuting variables if necessary), such that I is equal to $I'\, \Bbbk[\mathbf{X}] + \langle X_{r+1}, \ldots, X_n \rangle$ where I' is a pure prime binomial ideal of $\Bbbk[X_1, \ldots, X_r]$. Therefore, without loss of generality, we may suppose $I = I'$ and $r = n$. Now, by Theorem 8, $\Bbbk[\mathbf{X}]/I \cong \Bbbk[S] = \bigoplus_{\mathbf{a} \in S} \mathrm{Span}_{\Bbbk}\{\chi^{\mathbf{a}}\}$, for some commutative monoid S generated by $\mathcal{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$. Recall that the above isomorphism maps X_i to $\lambda_i \chi^{\mathbf{a}_i}$ for some $\lambda_i \in \Bbbk^*$, $i = 1, \ldots, n$. So, by rescaling variables if necessary, we may assume $\lambda_i = 1$ for every i. Now, if S is not contained in a group, by Proposition 32, there exist $\mathbf{a}, \mathbf{a}'$ and $\mathbf{b} \in S$ such that $\mathbf{a} + \mathbf{b} = \mathbf{a}' + \mathbf{b}$ and $\mathbf{a} \neq \mathbf{a}'$. Thus, $\mathbf{X}^{\mathbf{v}}(\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{u}'}) \in I$, but $\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{u}'} \notin I$, where $\mathbf{u} \in \deg_{\mathcal{A}}^{-1}(\mathbf{a})$, $\mathbf{u}' \in \deg_{\mathcal{A}}^{-1}(\mathbf{a}')$ and $\mathbf{v} \in \deg_{\mathcal{A}}^{-1}(\mathbf{b})$. So, since I is prime, we have that $\mathbf{X}^{\mathbf{v}} \in I$ which is a contradiction. On other hand, if $G(S)$ has torsion, there exist two different elements $\mathbf{a}$ and $\mathbf{a}' \in S$ such that $n\mathbf{a} = n\mathbf{a}'$ for some $n \in \mathbb{N}$. Therefore $\mathbf{X}^{n\mathbf{u}} - \mathbf{X}^{n\mathbf{u}'} \in I$, where $\mathbf{u} \in \deg_{\mathcal{A}}^{-1}(\mathbf{a})$ and $\mathbf{u}' \in \deg_{\mathcal{A}}^{-1}(\mathbf{a}')$. Since $\Bbbk$ is algebraically closed and I is prime, $\mathbf{X}^{\mathbf{u}} - \zeta_n \mathbf{X}^{\mathbf{u}'} \in I$, where ζ_n is a $n-$th root of unity; in particular, $\mathbf{a} = \mathbf{a}'$ which is a contradiction. Putting all this together, we conclude that S is an affine semigroup.

The opposite implication is a direct consequence of Lemma 33. $\square$

Definition 35. *A congruence $\sim$ on $\mathbb{N}^n$ is said to be* ***toric*** *if the ideal $I_\sim$ is prime.*

The following result proves that our definition agrees with the one given in [10].

Corollary 36. *A congruence $\sim$ on $\mathbb{N}^n$ is toric if and only if the non-nil elements of $\mathbb{N}^n/\sim$ form an affine semigroup.*

Proof. The direct implication follows from Theorem 34. Conversely, we assume that the non-nil elements of $\mathbb{N}^n/\sim$ form an affine semigroup S. In this case, we have that $[\mathbf{u}] + [\mathbf{v}] = \infty$ implies $[\mathbf{u}] = \infty$ or $[\mathbf{v}] = \infty$, for every $\mathbf{u}$ and $\mathbf{v} \in \mathbb{N}^n$, because S is contained in a group and groups have no nil element. Therefore, since $\mathbb{N}^n/\sim$ is generated by the classes $[\mathbf{e}_i]$ modulo $\sim$, $i = 1, \ldots, n$, we obtain that S is generated by $\mathcal{A} = \{[\mathbf{e}_i] \neq \infty \ \mid \ i = 1, \ldots, n\}$ Now, applying Theorem 34 again, we conclude that $I_\sim$ is a prime ideal. $\square$

3.2. **Lattice ideals and cancellative congruences.**

Consider now a subgroup $\mathcal{L}$ of $\mathbb{Z}^n$ and define the following congruence $\sim$ on $\mathbb{N}^n$:

$$\mathbf{u} \sim \mathbf{v} \Longleftrightarrow \mathbf{u} - \mathbf{v} \in \mathcal{L}.$$

Clearly, $\mathbb{N}^n/\sim$ is contained in the group $\mathbb{Z}^n/\mathcal{L}$ and the associated ideal $I_\sim$ is equal to

$$I_{\mathcal{L}} := \{\mathbf{X}^{\mathbf{u}} - \mathbf{X}^{\mathbf{v}} \ \mid \mathbf{u} - \mathbf{v} \in \mathcal{L}\}.$$

The subgroups of $\mathbb{Z}^n$ are also called lattices. This justifies the term “lattice” in the following definition.

Definition 37. *Let $\mathcal{L}$ be a subgroup of $\mathbb{Z}^n$ and $\rho : \mathcal{L} \to \Bbbk^*$ be a group homomorphism. The lattice ideal corresponding to $\mathcal{L}$ and ρ is*

$$I_{\mathcal{L}}(\rho) := \langle \mathbf{X}^{\mathbf{u}} - \rho(\mathbf{u} - \mathbf{v})\mathbf{X}^{\mathbf{v}} \ \mid \ \mathbf{u} - \mathbf{v} \in \mathcal{L} \rangle.$$

An ideal I of $\Bbbk[\mathbf{X}]$ is called a ***lattice ideal*** *if there is subgroup $\mathcal{L} \subset \mathbb{Z}^n$ and a group homomorphism $\rho : \mathcal{L} \to \Bbbk^*$ such that $I = I_{\mathcal{L}}(\rho)$.*

Observe that the ideal $I_{\mathcal{L}}$ above is a lattice ideal for the group homomorphism $\rho : \mathcal{L} \to \Bbbk^*$ such that $\rho(\mathbf{u}) = 1$, for every $\mathbf{u} \in \mathcal{L}$. Moreover, given a subgroup $\mathcal{L}$ of $\mathbb{Z}^n$, we have that the congruence on $\mathbb{N}^n$ defined by a lattice ideal $I_{\mathcal{L}}(\rho)$ is the same as the congruence on $\mathbb{N}^n$ defined by $I_{\mathcal{L}}$, for every group homomorphism $\rho : \mathcal{L} \to \Bbbk^*$.

