DECOMPOSITIONS OF COMMUTATIVE MONOID CONGRUENCES AND BINOMIAL IDEALS

THOMAS KAHLE AND EZRA MILLER

ABSTRACT. We demonstrate how primary decomposition of commutative monoid congruences fails to capture the essence of primary decomposition in commutative rings by exhibiting a more sensitive theory of *mesoprimary decomposition* of congruences, complete with witnesses, associated prime objects, and an analogue of irreducible decomposition called *coprincipal decomposition*. We lift the combinatorial theory of mesoprimary decomposition to binomial ideals in monoid algebras. The resulting *binomial mesoprimary decomposition* is a new type of intersection decomposition for binomial ideals that enjoys computational efficiency and independence from ground field hypotheses. Furthermore, binomial primary decomposition is easily recovered from mesoprimary decomposition, as is binomial irreducible decomposition—which was previously not known to exist—from binomial coprincipal decomposition.

CONTENTS

1.	Introduction	2
2.	Taxonomy of congruences on monoids	10
3.	Primary decomposition and localization in monoids	15
4.	Witnesses and associated prime ideals of congruences	18
5.	Associated prime congruences	21
6.	Characterization of mesoprimary congruences	23
7.	Coprincipal congruences	26
8.	Mesoprimary decompositions of congruences	27
9.	Augmentation ideals, kernels, and nils	30
10.	Taxonomy of binomial ideals in monoid algebras	33
11.	Monomial localization, characters, and mesoprimes	37
12.	Coprincipal and mesoprimary components of binomial ideals	40
13.	Mesoprimary decomposition of binomial ideals	45
14.	Binomial localization	47
15.	Irreducible and primary decomposition of binomial ideals	49
16.	Character witnesses and false witnesses	53
17.	Open problems	57
	References	60

Date: 8 September 2011.

2010 *Mathematics Subject Classification.* Primary: 20M14, 05E40, 20M25; Secondary: 20M30, 20M13, 05E15, 13F99, 13C05, 13A02, 13P99, 68W30, 14M25.

1. Introduction

Overview. Primary decomposition of ideals and modules has been a mainstay of commutative algebra since its introduction roughly a century ago [Noe21]. A formally analogous theory for congruences on commutative monoids made its first appearance around fifty years ago [Drb63], and subsequently the topic of decompositions has similarly played a central role in commutative semigroup theory [Gri01]. Our first goal is to demonstrate that the formal analogy in the setting of finitely generated monoids and congruences—the *combinatorial setting*—fails to capture the essence of primary decomposition in noetherian rings and modules. We rectify this failure by exhibiting a more sensitive theory of *mesoprimary decomposition* of congruences, complete with witnesses, associated prime objects, and other facets of control afforded in parallel with primary decomposition in rings. We justify our claim of insufficiency of the formal analogy in current use by lifting our witnessed theory of mesoprimary decomposition to the *arithmetic setting*: binomial ideals in semigroup rings, comprising the interface of commutative ring theory with finitely generated monoids.

Mesoprimary decomposition of binomial ideals is not binomial primary decomposition, but a new type of intersection decomposition for binomial ideals, with numerous advantages over ordinary primary decomposition, such as combinatorial clarity, independence from properties of the ground field, and computational efficiency. Nevertheless, binomial primary decomposition is easily recovered from mesoprimary decomposition, as is binomial irreducible decomposition, which was previously not known to exist; both are consequently seen to be chiefly combinatorial in nature. In essence, by lifting mesoprimary decomposition of congruences, binomial mesoprimary decomposition distills the coefficient-free combinatorics inherent in primary decomposition of binomial ideals and isolates the precise manner in which coefficients subsequently determine the primary components. The subtlety of coefficient arithmetic causes the lifting procedure to fail verbatim translation, thus requiring great care, particularly where redundancy is involved. Part of our study therefore contrasts the slightly different notions of witness and associatedness in the combinatorial and arithmetic settings.

General motivation. Beyond the intrinsic merit of mesoprimary decomposition, the need for natural decompositions in the monoid and binomial contexts has become increasingly important in recent years, in view of appearances and applications in numerous areas. Some of these directly involve commutative monoids, such as schemes over $\mathbb{F}_1$ [CC11, Dei05], where monoids form the foundation just as rings do for usual schemes. Another instance is the arrival of misère quotients in combinatorial game theory, where monoids provide data structures for recording and computing winning strategies [Pla05, PS07] (see also [Mil11a] for a gentle algebraic introduction). At the same time, binomial ideals are finding ever deeper interactions with other parts of mathematics and the sciences, motivating research into applicable descriptions—including computational and combinatorial ones—of their decompositions. For example, dynamics of mass-action kinetics, where steady states in detailed-balanced cases are described by vanishing of binomial trajectories, arise from stoichiometric exponential growth and decay [AGHMR09]; binomial primary decompositions in mass-action kinetics can identify which species persist or become extinct [SS10]. In algebraic statistics, decompositions of binomial ideals give insight into how a set of conditional independence statements among random variables can be realized [DSS09, HHHKR10]. The algebra, geometry, and combinatorics of binomial primary decomposition interacts with systems of differential equations of hypergeometric type [GGZ87, GKZ89], whose solutions are eigenfunctions for binomial differential operators encoding the infinitesimal action of an algebraic torus.

In fact, it was in the hypergeometric framework that the combinatorics of binomial primary decomposition had its origin [DMM10, DMM09], providing tight control over series solutions. In the meantime, mesoprimary decomposition serves as an improved method for presenting and visualizing binomial primary decomposition in algorithmic output [Kah11]. Beyond that, the methods here have already found a theoretical application to combinatorial game theory [Mil11b].

Gathering primary components rationally. Staring at output of binomial primary decomposition algorithms intimates that certain primary components belong together.

Example 1.1. During investigations of presentations of misère quotients of combinatorial games (culminating in the definition of lattice games [GMW09, GM10]), Macaulay2 [GS] produced long lists of primary binomial ideals. In one instance, eight of the forty or so components were

$$\begin{gathered}\langle e-1, d-1, b-1, a-1, c^3\rangle,\ \langle e-1, d-1, b-1, a+1, c^3\rangle,\\ \langle e-1, d+1, b-1, a-1, c^3\rangle,\ \langle e-1, d+1, b-1, a+1, c^3\rangle,\\ \langle e+1, d-1, b+1, a-1, c^3\rangle,\ \langle e+1, d-1, b+1, a+1, c^3\rangle,\\ \langle e+1, d+1, b+1, a-1, c^3\rangle,\ \langle e+1, d+1, b+1, a+1, c^3\rangle.\end{gathered}$$

The urge to gather these eight into one piece (a piece of eight?), namely their intersection

$$\langle b-e, e^2-1, d^2-1, a^2-1, c^3\rangle,$$

is irresistible. (Who would rather sift through the big list?) And it would have become more so had the exponents in the single gathered component been odd primes, for then the coefficients in the long list of primary ideals would not even have been rational numbers, though the intersection would still have been rational.

In general, a binomial prime ideal $I_{\rho,P}$ in a finitely generated monoid algebra $\Bbbk[Q]$ is determined by a monoid prime ideal $P \subset Q$ and a character $\rho : K \to \Bbbk^*$ defined on a subgroup of the local unit group $G_P \subseteq Q_P$ (Theorem 11.15). A given binomial ideal $I \subseteq \Bbbk[Q]$ (Definition 2.14) might possess a multitude of associated primes sharing the same P and K, differing only in the character ρ. We originally conceived of *mesoprimary ideals* (Definition 10.4; see also Proposition 12.6) as data structures for keeping track of primary components for such groups of associated binomial primes. The term "group" here is used in the ordinary, nonmathematical sense, but it is entirely appropriate mathematically: the primary components of a mesoprimary ideal over an algebraically closed field are indexed by the characters of a finite abelian group, namely the quotient $\mathrm{sat}(K)/K$ of the saturation of K in G_P (Proposition 15.7 and Remark 15.8). The efficiency of space afforded by describing primary decompositions after gathering components into mesoprimary ideals is thus more or less equivalent to writing presentations for a collection of finite abelian groups instead of listing every one of their characters.

The situation is not typically as simple as in Example 1.1. Indeed, upon inspecting a binomial primary decomposition, it can be difficult to determine which mesoprimary ideals ought to occur, and which mesoprimary ideal each primary component ought to contribute to. Furthermore, some primary components of a mesoprimary ideal can be absent, even if the mesoprimary ideal clearly ought to appear. Nonetheless, *mesoprimary decompositions* of binomial ideals always exist (Definition 13.1 and Theorem 13.2) in a form that realizes our initial intent (Corollary 15.11 and Theorem 15.14) by canonical primary decomposition of mesoprimary ideals (Proposition 15.7 and Remark 15.8). In summary, mesoprimary decomposition gathers primary components so that:

1. the decomposition into binomial ideals requires no hypotheses on the ground field;
2. specifying one mesoprimary component takes the place of individually listing all primary components arising from saturated extensions of a fixed character; and
3. the combinatorics of the components and their associated prime objects accurately and faithfully reflects the combinatorics of the decomposed binomial ideal.

The key role of item 3, in both the existence and chronological development of mesoprimary decomposition, is discussed at length in the remainder of this Introduction.

Example 1.2. The ideal $I = \langle y - x^2y, y^2 - xy^2, y^3\rangle \subseteq \Bbbk[x, y]$ has primary decomposition $I = \langle y\rangle \cap \langle 1 + x, y^2\rangle \cap \langle 1 - x, y^3\rangle$. The ideal I is *unital* (Remark 2.16), being generated by differences of monomials, so the component $\langle 1 + x, y^2\rangle$ feels out of place. Yet there are no obvious components to gather. What's missing is a "phantom" component $\langle 1 - x, y^2\rangle$, hidden by $\langle 1 - x, y^3\rangle$. Gathering yields $\langle 1 + x, y^2\rangle \cap \langle 1 - x, y^2\rangle = \langle 1 - x^2, y^2\rangle$. The mesoprimary decomposition is $I = \langle y\rangle \cap \langle 1 - x^2, y^2\rangle \cap \langle 1 - x, y^3\rangle$.

What criterion determines when a set of primary components of an ideal I should be gathered, and when not? Our answer takes its cues from two sources.

The first cue is arithmetic: the gathering problem has already been solved—quite naturally—when $I = \langle \mathbf{t}^u - \mathbf{t}^v \mid u - v \in L\rangle \subseteq \Bbbk[t_1, \ldots, t_n]$ is a *lattice ideal* in a polynomial ring over an algebraically closed field $\Bbbk = \overline{\Bbbk}$ of characteristic 0, for some sublattice $L \subseteq \mathbb{Z}^n$ [ES96, Corollary 2.2] (see Proposition 11.10). Its primary components are the "twisted lattice ideals" $\langle \mathbf{t}^u - \rho(u - v)\mathbf{t}^v \mid u - v \in \mathrm{sat}(L)\rangle$ for extensions $\rho : \mathrm{sat}(L) \to \Bbbk^*$ of the trivial character on L. In keeping with Example 1.1, if $\Bbbk$ were not algebraically closed, then these characters ρ would not necessarily be defined over $\Bbbk$, but the intersection of the primes, namely the lattice ideal itself, is defined over $\Bbbk$ automatically.

The second cue is combinatorial: primary binomial ideals have particularly simple combinatorics (again, we only know this over fields $\Bbbk = \overline{\Bbbk}$ of characteristic 0), and primary components of a given binomial ideal are constructed by relatively straightforward operations [DMM09, Theorem 3.2]. However, the procedure goes only one way: it is not obvious (even now, given the results in this paper) how to reconstruct the combinatorics of a binomial ideal from an arbitrary binomial primary decomposition.

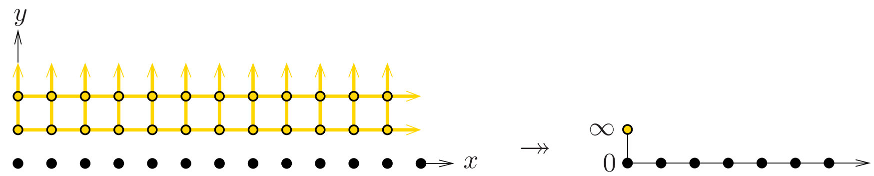
Mesoprimary decomposition of a binomial ideal I is an expression of I as an intersection of *mesoprimary components* (Definition 12.15), each of which is a mesoprimary ideal—a binomial ideal whose combinatorics feels like that of a primary ideal but whose arithmetic feels like that of a lattice ideal. An arbitrary intersection of mesoprimary ideals is not a mesoprimary decomposition, even if the intersection is a binomial ideal; exigent additional conditions must be met regarding the interaction of the combinatorics and the arithmetic of the mesoprimary components, as compared with that of I (Remark 13.7). In particular, the combinatorics of I is easily reconstructed from any mesoprimary decomposition, by fiat (Definition 13.1).

Congruences: binomial combinatorics. Our first approaches to mesoprimary decomposition reduced to the case of *cellular* binomial ideals in polynomial rings (Definition 10.4), since all binomial ideals are expressible as intersections of these [ES96, Section 6]. However, our many attempts, complicated by the non-canonical nature of cellular decomposition, and restricted by keeping to polynomial rings, inexorably led us to conclude that a proper combinatorial theory of binomial primary decomposition could be achieved only with input from the language and theory of monoid *congruences* (Section 2; or see [Gil84] for more background).

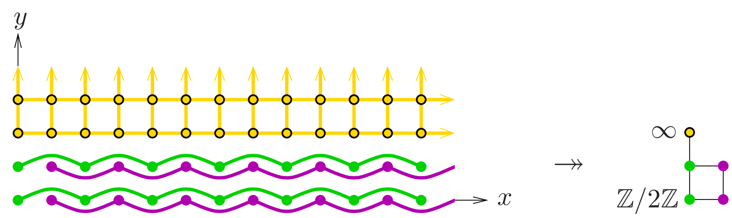
Every mention of "combinatorics" in binomial contexts prior to this point refers to congruences on monoids. The simple (and not new) idea is that a binomial ideal $I \subseteq \Bbbk[Q]$ in the monoid algebra for a commutative monoid Q determines an equivalence relation $\sim$ on Q that sets $u \sim v$ if I contains a two-term binomial $\mathbf{t}^u - \lambda\mathbf{t}^v$ (Definition 2.14). The quotient $\overline{Q} = Q/\!\sim$ modulo this relation is a monoid. When $Q = \mathbb{N}^n$ is finitely generated and free, $\Bbbk[Q]$ is a polynomial ring, and binomial combinatorics amounts to a certain type of lattice point geometry.

Example 1.3. The following ideals induce the depicted congruences on $\mathbb{N}^2$ and quotient monoids. The congruence classes are the connected components of the graphs drawn in the left-hand pictures. Each element labeled 0 is the identity of the quotient monoid. Each element labeled ∞ in the right-hand picture is *nil* (Definition 2.8 and Remark 2.9) in the quotient monoid; its congruence class comprises all monomials in the given binomial ideal. In items 2 and 4, the groups labeling the rows indicate how the group in the bottom row acts on the higher rows. In all four items, every element outside of the bottom row of the quotient monoid is *nilpotent* (Definition 2.8).

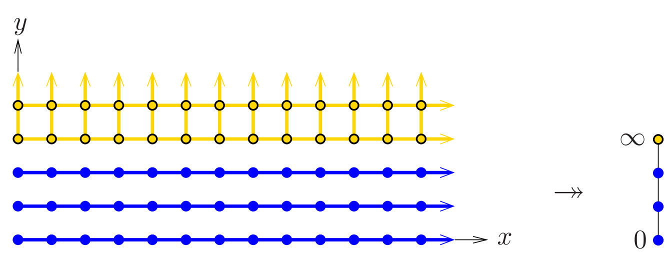
1. For the ideal $\langle y\rangle \subset \Bbbk[x,y]$, the quotient monoid is $\mathbb{N}\cup\infty$:



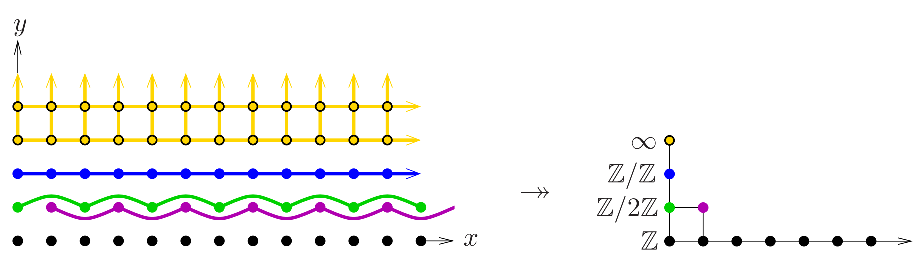
2. For the ideal $\langle 1-x^2, y^2\rangle \subset \Bbbk[x,y]$, the quotient monoid is a copy of the group $\mathbb{Z}/2\mathbb{Z}$ (the bottom row), a free module over $\mathbb{Z}/2\mathbb{Z}$ (the middle row), and a nil:



3. For the ideal $\langle 1-x, y^3\rangle \subset \Bbbk[x,y]$, the quotient monoid is the quotient $\mathbb{N}/(3+\mathbb{N})$ of the natural numbers modulo the *Rees congruence* of the ideal $3+\mathbb{N}$, which makes all elements of the ideal equivalent and leaves the other elements of $\mathbb{N}$ alone:



4. For the ideal $\langle y - x^2y, y^2 - xy^2, y^3\rangle \subset \Bbbk[x,y]$, the quotient monoid is a disjoint union of the group $\mathbb{Z}$ and three $\mathbb{Z}$-modules:



We examined monoid congruences on the premise that an appropriate decomposition theory for them should lift, either analogously or directly, to the desired mesoprimary theory for binomial ideals. However, although we found rich decomposition theories for commutative semigroups [Gri01], the expected analogue of binomial primary decomposition was absent. The most promising development we encountered along these lines is Grillet's discovery of conditions guaranteeing that a commutative semigroup can be realized as a subsemigroup of the multiplicative semigroup of a primary ring—that is, a ring with just one associated prime [Gri75]. That work covers ground anticipating—in a more general setting but necessarily with less precise results—the characterization of primary binomial ideals over algebraically closed fields of characteristic zero [DMM09].

The closest monoid relative in the literature to primary decomposition in rings seems to be primary decomposition of congruences [Drb63] (see [Gil84] for a treatment in the context of semigroup rings). However, one of our motivating discoveries is that primary decomposition of congruences, being much closer to a shadow of cellular binomial decomposition (by Theorem 10.6), falls quite short of serving as a rubric for either primary or mesoprimary decomposition of binomial ideals. Indeed, congruences that are *prime*, meaning that quotients modulo them are cancellative except perhaps for a nil (Definition 2.11.4), fail to be irreducible (Example 2.22). Furthermore, congruences that are *primary*, meaning that every element in the quotient is either nilpotent or cancellative (Definition 2.11.1), admit further decompositions into pieces that are visibly more "homogeneous", in a manner more analogous to primary decomposition in the presence of embedded primes than to irreducible decomposition of primary ideals.

Example 1.4. All of the congruences depicted in Example 1.3 are primary, but the first three are visibly more homogeneous: in each one, the non-nil rows all look the same. In fact, the fourth congruence is the *common refinement* (Section 3) of the first three. This is equivalent to saying that the fourth binomial ideal equals the intersection of the first three—this is the mesoprimary decomposition from Example 1.2—since the ideals in question are all unital and contain monomials; see Remark 2.16 and Theorem 9.12.

Given the role of primary (binomial) ideals in the setting of primary decomposition over noetherian (monoid) rings, it would be reasonable to seek a theory of "primitive decomposition" for congruences, since primary binomial ideals induce *primitive* congruences (Definition 2.11 and Theorem 10.6). However, congruences usually do not admit expressions as intersections (common refinements) of primitive congruences. The reason stems from the same phenomenon that requires one to assume, for binomial primary decomposition, that the base field is algebraically closed: even ideals generated by unital binomials usually require nontrivial roots of unity. Viewed another way, the arithmetic part of binomial primary decomposition has a combinatorial ramification: intersecting multiple primary ideals inducing the same primitive congruence results in a single mesoprimary ideal whose associated prime congruence has finite index in the primitive one (Proposition 15.7). In essence, primary congruences on Q are too coarse to reflect binomial primary decomposition in $\Bbbk[Q]$ accurately, and primitive congruences on Q are too fine, requiring additional arithmetic data from $\Bbbk$ to resolve otherwise indistinguishable associated primes in $\Bbbk[Q]$.

Thus the true monoid congruence analogue of primary decomposition in rings is a suitable compromise, developed (in Sections 2–8) as *mesoprimary decomposition for congruences* (Definition 8.1 and Theorem 8.3). The type of homogeneity mentioned before Example 1.4, discovered by Grillet [Gri75] (Remark 2.12.4), characterizes mesoprimary congruences (Corollary 6.6 and Remark 6.7). These are also distinguished (Theorem 6.1) as those with just one *associated prime congruence* (Definitions 2.11.4 and 5.2), a notion new to monoid theory.

The development of binomial mesoprimary decomposition in the latter half of the paper (Sections 9–16) mirrors the first half directly. Arithmetic existence statements build on combinatorial ones by exhibiting lifts of statements or requirements concerning equivalent elements under congruences to statements or requirements concerning binomials with nonzero coefficients. The combinatorics and arithmetic are so parallel that the coming structural outline works, on the whole, simultaneously for both.

It is worth warning the reader at this juncture of the inevitable clash of terminology in translating between combinatorics and arithmetic; see the table in Section 10, which in particular explains the source of our term *mesoprimary* to mean "between the two occurrences of 'primary'". To aid readers coming from commutative ring theory, the basic notions from semigroup theory are reviewed from scratch (Sections 2 and 3). For readers interested primarily in monoids, we complete the entire combinatorial theory in Section 8, before starting the arithmetic theory in Section 9.

Irreducible decomposition via coprincipal decomposition. The development of mesoprimary decomposition, in both the combinatorial and arithmetic settings, mimics the development of ordinary primary decomposition for ideals in noetherian rings. In the latter case, irreducible ideals serve as atoms by which existence is derived, and from which the rest of the theory unfolds readily. The analogous *coprincipal* mesoprimary congruences (Definition 7.1) and ideals (Definition 12.18) must be defined de novo, using intuition derived from characterizations of irreducibility in the context of monomial ideals in affine semigroup rings. This intuition supplants the inexpressibility-as-an-intersection condition that works so well for ideals in noetherian rings because irreducible binomial ideals induce congruences that are slightly too fine (Theorem 15.5; see the remarks following Example 1.4), and irreducible congruences on monoids are far too coarse (Example 2.22).

In the absence of true irreducibility, coprincipal objects derive their utility from combinatorial analogues of the simple socle condition [Vas98, Proposition 3.15] that characterizes irreducible ideals (see Lemma 15.4). It is not hard to construct coprincipal congruences and ideals with given socles (Definitions 7.7 and 12.18), once the ambient data of a congruence or an ideal has been fixed. The crucial task, in contrast, is to determine the socle elements for the relevant coprincipal objects, so that the intersection of the coprincipal objects equals the fixed congruence or ideal. These special socle elements are *witnesses* (Definitions 4.7, 12.1, and 16.3). In retrospect, hints toward the notion of witness, and toward the algebra of mesoprimary decomposition in general, appear already in the paper by Eisenbud and Sturmfels [ES96], particularly their unmixed decomposition for cellular ideals in characteristic zero [ES96, Corollary 8.2].

As in ordinary primary decomposition, witnesses have corresponding prime objects *associated* to them (Definitions 4.7, 5.2, and 12.1). Continuing the parallel, these notions of associatedness are defined by local combinatorial or algebraic conditions, but are equivalently characterized by consistent appearance of prime objects in every primary decomposition (Theorems 4.12 and 15.16). The local conditions defining witnesses incorporate the combinatorial quiddity of having prime annihilator in the ordinary setting context of ring theory. This particular analogy took a lot of tweaking, and generated a lot of subtly incorrect attempts—many spawning examples here.

The proof of concept for mesoprimary decomposition as a mode to connect the combinatorial and arithmetic settings lies in a fundamental discovery: there is a combinatorially defined set of witnesses that captures decompositions of both an ideal and its induced congruence (Corollary 8.11 and Theorem 13.5). To arrive at a decomposition that is as minimal as possible without disturbing symmetry, however, one must restrict to a subset of witnesses, the *key witnesses* for congruences (Definition 4.7) and the *character witnesses* for binomial ideals (Definition 16.3), and these subsets differ (Theorems 8.4 and 16.9). Section 16 serves as a caveat on this point, lest we be lulled into thinking the combinatorial and arithmetic theories to be completely parallel. Not only do key witnesses not suffice for binomial ideals (Example 16.6), but in fact some key witnesses are systematically redundant: a key witness can be a *false witness* rather than a character witness (Definition 16.3 and Example 16.5). These and other subtle distinctions between the combinatorial and arithmetic aspects of the theory demand care, as they necessitate occasional slight weakenings, or failures of the combinatorics to lift; see Remarks 12.20 and 12.21, for instance.