Let us characterize the cancellative congruences on $\mathbb{N}^n$ in terms of their associated binomial ideals. In order to do this, we first recall the following result from [5].

Proposition 38. [5, Corollary 2.5] *If I is a pure binomial ideal of $\Bbbk[\mathbf{X}]$, then there is a unique group morphism $\rho : \mathcal{L} \subseteq \mathbb{Z}^n \to \Bbbk^*$ such that $I : (\prod_{i=1}^n X_i)^\infty = I_{\mathcal{L}}(\rho)$.*

Observe that from Proposition 38, it follows that no monomial is a zero divisor modulo a lattice ideal.

Corollary 39. *A congruence $\sim$ on $\mathbb{N}^n$ is cancellative if and only if $I_\sim$ is a lattice ideal.*

Proof. By Proposition 32, $\sim$ is cancellative if and only if $\mathbb{N}^n/\sim$ is contained in a group G. Thus, the natural projection $\pi : \mathbb{N}^n \to \mathbb{N}^n/\sim$ can be extended to a group homorphism $\bar{\pi} : \mathbb{Z}^n \to G$ whose restriction to $\mathbb{N}^n$ is π. Since the kernel, $\mathcal{L}$, of $\bar{\pi}$ is a subgroup of $\mathbb{Z}^n$ that defines the same congruence as $\sim$, we conclude that both ideals $I_\sim$ and $I_{\mathcal{L}}$ are equal. For the converse, we first note that the congruence on $\mathbb{N}^n$ defined by a lattice ideal $I_{\mathcal{L}}(\rho)$ is the same as the congruence on $\mathbb{N}^n$ defined by $I_{\mathcal{L}}$, for every group homomorphism $\rho : \mathcal{L} \subset \mathbb{Z}^n \to \Bbbk^*$ (see the comment after equation (5)). Now, it suffices to note that if $I_\sim = I_{\mathcal{L}}$ for some subgroup $\mathcal{L}$ of $\mathbb{Z}^n$, then $\mathbb{N}^n/\sim$ is contained in $\mathbb{Z}^n/\mathcal{L}$. ☐

Observe that a lattice ideal $I_{\mathcal{L}}$ is not prime in general. Indeed, $I = \langle X^2 - Y^2 \rangle$ is a lattice ideal corresponding to the subgroup of $\mathbb{Z}^2$ generated by $(2, -2)$ which is clearly not prime. Let us give a necessary and sufficient condition for a lattice ideal to be prime.

Definition 40. *Let $\mathcal{L}$ be subgroup of $\mathbb{Z}^n$ and set*

$$\mathrm{Sat}(\mathcal{L}) := (\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{L}) \cap \mathbb{Z}^n = \{\mathbf{u} \in \mathbb{Z}^n \mid d\,\mathbf{u} \in \mathcal{L} \text{ for some } d \in \mathbb{Z}\}.$$

Clearly, $\mathrm{Sat}(\mathcal{L})$ *is subgroup of $\mathbb{Z}^n$ and it is called the* ***saturation*** *of $\mathcal{L}$. We say that $\mathcal{L}$ is* ***saturated*** *if $\mathcal{L} = \mathrm{Sat}(\mathcal{L})$.*

Proposition 41. *A lattice ideal $I_{\mathcal{L}}(\rho)$ is prime if and only if $\mathcal{L}$ is saturated.*

Proof. By using the same argument as in the proof of Corollary 39, we obtain that $\mathbb{Z}^n/\sim\, = \mathbb{Z}^n/\mathcal{L}$, where $\sim$ the congruence defined by $I_{\mathcal{L}}(\rho)$ on $\mathbb{Z}^n$. Now, since $\mathbb{Z}^n/\mathcal{L}$ is the group generated by $\mathbb{N}^n/\sim$, and $\mathbb{Z}^n/\mathcal{L}$ is torsion-free if and only if $\mathcal{L}$ is saturated, we obtain the desired equivalence. ☐

Notice that the congruence defined by $\mathcal{L}$ is contained in the congruence defined by $\mathrm{Sat}(\mathcal{L})$. In fact, $\mathrm{Sat}(\mathcal{L})$ defines the smallest toric congruence on $\mathbb{N}^n$ containing the congruence defined by $\mathcal{L}$ on $\mathbb{N}^n$. Therefore, we may say each cancellative congruence *has exactly one toric congruence associated.*

The primary decomposition of a lattice ideal $I_{\mathcal{L}}(\rho)$ can be completely described in terms of $\mathcal{L}$ and ρ. Let us reproduce this result. For this purpose, we need additional notation.

Definition 42. *If p is a prime number, we define* $\mathrm{Sat}_p(\mathcal{L})$ *and* $\mathrm{Sat}'_p(\mathcal{L})$ *to be the largest sublattices of* $\mathrm{Sat}(\mathcal{L})$ *containing L such that* $\mathrm{Sat}_p(\mathcal{L})/\mathcal{L}$ *has order a power of p and* $\mathrm{Sat}'_p(\mathcal{L})/\mathcal{L}$ *has order relatively prime to p. If $p = 0$, we adopt the convention that* $\mathrm{Sat}_p(\mathcal{L}) = \mathcal{L}$ *and* $\mathrm{Sat}'_p(\mathcal{L}) = \mathrm{Sat}(\mathcal{L})$.

Theorem 43. [5, Corollaries 2.2 and 2.5] *Let* $\mathrm{char}(\Bbbk) = p \geq 0$ *and consider a group morphsim* $\rho : \mathcal{L} \subseteq \mathbb{Z}^n \to \Bbbk^*$. *If the order of* $\mathrm{Sat'}_p(\mathcal{L})/\mathcal{L}$ *is* g, *there are* g *distinct group morphisms* $\rho_1, \ldots, \rho_g$ *extending* ρ *to* $\mathrm{Sat'}_p(\mathcal{L})$ *and for each* $j \in \{1, \ldots, g\}$ *a unique group morphism* ρ'_j *extending* ρ *to* $\mathrm{Sat}(\mathcal{L})$. *Moreover, there is a unique group morphism* ρ' *extending* ρ *to* $\mathrm{Sat}_p(\mathcal{L})$. *The radical, associated primes and minimal primary decomposition of* $I_{\mathcal{L}}(\rho) \subset \Bbbk[\mathbf{X}]$ *are:*

$$\sqrt{I_{\mathcal{L}}(\rho)} = I_{\mathrm{Sat}_p(\mathcal{L})}(\rho'),$$

$$\mathrm{Ass}(\Bbbk[\mathbf{X}]/I_{\mathcal{L}}(\rho)) = \{I_{\mathrm{Sat}(\mathcal{L})}(\rho'_j) \mid j = 1, \ldots, g\}$$

and

$$I_{\mathcal{L}}(\rho) = \bigcap_{j=1}^{g} I_{\mathrm{Sat}'_p(\mathcal{L})}(\rho_j)$$

where $I_{\mathrm{Sat}'_p(\mathcal{L})}(\rho_j)$ *is* $I_{\mathrm{Sat}(\mathcal{L})}(\rho'_j)$*-primary. In particular, if* $p = 0$, *then* $I_{\mathcal{L}}(\rho)$ *is a radical ideal. The associated primes* $I_{\mathrm{Sat}(\mathcal{L})}(\rho'_j)$ *of* $I_{\mathcal{L}}(\rho)$ *are all minimal and have the same codimension* $\mathrm{rank}(\mathcal{L})$.

3.3. Mesoprime ideals and prime congruences.

Given $\delta \subseteq \{1, \ldots, n\}$, set $\mathbb{N}^\delta := \{(u_1, \ldots, u_n) \in \mathbb{N}^n \mid u_i = 0, \text{ for all } i \notin \delta\}$ and define $\mathbb{Z}^\delta$ as the subgroup of $\mathbb{Z}^n$ generated by $\mathbb{N}^\delta$. Morover, if $\delta = \varnothing$, by convention, then $\mathbb{Z}^\delta = \{\mathbf{0}\} \subset \mathbb{Z}^n$.

Definition 44. *Given* $\delta \subseteq \{1, \ldots, n\}$ *and a group homomorphism* $\rho : \mathcal{L} \subseteq \mathbb{Z}^\delta \to \Bbbk^*$, *a* $\delta-$***mesoprime ideal*** *is an ideal of the form*

$$I_{\mathcal{L}}(\rho) + \mathfrak{p}_{\delta^c}$$

with $\mathfrak{p}_{\delta^c} := \langle X_j \mid j \notin \delta \rangle$. *By convention,* $\mathfrak{p}_{\varnothing^c} = \langle X_1, \ldots, X_n \rangle$ *and* $\mathfrak{p}_{\varnothing} = \langle 0 \rangle$.

Example 45.

(1) The ideal $\langle X_1^{17} - 1, X_2 \rangle \subset \Bbbk[X_1, X_2]$ is mesoprime for $\delta = \{1\}$
(2) By Theorem 34, every binomial prime ideal is mesoprime, for a suitable δ.
(3) Lattice ideals are mesoprime for $\delta = \{1, \ldots, n\}$.

Due to Theorem 43, a mesoprime ideal can be understood as a condensed expression that includes all the information necessary to produce the primary decomposition of the ideal simply by using arithmetic arguments.

Observe that the congruence on $\mathbb{N}^n$ defined by $I_{\mathcal{L}} + \mathfrak{p}_{\delta^c}$ is the same as the congruence defined by $I_{\mathcal{L}}(\rho) + \mathfrak{p}_{\delta^c}$, for every $\delta \subseteq \{1, \ldots, n\}$ and every group homomorphism $\rho : \mathcal{L} \subseteq \mathbb{Z}^\delta \to \Bbbk^*$.

Lemma 46. *Let* $\delta \subseteq \{1, \ldots, n\}$. *If* I *is a* $\delta-$*mesoprime ideal, then* $I : X_i = I$, *for all* $i \in \delta$. *Equivalently,* $I : (\prod_{i \in \delta} X_i)^\infty = I$.

Proof. If I is a $\delta-$mesoprime ideal, there exists $\rho : \mathcal{L} \subseteq \mathbb{Z}^\delta \to \Bbbk^*$ such that $I = I_{\mathcal{L}}(\rho) + \mathfrak{p}_{\delta^c}$. Let $X_i f \in I,\ i \in \delta$. We want to show that $f \in I$. So, without loss of generality, we may assume that no term of f lies in $\mathfrak{p}_{\delta^c}$. In this case, $X_i f \in I_{\mathcal{L}}(\rho)$. Now, by Proposition 38, we conclude that $f \in I_{\mathcal{L}}(\rho)$, and hence $f \in I$. □

Definition 47. *A congruence* $\sim$ *on* $\mathbb{N}^n$ *is said to be* ***prime*** *if the ideal* $I_\sim$ *is mesoprime for some* $\delta \subseteq \{1, \ldots, n\}$.

Let us prove that this notion of prime congruence is the same as the usual one (see [7, p. 44]).