Coprincipal decomposition constitutes the true binomial generalization of irreducible decomposition for monomial ideals (Example 8.6), although nonminimality is forced, if canonicality is desired (Example 8.7 and Remark 13.8). For this reason, we envision binomial parallels to much of the extensive body of literature on monomial ideals, particularly where natural homological constructions are concerned: free and injective resolutions, local cohomology, and so on (see Section 17, where we detail this and other open problems). Our expectations are partly based on well behaved interactions of binomiality with localization.

Indeed, the transition from combinatorics of mesoprimary decomposition in Section 13 to arithmetic of irreducible and primary decomposition in Section 15 requires stronger localization techniques than monomial localization to tease apart primary components sharing the same associated monoid prime ideal. Binomial localization (Section 14) purposely falls just far enough shy of ordinary inhomogeneous localization at a prime ideal to prevent the loss of binomiality while retaining the usual advantages of localization, such as scraping away undesired associated primes. Binomial localization imposes the effect that ordinary localization at a binomial prime has on monomials in the quotient by a binomial ideal. More precisely, it identifies monomials that lie in the kernel of ordinary localization at a binomial prime (Theorem 14.9), and these are precisely the right monomials in the cellular case.

The development of coprincipal decomposition, together with binomial localization, culminates in the solution to a question left open by Eisenbud and Sturmfels [ES96, Problem 7.5]: they ask for a combinatorial characterization of irreducible binomial ideals, and for the construction of an irreducible decomposition. Both are provided in Section 15 (Theorem 15.5 and Corollary 15.11). We conceived of coprincipal ideals and decompositions as analogies to monomial irreducible ideals and decompositions [Mil02, Theorem 2.4] (see also [MS05, Corollary 11.5 and Proposition 11.41]), drawing particularly from the monoid ideal case, where the analogy is tight (Example 8.6). But once the connection between mesoprimary decomposition and ordinary primary decomposition is elucidated (Proposition 15.7), coprincipal decomposition becomes the door to binomial irreducible decomposition, the key being that for binomial ideals, irreducible is the combination of primary and coprincipal (Theorem 15.5). The overarching conclusion is that binomial primary and irreducible decomposition are naturally governed by combinatorics almost completely; arithmetic only enters at the end, in decomposing coprincipal or mesoprimary components.

Acknowledgements. The authors are very grateful to Howard M Thompson for his detailed reading of a previous draft; his comments led to substantial mathematical corrections and expositional improvements. TK was supported by an EPDI fellowship and gratefully acknowledges the hospitality of Institut Mittag-Leffler, where substantial parts of the research for this paper were carried out. EM had support from NSF grants DMS-0449102 = DMS-1014112 and DMS-1001437.

Conventions. Unless otherwise stated, Q denotes a finitely generated (equivalently, noetherian) commutative monoid, and $\Bbbk$ denotes an arbitrary field.

2. Taxonomy of congruences on monoids

Fix a *commutative semigroup* Q: a set with an associative, commutative binary operation (usually denoted by + here). Assume that Q has an identity, usually denoted by 0 here, so Q is a *monoid*. An *ideal* $T \subseteq Q$ is a subset such that $T + Q \subseteq T$, and T is *prime* if $t + s \in T$ implies $t \in T$ or $s \in T$. The ideal generated by elements $q_1, \ldots q_s$ is written $\langle q_1, \ldots, q_s\rangle$. A *congruence* $\sim$ on Q is an additively closed equivalence relation: $a \sim b \Rightarrow a + c \sim b + c$ for all $a, b, c \in Q$. The quotient $Q/\sim$ by any congruence is a monoid. The minimal relation satisfying this definition is equality itself, called the *identity congruence*. The congruence that identifies all pairs of elements in Q, and has trivial quotient, is the *universal congruence*.

Definition 2.1. A *module* over a commutative monoid Q is a non-empty set T with an *action* of Q, which means a map $Q \times T \to T$, written $(q, t) \mapsto q \cdot t$, that satisfies

- $0 \cdot t = t$ for all $t \in T$, and
- $(q + q') \cdot t = q \cdot (q' \cdot t)$,

the latter meaning that the action respects addition. A *congruence* on a module is an equivalence relation that is preserved by the action. A *module homomorphism* over a given monoid is a set map that respects the actions. For any element $q \in Q$, the *addition morphism* $\phi_q : Q \to \langle q \rangle$ is the module morphism defined by $p \mapsto p + q$. The *kernel* $\ker(\phi)$ of a module homomorphism $\phi : T_1 \to T_2$ is the congruence on T_1 under which $t \sim s \Leftrightarrow \phi(t) = \phi(s)$.

Remark 2.2. For general semigroups Grillet defines an *act* as a set with an action of a semigroup that satisfies only the second bullet in Definition 2.1, even if the semigroup was a monoid to start with [Gri07]. To every semigroup S a formal identity element e can be adjoined (even if S is already a monoid) to form the monoid $S \cup \{e\}$. Upon this operation an S-act turns into an $(S \cup \{e\})$-module as it automatically satisfies the first item in Definition 2.1.

Definition 2.3. A *subgroup* of a monoid is a subsemigroup that is a group.

Remark 2.4. The identity of a subsemigroup of a monoid need not equal the identity of the monoid.

Definition 2.5. *Green's preorder* on a monoid is the divisibility preorder $p \preceq q \Leftrightarrow \langle p \rangle \supseteq \langle q \rangle$. *Green's relation* on a monoid is $p \sim q \Leftrightarrow \langle p \rangle = \langle q \rangle$.

Lemma 2.6. *The quotient of a commutative monoid modulo Green's relation is partially ordered.*

Proof. [Gri01, Proposition I.4.1]. □

Remark 2.7. Green's relation measures the extent to which group-like behavior is found in a monoid. Idempotents and units are obstructions to partially ordering a monoid by divisibility. In particular, a monoid with trivial unit group is partially ordered if Green's relation is trivial. Note that our divisibility preorder is the opposite direction compared to Grillet's, to be compatible with divisibility of monomials.

Definition 2.8. An element ∞ in a monoid Q is *nil* if it is *absorbing*, meaning that $q + \infty = \infty$ for all $q \in Q$. An element $q \in Q$ is

- *nilpotent* if one of its multiples nq is nil for some nonnegative integer $n \in \mathbb{N}$.
- *cancellative* if addition by it is injective: $q + a = q + b \Rightarrow a = b$ in Q.
- *partly cancellative* if $q + a = q + b \neq \infty \Rightarrow a = b$ for all cancellative $a, b \in Q$.

A set of elements in a monoid is *torsion-free* if $na = nb \Rightarrow a = b$ for all $n \in \mathbb{N}$, whenever a and b lie in the given set. An *affine semigroup* is a monoid isomorphic to a finitely generated submonoid of a free abelian group. A *nilmonoid* is a monoid whose nonidentity elements are all nilpotent.

Remark 2.9. An absorbing element is often called a zero instead of a nil; but when we work with monoid algebras, we need to distinguish the nil monomial $\mathbf{t}^\infty$ from the zero element 0 of the algebra (see Section 9 for ramifications of this distinction), and we need to identify the identity monomial $\mathbf{t}^0$ with the unit element 1 of the algebra.

Remark 2.10. The condition $a + c = b + c'$ for cancellative c, c' means that a and b are off by a unit in the localization Q' of Q obtained by inverting all of its cancellative elements. We sometimes say that "a and b differ by a cancellative element," or that "the difference of a and b is cancellative." Note that the natural map $Q \to Q'$ is injective.

Definition 2.11. Fix a commutative monoid Q, a congruence $\sim$, and use a bar to denote passage to the quotient $\overline{Q} = Q/\sim$. The congruence $\sim$ is

1. *primary* if every element of $\overline{Q}$ is either nilpotent or cancellative.
2. *mesoprimary* if it is primary and every element of $\overline{Q}$ is partly cancellative.
3. *primitive* if it is mesoprimary and the cancellative subset of $\overline{Q}$ is torsion-free.
4. *prime* if every element of $\overline{Q}$ is either nil or cancellative.
5. *toric* if the non-nil elements of $\overline{Q}$ form an affine semigroup.

Remark 2.12. The notions just defined are nearly or exactly the same as concepts that have appeared in the literature on monoids.

1. Our definition of prime and primary congruences agrees with those in the literature [Gil84, §5]. In the case of prime congruences, where the non-nil elements of $\overline{Q}$ form a cancellative monoid, this is easy. In the case of primary congruences, for $q \in Q$ the condition Gilmer expresses as $q + a \sim q + b$ for all $a, b \in Q$ is equivalent to the class $\overline{q}$ being a nil in $\overline{Q} = Q/\sim$, so q lies in the nil class; and the condition that Gilmer expresses by saying that q lies in the radical of the nil class is equivalent to $\overline{q}$ being nilpotent in $\overline{Q}$.
2. Our definition of affine semigroup differs slightly from [Gri01, §II.7]: Grillet requires the unit group to be trivial, whereas we do not. Equivalently, our affine semigroups are the finitely generated, cancellative, torsion-free commutative monoids, while Grillet additionally requires affine semigroups to be reduced (trivial unit group).
3. A congruence on Q is primary if and only if $\overline{Q}$ is a *subelementary* monoid, by definition [Gri01, §VI.2.2].
4. A congruence on Q is mesoprimary if and only if the subelementary monoid $\overline{Q}'$, obtained from the monoid $\overline{Q}$ in the previous item by inverting its cancellative elements, is *homogeneous* [Gri01, §VI.5.3]; this is Corollary 6.6, below.

Lemma 2.13. *For monoid congruences,*

- *toric $\Rightarrow$ prime $\Rightarrow$ mesoprimary $\Rightarrow$ primary; and*
- *toric $\Rightarrow$ primitive $\Rightarrow$ mesoprimary $\Rightarrow$ primary.*

Proof. By Definition 2.11 and Remark 2.12, it suffices to prove that prime $\Rightarrow$ mesoprimary. Assume $\sim$ is a prime congruence and that $\overline{q} + \overline{a} = \overline{q} + \overline{b}$ in $\overline{Q}$ with neither side being nil. Then $\overline{q}$ is not nil, whence $\overline{a} = \overline{b}$ by cancellativity. □

Notationally, one of the simplest ways to present a congruence on a monoid is using a unital ideal in its monoid algebra.

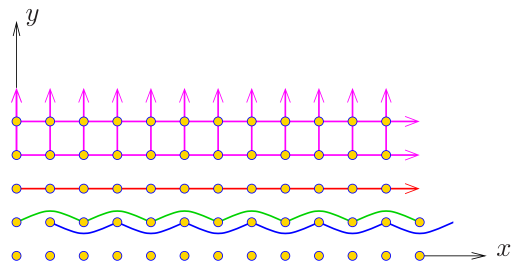
Definition 2.14. Fix a commutative ring $\Bbbk$. The *semigroup algebra* $\Bbbk[Q] = \bigoplus_{q \in Q} \Bbbk \cdot \mathbf{t}^q$ is the direct sum with multiplication $\mathbf{t}^p\mathbf{t}^q = \mathbf{t}^{p+q}$. Any congruence $\sim$ on Q induces a grading of $\Bbbk[Q]$ by $\overline{Q} = Q/\sim$ in which the *monomial* $\mathbf{t}^q$ has degree $\overline{q} \in \overline{Q}$ whenever $q \mapsto \overline{q}$ under the quotient map $Q \to \overline{Q}$. A *binomial ideal* $I \subseteq \Bbbk[Q]$ is an ideal generated by *binomials* $\mathbf{t}^p - \lambda\mathbf{t}^q$, where $\lambda \in \Bbbk$ is a scalar, possibly equal to $0 \in \Bbbk$. The ideal I *induces* the congruence $\sim_I$ in which $p \sim_I q$ whenever $\mathbf{t}^p - \lambda\mathbf{t}^q \in I$ for some unit $\lambda \in \Bbbk^*$.

Convention 2.15. In this paper, $\Bbbk$ is an arbitrary field unless otherwise stated.

Remark 2.16. Giving a congruence on Q is the same as giving a *unital ideal* in $\Bbbk[Q]$, generated by *unital* binomials $\mathbf{t}^p - \mathbf{t}^q$, with unit coefficients that are negatives of one another [Gil84, §7]. In particular, every congruence is induced by some binomial ideal. That said, other binomial ideals can induce the same congruence as the canonical unital ideal, by rescaling the variables or via Theorem 9.12, for instance.

Example 2.17 (Some congruences from unital ideals)**.**

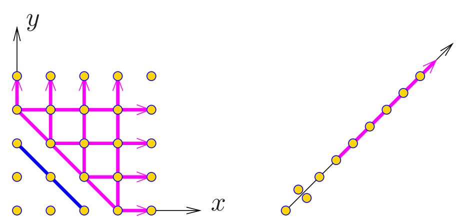
1. The prime ideal $\langle x - y \rangle \subset \Bbbk[x, y]$ induces a toric congruence such that $\overline{\mathbb{N}^2} \cong \mathbb{N}$.
2. The ideal $\langle x^2 - y^2 \rangle \subset \Bbbk[x, y]$ induces a prime congruence with $\overline{\mathbb{N}^2}$ isomorphic to the submonoid $Q \subseteq G = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ generated by $(1, 0)$ and $(1, 1)$. Although Q contains no torsion elements of G, the monoid is not torsion-free, so the congruence on $\mathbb{N}^2$ is not toric, since Q generates G as a group. The torsion in Q is exhibited by x and y, since $x^2 = y^2$ but $x \neq y$ in $\Bbbk[Q]$.
3. The ideal $\langle x^2 - x \rangle \subset \Bbbk[x]$ induces the same toric congruence on $\mathbb{N}$ as the prime ideal $\langle x \rangle$ does, but $\langle x^2 - x \rangle$ is not even a cellular binomial ideal (Definition 10.4).
4. The $\langle x, y \rangle$-primary ideal $\langle x^2, x - y \rangle$ induces the primitive congruence on $\mathbb{N}^2$ with $\overline{\mathbb{N}^2} \cong \{0, x, \infty\} =: Q$. The monoid algebra $\Bbbk[Q]$ has a presentation $\Bbbk[x, y]/J$ where $J = \langle x - y, x - x^2 \rangle = \langle x - 1, y - 1 \rangle \cap \langle x, y \rangle$ induces the same congruence.
5. The binomial ideal $\langle y - x^2y, y^2 - xy^2, y^3 \rangle$ induces a primary congruence whose classes are depicted as the connected components of the graph in the figure.



This congruence exhibits the distinction between primary and mesoprimary congruences: for a primary congruence, no injectivity is required of addition by a nilpotent element. In the picture, this means that translating two dots in different classes upward by one unit can force them into the same non-nil class. To make the congruence mesoprimary, homogenize the bottom three rows by replacing any two of them with the third; after that, upward translation on two dots keeps them in separate classes unless both land in the nil class. This replacement procedure also exhibits the distinction between mesoprimary and primitive congruences: it results in a primitive congruence only if the bottom row or the third row is preserved; preserving the second row yields torsion in the cancellative part of $\overline{Q}$.

The following example demonstrates the partly cancellative property.

Example 2.18. Partly cancellative elements can merge congruence classes that do not differ by cancellative elements. For instance, consider the congruence on $\mathbb{N}^2$ induced by $I = \langle x^2 - xy, xy - y^2, x^3, y^3\rangle \subseteq \Bbbk[x, y]$. In the following figure,



the congruence on $\mathbb{N}^2$ appears at left, and the quotient $\overline{\mathbb{N}}^2$ appears at right. The quotient is the monoid $\mathbb{N}$ with two copies of 1, modulo the Rees congruence of $\langle 3\rangle$ (declare all elements in $\langle 3\rangle$ congruent). The two copies of 1 become identified upon addition by either: $1 + 1 = 1 + 1' = 1' + 1' = 2$. Nonetheless, both 1 and $1'$ are partly cancellative.

The next result will be applied in the proofs of Theorems 8.4 and 10.6. The conclusion says that Q/F is a nilmonoid whose Green's preorder is an order. (i.e. is antisymmetric). Equivalently, it says that Q/F is *naturally partially ordered*, or a *holoid* [Gri01, §V.2.2].

Lemma 2.19. *Fix a monoid Q whose identity congruence is primary, so the non-nilpotent elements of Q constitute a cancellative submonoid $F \subseteq Q$. The quotient* *monoid Q/F defined by the congruence*

$$p \sim q \;\Leftrightarrow\; p + f = q + g \text{ for some } f, g \in F$$

is a nilmonoid partially ordered by divisibility. If Q is finitely generated, Q/F is finite.

Proof. This is more or less [Gri01, Proposition VI.3.3], but here's the proof anyway. Every nonidentity element of Q/F is nilpotent by definition, so when Q is finitely generated, Q/F is finite. The rest follows because every nilmonoid is partially ordered by divisibility; this is easy, and can be found in [Gri01, Proposition IV.3.1]. □

Remark 2.20. It is a crucial assumption for Lemma 2.19 that every element is cancellative or nilpotent, excluding idempotents. If every cancellative element is a unit, e.g. after localizing at the nilpotent ideal (see Section 4), then Q/F equals Q modulo Green's relation.

Concluding this section we comment on the notion of irreducibility for congruences which is, despite the close connection between binomial ideals and their congruences, quite different from irreducibility for ideals.

Definition 2.21. A congruence is *irreducible* if it cannot be expressed as the common refinement of two congruences neither of which equals the given one.

The theories of irreducible and primary decomposition for congruences in commutative monoids are not as nice as for (binomial) ideals in rings. The following example might come as a nasty surprise (it did to us). Quotients by irreducible congruences are characterized in [Gri01, Theorem VI.5.3].

Example 2.22. The identity congruence on $\mathbb{N}^2$ is reducible: it is the common refinement of the congruences induced by $\langle x-1\rangle$ and $\langle y-1\rangle$. Ring-theoretically, this is due to the fact that $\langle x-1\rangle \cap \langle y-1\rangle$ does not contain binomials.

Example 2.22 demonstrates the sad reality that prime congruences need not be irreducible. In a wider sense, unrestricted primary or irreducible decomposition of congruences fails to reflect the combinatorics of congruences accurately. The theory of mesoprimary decomposition, with its well founded notions of associatedness for prime ideals and prime congruences, is our remedy.

3. Primary decomposition and localization in monoids

We review the notion of primary decomposition for congruences on finitely generated commutative monoids, which traces back to Drbohlav [Drb63]. This decomposition is only a coarse approximation of mesoprimary decomposition, a central goal of this paper. In general, a *decomposition* of a congruence is an expression of it as a common refinement of congruences. The notion of common refinement used here is the standard one: formally, an equivalence relation on Q is a reflexive, symmetric, transitive subset of $Q \times Q$, and the *common refinement* of a family of equivalence relations is their intersection in $Q \times Q$.

Remark 3.1. Every congruence in this setting admits a *primary decomposition*: an expression as the common refinement of finitely many primary congruences [Gil84, Theorem 5.7]. Similarly to the case of rings, this follows from the existence of irreducible decomposition using a noetherian induction argument. Mesoprimary decomposition refines the notion of primary decomposition, in the sense that each primary component could require a nontrivial mesoprimary decomposition. Note that the mesoprimary components will therefore be coarser congruences than the primary components; that is, a finer decomposition typically consists of a greater number of coarser components.

Remark 3.2. The preimage under any monoid homomorphism of a prime ideal is prime. Since $\mathbb{N}^n$ has only finitely many prime ideals and a finitely generated commutative monoid Q has a presentation $\mathbb{N}^n \twoheadrightarrow Q$, it follows that Q has only finitely many prime ideals.

Convention 3.3. To avoid tedious case distinctions in the following, we consider the empty set as an ideal of any monoid. Declare the empty set to be a prime ideal of Q whenever Q has no nil. The empty set considered as a prime ideal will be denoted by $\varnothing \subset Q$; this symbol is never used for any other purpose in this paper.

Remark 3.4. Our definition of the empty prime ideal is motivated by the observation that localizing by adjoining inverses for elements outside of a prime ideal should never invert a nil element. It is also in analogy with associated primes in (say) affine semigroup rings, where the zero ideal is prime, the point being that the zero ideal in a ring-theoretic setting has as its monoid analogue the empty ideal. This analogy will become increasingly apparent and nuanced in later sections, when we translate mesoprimary decomposition from monoids to monoid algebras.

Another way to deal with the empty ideal issue would be to adjoin a new absorbing element to every monoid and work in the category of "zeroed monoid": pairs consisting of a monoid and an absorbing element. The new absorbing element is meant to echo the zero element in the corresponding monoid algebra, which is convenient when translating between monoids and rings. However, at the expense of having to abide by Convention 3.3, we chose to avoid the additional absorbing element because it obscures the role of nil elements in ordinary ("unzeroed") monoids, and because the first part of the paper works entirely in the monoid context, without substantial reference to rings.

Definition 3.5. The *nilpotent ideal* of a congruence $\sim$ on Q is the ideal of Q consisting of all elements with nilpotent image in $Q/{\sim}$. If P is the nilpotent ideal of a primary congruence $\sim$, then $\sim$ is *P-primary.*

Lemma 3.6. *If $\sim$ is a primary congruence, then the nilpotent ideal is prime. If $Q/{\sim}$ is cancellative, then $\sim$ is $\varnothing$-primary.* □

Lemma 3.7. *If $q_1, \ldots, q_n$ generate Q, then a primary congruence defines a partition of $[n]$ into generators with cancellative and nilpotent images, respectively. In this case the nilpotent ideal is generated by the generators q_i with nilpotent images.* □

Proposition 3.8. *The common refinement of finitely many P-primary congruences is P-primary.*

Proof. It suffices by induction to show this for two P-primary congruences $\sim_1$ and $\sim_2$. Reducing modulo their intersection, we can assume that the intersection is the identity congruence on Q. Denote by Q_1 and Q_2 the quotients modulo $\sim_1$ and $\sim_2$, respectively. By assumption $P \subset Q$ is the nilpotent ideal of both $\sim_1$ and $\sim_2$. We claim that if $p \in P$ then p is nilpotent already in Q. Indeed, a sufficiently high multiple of p is congruent to nil under both $\sim_1$ and $\sim_2$, and since their intersection is trivial this can only happen if that multiple is nil. On the other hand, if $p \notin P$, then it must be cancellative: if there exist $a, b \in Q$ with $a + p = b + p$, then $a \sim_1 b$ and $a \sim_2 b$ both hold—whence $a = b$, in fact—since p is cancellative modulo $\sim_1$ and $\sim_2$. □

Remark 3.9. Albeit in different language, [Gil84, Theorem 5.6.2] contains a variant of the statement of Proposition 3.8.

Passing from the theory surrounding P-primary congruences to that for general congruences is best accomplished by localizing.

Definition 3.10. The *localization* of Q at a prime ideal $P \subset Q$ is the monoid Q_P obtained by adjoining inverses for every element outside of P. The image of P in Q_P is denoted P_P. Any given congruence $\sim$ on Q induces a congruence on Q_P, also denoted $\sim$. If $\overline{Q} = Q/{\sim}$ then we write $\overline{Q}_P = Q_P/{\sim}$. The group of *units at* P is the subgroup $G_P = Q_P \smallsetminus P_P$.

Example 3.11. If Q has no nil, then localizing Q at the empty prime yields the universal group $Q_\varnothing$. When Q has a nil, we still write $Q_\varnothing$ for the universal group of Q, but in this case $Q_\varnothing$ is trivial. In fact, the universal group $Q_\varnothing$ is trivial precisely when Q has a nil. (Proof: If $Q_\varnothing$ is trivial, then q becomes equal to 0 after inverting every element of Q. Thus there is an element $x_q \in Q$ such that $x_q + q = x_q$. As Q is generated by a finite set $S \subseteq Q$, the sum of the elements x_s for $s \in S$ exists, and it is nil in Q.)

With localization of monoids comes localization of their modules.

Definition 3.12. The *localization* T_P of a Q-module T at a prime ideal $P \subset Q$ is the Q_P-module of formal differences $t - q$ for $t \in T$ and $q \notin P$, with $t - q$ and $t' - q'$ identified whenever $w \cdot q' \cdot t = w \cdot q \cdot t'$ for some $w \in Q \smallsetminus P$.

By definition, the group of units of Q_P acts on itself and also on the set $\overline{Q}_P$ of equivalence classes modulo any congruence on Q_P. Here and in what follows, we often think of the quotient $\overline{Q}$ explicitly as a set of congruence classes in Q. Thus $\overline{Q}_P$ is a set of congruence classes in Q_P. We record this fact for future reference.

Lemma 3.13. *Let $P \subset Q$ be a prime ideal. Given any congruence on Q, the unit group of Q_P acts on the quotient $\overline{Q}_P$ modulo the induced congruence on Q_P.* □

4. Witnesses and associated prime ideals of congruences

Our aim in this section is to show that primary decompositions of congruences in finitely generated commutative monoids have well-defined associated prime ideals. These, and their witnesses, reflect the combinatorial features of a given congruence more accurately than does primary decomposition alone.