Proposition 48. *A congruence* $\sim$ *on* $\mathbb{N}^n$ *is* ***prime*** *if and only if every element of* $\mathbb{N}^n/\sim$ *is either nil or cancellable.*

Proof. If $\sim$ is prime congruence on $\mathbb{N}^n$, then there exist $\delta \subseteq \{1,\ldots,n\}$ and a subgroup $\mathcal{L} \subseteq \mathbb{Z}^\delta$ such that $I_\sim = I_\mathcal{L} + \mathfrak{p}_{\delta^c}$. Let $[\mathbf{u}]$ be non-nil and let $[\mathbf{v}]$ and $[\mathbf{w}] \in \mathbb{N}^n/\sim$ be such that $[\mathbf{v}]+[\mathbf{u}] = [\mathbf{v}+\mathbf{u}] = [\mathbf{w}+\mathbf{u}] = [\mathbf{w}]+[\mathbf{u}]$. In particular, $\mathbf{X}^\mathbf{u}(\mathbf{X}^\mathbf{v} - \mathbf{X}^\mathbf{w}) = \mathbf{X}^{\mathbf{v}+\mathbf{u}} - \mathbf{X}^{\mathbf{w}+\mathbf{v}} \in I_\sim$. Since $[\mathbf{u}]$ is non-nil, $\mathbf{X}^\mathbf{u}$ does not belong to $I_\sim$. Therefore, $\mathbf{u} \in \{X_i\}_{i\in\delta}$ and, by Lemma 46, $\mathbf{X}^\mathbf{v} - \mathbf{X}^\mathbf{w} \in I_\sim$, that is, $[\mathbf{v}] = [\mathbf{w}]$. So $[\mathbf{u}]$ is cancellable.

Conversely, suppose that every element of $\mathbb{N}^n/\sim$ is either nil or cancellable, set $\delta = \{i \in \{1,\ldots,n\} : [\mathbf{e}_i] \text{ is cancellable}\}$. Clearly, $j \notin \delta$ if and only if $X_j \in I_\sim$. So, there exist a binomial ideal J in $\Bbbk[\{X_i\}_{i\in\delta}]$ such that $I_\sim = J\,\Bbbk[\mathbf{X}] + \mathfrak{p}_{\delta^c}$ (if $\delta = \varnothing$, take $J = \langle 0\rangle$). Moreover, since $[\mathbf{e}_i]$ is cancellable for every $i \in \delta$, if $\mathbf{X}^{\mathbf{e}_i} f = X_i f \in J$, for some $i \in \delta$, then $f \in J$. Thus, by Proposition 38, J is lattice ideal of $\Bbbk[\{X_i\}_{i\in\delta}]$ and, consequently, $J\,\Bbbk[\mathbf{X}]$ is a lattice ideal. Therefore, $I_\sim = J\,\Bbbk[\mathbf{X}] + \mathfrak{p}_{\delta^c}$ is a $\delta-$mesoprime ideal and we are done. □

4. Cellular binomial ideals

In this section we study the so-called cellular binomial ideals defined by D. Eisenbud and B. Sturmfels in [5]. Cellular binomial ideals play a central role in the theory of primary decomposition of binomials ideals (see [5] and also [6, 13, 14]). As in the previous section, we will determine the congruences on $\mathbb{N}^n$ corresponding to those ideals. We will also outline an algorithm to compute a decomposition of a binomial ideal into cellular binomial ideals which will produce (primary) decompositions of the corresponding congruences.

Let us start by defining the notion of cellular ideal.

Definition 49. *A proper ideal I of $\Bbbk[\mathbf{X}]$ is* ***cellular*** *if, for some $\delta \subseteq \{1,\ldots,n\}$, we have that*

(1) $I : (\prod_{i\in\delta} X_i)^\infty = I$; equivalently $I : X_i = I$, for every $i \in \delta$,
(2) there exists $d_i \in \mathbb{N}$ such that $X_i^{d_i} \in I$, for every $i \notin \delta$.

In this case, we say that I is cellular with respect to δ or, simply, $\delta-$cellular. By convention, the $\varnothing-$cellular ideals are the binomial ideals whose radical is $\langle X_1,\ldots,X_n\rangle$.

Observe that an ideal I of $\Bbbk[\mathbf{X}]$ is cellular if, and only if, every variable of $\Bbbk[\mathbf{X}]$ is either a nonzerodivisor or nilpotent modulo I. In particular, prime, lattice, mesoprime and primary ideals are cellular.

The following proposition establishes the relationship between cellular binomial and mesoprime ideals.

Proposition 50. *Let $\delta \subseteq \{1,\ldots,n\}$. If I is a $\delta-$cellular binomial ideal in $\Bbbk[\mathbf{X}]$, there exists a group morphism $\rho : \mathcal{L} \subseteq \mathbb{Z}^\delta \to \Bbbk^*$ such that*

(1) $(I \cap \Bbbk[\{X_i\}_{i\in\delta}])\,\Bbbk[\mathbf{X}] = I_\mathcal{L}(\rho)$.
(2) $I + \mathfrak{p}_{\delta^c} = I_\mathcal{L}(\rho) + \mathfrak{p}_{\delta^c}$.
(3) $\sqrt{I + \mathfrak{p}_{\delta^c}} = \sqrt{I_\mathcal{L}(\rho)} + \mathfrak{p}_{\delta^c}$.
(4) $\sqrt{I} = \sqrt{I_\mathcal{L}(\rho)} + \mathfrak{p}_{\delta^c}$.

In particular, the radical of a cellular binomial ideal is a mesoprime ideal, and the minimal associated primes of I are binomial.

Proof. If $\delta = \varnothing$, then $I \cap \Bbbk[\{X_i\}_{i\in\delta}]) = 0$ and it suffices to take $\rho : \{\mathbf{0}\} \to \Bbbk^*; \mathbf{0} \mapsto 1$. So, assume without loss of generality that $\delta \neq \varnothing$.

In order to prove part (a), we first note that $J := I \cap \Bbbk[\{X_i\}_{i\in\delta}]$ is binomial by Corollary 3, and that $J : (\prod_{i\in\delta} X_i)^\infty = J$ by the definition of cellular ideal. Thus, $J\,\Bbbk[\mathbf{X}] : (\prod_{i=1}^n X_i)^\infty = J\,\Bbbk[\mathbf{X}]$ and, by Proposition 38, there is a unique group morphism $\rho : \mathcal{L} \subseteq \mathbb{Z}^\delta \to \Bbbk^*$ such that $J\,\Bbbk[\mathbf{X}] = I_\mathcal{L}(\rho)$.

Part (b) is an immediate consequence of (a).

By part (b) and according to the properties of the radical, we have that

$$\sqrt{I+\mathfrak{p}_{\delta^c}} = \sqrt{I_{\mathcal{L}}(\rho)+\mathfrak{p}_{\delta^c}} = \sqrt{\sqrt{I_{\mathcal{L}}(\rho)}+\mathfrak{p}_{\delta^c}} \supseteq \sqrt{I_{\mathcal{L}}(\rho)}+\mathfrak{p}_{\delta^c} \supseteq \sqrt{I_{\mathcal{L}}(\rho)}+\mathfrak{p}_{\delta^c}.$$

On other hand, given $f \in \sqrt{I_{\mathcal{L}}(\rho)}+\mathfrak{p}_{\delta^c}$, we can write $f = h + \sum_{i\notin\delta} g_i X_i$ where $h^e \in I_{\mathcal{L}}(\rho)$ for some $e > 0$. Now, since $I_{\mathcal{L}}(\rho) \subseteq I_{\mathcal{L}}(\rho)+\mathfrak{p}_{\delta^c} = I+\mathfrak{p}_{\delta^c}$, we have that $f^e = \big(h+\sum_{i\notin\delta} g_i X_i\big)^e \in I+\mathfrak{p}_{\delta^c}$, that is to say, $f \in \sqrt{I+\mathfrak{p}_{\delta^c}}$. Thus, we obtain that $\sqrt{I+\mathfrak{p}_{\delta^c}} = \sqrt{I_{\mathcal{L}}(\rho)}+\mathfrak{p}_{\delta^c}$, as claimed in (c).

For part (d), we observe that

$$\sqrt{I_{\mathcal{L}}(\rho)+\mathfrak{p}_{\delta^c}} = \sqrt{I_{\mathcal{L}}(\rho)+\langle X_i^{d_i} \ \mid \ i\notin\delta\rangle},$$

and that

$$I_{\mathcal{L}}(\rho)+\langle X_i^{d_i} \ \mid \ i\notin\delta\rangle = (I\cap \Bbbk[\{X_i\}_{i\in\delta}])\,\Bbbk[\mathbf{X}]+\langle X_i^{d_i} \ \mid \ i\notin\delta\rangle \subseteq I \subseteq I+\mathfrak{p}_{\delta^c},$$

for every $d_i \geq 1,\ i\notin\delta$. Therefore, taking radicals, by part (c) we conclude that $\sqrt{I_{\mathcal{L}}(\rho)+\mathfrak{p}_{\delta^c}} = \sqrt{I} = \sqrt{I+\mathfrak{p}_{\delta^c}}$.

Now, the last statements are direct consequences of the definition of mesoprimary ideal and Theorem 43. □

In the following definition we introduce the concept of primary congruence on $\mathbb{N}^n$. We prove that our notion of primary congruence is equivalent to the one given in [7, p. 44].

Definition 51. *A congruence $\sim$ on $\mathbb{N}^n$ is said to be **primary** if the ideal $I_\sim$ is cellular.*

Definition 52. *Let $\sim$ be a congruence on $\mathbb{N}^n$. An element $\mathbf{a}\in\mathbb{N}^n/\sim$ is said to be **nilpotent** if $d\,\mathbf{a}$ is nil, for some $d\in\mathbb{N}$.*

Proposition 53. *A congruence $\sim$ on $\mathbb{N}^n$ is primary if and only if every element of $\mathbb{N}^n/\sim$ is nilpotent or cancellable.*

Proof. If $\sim$ is a primary congruence on $\mathbb{N}^n$, the binomial associated ideal $I_\sim$ is $\delta-$cellular for some $\delta\subseteq\{1,\ldots,n\}$. Let $[\mathbf{u}]$ be a non-nilpotent element of $\mathbb{N}^n/\sim$. Given $[\mathbf{v}]$ and $[\mathbf{w}]\in\mathbb{N}^n/\sim$ such that $[\mathbf{v}]+[\mathbf{u}]=[\mathbf{v}+\mathbf{u}]=[\mathbf{w}+\mathbf{u}]=[\mathbf{w}]+[\mathbf{u}]$, we have that $\mathbf{X}^{\mathbf{u}}(\mathbf{X}^{\mathbf{v}}-\mathbf{X}^{\mathbf{w}})\in I_\sim$. Since $[\mathbf{u}]$ is not nilpotent, $(\mathbf{X}^{\mathbf{u}})^d\notin I_\sim$, for every $d\in\mathbb{N}$. Therefore, no variable X_i with $i\notin\delta$ divides $\mathbf{X}^{\mathbf{u}}$ and, by the definition of cellular ideal, we conclude that $I_\sim : \mathbf{X}^{\mathbf{u}} = I_\sim$; in particular, $\mathbf{X}^{\mathbf{v}}-\mathbf{X}^{\mathbf{w}}\in I_\sim$, that is, $[\mathbf{v}]=[\mathbf{w}]$, and hence $[\mathbf{u}]$ is cancellable.

Conversely, suppose that every element of $\mathbb{N}^n/\sim$ is nilpotent or cancellable. Set $\delta=\{i\in\{1,\ldots,n\} : [\mathbf{e}_i]$ is cancellable$\}$. Clearly, $j\in\delta$ if and only if X_j is a nonzerodivisor modulo $I_\sim$ and $j\notin\delta$ if and only if $X_j^{d_j}\in I_\sim$, for some $d_j\geq 1$. Therefore, $I_\sim$ is a $\delta-$cellular ideal (see the paragraph just after Definition 49). □

As a consequence, if $\sim$ is a primary congruence on $\mathbb{N}^n$, then, by Proposition 50, $J := \sqrt{I_\sim}$ is a mesoprime ideal. Therefore, associated to $\sim$ there is one and only one prime congruence, $\sim_J$, obtained by removing nilpotent elements.