Definition 4.1. For any ideal $T \subseteq Q$, the *annihilator modulo* T is the common refinement $\operatorname{ann}(T) = \bigcap_{t \in T} \ker(\phi_t)$ of the kernels of the addition morphisms ϕ_t for $t \in T$.

Remark 4.2. If $q_1 + v = q_2$ then $\ker(\phi_{q_1})$ refines $\ker(\phi_{q_2})$. Therefore, in the definition of $\operatorname{ann}(T)$, it suffices to intersect only over generators of T. Equivalently, if T is generated by $t_1, \ldots, t_r$, then $\operatorname{ann}(T) = \ker(\phi_{t_1} \oplus \cdots \oplus \phi_{t_r} : Q \to T^{\oplus r})$.

Example 4.3. To explain the "annihilator" terminology, let Q be a monoid with nil ∞ and write $\Bbbk[Q]^- := \Bbbk[Q]/\langle \mathbf{t}^\infty \rangle$ as in Definition 9.3, below. If $T \subseteq Q$ is a monoid ideal, then $\operatorname{ann}(T)$ is the congruence induced by the binomials (and monomials) in the ideal $(0 : \Bbbk\{T\}) = \{f \in \Bbbk[Q] \mid f\, \Bbbk\{T\} = 0 \text{ in } \Bbbk[Q]^-\}$.

Definition 4.4. Fix a prime ideal $P \subset Q$ with $P_P \subset Q_P$ minimally generated by $p_1, \ldots, p_r$. The *P-covers* of $q \in Q$ are the elements $q + p_i \in Q_P$ for $i = 1, \ldots, r$. The *cover morphisms at* P are the morphisms $\phi_i : Q_P \to \langle p_i \rangle_P$ defined via $q \mapsto q + p_i$; if P is the maximal ideal, then the ϕ_i are called simply *the cover morphisms* of Q.

Remark 4.5. The set of P-cover morphisms depends on the choice of generators $p_1, \ldots, p_r$ and may be infinite if, for example, Q_P has a lot of units. However, modulo Green's relation on Q_P there is a unique finite minimal generating set of any ideal, and every minimal generating set for P_P maps bijectively to it.

Lemma 4.6. *For a fixed prime P, the set of kernels of P-cover morphisms is finite.*

Proof. Two cover morphisms ϕ_p and $\phi_{p'}$ for elements p, p' that are Green's equivalent in Q_P have the same kernel, because if $p \in \langle p' \rangle$ then there exists an element u such that $p = p' + u$, and thus the kernel of $\phi_{p'}$ refines the kernel of ϕ_p and vice versa. □

Definition 4.7. Let $\sim$ be a congruence on Q and $P \subset Q$ a prime ideal. Consider the localized quotient $\overline{Q}_P$. For each $q \in Q$ let $\overline{q}$ be its image in $\overline{Q}_P$. An element $q \in Q$ is a

1. *witness for* P if the class of $\overline{q}$ is non-singleton under the kernel of each cover morphism (i.e. the class $\overline{p} + \overline{q}$ is non-singleton for all $p \in P$);
2. *key witness for* P if the class of $\overline{q}$ is non-singleton under the intersection of the kernels of all cover morphisms, i.e. if the class of $\overline{q}$ is non-singleton under $\operatorname{ann}(\overline{P}_P)$.

The ideal P is an *associated prime ideal of* $\sim$ if the annihilator modulo $\overline{P}_P \subset \overline{Q}_P$ is not the identity. Equivalently, P is associated if either there exists a key witness for P in Q_P, or Q has no nil and $P = \varnothing$ (in which case Q_P is nontrivial; see Example 3.11).

Convention 4.8. A (key) witness is a (key) witness for some associated prime ideal P. When we speak of the set of (key) witnesses for a given congruence we mean the set of pairs (w, P) where $w \in Q$ is a (key) witness for a prime ideal $P \subset Q$. If the congruence $\sim$ is not clear from context, a (key) witness may be called a (key) $\sim$-witness.

In the set of (key) witnesses for a congruence, a single $w \in Q$ can occur multiple times for different P. For instance, this happens when $\varnothing$ is associated.

Example 4.9. When Q has no nil, the condition of being a (key) witness for $\varnothing$ is vacuous, as $\operatorname{ann}(\varnothing)$ is the universal congruence on $Q_\varnothing$. Thus the empty ideal is prime and associated to a congruence if and only if the universal group of the quotient modulo that congruence is nontrivial (see Example 3.11). Every $q \in Q$ is a (key) witness in this case but at the same time $Q_\varnothing$ has only one class under Green's relation.

The following series of examples demonstrates various features of associatedness of prime ideals and their witnesses.

Example 4.10. As usual it will be convenient to describe congruences on $\mathbb{N}^n$ by unital binomial ideals in polynomial rings. We use $e_x, e_y, \ldots$ to denote the generators of $\mathbb{N}^n$ corresponding to variables $x, y, \ldots$ in the polynomial ring $\Bbbk[\mathbb{N}^n]$, but we denote the addition morphisms by $\phi_x, \phi_y, \ldots$ instead of $\phi_{e_x}, \phi_{e_y}, \ldots$, for simplicity.

1. Let $\sim$ be the congruence on $\mathbb{N}^2$ induced by the binomial ideal $\langle x^2 - xy, xy - y^2\rangle \subset \Bbbk[x, y]$. The set of associated prime ideals consists of the empty ideal $\varnothing$ and the maximal ideal $P = \langle e_x, e_y\rangle$. Localization at the maximal ideal does nothing and there are only two cover morphisms, given by adding e_x and e_y, respectively. To establish that P is associated, note that e_x and e_y themselves are key witnesses for P and congruent under $\operatorname{ann}(P)$. Indeed, $\operatorname{ann}(P)$, the intersection of the two kernels, contains the pair (e_x, e_y) since $e_x + e_x \sim e_y + e_x$ and also $e_x + e_y \sim e_y + e_y$. The identity $0 \in \mathbb{N}^2$ is not a witness for P. Neither $\langle e_x\rangle$ nor $\langle e_y\rangle$ is associated since adjoining inverses to either turns the quotient $\mathbb{N}^2/{\sim}$ into a cancellative monoid. In this case all kernels of addition morphisms are trivial. Finally, localizing at the empty prime ideal amounts to considering the induced congruence on $\mathbb{Z}^2$, which is induced by the binomial ideal $\langle x - y\rangle \subset \Bbbk[x^\pm, y^\pm]$. Since the quotient is nontrivial, $\varnothing$ is associated too. Every element of $\mathbb{N}^2$ is a witness for $\varnothing$, but taken together they form only one Green's class in $\mathbb{Z}^2$.
2. Let $\sim$ be the congruence on $\mathbb{N}^3$ induced by $\langle x^2 - xy, y^2 - xy, x(z-1)\rangle \subset \Bbbk[x, y, z]$. The associated prime ideals are $\langle e_x, e_y\rangle$ and $\varnothing$. The argument for $\varnothing$ is the same as in item 1. The localization of $\sim$ at $\langle e_x, e_y\rangle$ is induced by the same ideal, considered in $\Bbbk[x, y, z^\pm]$. This says that e_z is cancellative; i.e. that the addition morphism $\phi_z : q \mapsto q + e_z$ is injective. The set of key witnesses is invariant under the ϕ_z-action. It consists of $e_y + ke_z$ for $k \in \mathbb{N}$. Indeed, any two elements in this set become equivalent when adding e_x or e_y because they differ by a multiple of e_z. No e_z-translate of e_x or 0 is a witness, though. Again, all witnesses are key.

3. Let $\sim$ be the congruence on $\mathbb{N}^4$ induced by $\langle x^2-xy, y^2-xy, x(z-1), y(w-1)\rangle \subset \Bbbk[x,y,z,w]$. The associated prime ideals are again $\varnothing$ and $P = \langle e_x, e_y\rangle$. The set of witnesses for P is determined as follows. The element $0 \in \mathbb{N}^4$ is a witness that is not key. The kernel congruences of ϕ_x and ϕ_y are generated by $\{(0,e_z),(e_x,e_y)\}$ and $\{(0,e_w),(e_x,e_y)\}$ in $\mathbb{N}^4 \times \mathbb{N}^4$, respectively. This shows the witness property and also, because their common refinement leaves it singleton similar to Example 2.22, that 0 is not key. In contrast, e_x and e_y are key witnesses because $\phi_x(e_x) = \phi_x(e_y)$ and likewise for ϕ_y. For future reference, a mesoprimary decomposition (Theorem 13.2) of the binomial ideal defining $\sim$ has components corresponding to all three witnesses, while a mesoprimary decomposition of the congruence $\sim$ itself needs components only for the two key witnesses (Theorem 8.4). Why the extra binomial component? The common refinement of the congruences induced by $\langle z-1, x^2, y\rangle$ and $\langle w-1, x, y^2\rangle$ leaves the class of 0 singleton, but the intersection of the ideals is not binomial.

This final example demonstrates how the monoid prime ideal P matters in the definition of a (key) witness for P, and how the same element can be a witness for different P.

Example 4.11. Fix the congruence $\sim$ induced by $\langle x(z-1), x(w-1), y(z-1), y^2\rangle \subset \Bbbk[x,y,z,w]$ on $\mathbb{N}^4$. The associated prime ideals of $\sim$ are $\langle e_x, e_y\rangle$ and $\langle e_y\rangle$. Consider the addition morphisms ϕ_x and ϕ_y. The key witnesses for $\langle e_y\rangle$ are $e_y + ke_x$ and all their translates in the e_z and e_w directions. No element in the ideal $\langle e_x\rangle$ can be a witness for a monoid prime containing e_x because ϕ_x acts injectively on that ideal. Indeed, the witnesses for $\langle e_x, e_y\rangle$ are $0 \in \mathbb{N}^4$ together with all its translates in the e_z direction, and e_y together with all its translates in the e_z and e_w directions.

We finish the section by relating associated prime ideals of congruences to their primary decompositions.

Theorem 4.12. *A prime $P \subset Q$ is associated to a congruence on Q if and only if every primary decomposition of that congruence has a P-primary component.*

The proof comes after Lemma 4.14, below.

Lemma 4.13. *If P is maximal among the occurring associated primes in a primary decomposition, then* $\mathrm{ann}(P)$ *refines all occurring P'-primary components with $P' \subsetneq P$.*

Proof. Let P be maximal among the occurring associated primes. Fix elements $a, b \in Q$ that are congruent modulo $\mathrm{ann}(P)$ and a P'-primary component $\approx$ with $P' \subsetneq P$. Choose $p \in P \smallsetminus P'$, so that $\overline{p} \in Q/{\approx}$ is cancellative. By definition, $a+p$ and $b+p$ are congruent under $\approx$ if and only if a and b are; thus $\mathrm{ann}(P)$ refines $\approx$. $\square$

Lemma 4.14. *For all primes $P \not\supseteq P'$, the congruence on Q_P induced by any P'-primary congruence on Q is universal on Q_P.*

Proof. Localization adjoins an inverse for a nilpotent element. $\square$

Proof of Theorem 4.12. Working modulo $\sim$ we can assume that the congruence to be decomposed is the identity congruence on Q. After localizing along P, the induced congruences on Q_P form a primary decomposition of the identity there, with all P'-primary components for $P' \not\subseteq P$ being universal and thus redundant by Lemma 4.14. That is to say, we can assume that P is the maximal monoid prime ideal of Q.

If a primary decomposition has no P-primary component, then by Lemma 4.13 $\mathrm{ann}(P)$ refines all primary components, and thus it refines their intersection. Thus $\mathrm{ann}(P)$ is trivial and P is not associated.

Conversely, if every decomposition has a P-primary component, then there exists an irredundant decomposition that has a P-primary component $\sim_P$. Write $\approx$ for the (not necessarily primary) common refinement of all other congruences in the decomposition. Thus $\sim_P \cap \approx$ is a nontrivial decomposition of the identity congruence. Choose $a \neq b \in Q$ with $a \approx b$ but $a \not\sim_P b$. Let $T = \{t \in Q \mid t + a \sim_P t + b\}$. Since P acts nilpotently on $Q/{\sim_P}$, the radical of T is P. Modulo Green's relation find a maximal element $\hat{t}$ not in the image of T. By definition, if $t \in Q$ maps to $\hat{t}$ then $t + a$ is a key witness for P. $\square$

Finally, we can conclude that primary decomposition of congruences is, despite the oddities in Example 2.22, combinatorially well behaved: the associated prime ideals of a congruence reflect which components are necessary in every primary decomposition.

5. Associated prime congruences

Each primary congruence on a finitely generated commutative monoid Q has a unique associated prime ideal. One of the most basic insights in this paper is that a single primary congruence can have several associated prime congruences. The first definition says how a congruence looks near a given $q \in Q$.

Definition 5.1. Fix a prime ideal $P \subseteq Q$, a congruence $\sim$ on Q, and an element $q \in Q$. The *P-prime congruence* of $\sim$ *at* q is the kernel of the morphism $Q \to \big(\langle \overline{q}\rangle / \langle \overline{q} + P\rangle\big)_P$ induced by the quotient $Q \to Q/{\sim} = \overline{Q}$, addition $\phi_{\overline{q}} : \overline{Q} \to \langle \overline{q}\rangle$, and localization at P.

Definition 5.2. A prime congruence $\approx$ on Q is *associated* to an arbitrary congruence $\sim$ if $\approx$ equals the P-prime congruence of $\sim$ at a key witness for P.

Remark 5.3. The definition implies that the associated prime P of $\approx$ is associated to $\sim$ too. If P is clear from the context, such as after $\approx$ is fixed, then we also speak of a key witness for P simply as a *key witness.*

Lemma 5.4. *If $p, q \in Q$ are equivalent under Green's relation, then their P-prime congruences agree for each P.*

Proof. The same argument as for Lemma 4.6 applies. $\square$

Example 5.5. In the situation of Example 4.11, the associated prime congruences are induced by the ideals $\langle x, y\rangle$, $\langle x, y, z-1\rangle$, and $\langle y, z-1, w-1\rangle$. The first two correspond to witnesses for $\langle e_x, e_y\rangle$, while the third corresponds to all of the witnesses for $\langle e_y\rangle$.

Lemma 5.6. *Every infinite subset of a partially ordered noetherian monoid contains an infinite ascending chain.*

Proof. Let Q be a noetherian partially ordered monoid with an infinite subset W all of whose increasing chains are finite. Write $W_{\min}$ for the (finite) set of minimal elements of W. Let $W_0 = W$. For $i \in \mathbb{N}$, having defined W_i let M_i be the set of maximal elements of W_i, and let W_{i+1} be $W_i \smallsetminus (M_i \smallsetminus W_{\min})$. As M_i is an antichain for each i, it is finite. Therefore W_i is infinite for all i, and hence $M_i \smallsetminus W_{\min}$ is nonempty for all i (that is, W_i has maximal elements that are not minimal) by the finiteness hypothesis on the chains in W. Now observe that $\langle M_0\rangle \subsetneq \langle M_0 \cup M_1\rangle \subsetneq \langle M_0 \cup M_1 \cup M_2\rangle \subsetneq \dots$ is an infinite strictly increasing chain of ideals, contradicting the noetherianity of Q. $\square$

The following and Lemma 2.19 are the central finiteness results, reflected in all of the following development, particularly Theorem 8.4.

Theorem 5.7. *Each congruence on a finitely generated commutative monoid Q has only finitely many Green's classes of witnesses. Consequently, each congruence on Q has only finitely many associated prime congruences.*

Proof. Fix a congruence on Q. As Q has finitely many prime ideals—each is generated by a subset of a generating set for Q—it suffices to bound the number of witnesses for a fixed prime ideal P. Denote by Q'_P the quotient of Q_P modulo its Green's relation, and likewise $\overline{Q}'_P$ for $\overline{Q}_P$. If some element of $\overline{Q}_P$ in the Green's class $\overline{q}' \in \overline{Q}'_P$ of $\overline{q} \in \overline{Q}_P$ is a witness, then $\overline{q}'$ consists of witnesses for the same associated congruence by Lemma 5.4. Therefore it suffices to consider witnesses in $\overline{Q}'_P$, and this monoid is partially ordered under the partial order $\leq$ of Lemma 2.19, although $\overline{Q}'_P$ is generally not finite. For each witness $\overline{q}' \in \overline{Q}'_P$ consider the congruence $\sim_{\overline{q}'} = \ker(\phi_{\overline{q}} \circ \pi)$, where $\pi : Q_P \to \overline{Q}_P$ is the quotient map and $\phi_{\overline{q}} : \overline{Q}_P \to \overline{Q}_P$ is the addition morphism; thus $a \sim_{\overline{q}'} b$ in Q_P if and only if $a + q$ and $b + q$ become congruent in $\overline{Q}_P$. By definition, if $\overline{q}'_1 \leq \overline{q}'_2$, then $\sim_{\overline{q}'_1}$ refines $\sim_{\overline{q}'_2}$. Since $\overline{Q}'_P$ is finitely generated, it cannot have an infinite antichain (this is equivalent to the noetherian property for $\overline{Q}'_P$). Finally, if the original congruence on Q had infinitely many associated prime congruences, then Lemma 5.6 would produce an infinite ascending chain of witnesses, giving an infinite ascending chain of congruences. Since Q is noetherian this is impossible. $\square$

Example 5.8. The congruence in Example 2.18 is primary with respect to the maximal ideal. The (key) witnesses are e_x, e_y, and also $2e_x, e_x + e_y$, and $2e_y$, since their class gets joined to nil under ϕ_x and ϕ_y. Although the witnesses look combinatorially different, the only associated prime congruence is the identity congruence on the monoid $\{0, \infty\}$. This is forced, as the identity is the only cancellative element in $\overline{Q}$.

If on Q the identity congruence is primary, then it is easy to see that the assignment of witnesses to their P-prime congruences is order preserving. It would be interesting to understand which posets of witnesses and associated prime congruences can occur (Problem 17.4).

6. Characterization of mesoprimary congruences

Our ultimate goal, for the purely monoid-theoretic side of the story, is Corollary 8.10, via Theorem 8.4: every congruence admits a mesoprimary decomposition satisfying strict combinatorial conditions. The first step is to characterize the mesoprimary condition in terms of associated prime congruences. In fact, Definition 2.11 was made with this proposition in mind.

Theorem 6.1. *A congruence is mesoprimary if and only if it has exactly one associated prime congruence.*

Proof. Fix a P-primary congruence $\sim$ on Q. If $\sim$ is mesoprimary and w is not nil, then the P-prime congruence of $\sim$ at w coincides with the P-prime congruence of $\sim$ at the identity because $\overline{w}$ is partly cancellative. The uniqueness of the associated prime congruence only uses the case where w is a key witness.

On the other hand, assume $\sim$ has a unique associated prime congruence. Replacing Q with $\overline{Q}$, we may as well assume $\sim$ is the identity congruence on Q. Suppose that a and b are distinct cancellative elements. Using the partial order from Lemma 2.19, choose an element $w \in Q$ such that $w + a \neq w + b$ and the image of w modulo the cancellative elements $F \subseteq Q$ is maximal with this property; this is possible by the finiteness of Q/F in Lemma 2.19. Now choose an element $w' \in Q$ whose image in Q/F is maximal among the non-nil elements above w. To prove the partly cancellative property for all elements of Q, it suffices to show that w and w' have the same image in Q/F, for it follows that every non-nil element $v \in Q$ satisfies $v + a \neq v + b$.

The choices of w and w' make them both key witnesses. Replacing w' with $w' + c$ for some cancellative element c if necessary, assume that $w' = w + q$ for some $q \in Q$. Uniqueness of the associated prime congruence, combined with the relation $\phi_{w'} = \phi_q \circ \phi_w$ among addition morphisms, implies $w' + a \neq w' + b$. Thus w' and w become equal in Q/F by maximality of w. $\square$

Quotients by mesoprimary congruences can be described fairly explicitly in terms related to the action in Lemma 3.13. Making this description into a precise alternative characterization of mesoprimary congruences requires some specialized notions involving monoid actions.

Definition 6.2. The action of a monoid F on an F-module T is *semifree* if

- $t \mapsto f \cdot t$ is an injection $T \hookrightarrow T$ for all $f \in F$, and
- $f \mapsto f \cdot t$ is an injection $F \hookrightarrow T$ for all $t \in T$.

Remark 6.3. The letter "F" stands for "face": in practice, the monoid F is often a face of an affine semigroup, and thinking of it that way is good for intuition.

Lemma 6.4. *An action of a cancellative monoid F on an F-module T is semifree if and only if the localization map $T \hookrightarrow T_\varnothing$ is injective and the universal group $F_\varnothing$ acts freely on $T_\varnothing$.*

Proof. The cancellative condition means that the natural map $F \hookrightarrow F_\varnothing$ is injective. Using this fact, the "if" direction is elementary, and omitted. In the other direction, the semifree case, the first injectivity condition guarantees that $t - f = t' - f' \Leftrightarrow f' \cdot t = f \cdot t'$. In particular, $t - 0 = t' - 0 \Leftrightarrow t = t'$, so the natural map $T \hookrightarrow T_\varnothing$ is injective. The second injectivity condition guarantees that the action of $F_\varnothing$ is free: $(f - f') \cdot (t - w) = t - w \Leftrightarrow f \cdot t - (f' + w) = t - w \Leftrightarrow (w + f) \cdot t = (f' + w) \cdot t$, and by the second injectivity condition this occurs if and only if $w + f = f' + w$, which is equivalent to $f = f'$ because F is cancellative. □

In contrast to group actions, monoid actions need not define equivalence relations, because the relation $t \sim f \cdot t$ can fail to be symmetric. The relation is already reflexive and transitive, however, precisely by the two axioms for monoid actions.

Definition 6.5. An *orbit* of a monoid action of F on T is an equivalence class under the symmetrization of the relation $\{(s, t) \mid f \cdot s = t \text{ for some } f \in F\} \subseteq T \times T$.

Combinatorially, from an F-module T, one can construct a directed graph with vertex set T and an edge from s to t if $t = f + s$ for some $f \in F$. Then an orbit is a connected component of the underlying undirected graph.

Corollary 6.6. *A congruence $\sim$ on a finitely generated commutative monoid Q is mesoprimary if and only if the set F of non-nilpotent elements in $\overline{Q} = Q/{\sim}$ is a cancellative monoid that acts semifreely on $\overline{Q} \smallsetminus \{\infty\}$ with finitely many orbits.*

Proof. Whether we assume the mesoprimary condition on $\sim$ or the condition on the non-nilpotent elements in $\overline{Q}$, we always deduce that $\sim$ is P-primary for some prime $P \subset Q$. The image of $Q \smallsetminus P$ in $\overline{Q}$ is the cancellative submonoid F by definition, which has finitely many orbits by Lemma 2.19. The only feature of the statement that distinguishes mesoprimary congruences from general primary ones is semifreeness, which we claim is equivalent to uniqueness of the associated prime congruence in Theorem 6.1. Indeed, F acts semifreely if and only if the P-prime congruences at all non-nil elements of $\overline{Q}$ coincide. That condition certainly implies that the P-prime congruences at all witnesses coincide, in which case $\sim$ is mesoprimary. On the other hand, if $\sim$ is mesoprimary, then the P-prime congruences at all key witnesses coincide. They all coincide with the P-prime congruence at the identity, or else there would be two key witnesses, one sharing its P-prime congruence with the identity (any element maximal modulo F among those with that P-prime congruence) and the other not. Since the image in Q/F of every non-nil element of Q lies between the identity and a key witness, the P-prime congruence of every non-nil element is forced to agree with the one shared by the identity and the key witnesses. □

Remark 6.7. As the proof of Corollary 6.6 shows, one interpretation of the structure theorem in the statement is that a P-primary congruence has the same P-prime congruence at every non-nil element as soon as it has the same P-prime congruence at every key witness, and that is what it means to be mesoprimary.

This principle underlies our next few results, especially the proof of Proposition 6.12 and the construction of coprincipal congruences in Definition 7.7. Some of these results are best phrased using the following notion, borrowed directly from ring theory.

Definition 6.8. The *socle* of a monoid Q is the set of non-nil elements $q \in Q$ such that $q + a = \infty$ for all nonunit elements $a \in Q$.

Example 6.9. The socle of the quotient $\overline{Q}$ of a monoid Q modulo a mesoprimary congruence $\sim$ consists of the witnesses for $\sim$, every one of which is automatically a key witness by Corollary 6.6.

Example 6.10. In contrast, primary congruences that are not mesoprimary can have key witnesses that lie outside of the socle. Such is the case for the congruence on $\mathbb{N}^2$ induced by the binomial ideal $\langle 1 - x^2, y(1-x), y^2\rangle \subset \Bbbk[x, y]$: the elements 0 and e_y in $\mathbb{N}^2$ are key witnesses for $\langle e_y\rangle$, but the socle consists entirely of the image of e_y in $\overline{\mathbb{N}}^2$.

Remark 6.11. If Q is a group, then the universal quantifier in Definition 6.8 is automatically satisfied, so the socle of Q is the entirety of Q.