4.1. Cellular Decomposition of Binomial Ideals.

Definition 54. *A cellular decomposition of an ideal $I\subseteq\Bbbk[\mathbf{X}]$ is an expression of I as an intersection of cellular ideals with respect to different $\delta\subseteq\{1,\ldots,n\}$, say*

$$I = \bigcap_{\delta\in\Delta} \mathcal{C}_\delta, \tag{8}$$

for some subset Δ *of the power set of* $\{1,\ldots,n\}$*. Moreover, the cellular decomposition (8) is said to be minimal if* $\mathcal{C}'_\delta \not\supseteq \bigcap_{\delta\in\Delta\setminus\{\delta'\}} \mathcal{C}_\delta$ *for every* $\delta' \in \Delta$*; in this case, the cellular component* $\mathcal{C}_\delta$ *is said to be a* $\delta-$*cellular component of* I*.*

Example 55. Every minimal primary decomposition of a monomial ideal $I \subseteq \Bbbk[\mathbf{X}]$ into monomial ideals is a minimal cellular decomposition of I. Consequently, there is non-uniqueness for cellular decomposition in general: consider for instance the following cellular (primary) decomposition

$$\langle X^2, XY\rangle = \langle X\rangle \cap \langle X^2, XY, Y^n\rangle,$$

where n can take any positive integral value.

Cellular decompositions of an ideal I of $\Bbbk[\mathbf{X}]$ always exist. A simple algorithm for cellular decomposition of binomial ideals can be found in [13, Algorithm 2], this algorithm forms part of the `binomials` package developed by T. Kahle and it is briefly described below. The interested reader may consult [9] and [13] for further details.

The following result is the key for producing cellular decompositions of binomial ideals into binomial ideals.

Lemma 56. *Let* I *be a proper binomial ideal in* $\Bbbk[\mathbf{X}]$*. If* I *is not cellular then there exists* $i \in \{1,\ldots,n\}$ *and a positive integer* d *such that* $I = (I : X_i^d) \cap (I + \langle X_i^d\rangle)$*, with* $I : X_i^d$ *and* $I + \langle X_i^d\rangle$ *binomial ideals strictly containing* I*.*

Proof. If I is not cellular, there exists at least one variable X_i which is zerodivisor and not nilpotent modulo I. Then, by the Noetherian property of $\Bbbk[\mathbf{X}]$, there is a positive integer d such that $I : \langle X_i^d\rangle = I : \langle X_i^e\rangle$ for every $e \geq d$. We claim that I decomposes as $(I : X_i^d) \cap (I + \langle X_i^d\rangle)$. Indeed, let $f \in (I : X_i^d) \cap (I + \langle X_i^d\rangle)$ and let $f = g + hX_i^d$ for some $g \in I$. Then $X_i^d f = X_i^d g + hX_i^{2d}$ and, thus $hX_i^{2d} = X_i f - X_i g \in I$. That is, $h \in I : \langle X_i^{2d}\rangle = I : \langle X_i^d\rangle$. Hence, $hX_i^d \in I$ and, consequently, $f \in I$.

It remains to see that both $I : X_i^d$ and $I + \langle X_i^d\rangle$ are binomial ideals which strictly contain I. On the one hand, the ideal $I + \langle X_i^d\rangle$ is binomial and I is strictly contained in it, as X_i is not nilpotent modulo I. On the other hand, $I : X_i^d$ is binomial by Corollary 5, and I is strictly contained in $I : X_i^d$ because X_i is a zerodivisor modulo I. □

Now, by Lemma 56, if I is not a cellular ideal then we can find two new proper ideals strictly containing I. If these ideals are cellular then we are done. Otherwise, we can repeat the same argument with these new ideals, getting strictly increasing chains of binomial ideals. Since $\Bbbk[\mathbf{X}]$ is a Noetherian ring, each one of these chains has to be stationary. So, in the end, we obtain a (redundant) cellular decomposition of I. Observe that this process does not depend on the base field.

Example 57. Consider the binomial ideal $I = \langle X^4Y^2 - Z^6, X^3Y^2 - Z^5, X^2 - YZ\rangle$ of $\mathbb{Q}[X,Y,Z]$. By using [13, Algorithm 2] we obtain the following cellular decomposition, $I = I_1 \cap I_2 \cap I_3$, where

$$\begin{aligned} I_1 &= \langle Y - Z, X - Z\rangle \\ I_2 &= \langle Z^2, XZ, X^2 - YZ\rangle \\ I_3 &= \langle X^2 - YZ, XY^3Z - Z^5, XZ^5 - Z^6, Z^7, Y^7\rangle. \end{aligned}$$

```
loadPackage "Binomials";
R = QQ[X,Y,Z];
I = ideal(X^4*Y^2-Z^6,X^3*Y^2-Z^5,X^2-Y*Z);
binomialCellularDecomposition I
```

As a final conclusion we may notice the following:

Corollary 58. *Let $\sim$ be a congruence on $\mathbb{N}^n$. A primary decomposition of $\sim$ can be obtained by computing a cellular decomposition of $I_\sim$.*

Proof. It is a direct consequence of Proposition 27 by the definition of primary congruence. □

5. Mesoprimary ideals

The main objective of this section is to analyze the mesoprimary ideals and their corresponding congruence. Mesoprimary ideals were introduced by Thomas Kahle and Ezra Miller in [10] as an intermediate construction between cellular and primary binomial ideals. Kahle and Miller proved combinatorially that every cellular binomial can be decomposed into finitely many mesoprimary ideals over an arbitrary field. However, not every decomposition of a binomial ideal as an intersection of mesoprimary ideals is a mesoprimary decomposition in the sense of Kahle and Miller. These mesoprimary decompositions feature refined combinatorial requirements, and currently there is no algorithm available to compute them. On the other hand, decompositions of binomial ideals into mesoprimary ideals can be produced algorithmically.. Despite of this, mesoprimary decompositions have been successfully used to solve open problems (see [11] and [12]).

The following preparatory result will be helpful in understanding what mesoprimary ideals are.