Proposition 6.12. *If two congruences on Q are mesoprimary with the same associated prime congruence, then their common refinement is also mesoprimary with that associated prime congruence. Furthermore, every common refinement witness is a witness under one of the two original congruences, and these witnesses are all key.*

Proof. First we show why every witness for the common refinement is a witness for one of the two given congruences. Next we deduce that the common refinement is mesoprimary, at which point the proof is done, because every witness is key by Example 6.9.

Call the congruences $\sim_1$ and $\sim_2$, with quotients $Q_1 = Q/{\sim_1}$ and $Q_2 = Q/{\sim_2}$, and write q_i for the image in Q_i of any $q \in Q$. The common refinement is the kernel of the diagonal morphism $\delta : Q \to Q_1 \times Q_2$ of modules. Let P be the shared associated monoid prime of the given congruences. If, for some $p \in P$ and $q \in Q$, the sum $p_i + q_i$ fails to be nil in Q_i, then the class of $p + q$ in $\ker \delta$ is singleton because p_i is partly cancellative in Q_i. Therefore q can only be a witness for the common refinement if

- q_i fails to be nil for some fixed i, but also
- for all $p \in P$ both of the elements $p_1 + q_1$ and $p_2 + q_2$ are nil.

These two conditions imply that q is a witness for $\sim_i$. Now it remains only to note that the P-prime congruence of $\ker \delta$ at q coincides with the unique associated prime congruence shared by $\sim_1$ and $\sim_2$, whether or not q is a witness for the other congruence $\sim_{2-i}$, by the structure theorem in Corollary 6.6. $\square$

7. Coprincipal congruences

In commutative rings, irreducible decomposition underlies primary decomposition. Analogously, coprincipal decomposition underlies mesoprimary decomposition of commutative monoid congruences (but see the remarks and examples after Theorem 8.4).

Definition 7.1. A congruence $\sim$ on Q is *coprincipal* if it is P-mesoprimary for some monoid prime P and additionally the socle of $\overline{Q}_P$ modulo its Green's relation has size 1.

In other words, on top of being mesoprimary, the nil class of a coprincipal congruence is required to be an irreducible monoid ideal.

Remark 7.2. In Definition 7.1, owing to Corollary 6.6, the quotient of $\overline{Q}_P$ modulo its Green's relation is simply the quotient of $\overline{Q}$ modulo its cancellative submonoid.

Definition 7.3. Fix a congruence on Q with quotient $\overline{Q}$. The *order ideal* $Q^P_{\preceq q}$ *cogenerated by* $q \in Q$ *at a prime ideal* $P \subset Q$ consists of those $a \in Q$ whose image precedes that of q in the partially ordered quotient of $\overline{Q}_P$ modulo its Green's relation (Lemma 2.6).

Example 7.4. Let $\sim$ be the congruence on $\mathbb{N}$ induced by the binomial ideal $\langle x^3 - x^6\rangle \subset \Bbbk[x]$. Set $P = \langle e\rangle$, where $e = e_x$ is the generator of $\mathbb{N}$. The quotient monoid $\mathbb{N}/\!\sim$ has a non-trivial *kernel* (see Definition 9.6) comprising a group of order 3 (with identity $3e$). The order ideal $Q^P_{\preceq e}$ consists of e itself and $0 \in \mathbb{N}$. The order ideals $Q^P_{\preceq q}$ of $q = m \cdot e$ for $m \geq 3$ are identical and consist of all of $\mathbb{N}$. Thus order ideals $Q^P_{\preceq q} \subseteq Q$ need not be finite, although their images in $\overline{Q}_P$ modulo Green's relation always are. Finally, the order ideals $Q^{\varnothing}_{\preceq q}$ are identical and equal to $\mathbb{N}$ for all $q \in \mathbb{N}$.

Example 7.5. Let $\sim$ be the identity congruence on $Q = \mathbb{N}^3$, and set $P = \langle e, f\rangle$, where $e = e_x$ and $f = e_y$ are two of the three generators of $\mathbb{N}^3$, the third being $g = e_z$. The order ideal $Q^P_{\preceq e+f+2g}$ consists of the translates of the (lattice points on the) nonnegative z-axis by 0, e, f, and $e + f$. The answer would have been the same if $e + f + 2g$ had been replaced by $e + f$, or $e + f + g$, or $e + f + mg$ for any $m \in \mathbb{N}$.

Lemma 7.6. *Fix $q \in Q$, a prime ideal $P \subset Q$, and a congruence $\sim$ on Q with quotient $\overline{Q}$. The equivalence relation $\sim^P_q$ on Q that sets all elements outside of $Q^P_{\preceq q}$ equivalent to one another, and sets $a \sim^P_q b$ if $\overline{u} + \overline{a} = \overline{u} + \overline{b} = \overline{q} \in \overline{Q}_P$ for some $u \in Q_P$, is a coprincipal congruence. If $Q \smallsetminus Q^P_{\preceq q}$ is nonempty then it is the nil class of $Q/\!\sim^P_q$.*

Proof. Immediate upon unraveling the definitions, or use Corollary 6.6. □

Definition 7.7. The coprincipal congruence $\sim^P_q$ from Lemma 7.6 is *cogenerated by q along P*. If q is a witness for an associated P-prime congruence of $\sim$, then $\sim^P_q$ is the *coprincipal component* of $\sim$ *cogenerated by q along P*. If the prime ideal P is clear from context, e.g. if q has already been specified to be a witness for the prime ideal P, then we simply speak of the coprincipal component cogenerated by q.

Example 7.8. In the setting of Example 7.4, the coprincipal component of $\sim$ cogenerated by $3e$ along $\varnothing$ is induced by the binomial ideal $\langle 1 - x^3\rangle$. The component cogenerated by the key witness $2e_x$ along $\langle e\rangle$ is induced by the binomial ideal $\langle x^3\rangle$.

Proposition 7.9. *Given any witness w for an associated P-prime congruence of $\sim$, the coprincipal component of $\sim$ cogenerated by w along P is refined by $\sim$.*

Proof. Starting from $\sim$ the coprincipal component is formed by identifying additional pairs of elements. $\square$

Example 7.10. In the setting of Example 2.18, the coprincipal component cogenerated by $q = (1, 1)$ along $P = \langle e_x, e_y\rangle$ starts with the given congruence on $\mathbb{N}^2$ and then joins together the two standard basis vectors, so that in the quotient $\mathbb{N}^2/{\sim_q^P}$ the two copies 1 and $1'$ are joined. This is the congruence induced by the binomial ideal $\langle x - y, x^3\rangle$.

8. Mesoprimary decompositions of congruences

Definition 8.1. Fix a congruence $\sim$ on a finitely generated commutative monoid Q.

1. An expression of $\sim$ as the common refinement of finitely many mesoprimary congruences is a *mesoprimary decomposition* if, for each mesoprimary congruence $\approx$ that appears in the decomposition with associated prime ideal $P \subset Q$, the P-prime congruences of $\sim$ and $\approx$ at every $\approx$-witness coincide.
2. Each mesoprimary congruence that appears is a *mesoprimary component* of $\sim$.
3. If every $\approx$-witness for every mesoprimary component $\approx$ is a key $\sim$-witness, then the decomposition is a *key* mesoprimary decomposition.

Example 8.2. According to Definition 8.1 the decomposition in Example 2.22 is not a mesoprimary decomposition because the intersectands are not components of the identity congruence: the combinatorics at the witnesses for the mesoprimary congruences in the decomposition do not agree with the combinatorics of the identity congruence. More precisely, the $\varnothing$-prime congruence at each element of $\mathbb{N}^2$ is the identity congruence, not the congruence induced by $\langle x - 1\rangle$ or $\langle y - 1\rangle$.

Theorem 8.3. *Every congruence on a finitely generated commutative monoid admits a key mesoprimary decomposition.*

Proof. Two examples are the decompositions in Theorem 8.4 and Corollary 8.10, by Remark 8.5 and finiteness of the set of Green's classes of witnesses in Theorem 5.7. $\square$

In the remainder of this section, Convention 4.8 leads to a welcome simplification of terminology. The first statement to benefit is our first main decomposition theorem (the other being Corollary 8.10), which generalizes to arbitrary monoid congruences the notion of irreducible decomposition for monoid ideals; see Examples 8.6 and 8.7.

Theorem 8.4. *Every congruence on a finitely generated commutative monoid is the common refinement of the coprincipal congruences cogenerated by its key witnesses.*

Proof. Fix a congruence $\sim$ on Q. Proposition 7.9 implies that the intersection of all of the coprincipal congruences for witnesses is refined by $\sim$. On the other hand, suppose that $q \not\sim q'$ for two elements $q, q' \in Q$. The proof is done once we find a prime $P \subset Q$ and a key witness $w \in Q$ whose coprincipal congruence $\sim_w^P$ on Q fails to join q to q'.

Let $T = \{t \in Q \mid t + q \sim t + q'\}$ be the ideal of elements joining q to q'. Fix a prime ideal P minimal among primes of Q containing T. The images $\hat{q}$ and $\hat{q}'$ of q and q' in the localization Q_P remain incongruent because P contains T. In contrast, every element in the localized image T_P joins $\hat{q}$ to $\hat{q}'$; that is, $\hat{t}+\hat{q} \sim \hat{t}+\hat{q}'$ for all $\hat{t} \in T_P$. Since the maximal ideal P_P of Q_P is minimal over T_P, by minimality of P over T, there is a maximal Green's class among the elements $\{\hat{t} \in Q_P \mid \hat{t}+\hat{q} \not\sim \hat{t}+\hat{q}'\}$. Any element $w = t+q \in Q$ with t mapping to such a Green's class is a key witness by definition, and the localization of the congruence $\sim_w^P$ satisfies $\hat{q} \not\sim_w^P \hat{q}'$, so $q \not\sim_w^P q'$ before localization. $\square$

Remark 8.5. In Theorem 8.4 it makes no difference whether one uses all the key witnesses or just one per Green's class. This follows instantly from the definition of a coprincipal component; indeed, for a given Green's class of key witnesses, the coprincipal components are all equal—not just equivalent, but literally the same congruence.

Example 8.6. For monomial ideals in finitely generated free commutative monoids, or more generally in affine semigroup rings, the decomposition of the Rees congruence of any monoid ideal afforded by Theorem 8.4 is the unique irredundant irreducible decomposition, as deduced from irreducible decompositions of monomial ideals in the corresponding monoid algebras [Mil02, Theorem 2.4]; see also [MS05, Corollary 11.5 and Proposition 11.41].

Example 8.7. Unlike the case in Example 8.6, the decomposition in Theorem 8.4 can be redundant in general. This happens for the congruence in Example 2.18. The decomposition produced by Theorem 8.4 has four mesoprimary components: $\sim_q^P$ for $P = \langle e_x, e_y \rangle$ and $q \in \{(0,0),(1,0),(0,1),(1,1)\}$. The one cogenerated by $(1,1)$ was described in Example 7.10. The decomposition into four congruences is redundant: the given congruence is already the common refinement of $\sim_{(1,0)}$ and $\sim_{(1,1)}$, the point being that once $\sim_{(1,1)}$ is given, one only needs to separate $(1,0)$ from $(0,1)$. That said, the points $(1,0)$ and $(0,1)$ represent distinct Green's classes of key witnesses for the associated prime congruence induced by the binomial ideal $\langle x, y \rangle$. There is simply no way of constructing an irredundant coprincipal decomposition without breaking the symmetry: any systematic method of eliminating one of the redundant components in this example would have no way to choose between them.

Remark 8.8. Coprincipal congruences are generally not irreducible: for the same reasons as in Example 2.22 they can often be decomposed nontrivially as intersections of coarser congruences.

Remark 8.9. Any irreducible congruence is mesoprimary: if a congruence is not mesoprimary then it has at least two associated primes by Theorem 6.1, and then it is reducible by mesoprimary decomposition. However, irreducible decompositions of congruences do not, in general, reflect the combinatorics of congruences in a manner that is witnessed combinatorially by the congruence itself.

Combining Theorem 8.4 with Proposition 6.12 and Example 6.9 yields the following, the culmination of our study of commutative monoid congruence decompositions.

Corollary 8.10. *Every congruence on a finitely generated commutative monoid admits a key mesoprimary decomposition with one component per associated prime congruence.*

For comparison with Theorem 13.5, we record the weakening of Theorem 8.4 that uses all of the witnesses, not just the key witnesses. The statement also includes an alternate description of what it means to be a decomposition of a congruence.

Corollary 8.11. *Every congruence on a finitely generated commutative monoid is the common refinement of the coprincipal congruences cogenerated by its witnesses. Equivalently, the morphism*

$$Q/{\sim} \;\hookrightarrow\; \prod_{(w,P)\in W} Q/{\sim_w^P}$$

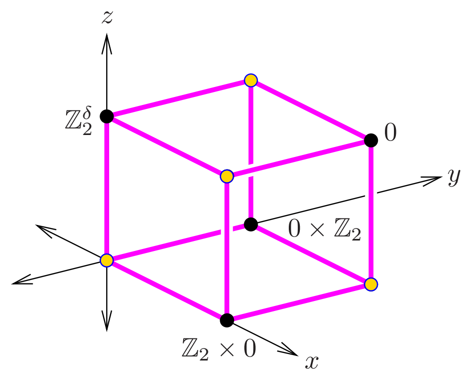
is injective, where $W = \{(w,P) \mid w \text{ is a witness for } P\}$ is a system of witnesses, one for each Green's class of $\sim$-witnesses.

Proof. Each of the coprincipal congruences in question is refined by the given congruence by Proposition 7.9, so their common refinement is, too. But already the common refinement of the coprincipal congruences cogenerated by the key witnesses is the given congruence by Theorem 8.4. $\square$

Example 8.12. In general the set of key witnesses is properly contained in the set of witnesses. Example 4.10.3 shows one way how this can happen. Exploiting the weirdness of irreducible decomposition of the identity congruence is not necessary: consider the primary congruence induced by the (cellular) binomial ideal

$$I = \langle a^2 - 1, b^2 - 1, x(b-1), y(a-1), z(a-b), x^2, y^2, z^2 \rangle.$$

The geometry of the quotient is shown here, where $\mathbb{Z}_2^\delta$ is the diagonal copy of $\mathbb{Z}_2$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$, i.e. generated by $(1,1)$:



The solid dots indicate key witnesses and are labeled with the quotients of $\overline{Q}$ modulo the corresponding stabilizers, under the action from Lemma 3.13. The origin is not a key witness because the common refinement of the three kernels of addition morphisms is trivial. According to Theorem 8.4, a coprincipal mesoprimary decomposition of $\sim_I$ is induced by the following decomposition of I into unital binomial ideals:

$$\begin{aligned} I = {} & \langle a-1, b-1, z^2, y^2, x^2\rangle \cap \langle a^2-1, b-1, z, y, x^2\rangle \\ & \cap \langle a-1, b^2-1, z, x, y^2\rangle \cap \langle ab-1, a-b, y, x, z^2\rangle. \end{aligned}$$

The heart of the remainder of this paper—the ring-theoretic part—is to make the corresponding decomposition of arbitrary (non-unital) binomial ideals precise. For reference, the primary decomposition of I is

$$\begin{aligned} I = {} & \langle a-1, b-1, z^2, y^2, x^2\rangle \cap \langle a+1, b-1, z, y, x^2\rangle \\ & \cap \langle a-1, b+1, z, x, y^2\rangle \cap \langle a+1, b+1, y, x, z^2\rangle. \end{aligned}$$

9. Augmentation ideals, kernels, and nils

One of our goals is to compare the combinatorics of congruences on a commutative monoid Q in purely monoid-theoretic settings with their ring-theoretic counterparts. It is therefore important to note that various binomial ideals $I \subset \Bbbk[Q]$ can induce the same congruence on Q. One way for this to happen is an arithmetic way, via binomials involving the same monomials but different sets of coefficients; this occurs for binomial primes $I_{\rho,P}$ whose characters share their domain of definition (see Section 12).

Example 9.1. In the polynomial ring $\Bbbk[x, y, z]$ in three variables, both of the ideals $I = \langle x(z-1), y(z-1), z^2-1, x^2, xy, y^2\rangle$ and $I' = \langle x(z-1), y(z+1), z^2-1, x^2, y^2\rangle$ induce the same congruence; note that I' contains $\langle xy\rangle$, so the only difference between these two ideals is the character on $\mathbb{Z} = \{0\} \times \{0\} \times \mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ induced by the monomials $y, zy, z^2y, \ldots$ due to the generator $y(z+1)$ instead of $y(z-1)$.

Another way, demonstrated in parts 3 and 4 of Example 2.17, is combinatorial: when Q has a nil ∞, the binomial ideal $\langle \mathbf{t}^\infty \rangle$ induces the same (trivial) congruence on Q as the zero ideal $\langle 0 \rangle \subseteq \Bbbk[Q]$. Nils are the only way for this to occur.

Lemma 9.2. *Fix a binomial ideal $I \subseteq \Bbbk[Q]$ whose congruence $\sim_I$ is trivial (every class is a singleton). Then $I = 0$ or $I = \langle \mathbf{t}^\infty \rangle$ for a nil $\infty \in Q$.*

Proof. If $I \neq 0$ then I must be a monomial ideal with a unique monomial, or else the congruence $\sim_I$ has a class of size at least 2. Hence the result follows because a monoid can have at most one nil. □

Definition 9.3. If $\infty \in Q$ is a nil, then the *truncated algebra* is $\Bbbk[Q]^- := \Bbbk[Q]/\langle \mathbf{t}^\infty \rangle$. By convention, if Q has no nil, then we set $\Bbbk[Q]^- := \Bbbk[Q]$.

Remark 9.4. Truncated algebras arise naturally from monoid algebras because of differences in the way quotients of monoids and monoid algebras by ideals are formed. To wit, any ideal $F \subseteq Q$ determines the *Rees congruence* $\sim_F$ in which the only non-singleton class consists of the elements in F. The morphism from Q to the *Rees factor semigroup* $Q/{\sim_F}$ takes F to a nil element ∞. On the other hand, the quotient $\Bbbk[Q] \to \Bbbk[Q]/M_F$ modulo the monomial ideal $M_F = \langle \mathbf{t}^f \mid f \in F \rangle$ equals $\Bbbk[Q/{\sim_F}]^-$ rather than $\Bbbk[Q/{\sim_F}]$ itself. We shall see that if Q has a nil, then $\Bbbk[Q]$ and $\Bbbk[Q]^-$ reflect certain aspects of the algebra of Q to varying degrees of accuracy.

More generally, if the congruence induced by a (not necessarily unital) binomial ideal I results in a quotient $Q/{\sim_I}$ that has a nil, then throwing in monomials from the nil class results in an ideal that determines the same congruence.

Proposition 9.5. *Fix a binomial ideal $I \subseteq \Bbbk[Q]$. The only binomial ideals containing I that determine the same congruence $\sim_I$ are I itself and, if $\overline{Q} = Q/{\sim_I}$ has a nil ∞, the ideal $I + \langle \mathbf{t}^q \mid \overline{q} = \infty \rangle$, where the bar denotes passage from $q \in Q$ to its image $\overline{q} \in \overline{Q}$.*

Proof. Under the grading of the quotient algebra $\Bbbk[Q]/I$ by $\overline{Q} = Q/{\sim_I}$ the dimension of the graded piece $(\Bbbk[Q]/I)_{\overline{q}}$ as a vector space over $\Bbbk$ is either 0 or 1, depending on whether I contains a monomial in the corresponding class. Since the (exponents on) monomials in I form a single class, the dimension can only be 0 for at most one $\overline{q}$, and $\overline{q}$ must be a nil in $\overline{Q}$. Now note that $\Bbbk[Q]/I$ is close enough to the monoid algebra $\Bbbk[\overline{Q}]$ for the argument from Lemma 9.2 to work, and lift the result from $\Bbbk[Q]/I$ to $\Bbbk[Q]$. □

The two binomial ideals in Proposition 9.5 are unequal precisely when I contains no monomials, and in this case it is trivial to form the second ideal by inserting monomials. In special circumstances, it is possible to reverse this procedure. To this end, we wish to examine the transition from $\Bbbk[Q]$ to the truncated algebra $\Bbbk[Q]^-$ (when Q has a nil) in terms of primary decomposition of binomial ideals. This naturally leads to the following familiar concept refining that of a nil.

Definition 9.6. A *kernel* of a commutative monoid Q is a nonempty ideal contained in all nonempty ideals of Q. (Such an ideal might not exist.)

Example 9.7. A nil is the same thing as a kernel of cardinality 1.

The existence of a nil in Q, or a finite kernel more generally, is reflected by a certain kind of maximal ideal of $\Bbbk[Q]$ being an associated prime of $\Bbbk[Q]$.

Definition 9.8. Fix a commutative monoid Q, and write $\Bbbk^* = \Bbbk \smallsetminus \{0\}$. The *unital augmentation ideal* in the monoid algebra $\Bbbk[Q]$ is the ideal

$$I^1_{\mathrm{aug}} := \langle \mathbf{t}^q - 1 \mid q \in Q\rangle$$

generated by all monomial differences. More generally, an *augmentation ideal* for a given binomial ideal $I \subseteq \Bbbk[Q]$ is a proper ideal of the form

$$I_{\mathrm{aug}} := \langle \mathbf{t}^q - \lambda_q \mid q \in Q, \lambda_q \in \Bbbk^*\rangle \subseteq \Bbbk[Q],$$

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

Example 9.9. The ideal $I = \langle x^2\rangle \subset \Bbbk[x, y]$ induces a primary congruence (a Rees congruence) identifying all monomials in I. A compatible augmentation ideal is $I_{\mathrm{aug}} = \langle x - 1, y - 1\rangle$, which satisfies $I \cap I_{\mathrm{aug}} = \langle x^2 - x^3, yx^2 - x^2\rangle$. This intersection induces the same congruence $\sim$ as I does. Note that $\Bbbk[x, y]/(I \cap I_{\mathrm{aug}}) \cong \Bbbk[\mathbb{N}^2/{\sim}]$ is isomorphic to the semigroup algebra of $\mathbb{N}^2/{\sim}$ while $\Bbbk[\mathbb{N}^2]/I \cong \Bbbk[\mathbb{N}^2/{\sim}]^-$ is the truncated algebra.

Lemma 9.10. *Given an augmentation ideal I_{aug} as in Definition 9.8, the association $q \mapsto \lambda_q$ constitutes a monoid homomorphism $\phi : Q \to \Bbbk^*$.*

Proof. The maximal ideals of $\Bbbk[Q]$ with residue field $\Bbbk$ are in bijection with the monoid homomorphisms $Q \to \Bbbk$; Definition 9.8 guarantees that the image lies in $\Bbbk^*$. □

Proposition 9.11. *Fix a monoid algebra $\Bbbk[Q]$ over a field $\Bbbk$ with Q finitely generated. An augmentation ideal is associated to $\Bbbk[Q]$ if and only if Q has a finite kernel, and in that case the unital augmentation ideal is associated to $\Bbbk[Q]$.*

Proof. If Q has a finite kernel K, then I^1_{aug} is the annihilator of the sum $f = \sum_{k\in K} \mathbf{t}^k$. Indeed, $q + K \subseteq K$ is an ideal of $Q \Rightarrow q + K = K$ for all $q \in Q \Rightarrow \mathbf{t}^q f = f$ for all $q \in Q \Rightarrow (\mathbf{t}^q - 1)f = 0$ for all $q \in Q \Rightarrow I^1_{\mathrm{aug}} \subseteq \mathrm{ann}(f)$; but I^1_{aug} is a maximal ideal.