Proposition 59. *Let I be a $\delta-$cellular binomial ideal in $\Bbbk[\mathbf{X}]$. If $\mathbf{X}^{\mathbf{u}} \in \Bbbk[\{X_i\}_{i\notin\delta}] \setminus I$, then $I : \mathbf{X}^{\mathbf{u}}$ is a $\delta-$cellular binomial ideal.*

Proof. First of all, we note that $I : \mathbf{X}^{\mathbf{u}} \neq \langle 1\rangle$ because $\mathbf{X}^{\mathbf{u}} \notin I$. Moreover, we have that $I : \mathbf{X}^{\mathbf{u}}$ is binomial by Corollary 5. Now, since $I : (\prod_{i\in\delta} X_i)^\infty = I$, then

$$(I : \mathbf{X}^{\mathbf{u}}) : (\prod_{i\in\delta} X_i)^\infty = (I : (\prod_{i\in\delta} X_i)^\infty) : \mathbf{X}^{\mathbf{u}} = I : \mathbf{X}^{\mathbf{u}}.$$

And, clearly, for every $i \notin \delta$, $X_i^{d_i} \in I : \mathbf{X}^{\mathbf{u}}$ for some $d_i \geq 1$ because $I \subseteq I : \mathbf{X}^{\mathbf{u}}$. Putting all this together, we conclude that $I : \mathbf{X}^{\mathbf{u}}$ is a $\delta-$cellular binomial ideal. □

If I is a $\delta-$cellular binomial ideal, then the ideal $(I : \mathbf{X}^{\mathbf{u}}) + \mathfrak{p}_{\delta^c}$ is $\delta-$mesoprime by Propositions 59 and 50(b). Moreover, there exists $d_i \geq 1$ such that $X_i^{d_i} \in I$ for each $i \notin \delta$. Thus there are finitely many mesoprime ideals of the form $(I : \mathbf{X}^{\mathbf{u}}) + \mathfrak{p}_{\delta^c}$. These are the so-called mesoprimes associated to I:

Definition 60. *Let I be a $\delta-$cellular binomial ideal in $\Bbbk[\mathbf{X}]$. We will say that $I_{\mathcal{L}}(\rho) + \mathfrak{p}_{\delta^c}$ is a mesoprime ideal associated to I if there exist a monomial $\mathbf{X}^{\mathbf{u}} \in \Bbbk[\{X_i\}_{i\notin\delta}]$ such that*

$$\big((I : \mathbf{X}^{\mathbf{u}}) \cap \Bbbk[\{X_i\}_{i\in\delta}]\big)\, \Bbbk[\mathbf{X}] = I_{\mathcal{L}}(\rho).$$

Now we may introduce the notion of mesoprimary ideal.

Definition 61. *A binomial ideal is said to be* ***mesoprimary*** *if it is cellular and it has only one associated mesoprime ideal. A congruence $\sim$ on $\mathbb{N}^n$ is mesoprimary if $I_\sim$ is a mesoprimary ideal of $\Bbbk[\mathbf{X}]$*

The following lemma clarifies the notion of mesoprimary ideal.

Lemma 62. *A $\delta-$cellular binomial ideal I in $\Bbbk[\mathbf{X}]$ is mesoprimary if and only if $(I : \mathbf{X}^{\mathbf{u}}) \cap \Bbbk[\{X_i\}_{i\notin\delta}] = I \cap \Bbbk[\{X_i\}_{i\notin\delta}]$, for all $\mathbf{X}^{\mathbf{u}} \in \Bbbk[\{X_i\}_{i\notin\delta}] \setminus I$.*

Proof. It suffices to note that I has two different associated mesoprimes if and only if there exists $\mathbf{X}^{\mathbf{u}} \in \Bbbk[\{X_i\}_{i\notin\delta}]$ such that $(I : \mathbf{X}^{\mathbf{u}}) \cap \Bbbk[\{X_i\}_{i\notin\delta}] \neq I \cap \Bbbk[\{X_i\}_{i\notin\delta}]$ because, in this case, by Proposition 50, $(I : \mathbf{X}^{\mathbf{u}}) + \mathfrak{p}_{\delta^c}$ and $I + \mathfrak{p}_{\delta^c}$ are two different associated mesoprimes to I. □

Definition 63. *Let $\sim$ be a congruence on $\mathbb{N}^n$. An element $\mathbf{a} \in \mathbb{N}^n/\sim$ is said to be **partly cancellable** if $\mathbf{a}+\mathbf{b} = \mathbf{a}+\mathbf{c} \neq \infty \Rightarrow \mathbf{b} = \mathbf{c}$, for all cancellable $\mathbf{b}, \mathbf{c} \in \mathbb{N}^n$*

Proposition 64. *A congruence $\sim$ on $\mathbb{N}^n$ is mesoprimary if and only if it is primary and every element in $\mathbb{N}^n/\sim$ is partly cancellable.*

Proof. If $\sim$ is a mesoprimary congruence on $\mathbb{N}^n$, then $I = I_\sim$ is $\delta-$cellular for some $\delta \subseteq \{1,\ldots,n\}$. Thus, $\sim$ is primary. Moreover, $(I : \mathbf{X}^\mathbf{u}) \cap \Bbbk[\{X_i\}_{i\in\delta}] = I \cap \Bbbk[\{X_i\}_{i\in\delta}]$, for all $\mathbf{X}^\mathbf{u} \in \Bbbk[\{X_i\}_{i\notin\delta}] \setminus I$ (equivalently, for all $\mathbf{u} \in \mathbb{N}^n$ such that $[\mathbf{u}]$ is nilpotent and it is not a nil). Therefore, if $[\mathbf{u}] \in \mathbb{N}^n/\sim$ is nilpotent and $[\mathbf{v}], [\mathbf{w}]$ are cancellable elements such that $[\mathbf{u}] + [\mathbf{v}] = [\mathbf{u}] + [\mathbf{w}] \neq \infty$, then

$$\mathbf{X}^\mathbf{v} - \mathbf{X}^\mathbf{w} \in (I : \mathbf{X}^\mathbf{u}) \cap \Bbbk[\{X_i\}_{i\in\delta}] = I \cap \Bbbk[\{X_i\}_{i\in\delta}],$$

that is to say $[\mathbf{v}] = [\mathbf{w}]$. So, $[\mathbf{u}]$ is partly cancellative.