Now suppose that an augmentation ideal I_{aug} is associated to $\Bbbk[Q]$. The homomorphism $q \mapsto \lambda_q$ in Lemma 9.10 induces an automorphism of $\Bbbk[Q]$ that rescales the monomials by $\mathbf{t}^q \mapsto \lambda_q\mathbf{t}^q$. This automorphism takes I_{aug} to I^1_{aug}. Therefore, we may as well assume $I_{\mathrm{aug}} = I^1_{\mathrm{aug}}$ is the unital augmentation ideal. Let $K \subseteq Q$ be a nonempty subset such that $f = \sum_{k\in K} \mu_k\mathbf{t}^k$ is annihilated by I^1_{aug}, where $\mu_k \in \Bbbk^*$ for all $k \in K$. It suffices to show that K is a kernel of Q. But $\mathbf{t}^q f = f$ for all $q \in Q$ implies that $q + K = K$ for all $q \in Q$, which implies both that K is an ideal of Q (since $q + K \subseteq K$ for all q) and also that K is contained in every ideal of Q (since $K + q \supseteq K$ for any given q). □

Theorem 9.12. *If $I_\ell \supset \cdots \supset I_0$ is a chain of distinct binomial ideals in $\Bbbk[Q]$ inducing the same congruence on Q, then $\ell \leq 1$. Moreover, if $\ell = 1$ then I_1 contains monomials and I_0 does not: $I_0 = I_1 \cap I_{\mathrm{aug}}$ for an augmentation ideal I_{aug} compatible with I_1.*

Proof. The first sentence follows from Proposition 9.5, as does the statement about monomials when $\ell = 1$. It remains to show that $I_0 = I_1 \cap I_{\mathrm{aug}}$ if $\ell = 1$. Set $I = I_0$. Under the grading of the quotient algebra $\Bbbk[Q]/I$ by $\overline{Q} = Q/\sim_I$ the dimension of the graded piece $(\Bbbk[Q]/I)_{\overline{q}}$ as a vector space over $\Bbbk$ is 1 for all $\overline{q} \in \overline{Q}$. Let $\overline{\infty} \in \overline{Q}$ be the nil, which exists because it is the class of all exponents on monomials in I_1. Fix a nonzero element $\mathbf{t}^{\overline{\infty}} \in \Bbbk[Q]/I$ of degree $\overline{\infty}$. Then $\mathbf{t}^q\mathbf{t}^{\overline{\infty}} = \lambda_q \mathbf{t}^{\overline{\infty}}$ for each $q \in Q$. Set $I_{\mathrm{aug}} = \langle \mathbf{t}^q - \lambda_q \mid q \in Q\rangle$. Then $I_{\mathrm{aug}} \supseteq I$ by construction, but $I_{\mathrm{aug}} \not\supseteq I_1$, since I_1 contains monomials and I_{aug} does not. Therefore $I_1 \supsetneq I_1 \cap I_{\mathrm{aug}} \supseteq I$, whence $I_1 \cap I_{\mathrm{aug}} = I$, because $I_1/I = \langle \mathbf{t}^{\overline{\infty}}\rangle \subseteq \Bbbk[Q]/I$ has dimension 1 as a vector space over $\Bbbk$ by Proposition 9.5. □

Example 9.13. The ideal $I = \langle x^2 - xy, xy - 2y^2\rangle \subseteq \Bbbk[x, y]$ contains monomials even when $\mathrm{char}(\Bbbk) \neq 2$, because I contains both of $x^2y - xy^2$ and $x^2y - 2xy^2$, so x^2y and xy^2 lie in I. However, Theorem 9.12 implies that there is no augmentation ideal compatible with I. Indeed, every binomial ideal I' contained in I and inducing the same congruence necessarily contains a binomial of the form $x^2 - \lambda xy$ and one of the form $xy - \mu y^2$, so I' contains both $x^2 - xy$ and $xy - 2y^2$ (and therefore $I' = I$) since $xy \notin I$.

10. Taxonomy of binomial ideals in monoid algebras

The concepts of primary, mesoprimary, primitive, prime, and toric congruence from Definition 2.11 have precise analogues for binomial ideals in monoid algebras. As a small measure to aid the reader with conflicting usages of the terms “primary” and “prime”, long since immovably set in the literature, the items in the following definition are listed in the order corresponding exactly to Definition 2.11, as Theorem 10.6 makes precise; for quick reference, consult the following table.

. . . congruence on Q	. . . binomial ideal in $\Bbbk[Q]$
primary	cellular
mesoprimary	mesoprimary
primitive	primary
prime	mesoprime
toric	prime

The table explains our choice of terminology: “mesoprimary” sits between the two occurrences of “primary”, being stronger than one and weaker than the other.

Our choice work over fields that need not be algebraically closed forced us to consider slight generalizations of group algebras.

Definition 10.1. A *twisted group algebra* over a field $\Bbbk$ is a $\Bbbk$-algebra that is graded by a group G and isomorphic over the algebraic closure $\overline{\Bbbk}$ to the group algebra $\overline{\Bbbk}[G]$

via a G-graded isomorphism. A *monomial homomorphism* from a monoid algebra to a twisted group algebra takes each monomial to a homogeneous element (possibly 0).

Example 10.2. The ring $R = \mathbb{Q}[x]/\langle x^3 - 2\rangle$ is not isomorphic to the group algebra $\mathbb{Q}[G]$ for $G = \mathbb{Z}/3\mathbb{Z}$ over $\mathbb{Q}$, because no element of R is a cube root of 2. On the other hand, the element $y = x\sqrt[3]{2} \in R_{\mathbb{C}} := R \otimes_{\mathbb{Q}} \mathbb{C}$ generates $R_{\mathbb{C}}$, yielding the presentation $R_{\mathbb{C}} = \mathbb{C}[y]/\langle y^3 - 1\rangle \cong \mathbb{C}[G]$. Therefore R is a nontrivial twisted group algebra for the group $G = \mathbb{Z}/3\mathbb{Z}$ over the rational numbers $\mathbb{Q}$.

Generalizing the manipulations in Example 10.2 yields the following.

Proposition 10.3. *A twisted group algebra R over $\Bbbk$ (for a finitely generated group G) is the same thing as a quotient of a Laurent polynomial ring over $\Bbbk$ by a binomial ideal.*

Proof. Every G-graded piece of R has dimension $\dim_{\Bbbk}(R_g) = 1$ for all $g \in G$, because this is true after tensoring with $\overline{\Bbbk}$ by definition. Thus R admits a binomial presentation $R \cong \Bbbk[\mathbb{N}^n]/I$ [ES96, Proposition 1.11]. Every monomial $\mathbf{x}^u \in \Bbbk[\mathbb{N}^n]$ becomes invertible in R because every such monomial becomes invertible in $R_{\overline{\Bbbk}} := R \otimes_{\Bbbk} \overline{\Bbbk}$. Therefore $R \cong \Bbbk[\mathbb{Z}^n]/I$ is a binomial quotient of a Laurent polynomial ring. On the other hand, the characterization of Laurent binomial ideals I [ES96, Theorem 2.1] (or see Lemma 11.11, below) implies that there is a unique sublattice $L \subseteq \mathbb{Z}^n$ and character $\sigma : L \to \Bbbk$ such that $I = \langle \mathbf{x}^q - \sigma(q) \mid q \in L\rangle$. Over $\Bbbk$, not much more can be said, in general; but over $\overline{\Bbbk}$, the fact that $\overline{\Bbbk}^*$ is an injective abelian group implies that σ extends to a character $\rho : \mathbb{Z}^n \to \overline{\Bbbk}^*$. If y_i is the image in $R_{\overline{\Bbbk}}$ of $\rho(x_i)x_i \in \overline{\Bbbk}[\mathbb{Z}^n]$, then naturally $R_{\overline{\Bbbk}} = \overline{\Bbbk}[y_1, \ldots, y_n] = \overline{\Bbbk}[G]$ for $G = \mathbb{Z}^n/L$. □

Definition 10.4. A binomial ideal $I \subset \Bbbk[Q]$ in the monoid algebra for a monoid Q is

1. *cellular* if every monomial $\mathbf{t}^q \in \Bbbk[Q]/I$ is either a nonzerodivisor or nilpotent.
2. *mesoprimary* if it is maximal among the proper binomial ideals inducing a given mesoprimary congruence (as per Theorem 9.12).
3. *primary* if the quotient $\Bbbk[Q]/I$ has precisely one associated prime ideal.
4. *mesoprime* if I is the kernel of a monomial homomorphism from $\Bbbk[Q]$ to a twisted group algebra over $\Bbbk$.
5. *prime* if $\Bbbk[Q]/I$ is an integral domain: $fg = 0$ in $\Bbbk[Q]$ implies $f = 0$ or $g = 0$.

Remark 10.5. The maximality for a mesoprimary ideal $I \subseteq \Bbbk[Q]$ amounts to stipulating that the nil class of $\sim_I$ consists of elements $q \in Q$ with $\mathbf{t}^q \in I$, the alternative being that none of these monomials lie in I but differences of scalar multiples thereof do.

Theorem 10.6. *Let $\alpha \in \{1, 2, 4\}$. A binomial ideal I satisfies part α of Definition 10.4 if and only if its induced congruence satisfies part α of Definition 2.11 and I is maximal among proper ideals inducing that congruence. For $\alpha = 5$ the same holds if $\Bbbk$ is algebraically closed. When $\alpha = 3$ the implication Definition 2.11.3 $\Rightarrow$ Definition 10.4.3 holds in general, and the converse holds if $\Bbbk$ is algebraically closed of characteristic 0.*

Proof. Fix a binomial ideal I and use notation as in Definition 2.11 for $\sim\, = \,\sim_I$. First we assume that I satisfies Definition 10.4.α and show that I satisfies Definition 2.11.α.

1. If a monomial $\mathbf{t}^q \in \Bbbk[Q]/I$ is a nonzerodivisor or nilpotent then the image $\overline{q} \in \overline{Q}$ of q is cancellative or nilpotent, respectively.
2. By definition.
3. Pick a presentation $\mathbb{N}^n \twoheadrightarrow Q$. The kernel of the induced surjection $\Bbbk[\mathbb{N}^n] \twoheadrightarrow \Bbbk[Q]$ is a binomial ideal [Gil84, §7], so the preimage of I in $\Bbbk[\mathbb{N}^n]$ is a primary binomial ideal $I' \subseteq \Bbbk[\mathbb{N}^n]$ such that $\mathbb{N}^n/{\sim_{I'}} = \overline{Q}$. Replacing I by I' if necessary, we therefore may as well assume $Q = \mathbb{N}^n$, since the definitions of primitive congruence and primary ideal depend only on the quotients $\overline{\mathbb{N}}^n = \overline{Q}$ and $\Bbbk[\mathbb{N}^n]/I' = \Bbbk[Q]/I$.

   Each binomial prime in $\Bbbk[\mathbb{N}^n] = \Bbbk[x_1, \ldots, x_n]$ can be expressed as a sum $\mathfrak{p}_b + \mathfrak{m}_J \subseteq \Bbbk[\mathbb{N}^n]$ of its "binomial portion" $\mathfrak{p}_b$, which is a prime binomial ideal containing no monomials, and a monomial prime $\mathfrak{m}_J := \langle x_i \mid i \notin J\rangle$, which is generated by the variables whose indices are *not* contained in $J \subseteq \{1, \ldots, n\}$ [ES96, Corollary 2.6]; this deduction relies on the algebraically closed hypothesis. Rescaling the variables of $\Bbbk[\mathbb{N}^n]$ if necessary, we can assume that the unique associated prime $\mathfrak{p} = \mathfrak{p}_b + \mathfrak{m}_J$ of $\Bbbk[\mathbb{N}^n]/I$ is *unital*—that is, $\mathfrak{p}_b$ is a unital ideal. Given that $\Bbbk$ is algebraically closed of characteristic 0, the $\mathfrak{p}$-primary condition on I implies that it contains $\mathfrak{p}_b$ [ES96, Theorem 7.1′]. Therefore, replacing $\Bbbk[\mathbb{N}^n]$ by $\Bbbk[\mathbb{N}^n]/\mathfrak{p}_b$ and I by $I/\mathfrak{p}_b$, we assume that Q is an affine semigroup and $\mathfrak{p}$ is generated by monomials. The desired result now follows from [DMM09, Theorem 2.15 and Proposition 2.13] or [Mil11a, Theorem 2.23], the latter being an equivalent statement that directly implies the characterization of mesoprimary congruences in Corollary 6.6.
4. If $\overline{q}$ is not nil then $\mathbf{t}^q \in \Bbbk[Q]$ lies outside of I, so $\mathbf{t}^q$ maps to a nonzero monomial in the twisted group algebra, whence $\overline{q}$ is cancellative because G is cancellative.
5. When I is a monomial prime in an affine semigroup ring, the result is obvious. But prime $\Rightarrow$ primary, so the reduction to that case in part 3 applies. Moreover, since $I = \mathfrak{p}$ contains $\mathfrak{p}_b$ already, the characteristic 0 hypothesis is superfluous.

For this half of the theorem, it remains to explain, for $\alpha \neq 2$, why I is maximal among ideals inducing $\sim$. For that, it suffices by Theorem 9.12 to show that I contains a monomial if $\overline{Q}$ has a nil ∞. For part 1 (the cellular case), if $\overline{q} = \infty$, then by definition of nil there is for each $r \in \mathbb{N}$ a binomial $\mathbf{t}^q - \lambda_r \mathbf{t}^{rq} \in I$ for some $\lambda_r \in \Bbbk^*$, so $\mathbf{t}^q(1 - \lambda_r \mathbf{t}^{(r-1)q}) \in I$, whence $\mathbf{t}^q$ is a zerodivisor modulo I and thus nilpotent modulo I—say $\mathbf{t}^{rq} \in I$; then $\mathbf{t}^q - \lambda_r \mathbf{t}^{rq} \in I \Rightarrow \mathbf{t}^q \in I$. For part 3 (the primary case), Theorem 9.12 implies that I has at least two associated primes—one or more arising from an augmentation ideal—if maximality fails. For part 4 (the mesoprime case), any monomial $\mathbf{t}^q$ with $\overline{q} = \infty$ must lie in I because a group has no nil. For part 5 (the prime case), the maximality is a special case of part 1, because prime $\Rightarrow$ cellular for binomial ideals.

Next, assuming that I is maximal among the binomial ideals inducing a congruence $\sim$ on Q satisfying Definition 2.11.α, we prove that I satisfies Definition 10.4.α. As a matter of notation, write $\bar{\mathbf{t}}^q$ for the image of $\mathbf{t}^q$ in $\Bbbk[Q]/I$. In all cases, if $q \in Q$ is an element whose image $\bar{q} \in \overline{Q}$ is nil, then $\bar{\mathbf{t}}^q = 0$ by Theorem 9.12, using the maximality property of I. Consequently, if $q \in Q$ is nilpotent, then $\bar{\mathbf{t}}^q$ is nilpotent in $\Bbbk[Q]/I$.

1. By the previous paragraph, if $q \in Q$, then either the monomial $\bar{\mathbf{t}}^q$ is nilpotent or $\bar{q}$ is cancellative. In the latter case, multiplication by $\bar{\mathbf{t}}^q$ is injective on $\Bbbk[Q]/I$ because $\Bbbk[Q]/I$ is $\overline{Q}$-graded and addition by $\bar{q}$ is injective on $\overline{Q}$.
2. By definition.
3. The quotient $\overline{Q}$ satisfies the condition of Corollary 6.6 in which the cancellative monoid $F \subseteq \overline{Q}$ is an affine semigroup. Each orbit is a finite union of translates $\bar{q} + F$ because $\overline{Q}$ itself is generated by F and finitely many nilpotent elements. The proof now proceeds as [DMM09, Proposition 2.13] does: owing to the partial order on the set of orbits afforded by Lemma 2.19, the $\overline{Q}/F$-grading on $\Bbbk[Q]/I$ induces a filtration by $\Bbbk[Q]$-submodules with associated graded module
$$\mathrm{gr}(\Bbbk[Q]/I) \cong \bigoplus_{F\text{-orbits } T} \Bbbk\{T\},$$
where $\Bbbk\{T\}$ is the vector space over $\Bbbk$ with basis T. The isomorphism above is as $\Bbbk[F]$-modules, or equivalently, as $\Bbbk[Q]$-modules annihilated by the kernel $\mathfrak{p}_F$ of the surjection $\Bbbk[Q] \twoheadrightarrow \Bbbk[F]$, with the $\Bbbk[F]$-module structure on $\Bbbk\{T\}$ induced by the F-action on T. Since $\Bbbk\{T\}$ is torsion-free as a $\Bbbk[F]$-module, the direct sum over T has only one associated prime, namely $\mathfrak{p}_F$, whence $\Bbbk[Q]/I$ does, too.
4. Set $\overline{Q}' = \overline{Q} \smallsetminus \{\infty\}$ if $\overline{Q}$ has a nil, and $\overline{Q}' = \overline{Q}$ otherwise. By maximality of I, the quotient $\Bbbk[Q]/I$ is $\overline{Q}'$-graded. By part 1, every nonzero monomial $\bar{\mathbf{t}}^q \in \Bbbk[Q]/I$ is a nonzerodivisor. Therefore $\Bbbk[Q]/I$ injects into its localization R obtained by inverting the nonzero monomials. Any presentation $\mathbb{Z}^n \twoheadrightarrow G$ for the universal group G of Q results in a presentation $\Bbbk[\mathbb{Z}^n] \twoheadrightarrow \Bbbk[G] \twoheadrightarrow \Bbbk[G]/I = R$ whose kernel is a binomial ideal. Thus R is a twisted group algebra over $\Bbbk$ by Proposition 10.3.
5. The argument for part 4 works in this case, too, but now $\overline{Q}'$ is an affine semigroup, so that $\bar{\Bbbk} \otimes_{\Bbbk} R$, and hence also $\Bbbk[Q]/I$, is an integral domain. □

Corollary 10.7. *For binomial ideals in $\Bbbk[Q]$, over an arbitrary field except where noted,*

- *prime $\Rightarrow$ mesoprime $\Rightarrow$ mesoprimary $\Rightarrow$ cellular; and*
- *prime $\Rightarrow$ primary $\Rightarrow$ mesoprimary $\Rightarrow$ cellular (we only claim the second implication when $\Bbbk$ is algebraically closed of characteristic 0).*

Proof. Use Theorem 10.6: if I is maximal among binomial ideals inducing a congruence from Definition 2.11, then it is maximal among binomial ideals inducing any of the weaker congruences from Lemma 2.13. This proves every implication except for prime $\Rightarrow$ mesoprime, which a priori requires $\Bbbk$ to be algebraically closed, if Theorem 10.6 is being applied. But in fact the implication holds in general, even though the quotient by a prime binomial ideal I need not be an affine semigroup ring if $\Bbbk$ is not algebraically closed. This is a consequence of the stronger statement in Theorem 11.15, below. □

Remark 10.8. The given proof of the implication Definition 10.4.3 ⇒ Definition 2.11.3 fails in characteristic p, even if the field $\Bbbk$ is algebraically closed, because primary binomial ideals in characteristic p do not necessarily contain the binomial part of their associated prime [ES96, Theorem 7.1'].

Theorem 10.6 implies the following result, which reflects the table preceding Definition 10.4 homogeneously across all of its rows, and shows that all of the richness in Definition 10.4 is already exhibited by *unital ideals*: those generated by monomials and unital binomials.

Corollary 10.9. *A congruence satisfies part of Definition 2.11 if and only if the kernel of the surjection $\Bbbk[Q] \twoheadrightarrow \Bbbk[\overline{Q}]^{-}$ satisfies the corresponding part of Definition 10.4.* □

11. Monomial localization, characters, and mesoprimes

For arithmetic reasons, intersections of binomial ideals need not reflect their combinatorics completely accurately. The simplest example is $\langle x^2 - 1\rangle = \langle x - 1\rangle \cap \langle x + 1\rangle$, whose congruence fails to equal the common refinement of the congruences induced by $\langle x - 1\rangle$ and $\langle x + 1\rangle$. Precise statements about relations between combinatorics and arithmetic use characters on subgroups of the unit groups of localizations of Q.

Localizations of monoids at their prime ideals corresponds to inverting monomials in their monoid algebras.

Definition 11.1. For a prime ideal $P \subset Q$, the corresponding monomial ideal in $\Bbbk[Q]$ is $\mathfrak{m}_P = \langle \mathbf{t}^p \mid p \in P\rangle$.

Remark 11.2. When P is maximal, $\mathfrak{m}_P$ is the maximal proper Q-graded ideal in the monoid algebra $\Bbbk[Q]$, but it need not be maximal in the set of all proper ideals of $\Bbbk[Q]$.

Definition 11.3. The *monomial localization* $\Bbbk[Q]_P$ *of* $\Bbbk[Q]$ *along* P is the monoid algebra of the localization Q_P, arising by adjoining inverses to all monomials outside of $\mathfrak{m}_P$. The *monomial localization* of any $\Bbbk[Q]$-module M *along* P is $M_P = M \otimes_{\Bbbk[Q]} \Bbbk[Q]_P$.

Remark 11.4. Localization behaves well upon passing between algebra and combinatorics; it forms part of the justification for characterizing algebraic notions, such as Definition 12.1 in combinatorial terms.

Lemma 11.5. *If $I \subseteq \Bbbk[Q]$ is a binomial ideal inducing the congruence $\sim$ on Q with quotient $\overline{Q}$, then for any monoid prime $P \subset Q$, the quotient of Q_P modulo the congruence induced by I_P is the monoid localization $\overline{Q}_P$ from Definition 3.10.*

Proof. Immediate from the definitions. □

Definition 11.6. For any group L, a *character* is a homomorphism $\rho : L \to \Bbbk^*$. A character $\rho' : L' \to \Bbbk^*$ *extends* ρ if $L \subseteq L'$ is a subgroup and $\rho'(\ell) = \rho(\ell)$ for $\ell \in L$. The extension is *finite* if L'/L is finite.

Convention 11.7. The domain L is part of the data of a character $\rho : L \to \Bbbk^*$; that is, we simply speak of the character ρ, and write L_ρ if it is necessary to specify L.

Definition 11.8. Fix a subgroup $K \subseteq G_P$ of the *local unit group G_P at P*. For any character $\rho : K \to \Bbbk^*$, the *P-mesoprime of ρ* is the preimage $I_{\rho,P}$ in $\Bbbk[Q]$ of the ideal

$$(I_{\rho,P})_P := \langle \mathbf{t}^u - \rho(u-v)\mathbf{t}^v \mid u - v \in K\rangle + \mathfrak{m}_P \subseteq \Bbbk[Q]_P.$$

Viewing P as implicit in the definition of ρ, the symbol I_ρ refers to the preimage in $\Bbbk[Q]$ of the ideal $\langle \mathbf{t}^u - \rho(u-v)\mathbf{t}^v \mid u - v \in K\rangle \subseteq \Bbbk[Q]_P$.

Definition 11.9. A subgroup $L \subseteq G$ of an abelian group is *saturated* in G if there is no subgroup of G in which L is properly contained with finite index. The *saturation* $\mathrm{sat}(L)$ of L is the intersection of all saturated subgroups of G that contain L. For any prime number $p \in \mathbb{N}$, the largest subgroup of $\mathrm{sat}(L)$ whose quotient modulo L has order

- a power of p is $\mathrm{sat}_p(L)$.
- coprime to p is $\mathrm{sat}'_p(L)$.

For $p = 0$ set $\mathrm{sat}_p(L) = L$ and $\mathrm{sat}'_p(L) = \mathrm{sat}(L)$.

The following implies, in particular, that the set of saturations of a character is finite. The statement is actually a slight generalization of [ES96, Corollary 2.2], in that the domain L of ρ is allowed to be a subgroup of an arbitrary finitely generated abelian unit group G_P, and $I_{\rho,P}$ is not an arbitrary ideal in a finitely generated group algebra, but rather an ideal containing the maximal monomial ideal in an arbitrary finitely generated monoid algebra. However, the generalization follows from the original by working modulo the maximal monomial ideal and lifting to any presentation of G_P, taking note that all of the characters in question are trivial on the kernel of the presentation.

Proposition 11.10 ([ES96, Corollary 2.2])**.** *Fix an algebraically closed field $\Bbbk$ of characteristic $p \geq 0$. Let $\rho : L \to \Bbbk^*$ be a character on a subgroup $L \subseteq G_P$, and write g for the order of $\mathrm{sat}'_p(L)/L$. There are g distinct characters $\rho_1, \ldots, \rho_g$ on $\mathrm{sat}'_p(L)$ that extend ρ. For each ρ_j there is a unique character ρ'_j on $\mathrm{sat}(L)$ extending ρ_j. There is a unique character ρ' that extends ρ and is defined on $\mathrm{sat}_p(L)$. Moreover,*

1. $\sqrt{I_{\rho,P}} = I_{\rho',P}$,
2. $\mathrm{Ass}(S/I_{\rho,P}) = \{I_{\rho'_j,P} \mid j = 1, \ldots, g\}$, *and*
3. $I_{\rho,P} = \bigcap_{j=1}^g I_{\rho_j,P}$.

The following lemma is a variant of [DMM10, Lemma 2.9] and [ES96, Theorem 2.1].

Lemma 11.11. *If $\Bbbk[\Phi]$ is the group algebra of a finitely generated abelian group Φ, then for any proper binomial ideal $I \subset \Bbbk[\Phi]$ there is a subgroup $L \subseteq \Phi$ and a character $\rho : L \to \Bbbk^*$ such that $I = I_\rho$.*

Proof. The binomial ideal is of the form $\langle 1 - \lambda_u \mathbf{t}^u \mid u \in \mathcal{U}\rangle$ for some finite $\mathcal{U} \subseteq \Phi$. First off, $\mathcal{U}$ is a subgroup of Φ since $1 - \lambda\mu\mathbf{t}^{u+v} = \mu\mathbf{t}^v(1 - \lambda\mathbf{t}^u) + (1 - \mu\mathbf{t}^v)$ for all $\lambda, \mu \in \Bbbk$, including $\lambda = \lambda_u$ and $\mu = \lambda_v$. The set $\mathcal{U}$ is closed under inverses because $(1 - \lambda\mathbf{t}^u)/\lambda\mathbf{t}^u = -(1 - \mathbf{t}^{-u}/\lambda)$ when $\lambda \neq 0$, and $I \neq \Bbbk[\Phi] \Rightarrow \lambda_u \neq 0$. The very same arguments show that the map $\rho : \mathcal{U} \to \Bbbk^*$ defined by $u \mapsto \lambda_u$ is a homomorphism. □

Definition 11.12. Fix a binomial ideal $I \subseteq \Bbbk[Q]$. The *stabilizer* of an element $q \in Q$ along a prime ideal $P \subset Q$ is the subgroup $K_q^P \subseteq G_P$ (sometimes denoted by K_q if P is clear from context) fixing the class of $q \in Q_P$ under the action from Lemma 3.13 for the congruence $\sim_I$. The *character (of I_P) at q* is the homomorphism $\rho = \rho_q^P : K_q^P \to \Bbbk^*$ such that $(I_{\rho,P})_P = (I_P : \mathbf{t}^q) + \mathfrak{m}_P$. The ideal $I_q^P := I_{\rho,P}$ is the *P-mesoprime of I at q*.