Conversely, suppose that $\sim$ is primary congruence on $\mathbb{N}^n$ such that every element in $\mathbb{N}^n/\sim$ is partly cancellable. Since $\sim$ is primary, we have that $I_\sim$ is $\delta-$cellular, by setting $\delta = \{i \in \{1,\ldots,n\} : [\mathbf{e}_i] \text{ is cancellable}\}$. Now, if $\mathbf{X}^\mathbf{u} \in \Bbbk[\{X_i\}_{i\notin\delta}]\setminus I$, we have that $[\mathbf{u}]$ is partly cancellable. Thus, for every $\mathbf{X}^\mathbf{v} - \mathbf{X}^\mathbf{w} \in \Bbbk[\{X_i\}_{i\in\delta}]$, we have that $\mathbf{X}^\mathbf{u}(\mathbf{X}^\mathbf{v} - \mathbf{X}^\mathbf{w}) \in I \Rightarrow \mathbf{X}^\mathbf{v} - \mathbf{X}^\mathbf{w} \in I$. Therefore, $(I : \mathbf{X}^\mathbf{u}) \cap \Bbbk[\{X_i\}_{i\in\delta}] \subseteq I \cap \Bbbk[\{X_i\}_{i\in\delta}]$. Now, since the opposite inclusion is always fulfilled, by Lemma 62, we are done. □

There are other intermediate constructions between cellular and primary ideals, such as the unmixed decomposition (see [5, 13] and, more recently, [6]). The following example shows that unmixed cellular binomial ideals are not mesoprimary. Recall that an unmixed cellular binomial ideal is a cellular binomial ideal with no embedded associated primes (see [13, Proposition 2.4]).

Example 65. Consider the unmixed cellular binomial $I \subset \Bbbk[X,Y]$ generated by $\{X^2-1, Y(X-1), Y^2\}$. The ideal I is not mesoprimary, because

$$(I : Y) \cap \Bbbk[X] = \langle X-1\rangle \neq \langle X^2-1\rangle = I \cap \Bbbk[X].$$

```
loadPackage "Binomials";
R = QQ[X,Y]
I = ideal(X^2-1,Y*(X-1),Y^2)
cellularBinomialAssociatedPrimes I
eliminate(I:Y,Y)
eliminate(I,Y)
```

We end this section by exhibiting the statement of Kahle and Miller which describes the primary decomposition of a mesoprimary ideal, in order to give an idea of how useful would be to have an algorithm for the mesoprimary decomposition of a cellular binomial ideal.

Proposition 66 ([10, Corollary 15.2 and Proposition 15.4])**.** *Let I be a (δ-cellular) mesoprimary ideal, and denote by $I_\mathcal{L}(\rho)$ the lattice ideal $I \cap \Bbbk[\{X_i\}_{i\in\delta}]$. The associated primes of I are exactly the (minimal) primes of its associated mesoprime $I + \mathfrak{p}_{\delta^c}$. Moreover, if $I_\mathcal{L}(\rho) = \cap_{j=1}^g I_j$ is the primary decomposition of $I_\mathcal{L}(\rho)$ from Theorem 38, then*

$$I = \bigcap_{j=1}^{g} (I + I_j)$$

is the primary decomposition of I.

Notice that the hypothesis $\Bbbk$ algebraically closed is only needed when Theorem 38 is applied.

Acknowledgement We thank the anonymous referees for their detailed suggestions and comments, which have greatly improved this article. The present paper is based on a course of lectures delivered by the second author at the EACA's Third International School on Computer Algebra and Applications `https://www.imus.us.es/EACASCHOOL16/`. He thanks the organizers for giving him that opportunity.

References

[1] Briales, E. Campillo, A. Marijuán, C. Pisón, P. Combinatorics of syzygies for semigroup algebra. *Collect. Math.* **49**, 239–256 (1998)
[2] Brookfield, G. Commutative Noetherian semigroups are finitely generated. *Semigroup Forum* **66**(2), 323–327 (2003)
[3] Bruns, W., Herzog, J. *Cohen-Macaulay rings.* Cambridge studies in advanced mathematics, vol. 39, Cambridge University Press, 1993
[4] Budach, L. Struktur Noetherscher kommutativer Halbgruppen. *Monatsb. Deutsch. Akad. Wiss.* Berlin, **6**, 85–88 (1964)
[5] Eisenbud, D., Sturmfels, B.: Binomial ideals. *Duke Math. J.* **84**(1), 1–45 (1996)
[6] Eser, Z.S., Matusevich, L.F.: Decompositions of cellular binomial ideals. *J. London Math. Soc.* **94**, 409–426 (2016)
[7] Gilmer, R.: *Commutative semigroup rings.* Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1984
[8] Grayson, D.R., Stillman, M.E.: *Macaulay2, a software system for research in algebraic geometry.* Available at `http://www.math.uiuc.edu/Macaulay2/`
[9] Kahle, T. Decompositions of Binomial Ideals. *Journal of Software for Algebra and Geometry* **4**(1), 1–5 (2012)
[10] Kahle, T., Miller, E.: Decompositions of commutative monoid congruences and binomial ideals. *Algebra Number Theory* **8**(6), 1297–1364 (2014)
[11] Kahle, T., Miller, E., O'Neill, C.: Irreducible decomposition of binomial ideals. *Compositio Mathematica* **152**, 1319–1332 (2016)
[12] Matusevich, L.F., O'Neill C.: Some algebraic aspects of mesoprimary decomposition. arXiv:1706.07496 [math.AC]
[13] Ojeda, I., Piedra Sánchez, R. Cellular binomial ideals. Primary decomposition of binomial ideals. *J. Symbolic Comput.* **30**(4), 383–400 (2000)
[14] Ojeda, I.: Binomial canonical decompositions of binomial ideals. *Comm. Algebra* **39**(10), 3722–3735 (2011)

Mathematics Departament
Texas A&M University
College Station, TX 77843 (USA)

E-mail address: `laura@math.tamu.edu`

Departamento de Matemáticas
Universidad de Extremadura
E-06071 Badajoz (SPAIN)

E-mail address: `ojedamc@unex.es`