Remark 11.13. The ideal $(I_P : \mathbf{t}^q) + \mathfrak{m}_P$ can equivalently be described as the kernel of the composite map $\Bbbk[Q]_P \xrightarrow{\cdot\mathbf{t}^q} \langle\mathbf{t}^q\rangle_P \to \langle\mathbf{t}^q\rangle_P/\mathbf{t}^q(I + \mathfrak{m}_P)$. This kernel is a binomial ideal in $\Bbbk[Q]_P$ containing $\mathfrak{m}_P$ by construction. Lemma 11.11 with $\Bbbk[\Phi] = \Bbbk[G_P] = \Bbbk[Q]_P/\mathfrak{m}_P$ implies the kernel has the form $(I_{\rho,P})_P$ for some character ρ, so I_q^P is a mesoprime.

Saturations of subgroups (Definition 11.9) are more or less combinatorial in nature. Saturations of characters, on the other hand, are more subtle, because arithmetic properties of the target field $\Bbbk$ can enter.

Definition 11.14. Fix a subgroup L of an abelian group G. A character $\rho : L \to \Bbbk^*$ is

- *saturated* if the subgroup L is saturated, and
- *arithmetically saturated* if ρ has no finite proper extensions.

A *saturation* of ρ is an extension of ρ to $\mathrm{sat}(L)$.

The importance of saturated characters has been demonstrated in Proposition 11.10, which required the algebraically closed hypothesis. Without it, the arithmetically saturated condition holds sway, and the primality-saturation equivalence can break.

Theorem 11.15. *If a binomial ideal in $\Bbbk[Q]$ over an arbitrary field $\Bbbk$ is prime then it is a mesoprime $I_{\rho,P}$ for an arithmetically saturated character ρ. The converse holds if $\Bbbk$ is algebraically closed, and it can fail if not.*

Proof. Suppose that $\Bbbk[Q]/I$ is a domain. The ideal of monoid elements $p \in Q$ such that $\mathbf{t}^p \in I$ is a monoid prime P. Replacing Q with the monoid $Q \smallsetminus P$ and I with its image in $\Bbbk[Q \smallsetminus P] = \Bbbk[Q]/\langle\mathbf{t}^p \mid p \in P\rangle$, it suffices to prove that $I = I_\rho$ for an arithmetically saturated character when Q is cancellative and I contains no monomials. Since $\Bbbk[Q]$ injects into its localization $\Bbbk[Q]_\varnothing = \Bbbk[\Phi]$ for the universal group $\Phi = Q_\varnothing$, and I contains no monomials, Lemma 11.11 implies the existence of a subgroup $L \subseteq \Phi$ and a character $\rho : L \to \Bbbk^*$ such that $I = I_\rho$. It remains to show that I_ρ is not prime if ρ is not arithmetically saturated. Suppose $\sigma : K \to \Bbbk^*$ properly extends ρ to a subgroup $K \subseteq \mathrm{sat}(L)$. Then $I_\sigma \supsetneq I_\rho$. By restricting σ to a subgroup of K that still properly contains L, we can assume that $|K/L| > 1$ and one of the following occurs:

- $\Bbbk$ has positive characteristic p and $|K/L|$ is a power of p;
- $\Bbbk$ has positive characteristic p and $|K/L|$ is relatively prime to p; or
- $\Bbbk$ has characteristic 0.

Proposition 11.10 implies that in the first case, the extension $\overline{I}_\sigma$ of I_σ to $\overline{\Bbbk}$ has the same radical as the extension $\overline{I}_\rho$, in which case I_ρ itself is not a radical ideal. In the remaining two cases, Proposition 11.10 implies that $\overline{I}_\rho = \overline{I}_\sigma \cap \overline{J}$, with no associated prime of either intersectand containing an associated prime of the other. It follows that $I_\rho = I_\sigma \cap J$, where I_σ and $J := (I_\rho \mid I_\sigma)$ both properly contain I_ρ, so I_ρ is not prime.

The $\Bbbk = \overline{\Bbbk}$ converse is implicit in Proposition 11.10, and anyway follows easily from [ES96, Theorem 2.1]. Example 11.16 demonstrates failure of the general converse. □

Example 11.16. The ideal $I_\rho \subset \mathbb{Q}[x]$ for the character $\rho : 4\mathbb{Z} \to \mathbb{Q}^*$ defined by $\rho(1) = -4$ is $\langle x^4 + 4\rangle$. This ideal is not prime because it factors as $\langle x^4 - 4\rangle = \langle x^2 - 2x + 2\rangle \cap \langle x^2 + 2x + 2\rangle$. Nonetheless, ρ is arithmetically saturated because $x^4 + 4$ has no binomial factors of degree 2.

Example 11.17. The ideal $\langle x^3 - 2\rangle$ in Example 10.2 is prime (by Eisenstein's criterion, for example). Therefore the character $\rho : 3\mathbb{Z} \to \mathbb{Q}^*$ sending $3 \mapsto 2$ is arithmetically saturated, viewing $3\mathbb{Z}$ as a subgroup of $\mathbb{Z}$: any proper extension of ρ to a character $\mathbb{Z} \to \mathbb{Q}^*$ would require a cube root of 2.

12. Coprincipal and mesoprimary components of binomial ideals

Definition 12.1. Fix a binomial ideal $I \subseteq \Bbbk[Q]$ inducing a congruence $\sim$ on Q.

1. An element $w \in Q$ is an *I-witness* if it is a $\sim$-witness.
2. The monomial $\mathbf{t}^w$ is a *monomial I-witness* if w is an I-witness.
3. A mesoprime $I_{\rho,P}$ is an *associated mesoprime* if it is the P-mesoprime of I at some I-witness w for P (Definition 11.12), and then w is an *I-witness for $I_{\rho,P}$*.
4. An associated mesoprime is *minimal* if it is inclusion-minimal among the associated mesoprimes, and *embedded* otherwise.

Example 12.2. If $I = \langle y - x^2y, y^2 - xy^2, y^3\rangle$ is the binomial ideal from Example 2.17.5, then $I_{\rho,P} = \langle x^2 - \lambda, y\rangle$ for $P = \langle e_y\rangle$, $\rho : \langle(2,0)\rangle \to \Bbbk^*$ defined by $\rho(2,0) = \lambda$ induces the associated prime congruence of $\sim_I$ for any $\lambda \in \Bbbk^*$. The monomial $x^a y \in \Bbbk[x,y]$ is a witness for any $a \in \mathbb{N}$, and it lies in one of two possible witness classes, depending on the parity of a; see the figure in Example 2.17. However, only $\lambda = 1$ gives the associated mesoprime.

Example 12.3. All associated mesoprimes of a unital binomial ideal (generated by differences of monomials with unit coefficients) are unital.

Remark 12.4. If $Q = \mathbb{N}^n$ and I is unital, then all information about associated mesoprimes is contained in the set of *associated lattices* $L \subset \mathbb{Z}^J$, each of which comes with an *associated subset* $J \subseteq \{1, \ldots, n\}$. Indeed, a prime ideal P of $\mathbb{N}^n$ is the complement of a face $\mathbb{N}^J$ of $\mathbb{N}^n$, and specifying a prime congruence on $\mathbb{N}^n$ amounts to choosing such a face along with a lattice $L \subset \mathbb{Z}^J$. To see why, first observe that localization along P inverts the face, turning $\mathbb{N}^n$ into $\mathbb{Z}^J \times \mathbb{N}^{\bar{J}} = G_P \times \mathbb{N}^{\bar{J}}$. Subsequently passing to the quotient by a given prime congruence, the complement of the face maps to nil, and the subgroup L is the stabilizer of any class under the action of $\mathbb{Z}^J = G_P$ on the quotient. The notion of associated lattice was a precursor of what we now call an associated prime congruence. We were led to it in part by [ES96, Theorem 8.1]. Although that theorem only covers the cellular case, the upshot is that a collection of associated lattice ideals contributes associated primes. The J-notation for subsets was central to [DMM09], but we dispensed with it upon consideration of prime ideals and congruences in arbitrary finitely generated commutative monoids.

Remark 12.5. When the domain K of a character $\rho : K \to \Bbbk^*$ is a saturated subgroup of G_P, the ideal $I_{\rho,P}$ can be an associated prime of a binomial ideal I without being an associated mesoprime of I. The reason is that the congruences induced by associated P-mesoprimes are immediately visible in the congruence induced by I_P, whereas the associated primes of I usually induce coarser congruences (larger congruence classes) than those visible. The quintessential example to consider is the lattice ideal I for an unsaturated sublattice of $\mathbb{Z}^n$: the lattice ideal for the saturation is an associated prime of I, but the unique associated mesoprime of I is I itself.

Proposition 12.6. *A binomial ideal $I \subseteq \Bbbk[Q]$ is mesoprimary if and only if I has exactly one associated mesoprime.*

Proof. If I is mesoprimary then it is cellular by Corollary 10.7 and the congruence $\sim_I$ is mesoprimary by Definition 10.4. If q is any witness for the unique associated prime congruence and $I' = (I : \mathbf{t}^q)$ is the annihilator of the image of $\mathbf{t}^q$ in $\Bbbk[Q]/I$, then multiplication by $\mathbf{t}^q$ induces an isomorphism $I_P + \mathfrak{m}_P \to I'_P + \mathfrak{m}_P$, so every associated mesoprime of I is equal to $I + \mathfrak{m}_P$.

On the other hand, assume that I has only one associated mesoprime, and that its associate monoid prime is $P \subset Q$. The congruence $\sim$ induced by I is mesoprimary because the P-prime congruences agree at all I-witnesses, and hence all key $\sim$-witnesses, by Definition 12.1 and Theorem 6.1. Now, either I contains a monomial, in which case it is maximal among ideals inducing its congruence by Theorem 9.12, or else I contains no monomials, in which case the unique associated monoid prime ideal is $P = \varnothing$, so that no proper ideal containing any monomials can induce the same congruence. □

Remark 12.7. Building on Remark 6.7, Proposition 12.6 says that the character of I_P is the same at every nonzero monomial as soon as it is the same at every witness monomial, and that is what it means to be a mesoprimary ideal.

Definition 12.8. Fix a binomial ideal $I \subseteq \Bbbk[Q]$. The *P-socle modulo I* is the set $(I_P : \mathfrak{m}_P)/I$ of nonzero elements annihilated by $\mathfrak{m}_P$ in the localization $\Bbbk[Q]_P/I_P$

along P. A monomial $\mathbf{t}^q \in \Bbbk[Q]$ *lies in the P-socle modulo I* if its localized image in $\Bbbk[Q]_P/I_P$ does; that is, if $(I_P : \mathbf{t}^q) = \mathfrak{m}_P$.

Remark 12.9. The P-socle need not be generated by monomials (Example 12.10). The concept of socle in the monoid setting (Definition 6.8) captures only the monomials in the P-socle for the maximal ideal P, not the binomials or the elements with more than two terms. The fact that socles need not be binomial ideals (Example 12.11) convinced us to leave the monoid notion in the land of monomials instead of, say, defining the socle of a monoid to be a congruence, which would only additionally capture the binomials. In the end, the true notion of socle in the land of monoids requires knowledge of multiple congruences, and for us eventually gave rise to the concept of witness and key witness in Section 4. Explicitly correcting the non-binomiality in the land of binomial ideals in monoid algebras—a process not required in the land of monoids—gave rise to the notion of character witness in Section 16.

Example 12.10. The P-socle can be nonzero without containing monomials. This occurs for $\mathfrak{m}_P = \langle x, y\rangle \subset \Bbbk[x, y]$ and $I = \langle x^2-xy, xy-y^2\rangle$, where the P-socle is $\langle x-y\rangle$.

Example 12.11. Eisenbud and Sturmfels observed that socles modulo binomial ideals need not be binomial ideals [ES96, Example 1.8]. An example apropos to the developments here comes from Example 4.10.3: the ideal $I = \langle x^2-xy, xy-y^2, x(z-1), y(w-1)\rangle$ for $\mathfrak{m}_P = \langle x, y\rangle \subset \Bbbk[x, y, z, w]$ has P-socle $\langle x - y, x(z - 1), y(w - 1),(z - 1)(w - 1)\rangle$, and there is no remedy for the failure of the final generator to be a binomial.

Definition 12.12. Given a monoid prime $P \subset Q$, a mesoprimary binomial ideal in $\Bbbk[Q]$ is *P-mesoprimary* if the associated prime ideal of its induced congruence is P.

Example 12.13. As in Example 6.9—and in fact, as an immediate consequence of that example—the P-socle modulo a P-mesoprimary ideal is generated by monomials.

The principal use of the following definition, which builds on the notion of order ideal from Definition 7.3, concerns the case where the set $\mathbf{w}$ consists of a single witness. The more general case arises during the construction of mesoprimary decompositions with as few components as possible (Corollary 13.6).

Definition 12.14. Fix a binomial ideal $I \subseteq \Bbbk[Q]$, a prime $P \subset Q$, and a subset $\mathbf{w} \subseteq Q$. The *monomial ideal $M^P_{\mathbf{w}}(I) \subseteq \Bbbk[Q]$ cogenerated by $\mathbf{w}$ along P* is generated by the monomials $\mathbf{t}^u \in \Bbbk[Q]$ such that u lies outside of the order ideal $Q^P_{\preceq w}$ cogenerated by w at P (Definition 7.3) under the congruence $\sim_I$ for all $w \in \mathbf{w}$.

Definition 12.15. Fix a binomial ideal $I \subseteq \Bbbk[Q]$ and a set $\mathbf{w} \subseteq Q$ of elements such that the P-mesoprime I^P_w of I at w is $I_{\rho,P}$ for all $w \in \mathbf{w}$. The *P-mesoprimary component of I cogenerated by* $\mathbf{w}$ is the preimage $W^P_{\mathbf{w}}(I)$ in $\Bbbk[Q]$ of the ideal $I_P + I_\rho + M^P_{\mathbf{w}}(I) \subseteq \Bbbk[Q]_P$.

The nomenclature in Definition 12.15 is justified by Proposition 12.17, which requires a preliminary result.

Lemma 12.16. *Fix binomial ideals I and I' in $\Bbbk[Q]$ inducing congruences $\sim$ and $\sim'$, and let $\approx$ be the congruence induced by $I+I'$. The common refinement $\sim' \cap \sim$ refines $\approx$, and if $\approx \neq \sim' \cap \sim$ then $\approx$ is obtained from $\sim' \cap \sim$ by enlarging its nil class.*

Proof. If $\mathbf{t}^u - \lambda\mathbf{t}^v \in I + I'$ and neither of $\mathbf{t}^u$ and $\mathbf{t}^v$ lies in $I + I'$, then $\mathbf{t}^u - \lambda\mathbf{t}^v$ is a telescoping sum of two-term binomials (i.e., both coefficients nonzero) each of which lies in I or I'. $\square$

Proposition 12.17. *The ideal $W^P_{\mathbf{w}}(I)$ in Definition 12.15 is mesoprimary with associated mesoprime $I_{\rho,P}$. More precisely, if I induces the congruence $\sim$ on Q, then $W^P_{\mathbf{w}}(I)$ induces the common refinement of the coprincipal congruences $\sim^P_w$ cogenerated by the elements in $\mathbf{w}$ along P. Every witness in $\mathbf{w}$ lies in the P-socle modulo $W^P_{\mathbf{w}}(I)$.*

Proof. The claim has little content if $P = \varnothing$, as then $I_{\rho,P} = I_\rho = I_P$, so assume $P \neq \varnothing$. The common refinement $\approx$ of coprincipal congruences in question is mesoprimary by Proposition 6.12. Every witness in $\mathbf{w}$ lies in the socle modulo $\approx$ because witnesses have maximal image, under the further quotient by Green's relation, among elements at which the P-mesoprime of I is fixed to be $I_{\rho,P}$.

By construction (specifically, Definition 7.7 and Lemma 7.6), the mesoprimary congruence $\approx$ refines the congruence $\approx'$ induced by $W^P_{\mathbf{w}}(I)$: the monomial ideal $M^P_{\mathbf{w}}(I)$ sets all elements outside of the order ideal equivalent to one another, and the generators of I_ρ carry out the remaining required identifications. The harder direction is showing that no more relations are introduced.

Since $W^P_{\mathbf{w}}(I)$ is obtained from an extension to the localization $\Bbbk[Q]_P$ along P, we may as well assume that $Q = Q_P$, so P is the maximal ideal of Q. By construction, the congruences induced by I and I_ρ each individually refine the congruence $\approx$ (not to be confused with $\approx'$ here); for I_ρ this uses the fact that the P-mesoprime of I at $w \in \mathbf{w}$ induces the P-prime congruence of $\sim$ at w. Therefore both of I and I_ρ are ideals graded by $Q/{\approx}$. Furthermore, Lemma 12.16 implies that $W^P_{\mathbf{w}}(I)$ is graded by $Q/{\approx}$ as well: although $\approx'$ is refined by $\approx$ (which is a priori the wrong way for the refinement to go if $W^P_{\mathbf{w}}(I)$ is to be graded by $Q/{\approx}$), the refinement merely partitions the set of monomials that map to 0 modulo $W^P_{\mathbf{w}}(I)$.

With the gradings in mind, assume $a \approx' b$. If both $\mathbf{t}^a$ and $\mathbf{t}^b$ lie in $M^P_{\mathbf{w}}(I)$, then there is nothing to prove, so assume that $\mathbf{t}^a \notin M^P_{\mathbf{w}}(I)$. By Lemma 12.16, it suffices to show that $\mathbf{t}^a \notin W^P_{\mathbf{w}}(I)$. Choose $w \in \mathbf{w}$ with a in the order ideal $Q^P_{\preceq w} = Q^P_{\preceq w}(\sim)$, which can be done by definition of $M^P_{\mathbf{w}}(I)$. Next pick $u \in Q$ such that the images of $u + a$ and w in $Q/{\approx}$ are Green's equivalent to one another; this is possible by definition of the order ideal $Q^P_{\preceq w}$. Use a double tilde to denote passage from Q to $Q/{\approx}$, so $\approx\!\!\!\!\!q$ $\widetilde{\widetilde{q}} \in Q/{\approx}$ is the image of q for any $q \in Q$. The choice of the character ρ was made precisely so that the graded piece $(I)_{\widetilde{\widetilde{q}}}$ of the ideal I contains the graded piece $(I_\rho)_{\widetilde{\widetilde{q}}}$ whenever $\widetilde{\widetilde{q}}$ is Green's equivalent to $\widetilde{\widetilde{w}}$ in $Q/{\approx}$. This means that I_ρ adds no new relations to I in degree $\widetilde{\widetilde{q}}$. Since $M^P_{\mathbf{w}}(I)$ adds no new relations to I in degree $\widetilde{\widetilde{q}}$ by definition, $W^P_{\mathbf{w}}(I)_{\widetilde{\widetilde{q}}} = (I)_{\widetilde{\widetilde{q}}}$ for

$q = u + a$. In other words, $u + a \approx' u + b \Leftrightarrow u + a \sim u + b$. The class of $u + a$ is not nil in $Q/{\sim}$ because the character of I_P at $u + a$ is ρ. Hence $\mathbf{t}^a \notin W^P_{\mathbf{w}}(I)$. $\square$

Definition 12.18. A binomial ideal is *coprincipal* if it is maximal (as per Theorem 9.12) among the ideals inducing a given coprincipal congruence. A *coprincipal component of I cogenerated by q at P* is a P-mesoprimary component $W^P_q(I) := W^P_{\{q\}}(I)$ cogenerated by a single element q.

Corollary 12.19. *If $I \subseteq \Bbbk[Q]$ is a binomial ideal and q is an I-witness for P, then the coprincipal component of I cogenerated by q at P is a coprincipal binomial ideal.*

Proof. Immediate from Proposition 12.17 and the definitions. $\square$

Remark 12.20. It would be superb if intersecting any pair of mesoprimary ideals with the same associated mesoprime resulted in another mesoprimary ideal. More precisely, a direct binomial ideal analogue of Proposition 6.12 for congruences would be desirable. Unfortunately, the binomial analogue is false, in general: in $\Bbbk[x, y]$, the intersection of the mesoprimary ideals $\langle xy - 2y^2\rangle + \langle x, y\rangle^4$ and $\langle xy - y^2\rangle + \langle x, y\rangle^4$ is not mesoprimary; it is not even a binomial ideal. Heuristically, if I_1 and I_2 are mesoprimary ideals in $\Bbbk[Q_P]$ with associated mesoprime $I_{\rho,P}$, then in each of I_1 and I_2 there are "vertical" binomials from I_ρ, whose coefficients are dictated by the character ρ, and "horizontal" binomials conglomerating the vertical fibers, with more arbitrary coefficients. (The vertical and horizontal directions in Examples 1.3 and 2.17 are reversed for aesthetic reasons; the usage here makes sense in Examples 4.10, 4.11, 8.12, 9.1, 12.11, 16.7, and 17.5.) When the horizontal coefficients from I_1 and I_2 conflict, the intersection need not be binomial.

That said, the analogue of Proposition 6.12 is true once control is granted over binomiality, and that comes for free when I_1 and I_2 both arise from a single ideal via sets of witnesses as in Proposition 12.17. In that sense, the binomial analogue of Proposition 6.12 is "true enough" for the relevant aspects of the theory of mesoprimary decomposition to succeed, namely Corollary 13.6.

Remark 12.21. The existence of a mesoprimary ideal inducing a given congruence is automatic by Remark 2.16. However, the question becomes more subtle when a given associated mesoprime other than the unital one is desired. Roughly, we do not know how to construct mesoprimary ideals with given associated mesoprimes de novo, although by Proposition 12.17 we do know how to construct mesoprimary ideals given the foundation of a binomial ideal to start from. More precisely, fix a monoid prime $P \subset Q$, a P-mesoprimary congruence $\approx$ on Q, and a character $\rho : K \to \Bbbk^*$ on the stabilizer K of some element that is not nil in the localization of $Q/{\approx}$ along P. It would be convenient to say that there exists a mesoprimary ideal J inducing $\approx$ with associated mesoprime $I_{\rho,P}$, but it is not clear to us whether this should be true. What guarantees existence in the cases we care about, namely Proposition 12.17, is the I-witnessed nature of $\approx$: each I-witness prefers a particular character over all others—the one it sees by virtue of it being an I-witness—and that is the only one required for the theory of mesoprimary decomposition.

In a different light, the problem is one of automorphisms. The associated mesoprime of any unital P-mesoprimary ideal I is $I_{1,P}$ for the trivial character. Suppose, for simplicity, that the ground field $\Bbbk$ is algebraically closed. Then, for any mesoprime $I_{\rho,P}$, there is an automorphism of $\Bbbk[Q]$ taking $I_{1,P}$ to $I_{\rho,P}$; this amounts to the feasibility of extending the character $\rho : K \to \Bbbk^*$ to the entire group G_P of units of Q_P. To transform I into a mesoprimary ideal with associated mesoprime $I_{\rho,P}$, however, the character must be extended appropriately to all of Q_P, not just to G_P. It is not clear to us whether issues of horizontal coefficients can intervene, particularly when the inclusion of G_P into Q_P fails to split.

Remark 12.22. Independent of the existence question, it is not clear how to describe the class of mesoprimary ideals inducing a given congruence and with a given associated mesoprime. Certainly, a solution to the problem in Remark 12.21 need not be unique. For instance in the nilpotent situation, the one parameter family $\langle x - \lambda y, x^2, xy, y^2\rangle$ (for $\lambda \neq 0$) consists of mesoprimary ideals over the associated mesoprime $\langle x, y\rangle$, all inducing the same congruence.

13. Mesoprimary decomposition of binomial ideals

This section makes precise the sense in which mesoprimary decomposition of congruences lifts to a parallel combinatorial theory for binomial ideals in monoid algebras.

Definition 13.1. Fix a binomial ideal $I \subseteq \Bbbk[Q]$ in a finitely generated commutative monoid algebra over a field $\Bbbk$.

1. An expression of I as an intersection of finitely many mesoprimary ideals is a *mesoprimary decomposition* if, for each prime $P \subset Q$ and P-mesoprimary ideal J in the intersection, the P-mesoprimes of I and J at every J-witness coincide.
2. Each mesoprimary ideal that appears is a *mesoprimary component* of I.
3. If every J-witness for every mesoprimary component J is an I-witness, then the decomposition is a *combinatorial* mesoprimary decomposition.

Theorem 13.2. *Fix a finitely generated commutative monoid Q and a field $\Bbbk$. Every binomial ideal in the algebra $\Bbbk[Q]$ admits a combinatorial mesoprimary decomposition.*

Proof. Examples include those in Theorem 13.5 and Corollary 13.6, below. □

The proof has essentially the same structure as that of Theorem 8.4, except that we are forced (by cases such as Example 16.7) to work with general $\sim$-witnesses instead of just key $\sim$-witnesses. For later use in Theorem 16.9, we separate off the main part of the argument.

Proposition 13.3. *Fix a binomial ideal $I \subseteq \Bbbk[Q]$ inducing a congruence $\sim$ on Q. Given an element $q \in Q$, there is a monoid prime $P \subset Q$ and an element $a \in Q$ such that $a+q$ is an I-witness for P and the class in Q of q under $\sim$ coincides with its class under the coprincipal component $W^P_{a+q}(I)$.*

Proof. Consider the *liberator* of q under $\sim$, namely the ideal

$$T(q,\sim) = \{t \in Q \mid \text{the class in } \overline{Q} \text{ of } \overline{q} \in \overline{Q} \text{ is not singleton under } \ker(\phi_t : \overline{Q} \to t+\overline{Q})\}$$

of all elements whose addition morphism joins $\overline{q}$ to some other element in $\overline{Q} = Q/\sim$. There is a prime ideal $P \subset Q$ minimal among those containing T, since no unit lies in T. By construction, no other element of $\overline{Q}$ is joined to $\overline{q}$ under localization of $\overline{Q}$ at P. Minimality of P over T means that the localization T_P is primary to the maximal ideal P_P. Therefore there is a maximal Green's class of elements of Q outside of T_P. Pick $t \in Q$ in that class. By maximality, $w = t + q$ is a $\sim$-witness for P. The classes of q under $\sim$ and the coprincipal component $W^P_w(I)$ coincide by construction. $\square$

The proof of Theorem 13.5 also requires a general observation about graded ideals.

Lemma 13.4. *Let $I, J_1, \ldots, J_r$ be Q-graded ideals such that J_i contains I for all i. If there exists a map $q \mapsto i(q)$ such that for all $q \in Q$ the q-graded piece of I equals that of $J_{i(q)}$, then $I = \bigcap_i J_i$.*

Proof. The natural diagonal map $\delta : \Bbbk[Q]/I \to \bigoplus_i \Bbbk[Q]/J_i$ is injective if and only if $I = \bigcap_i J_i$. The condition on $i(q)$ guarantees that the composite map $\Bbbk[Q]/I \to \bigoplus_i \Bbbk[Q]/J_i \to \Bbbk[Q]/J_{i(q)}$ is injective in degree q for all $q \in Q$, so δ is injective. $\square$

Theorem 13.5. *Fix a finitely generated commutative monoid Q and a field $\Bbbk$. Every binomial ideal in the monoid algebra $\Bbbk[Q]$ is the intersection of the coprincipal ideals cogenerated by its witnesses.*

Proof. Apply Lemma 13.4 to the conclusion of Proposition 13.3. $\square$

Using Theorem 13.2 and Proposition 12.17, one can find a mesoprimary decomposition that minimizes the number of components by intersecting all components for a given associated mesoprime.

Corollary 13.6. *Fix a finitely generated commutative monoid Q and a field $\Bbbk$. Every binomial ideal in the monoid algebra $\Bbbk[Q]$ admits a combinatorial mesoprimary decomposition with one component per associated mesoprime.*

Remark 13.7. The existence of any mesoprimary decomposition—let alone a combinatorial one as in Theorem 13.2—is much stronger than mere existence of a decomposition as an intersection of mesoprimary ideals, essentially because of the phenomenon in Remark 12.5. The strength is particularly visible when the field $\Bbbk$ is algebraically closed of characteristic 0. In that case, every binomial primary decomposition of I expresses I as an intersection of mesoprimary ideals by Corollary 10.7, but a mesoprime must honor stringent combinatorial conditions to be an associated mesoprime of I, and a mesoprimary ideal for an associated mesoprime must honor stringent combinatorial conditions to be a mesoprimary component. The difference between ordinary and combinatorial mesoprimary decompositions is a relatively slight distinction among potential socle locations: in the ordinary case, I is merely required to possess the correct characters at the socle elements of the mesoprimary components, whereas in the combinatorial case only maximal elements possessing the correct characters from I are allowed in the socles of components.

Remark 13.8. No choices are necessary to construct the coprincipal decomposition in Theorem 13.5: both the combinatorics and the arithmetic are forced. Therefore coprincipal decomposition into coprincipal components cogenerated by witnesses is canonical—as canonical as monomial irreducible decomposition of monomial ideals—but canonicality in the binomial context comes at the price of non-minimality. Some of the redundancy is eliminated in Section 16, but without arbitrary, unmotivated (and often symmetry-breaking) choices, redundancy can stubbornly persist.

14. Binomial localization

Upon localization of a binomial quotient $\Bbbk[Q]/I$ at a binomial prime, some monomials become units and others are annihilated. The units are easy: if the prime is $I_{\sigma,P}$, then the monomials outside of $\mathfrak{m}_P$ become units. The question of which monomials die is much more subtle. There are two potential reasons that a monomial gets killed upon ordinary localization (Theorem 14.9): a combinatorial one and an arithmetic one. Combinatorially, a monomial dies if its class under $\sim_I$ points into P (Definition 14.1); arithmetically, a monomial dies if the character of I_P at it is incommensurate with ρ (Definition 14.6). These annihilations result from the inversion of two different types of binomials: in the combinatorial case the inverted binomials have one monomial outside of $\mathfrak{m}_P$, and in the arithmetic case the inverted binomials lie along the unit group G_P locally at P. The relevant monomials die because locally each becomes a binomial unit multiple of a binomial in I; see the proof of Theorem 14.9.

Definition 14.1. Given a prime $P \subset Q$, and a congruence $\sim$ on Q, the congruence class of $q \in Q$ *points into* P if $q + p \sim q$ in the localization Q_P for some $p \in P$.

Lemma 14.2. *Given a prime $P \subset Q$ and a congruence $\sim$ on Q, the set of elements in Q whose class points into P is an ideal of Q.*

Proof. If $q + p \sim q$ then $u + q + p \sim u + q$ by additivity of $\sim$. $\square$

Definition 14.3. The *P-infinite ideal* $M^P_\infty(\sim) \subseteq Q$ for a prime $P \subset Q$ and congruence $\sim$ on Q is generated by the elements of Q whose classes point into P. If $\sim = \sim_I$ is induced by a binomial ideal $I \subseteq \Bbbk[Q]$, then $M^P_\infty(I) \subseteq \Bbbk[Q]$ is the corresponding *P-infinite monomial ideal.*

Remark 14.4. The terminology involving infinity stems from [DMM09, Lemma 2.10], which concerns binomial localization at a monomial prime of an affine semigroup ring: when the ambient monoid Q is an affine semigroup, a class that points into P is infinite. The focus on monomial primes in affine semigroup rings arises there because the field is algebraically closed of characteristic 0 and the ideals to be localized are $I_{\rho,P}$-primary (and hence contain I_ρ), so the binomial localization procedure can be carried out in the affine semigroup ring $\Bbbk[Q]/I_\rho$. Definitions 14.1 and 14.3 lift the picture from $(I + I_\rho)/I_\rho \subseteq \Bbbk[Q]/I_\rho$ to $I + I_\rho \subseteq \Bbbk[Q]$ itself; but see Remark 14.7.

Lemma 14.5. *Let R be a set of characters on subgroups of the unit group G_P of Q_P. Given a binomial ideal $I \subseteq \Bbbk[Q]$, the set $\{q \in Q \mid$ the character ρ^P_q of I_P at q is not a restriction of every character from $R\}$ is an ideal of Q.*

Proof. The character ρ^P_{p+q} of I_P at $p + q$ is an extension of ρ^P_q. □

Definition 14.6. Given a binomial ideal $I \subseteq \Bbbk[Q]$ and a mesoprime $I_{\rho,P}$, the *incommensurate ideal* of I at ρ is the ideal $M^P_\rho(I) \subseteq \Bbbk[Q]$ spanned over $\Bbbk$ by all monomials $\mathbf{t}^q$ such that the character of I_P at q is not a restriction of ρ.

Remark 14.7. The condition for a monomial to lie in the incommensurate ideal is phrased arithmetically, but in reality many monomials in it are there for combinatorial reasons: if the domain of the character of I_P at q fails to be contained in the (saturation of) the domain of ρ—that is, if the stabilizer of the class of q in $Q/{\sim_I}$ is too big—then q has no hope of being commensurate with ρ. This type of combinatorial obstruction to commensurability also contributes infinite classes in [DMM09, Lemma 2.10].

Definition 14.8. The *binomial localization* of $I \subseteq \Bbbk[Q]$ at a binomial prime $I_{\sigma,P}$ is the sum $I + M^P_\infty(I) + M^P_\sigma(I) \subseteq \Bbbk[Q]$ of I plus its P-infinite and incommensurate ideals.

The point of this section is to compare the previous definition with ordinary (inhomogeneous) localization of a $\Bbbk[Q]$-module at a binomial prime $I_{\sigma,P}$, obtained by inverting all elements of $\Bbbk[Q]$ outside of $I_{\sigma,P}$.

Theorem 14.9. *Given a binomial ideal $I \subseteq \Bbbk[Q]$ over an arbitrary field $\Bbbk$, the kernel of the localization homomorphism from $\Bbbk[Q]$ to the ordinary localization of $\Bbbk[Q]/I$ at a binomial prime $I_{\sigma,P}$ contains the binomial localization of I at $I_{\sigma,P}$.*

Proof. First suppose that the class of $q \in Q$ points into P. Pick $p \in P$ such that $q + p \sim q$. This congruence means that there is a binomial $\mathbf{t}^q - \lambda\mathbf{t}^{q+p} = \mathbf{t}^q(1 - \lambda\mathbf{t}^p)$ in I. But $1-\lambda\mathbf{t}^p$ lies outside of $I_{\sigma,P}$ because its image modulo $\mathfrak{m}_P$ is already 1. Therefore $1 - \lambda\mathbf{t}^p$ is a unit in the ordinary localization of $\Bbbk[Q]/I$ at $I_{\sigma,P}$, so $\mathbf{t}^q$ is 0 there.

Next suppose that $\mathbf{t}^q \in M^P_\sigma(I)$. By definition, there is a binomial $1 - \lambda\mathbf{t}^g$ for some $g \in G_P$ such that $\lambda \neq \sigma(g)$ and $\mathbf{t}^q(1-\lambda\mathbf{t}^g) \in I_P$. The element $1-\lambda\mathbf{t}^g$ lies outside of $I_{\sigma,P}$ by definition. Therefore the argument in the previous paragraph works in this case, too. We conclude that the binomial localization of I is contained in the kernel. □

Remark 14.10. How is Theorem 14.9 to be applied? While the binomial localization I' of I at $I_{\sigma,P}$ might not coincide with the kernel of ordinary localization at $I_{\sigma,P}$, it is always the case, by Theorem 14.9, that I and I' have the same ordinary localization at $I_{\sigma,P}$. Therefore, for the purpose of detecting $I_{\sigma,P}$-primary components, I' is just as good as I was in the first place. But the combinatorics of I' might be much simplified, thereby clarifying the role of $I_{\sigma,P}$ in the primary decomposition of I. See the proof of Theorem 15.16 for a quintessential example.

15. Irreducible and primary decomposition of binomial ideals

Passing from mesoprimary and coprincipal ideals and decompositions to primary and irreducible ideals and decompositions requires a minimal amount of knowledge concerning primary decomposition of mesoprimary ideals themselves. To speak about binomial primary decomposition of binomial ideals in $\Bbbk[Q]$ we are forced to assume, in appropriate locations, that $\Bbbk$ is algebraically closed (Example 11.16); we write $\Bbbk = \overline{\Bbbk}$ in that case. Doing so guarantees that each binomial ideal $I \subset \Bbbk[Q]$ has binomial associated primes (Proposition 11.10). However, most of this section works for an arbitrary ground field, so we are explicit about our hypotheses in this section. One reason is that the characterization of binomial prime ideals (Theorem 11.15) does not rely on properties of $\Bbbk$: every binomial prime can be expressed uniquely as a sum $\mathfrak{p} + \mathfrak{m}_P$ in which $P \subset Q$ is a monoid prime ideal and $\mathfrak{p}$ is a (not necessarily prime) binomial ideal that contains no monomials.

Proposition 15.1. *Fix an arbitrary field $\Bbbk$. If $I \subset \Bbbk[Q]$ is mesoprimary with an associated mesoprime $I_{\rho,P}$, then $(\Bbbk[Q]/I)_P$ has a filtration by $\Bbbk[Q]_P$-submodules whose associated graded module is a direct sum of copies of $(\Bbbk[Q]/I_{\rho,P})_P$.*

Proof. Localizing along P, we assume that $Q = Q_P$, so P is the maximal ideal of Q. The group G of units in Q acts freely on the quotient $\overline{Q} = Q/\sim_I$ by Corollary 6.6. Owing to the partial order on the set of orbits afforded by Lemma 2.19, the grading by $\overline{Q}/G$ on $\Bbbk[Q]/I$ induces the desired filtration. As a vector space over $\Bbbk$, the associated graded module is $\mathrm{gr}(\Bbbk[Q]/I) \cong \bigoplus_{\text{orbits } T} \Bbbk\{T\}$, where $\Bbbk\{T\}$ is the vector subspace of $\Bbbk[Q]/I$ with basis the set of monomials $\mathbf{t}^q$ for $q \in T$. As a $\Bbbk[Q]$-module, the vector space $\Bbbk\{T\}$ is isomorphic to $\Bbbk[Q]/I_{\rho,P}$ by Proposition 12.6 and Remark 12.7. $\square$

Corollary 15.2. *Fix an arbitrary field $\Bbbk$. If $I \subset \Bbbk[Q]$ is mesoprimary, then the associated primes of I are exactly the minimal primes of its unique associated mesoprime.*

Proof. If I is P-mesoprimary, then the monomials outside of $\mathfrak{m}_P$ are nonzerodivisors on $\Bbbk[Q]/I$ by definition, so the result follows immediately from Proposition 15.1. $\square$

Remark 15.3. Corollary 15.2 says that, although one expects to derive information about associated primes of I from the characters at its witnesses, when I is mesoprimary the appropriate characters appear at the identity $1 \in \Bbbk[Q]$. This is another manifestation of semifreeness (Remark 6.7), detailed in the present case at Proposition 15.1.

Lemma 15.4. *Fix a P-coprincipal ideal $I \subseteq \Bbbk[Q]$ cogenerated by $\mathbf{t}^q$ such that its associated mesoprime $\mathfrak{p} = I_{\rho,P}$ is prime. Then the ordinary (inhomogeneous) localization $\Bbbk[Q]_\mathfrak{p}/I_\mathfrak{p}$ at $\mathfrak{p}$ has simple socle:* $\operatorname{soc}(\Bbbk[Q]_\mathfrak{p}/I_\mathfrak{p}) = \langle \mathbf{t}^q \rangle_\mathfrak{p}$, *without hypotheses on* $\Bbbk$.

Proof. The maximal ideal $\mathfrak{p}$ certainly annihilates the element $\mathbf{t}^q \in \Bbbk[Q]_\mathfrak{p}/I_\mathfrak{p}$. Any other monomial $\mathbf{t}^v$ has the property that $\mathbf{t}^u\mathbf{t}^v = \mathbf{t}^q$ already in $\Bbbk[Q]_P$ for some $u \in Q$. □

The next result should more honestly be part of the taxonomy of binomial ideals in Section 10, and truly it belongs in Theorem 10.6. The main reason it doesn't appear there is because coprincipal congruences do not appear in Definition 2.11, as they are introduced at a more leisurely pace in Section 7. In addition, it is hard to fit the lines

. . . congruence on Q	. . . binomial ideal in $\Bbbk[Q]$
coprincipal	coprincipal
primitive and coprincipal	irreducible

neatly in the table near the start of Section 10.

Theorem 15.5. *Fix a binomial ideal $I \subseteq \Bbbk[Q]$ for a finitely generated commutative monoid Q over an arbitrary field $\Bbbk$.*

1. *I is irreducible if I is coprincipal and its associated mesoprime is prime.*
2. *The converse holds when $\Bbbk = \overline{\Bbbk}$ is algebraically closed of characteristic* 0.

Proof. Assume I is coprincipal with prime associated mesoprime. Then I is primary by Corollary 15.2, and it is irreducible by [Vas98, Proposition 3.15] because of the simple socle condition in Lemma 15.4.

For the converse, assume $\Bbbk = \overline{\Bbbk}$ and $\operatorname{char}(\Bbbk) = 0$. If I is irreducible then it is primary (this is true for any ideal in any noetherian commutative ring), and hence mesoprimary by Corollary 10.7. Any coprincipal decomposition of I exhibits I as an intersection of finitely many coprincipal ideals, one of which must equal I because I is irreducible. □

Remark 15.6. The full extent to which the converse in Theorem 15.5.2 holds is inscrutable to us: we do not know the general conditions under which a binomial ideal is mesoprimary, given that it is irreducible (or even primary). Certainly having a base field that is algebraically closed of characteristic 0 suffices, because then Theorem 10.6.3 yields the mesoprimary conclusion once irreducibility—and thus primaryness—is given.

The transition from binomial irreducible ideals to binomial irreducible decompositions requires decompositions of mesoprimary ideals.

Proposition 15.7. *Fix $\Bbbk = \overline{\Bbbk}$. If $I \subset \Bbbk[Q]$ is mesoprimary, then its (unique minimal) primary decomposition is $I = \bigcap_{\mathfrak{p}\in A} I + \mathfrak{p}$, where A is the set of binomial parts of associated primes of I; that is, $A = \big\{ I_\sigma \mid I_{\sigma,P} \in \operatorname{Ass}(\Bbbk[Q]/I) \big\}$.*

Proof. Adding the binomials I_σ in an associated prime $I_{\sigma,P}$ to a mesoprimary ideal coarsens its congruence to a primitive one. Since the monomials are untouched, the result follows from the primary decomposition of mesoprimes in Proposition 11.10. $\square$

Remark 15.8. It is worth keeping in mind how concrete the set A in Proposition 15.7 is: if the unique associated mesoprime of I is $I_{\rho,P} = I_\rho + \mathfrak{m}_P = I + \mathfrak{m}_P$, then the ideals $I_\sigma \in A$ are indexed by the saturated finite extensions σ of ρ, by Proposition 11.10.

Lemma 15.9. *In the situation of Proposition 15.7, every component $I + I_\sigma$ induces a primitive congruence.*

Proof. Since σ is a saturation of ρ, the quotient of Q_P modulo the congruence induced by $I + I_\sigma$ is exactly the quotient of $Q_P/{\sim_I}$ by the torsion subgroup of its unit group. $\square$

Lemma 15.10. *If I is coprincipal in Proposition 15.7, then every primary component there is a coprincipal ideal.*

Proof. The partially ordered monoid of Green's classes that is used to detect (or construct) coprincipal ideals is the same for I and for $I + I_\sigma$. $\square$

Next we come to the main consequences of mesoprimary decomposition for primary and irreducible decomposition, including the following result and Theorem 15.16.

Corollary 15.11. *Fix a binomial ideal $I \subseteq \overline{\Bbbk}[Q]$ over an algebraically closed field $\overline{\Bbbk}$.*

1. *Refining any mesoprimary decomposition of I by canonical primary decomposition of its components yields a binomial primary decomposition of I each of whose components induces a primitive congruence on Q.*
2. *If the mesoprimary decomposition used in part 1 is a coprincipal decomposition, then the resulting primary decomposition is an irreducible decomposition each of whose components induces a primitive coprincipal congruence on Q.*

Proof. The first claim is immediate from Proposition 15.7 and Lemma 15.9. The second is immediate from the first along with Lemma 15.10 and Theorem 15.5. $\square$

Remark 15.12. Corollary 15.11 implies that binomial primary and irreducible decompositions are canonically recovered from essentially combinatorial data, just as in the monomial case. In the binomial case the decomposition can be redundant, but the redundancy is already inherent in the combinatorics; that is, it happens at the level of monoids, congruences, and witnesses, before coefficients enter the picture. Note that by "canonical" we mean in the sense of "determined without extra data or requirements". In contrast, Ortiz [Ort59] uses the adjective "canonical" in an unfortunate manner to refer to primary decompositions that minimize a certain index of nilpotency. We view Ortiz's decompositions as optimized for a particular choice of "cost function" rather than as canonical; it could be possible to use cost functions other than index of nilpotency to define other optimized primary decompositions. Regardless of the name, Ojeda [Oje10] proves that the components in Ortiz's "canonical" decompositions are binomial when the original ideal is binomial, but these decompositions generally differ from the ones here, which rely solely on intrinsic data.

Remark 15.13. Corollary 15.11 produces primary and irreducible decompositions whose components are mesoprimary binomial ideals. However, we do not know whether all binomial primary or irreducible ideals are mesoprimary over algebraically closed fields of positive characteristic.

When the base field $\Bbbk$ is not algebraically closed, the binomial ideal I need not possess a binomial primary decomposition over $\Bbbk$ (see Example 11.16, for instance), but it does have one over the algebraic closure $\overline{\Bbbk}$. One of our original motivations for seeking a theory of mesoprimary decomposition was to gather primary components in such a way that Galois automorphisms (of $\overline{\Bbbk}$ over $\Bbbk$) permute them. In particular, if two primes are Galois translates of one another, then we wanted their corresponding primary components to look combinatorially the same.

Theorem 15.14. *If the ideal I in Corollary 15.11 is defined over a subfield $\Bbbk$ of its algebraic closure $\overline{\Bbbk}$, then the primary (or irreducible) decomposition there is fixed by the Galois group* $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$*. More precisely, if $\pi \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ is a Galois automorphism and C is one of the primary (or irreducible) components of I from Corollary 15.11, then $\pi(C)$ is another of the primary (or irreducible) components of I from Corollary 15.11.*

Proof. The Galois group fixes every mesoprimary component of I elementwise, and the primary decomposition of a mesoprimary ideal (Proposition 15.7) is canonical. □

Our final result on the primary-to-mesoprimary correspondence shows that, for general binomial ideals, every associated prime is detected by an associated mesoprime. For cellular binomial ideals, the relationship between associated mesoprimes and associated primes is even more perfectly precise. The cellular case of the following result over an algebraically closed field is [ES96, Theorem 8.1] and its converse; the latter was stated and used without proof after [ES96, Algorithm 9.5]. First, a matter of notation.

Definition 15.15. Fix a cellular binomial ideal $I \subset \Bbbk[Q]$. If $P \subset Q$ is the prime ideal of exponents on monomials that are nilpotent modulo I, then I is *P-cellular.*

Theorem 15.16. *Fix a binomial ideal $I \subseteq \Bbbk[Q]$ over an arbitrary field $\Bbbk$.*

1. *Each associated prime of I is minimal over some associated mesoprime of I.*
2. *If I is cellular, then the binomial converse holds: every binomial prime that is minimal over an associated mesoprime of I is an associated prime of I.*

Proof. For part 1, apply Corollary 15.2 to the mesoprimary components of I under any mesoprimary decomposition from Theorem 13.2.

For the cellular converse, suppose that I is P-cellular, and that a binomial prime $I_{\sigma,P}$ is minimal over some associated mesoprime $I_{\rho,P}$ of I. The submodule of $\Bbbk[Q]/I$ generated by a witness for $I_{\rho,P}$ is isomorphic to a quotient $\Bbbk[Q]/I'$ for a binomial ideal I'

all of whose witness characters are extensions of ρ. After subsequently binomially localizing at $I_{\sigma,P}$, the only surviving characters are restrictions of σ, and hence sit between σ and ρ. In particular, this is true for the character at any given monomial $\mathbf{t}^q$ in the P-socle. Such a monomial generates a mesoprime submodule with $I_{\sigma,P}$ among its associated primes by Corollary 15.2. Therefore $I_{\sigma,P}$ is associated to I', and hence to I by Theorem 14.9; see Remark 14.10. □

Example 15.17. Given an associated prime of I as in Theorem 15.16.1, the associated mesoprime guaranteed by the theorem need not be unique. This phenomenon is illustrated by Example 2.17.5 (a smaller example is $\langle y^2, y(x-1), x^2-1\rangle$, but we already have a picture in the Example). The binomial prime $\langle x-1, y\rangle$ for the trivial character on the x-axis $\mathbb{N}\times\{0\}$ and $J=\{1\}$ is associated to I and has two possible choices of associated mesoprime, namely $\langle x-1, y\rangle$ and $\langle x^2-1, y\rangle$. Combinatorially, the row of dots at height 1 consists of two classes, each being the nonnegative points in a coset of an unsaturated lattice, while the row of dots at height 2 comprise just one class, the nonnegative points in a coset of the saturation. In general, when the group of units G_P acts, there could be a whole G_P-orbit of classes corresponding to an unsaturated subgroup K, and a higher G_P-orbit with an associated subgroup anything between K and its saturation.

Cellular decompositions of binomial ideals make choices and are inherently noncanonical, so in all of our development we avoided going through cellular decomposition.

16. Character witnesses and false witnesses

The development here of the notion of witness in the monoid algebra setting—that is, the arithmetic setting—is grounded in the combinatorial precursor in Sections 4–5.

Definition 16.1. Fix a binomial ideal $I \subset \Bbbk[Q]$, an element $q \in Q$, and a monoid prime ideal $P \subset Q$. A *P-cover extension at q* is an extension of the character $\rho_q^P : K_q \to \Bbbk^*$ of I_P at q to the character $\rho_{p+q}^P : K_{p+q} \to \Bbbk^*$ at a P-cover $p+q$ of q (Definition 4.4).

There can be many—even infinitely many—choices of minimal generating sets for P (Remark 4.5), but just as in Lemma 4.6, there are not too many P-cover extensions.

Lemma 16.2. *In the situation of Definition 16.1, the set of P-cover extensions at q is finite, in the sense that only finitely many stabilizers K_{p+q} occur, and only finitely many characters defined on each stabilizer occur among the characters ρ_{p+q}^P.*

Proof. Let $\overline{Q}$ be the quotient of Q modulo the congruence determined by I. If the images of p and p' are Green's equivalent in $\overline{Q}$, then the stabilizers K_{p+q} and $K_{p'+q}$ coincide, as do the extensions to ρ_{p+q}^P and $\rho_{p'+q}^P$. Now apply Remark 4.5. □

Definition 16.3. Fix a binomial ideal $I \subset \Bbbk[Q]$, a monoid prime $P \subset Q$, and $w \in Q$.

1. The *testimony* of w at P is its set $T_P(w)$ of P-cover extension characters.

2. The testimony $T_P(w)$ is *suspicious* if the intersection of the corresponding mesoprimes equals the P-mesoprime I_w^P of I at w; that is, if $I_w^P = \bigcap_{\rho \in T_P(w)} I_{\rho,P}$.
3. A *false witness* is an I-witness w for P whose testimony at P is suspicious.
4. An I-witness that is not false is a *character witness*.

Remark 16.4. For algebraically closed $\Bbbk = \overline{\Bbbk}$, Definition 16.3.4 becomes transparent, as follows. Minimal primary decompositions of mesoprimes $I_{\rho,P}$ (Proposition 11.10) are easy and canonical in that case: every saturated finite extension of ρ appears exactly once. A finite intersection of mesoprimes $I_{\sigma,P}$, each containing $I_{\rho,P}$, equals $I_{\rho,P}$ when, among all of the saturated finite extensions of the characters σ, every saturated finite extension of ρ appears at least once. A character witness for P with associated mesoprime $I_{\rho,P}$ is a witness in possession of a new character (a saturated finite extension) not present in its testimony. By the same token, a witness is false if it has no new characters to mention: the set of characters in its testimony is suspiciously complete.

The relation between the different types of witnesses from monoid land (key witnesses) and binomial land (character witnesses) is not as strong as one may hope. For example, a key witness can be a false witness (Example 16.5), and a character witness might not be a key witness (Example 16.6). It is also possible for a non-key witness to be a false witness (Example 16.7).

Example 16.5. Consider the ideal $I' = \langle x(z-1), y(z+1), z^2-1, x^2, y^2\rangle$ from Example 9.1 and let P be the monoid prime of $\mathbb{N}^3$ such that $\mathfrak{m}_P = \langle x, y\rangle$. Then $0 \in \mathbb{N}^3$ is a key I'-witness for P that is a false I'-witness: the P-mesoprimes at the P-covers of 0 are $\langle z-1\rangle$ and $\langle z+1\rangle$, whose characters form the complete set of saturated finite extensions of the character for $\langle z^2-1\rangle$. The testimony is suspicious because $\langle z-1\rangle \cap \langle z+1\rangle = \langle z^2-1\rangle$. In contrast, $0 \in \mathbb{N}^3$ is a character I-witness for P, where the ideal $I = \langle x(z-1), y(z-1), z^2-1, x^2, xy, y^2\rangle$ induces the same congruence as I'.

Example 16.6. In Definition 16.3, the intersection of the mesoprimes is the analogue of intersecting the kernels of the cover morphisms in Definition 4.7. The necessity of allowing all (non-key) witnesses as potential character witnesses stems from the phenomenon in Example 2.22 (the common refinement of the congruences induced by $\langle x-1\rangle$ and $\langle y-1\rangle$ is trivial whereas the intersection of these ideals not) but is better illustrated by Example 4.10.3. The ideal $\langle x^2-xy, y^2-xy, x(z-1), y(w-1)\rangle$ there induces the same congruence $\sim$ as the bigger ideal $I = \langle x^2, xy, y^2, x(z-1), y(w-1)\rangle$ as per Theorem 9.12. The P-prime congruence at the character I-witness $0 \in \mathbb{N}^4$ for $P = \langle e_x, e_y\rangle$ is trivial because it equals the common refinement of the congruences induced by $\langle z-1\rangle$ and $\langle w-1\rangle$. This trivial P-prime congruence at 0 indicates a total lack of binomials in the $\overline{Q}$-degree 0 part of the intersection $\langle z-1, x^2, y\rangle \cap \langle w-1, x, y^2\rangle$, but this lack is accompanied by non-binomial elements. A third intersectand, namely the prime ideal $\langle x, y\rangle$ itself, is required to enforce binomiality.

In terms of Definition 16.3, the testimony consists entirely of saturated but infinite extensions of the character of I_P at $0 \in \mathbb{N}^4$. Therefore no saturated finite extensions occur, in the sense of Remark 16.4, making $0 \in \mathbb{N}^4$ a rather strong character I-witness, even though it is not a key witness for the congruence induced by I.

Example 16.7. Set $I = \langle w^6 - 1, x(w^2 - 1), y(w^3 - 1), z(w^3 + 1)\rangle \subset \Bbbk[x, y, z, w]$ and let P be the monoid prime of $\mathbb{N}^4$ such that $\mathfrak{m}_P = \langle x, y, z\rangle$. Then $0 \in \mathbb{N}^4$ is an I-witness because the congruence induced by its P-mesoprime $\langle w^6 - 1\rangle$ changes at its P-covers, whose P-mesoprimes are $\langle w^2 - 1\rangle$, $\langle w^3 - 1\rangle$, and $\langle w^3 + 1\rangle$, corresponding to x, y, and z, respectively. The congruences induced by $\langle w^3 - 1\rangle$ and $\langle w^3 + 1\rangle$ coincide, but they are incompatible with the one induced by $\langle w^2 - 1\rangle$; the only elements along the w-axis joined to 0 under the kernels of all three cover morphisms at P are the multiples of 6. Therefore $0 \in \mathbb{N}^4$ is not a key witness. However, it is still a false witness, because $\langle w^6 - 1\rangle = \langle w^2 - 1\rangle \cap \langle w^3 - 1\rangle \cap \langle w^3 + 1\rangle$ exhibits its suspicious testimony.

Definition 16.8. Fix a binomial ideal $I \subseteq \Bbbk[Q]$ in a finitely generated commutative monoid algebra over a field $\Bbbk$. A mesoprimary decomposition of I is *characteristic* if every J-witness for every mesoprimary component J is a character I-witness.

Next comes the true analogue of Theorem 8.4, closer in spirit than even Theorem 13.5, because we take pains here to eliminate redundancy systematically. It is an analogue rather than an arithmetization because the eliminated witnesses are different here than in the combinatorial case, as demonstrated by the previous examples.

Theorem 16.9. *Fix a finitely generated commutative monoid Q and a field $\Bbbk$. Every binomial ideal $I \subseteq \Bbbk[Q]$ admits a characteristic mesoprimary decomposition. In particular, I is the intersection of the coprincipal ideals cogenerated by its character witnesses.*

Equivalently, in the coprincipal decomposition from Theorem 13.5, the components for false witnesses can be thrown out (with their testimony).

Proof. For a witness $w \in Q$ consider a P-cover $p + w$. The sum $W^P_{w+p}(I) + M^P_w(I)$ of the coprincipal component of I cogenerated by $w + p$ at P plus the monomial ideal cogenerated by w along P is a coprincipal ideal of $\Bbbk[Q]$. Like $W^P_w(I)$ itself, this sum is cogenerated by w along P, but instead of having the same associated mesoprime I^P_w as does $W^P_w(I)$, the sum has associated mesoprime I^P_{w+p}. Equivalently, if $I^P_{w+p} = I_{\sigma_p,P}$, then $W^P_{w+p}(I) + M^P_w(I) = W^P_w(I) + I_{\sigma_p}$. This ideal is graded by the quotient of Q_P/G_P modulo the congruence induced on it by $W^P_w(I)$. Working in that grading and monomially localizing along P, it follows that

$$\bigcap_{p\in P} \big(W^P_{w+p}(I) + M^P_w(I)\big) = \bigcap_{p\in P} \big(W^P_w(I) + I_{\sigma_p}\big) = W^P_w(I) + \bigcap_{p\in P} I_{\sigma_p} \supseteq W^P_w(I);$$

see Proposition 15.1 and its proof.

Now assume that w is a false witness. That condition precisely guarantees that the containment at the end of the display is equality. But $W_w^P(I)$ already contains $M_w^P(I)$ by definition, so surely $W_w^P(I) \supseteq \bigcap_{p\in P} W_{w+p}^P(I)$.

It remains only to show that for each cover $q = w + p$ there is a witness $a + q$ for a monoid prime $P' \subseteq P$ satisfying $W_q^P(I) \supseteq W_{a+q}^{P'}(I)$. The witness $a + q$ is produced by Proposition 13.3 applied to Q_P, once the prime in the proposition is renamed P'. Now, $W_q^P(I) = W_{a+q}^P(I) + M_q^P(I)$, so it suffices to show that $W_{a+q}^P(I) \supseteq W_{a+q}^{P'}(I)$. This containment need not hold in the absence of hypotheses on $a+q$ (see Example 16.11), but in fact Proposition 13.3 also guarantees that the class of $a + q$ is the same under the two congruences on Q induced by $W_{a+q}^P(I)$ and $W_{a+q}^{P'}(I)$, by semifreeness of mesoprimary congruences (Corollary 6.6). Therefore the desired result is precisely the statement of Lemma 16.10, below, with the q there replaced by $a + q$. □

Lemma 16.10. *Fix a binomial ideal $I \subseteq \Bbbk[Q]$ and primes $P \supseteq P'$ of Q. If the class of q is the same under the two congruences on Q induced by the coprincipal components $W_q^P(I)$ and $W_q^{P'}(I)$ at P and P', then $W_q^P(I) \supseteq W_q^{P'}(I)$.*

Proof. The containment $P \supseteq P'$ immediately implies that $M_q^P(I) \supseteq M_q^{P'}(I)$. The coprincipal component $W_q^P(I)$ can be equivalently described as $M_q^P(I)$ plus the preimage in $\Bbbk[Q]$ of $I_P + I_\rho \subseteq \Bbbk[Q]_P$, where $\rho = \rho_q^P$ is the character of I_P at q, because $M_q^P(I)$ is closed under localization along P. The hypothesis on the class of q implies that $I_\rho = I_{\rho'}$, where $\rho' = \rho_q^{P'}$. Suppose that $f \in \Bbbk[Q]$ is a binomial involving two monomials outside of $M_q^P(I)$. It is enough to show that if the image of f under localization along P' lies in $I_{P'} + I_\rho$, then the image of f under localization along P already lies in $I_P + I_\rho$. Some monomial multiple f' of f in $\Bbbk[Q]_P$ has a term that is a (unit) monomial multiple of $\mathbf{t}^q$ in $\Bbbk[Q]_P$. By definition of ρ, the element f' lies in $I_P + I_\rho$ if and only if f does. But for the same reason—and that fact that a (unit) multiple in $\Bbbk[Q]_P$ is also a unit multiple in $\Bbbk[Q]_{P'}$—the element f' lies in $I_{P'} + I_\rho$ if and only if f does. □

Example 16.11. Fix $I = \langle xz - yz\rangle \subset \Bbbk[x, y, z]$ with $\mathfrak{m}_P = \langle x, y, z\rangle$ and $\mathfrak{m}_{P'} = \langle z\rangle$. Set $\mathbf{t}^q = yz$. Then $M_q^P(I) = \langle x^2, xy, y^2, z^2\rangle$ and $I_\rho = 0$ for the character $\rho = \rho_q^P$, so

$$W_q^P(I) = I + M_q^P(I) = \langle xz - yz, x^2, xy, y^2, z^2\rangle,$$

while $M_q^{P'}(I) = \langle z^2\rangle$ and $I_\rho = \langle x - y\rangle$ for the character $\rho = \rho_q^{P'}$, so

$$W_q^{P'}(I) = I + \langle z^2\rangle + \langle x - y\rangle = \langle x - y, z^2\rangle.$$

Although $W_q^P(I)$ has more monomials, it fails to contain the binomial $x-y \in W_q^{P'}(I)$. In general, the ideals $W_q^P(I)$ and $W_q^{P'}(I)$ are incomparable because $W_q^P(I)$ contains more monomials, but $W_q^{P'}(I)$ contains more binomials along the local unit group $G_{P'}$.

Finally, here is the binomial ideal analogue of Corollary 8.10.

Corollary 16.12. *Fix a finitely generated commutative monoid Q and a field $\Bbbk$. Every binomial ideal in the monoid algebra $\Bbbk[Q]$ admits a characteristic mesoprimary decomposition with one component per associated mesoprime.*

Proof. The P-mesoprimary component of I cogenerated by the character I-witnesses for P has a coprincipal decomposition whose components are the coprincipal components of I cogenerated by its character I-witnesses by Proposition 12.17. Taken together over all primes P, the intersection of these is I by Theorem 16.9. □

We make no claim that one needs every character witness in the arithmetic setting, just as we make no claim that one needs every key witness in the combinatorial setting: the phenomenon in Example 8.7 lifts without trouble to the arithmetic setting (for instance unitally). In fact, it is possible that there is a systematic way of throwing out additional character witnesses beyond the false ones. Let us summarize this problem.

Question 16.13. *Are there redundant character witnesses? How about key witnesses?*

It is worth stressing: the issue is not whether certain witnesses are redundant in specific examples; the question is whether there are natural families of redundant witnesses, in the spirit of false witnesses for binomial ideals or non-key witnesses for congruences.

17. Open problems

Beyond the open problem in Question 16.13, the results of this paper raise other problems implicitly in the remarks, and still others that constitute future research directions beyond the scope of this paper. We collect some of these problems here.

17.1. **Intersections of binomial ideals.**

Problem 17.1. *Characterize when an intersection of binomial ideals is binomial.*

Problem 17.1 was originally posed by Eisenbud and Sturmfels [ES96, Problem 4.9], who answered it in the reduced situation [ES96, Theorem 4.1]. In our language, that theorem contains information about the associated prime ideals of the congruence induced by a radical binomial ideal. It is possible that the general case could reduce to the radical case, by considering what the congruence or the P-prime characters induced by the intersection could possibly look like at each monoid element. This type of consideration underlies the definition of character witness (Definition 16.3), where non-binomiality at specific monoid elements would otherwise occur, without specifically throwing in additional binomials, because of incompatibility of congruences or characters arising from covers.

As a stepping stone to a full answer to Problem 17.1, one might consider [ES96, Problem 6.6]: does intersecting the minimal primary components of a binomial ideal result in another binomial ideal?

17.2. **Choices of vertical coefficients.** Remarks 12.21 and 12.22 raise the following.

Problem 17.2. *Characterize the mesoprimary ideals that induce a fixed mesoprimary congruence with a fixed associated mesoprime. In particular, decide when the set of such mesoprimary ideals is nonempty.*

17.3. **Primary binomial ideals in positive characteristic.** Lack of knowledge concerning the combinatorics of primary binomial ideals in positive characteristic is an obstacle to characterization of irreducible binomial ideals (Remark 15.6), and it leaves us wondering whether our particular construction of binomial primary decomposition is combinatorially stronger than necessary (Remark 15.13). Here is the missing point.

Conjecture 17.3. *If* $\Bbbk$ *is algebraically closed of arbitrary characteristic, then every binomial primary ideal in the finitely generated monoid algebra* $\Bbbk[Q]$ *is mesoprimary.*

17.4. **Posets of mesoprimes.**

Problem 17.4. *Characterize the posets of associated prime congruences of primary congruences.*

The problem could have been stated for arbitrary congruences, but then every finite poset would be possible, because every finite poset occurs as the set of associated primes of a monomial ideal (this is a good exercise, but it follows from [Mil98]). Problem 17.4 is equivalent to characterizing posets of associated mesoprimes of unital cellular binomial ideals. Such posets always possess a unique minimal element, represented by the identity element of the finite partially ordered monoid of Green's classes in Lemma 2.19. When devising examples for the present paper, we often used a technique to "place" associated mesoprimes at desired locations, illustrated as follows.

Example 17.5. Let $\Delta \subsetneq \Gamma$ be simplicial complexes on $\{1, \ldots, n\}$ and consider the polynomial ring in $2n$ variables $S = \Bbbk[x_1, \ldots, x_n, y_1, \ldots, y_n]$. For any $A \in \Gamma \smallsetminus \Delta$ write $x_A := \prod_{i \in A} x_i$. Define

$$I_A = \langle x_A(y_i - 1) \mid i \in A\rangle \quad \text{and} \quad I_{\Gamma \smallsetminus \Delta} = \sum_{A \in \Gamma \smallsetminus \Delta} I_A + \langle x_i^2 \mid i = 1, \ldots, n\rangle \subset S.$$

The poset of associated mesoprimes of the cellular binomial ideal $I_{\Gamma \smallsetminus \Delta}$ is isomorphic to $(\Gamma \smallsetminus \Delta) \cup \{\varnothing\}$.

The construction in the previous example is fairly general, and one might hope that complete generality is possible (we did), but it is not: some posets do not occur.

Example 17.6. Set $\mathcal{P} = \big\{\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{123\}, \{124\}\big\}$, with the partial order being by inclusion. This poset $\mathcal{P}$ is not isomorphic to the poset of associated mesoprimes of any cellular binomial ideal. Indeed, if it was, then there would be witness monomials $\mathbf{t}_1$ and $\mathbf{t}_2$ for $\{1\}$ and $\{2\}$. By (a variant of) Proposition 13.3 there must be a witness for their join, but in $\mathcal{P}$ the incomparable elements $\{123\}$ and $\{124\}$ are both minimal over the join $\{1\} \vee \{2\}$.

In practice this problem will be about understanding what happens to the partial order on $\mathbb{N}^n$ when passing to a quotient and under the order-preserving map that assigns to a witness its associated prime congruence.

Remark 17.7. Definition 5.2 requires associated prime congruences to appear at key witnesses. If arbitrary witnesses were allowed, then an a priori different notion of associated prime congruence would have resulted. Indeed, although the P-prime congruence at an arbitrary witness for P agrees with the P-prime congruence at some key witness by Proposition 13.3, the key witness might be for a monoid prime that is smaller than P. This phenomenon does not occur for primary congruences, however, because they have only one associated monoid prime ideal. Thus Problem 17.4 would have the same answer if Definition 5.2 had allowed arbitrary witnesses.

Nonetheless, this line of thinking indicates that care must be taken in lifting Problem 17.4 to the arithmetic setting, where Definition 12.1 requires associated mesoprimes to appear at arbitrary witnesses, not at a subset of all witnesses. For instance, a P-mesoprime can be associated to an ideal even though it only appears at a false witness; this occurs in both Example 16.5 and Example 16.7. This idiosyncracy in the definition of associated mesoprime motivates a new definition.

Definition 17.8. An associated mesoprime of a binomial ideal I is *truly associated* if it is the P-mesoprime of I at a character I-witness for P.

Problem 17.9. *Characterize the posets of associated mesoprimes of cellular binomial ideals. Do the same for posets of truly associated mesoprimes.*

Remark 17.10. The family of posets referred to in (either version of) Problem 17.9 contains the family of posets in Problem 17.4 by Remark 17.7 applied to the case of unital binomial ideals.

17.5. **Mesoprimary decomposition of modules.** Grillet [Gri07] shows how subdirect decompositions of semigroups induce subdirect decompositions of sets acted on by semigroups; see Remark 2.2. In a similar vein, mesoprimary decomposition ought to extend to finitely generated monoid actions.

Problem 17.11. *Generalize mesoprimary decomposition of congruences to Q-modules.*

The generalization ought to parallel the manner in which ordinary primary decomposition of ideals in rings extends to primary decomposition of modules over rings. In the arithmetic setting of mesoprimary decomposition, however, even the first step of the extension requires thought.

Question 17.12. *What is a binomial module over a commutative monoid algebra?*

A good theory of such modules should yield the desired generalization.

Problem 17.13. *Extend mesoprimary decomposition to binomial $\Bbbk[Q]$-modules.*

17.6. **Homological invariants of binomial rings.** The combinatorics of the free commutative monoid $\mathbb{N}^n$ gives rise to formulas and constructions for all sorts of homological invariants involving monomial ideals—Betti numbers, Bass numbers, free resolutions, local cohomology, and so on—due to the $\mathbb{N}^n$-grading; see [MS05]. Gradings by more general affine semigroups yield formulas and constructions for local cohomology over affine semigroup rings (with maximal support [Ish87] as well as with more arbitrary monomial support [HM03, HM04]), and Betti numbers for toric ideals [Sta96, Theorem I.7.9], etc. Having identified the combinatorics controlling decompositions of binomial ideals, the way is open to generalize monomial homological algebra.

Question 17.14. *Do there exist combinatorial (that is, monoid-theoretic) formulas for local cohomology, Tor, and Ext involving binomial quotients of polynomial rings?*

Remark 17.15. In contrast, it is unclear to us whether combinatorial formulas for local cohomology with binomial support should exist, partly because of ill-behaved characteristic dependence; see [ILL$^+$07, Example 21.31].

As soon as there is some control over Betti tables, Boij–Söderberg theory [Flø11] enters the picture. There one decomposes the Betti table $\beta(M)$ of a module M over a polynomial ring S as a rational linear combination of certain *pure tables* π_d:

$$\beta(M) = \sum a_d \pi_d.$$

Question 17.16. *What combinatorics, if any, explains the coefficients a_d of $S/I_{\rho,P}$ as an S-module when $I_{\rho,P}$ is a mesoprime?*

Even the special case of Boij–Söderberg theory for toric ideals is currently open.

References

[AGHMR09] Leonard Adleman, Manoj Gopalkrishnan, Ming-Deh Huang, Pablo Moisset, and Dustin Reishus, *On the mathematics of the law of mass action*, SIAM Review, to appear, 2009.

[Alt00] Klaus Altmann, *The chain property for the associated primes of $\mathcal{A}$-graded ideals*, Math. Research Letters **7** (2000), 565–575.

[CC11] Alain Connes and Caterina Consani, *On the notion of geometry over* $\mathbb{F}_1$, J. Algebraic Geom. **20** (2011), 525–557.

[Dei05] Anton Deitmar, *Schemes over* $\mathbb{F}_1$, in Number fields and function fields—two parallel worlds, pages 87–100. Progr. Math. Vol. 239, Birkhäuser Boston, Boston, MA, 2005.

[Drb63] Karel Drbohlav, *On finitely generated commutative semigroups*, Comment. Math. Univ. Carolinae **4** (1963), 87–92.

[DMM09] Alicia Dickenstein, Laura Felicia Matusevich, and Ezra Miller *Combinatorics of binomial primary decomposition*, Mathematische Zeitschrift, 19 pages. DOI: 10.1007/s00209-009-0487-x

[DMM10] Alicia Dickenstein, Laura Felicia Matusevich and Ezra Miller, *Binomial D-modules*, Duke Math. J. **151**, no. 3 (2010), 385–429. arXiv:math.AG/0610353

[DSS09] Mathias Drton, Bernd Sturmfels, and Seth Sullivant, *Lectures on algebraic statistics*, Oberwolfach Seminars, vol. 39, Springer-Verlag, Berlin, 2009.

[ES96] David Eisenbud and Bernd Sturmfels, *Binomial ideals*, Duke Math. J. **84** (1996), no. 1, 1–45.

[Flø11] Gunnar Fløystad, *Boij–Söderberg theory: Introduction and survey*, preprint. arXiv: math.AC/1106.0381

[FS96] Klaus G. Fischer and Jay Shapiro, *Mixed matrices and binomial ideals*, J. Pure Appl. Algebra **113** (1996), no. 1, 39–54.

[GGZ87] I. M. Gelfand, M. I. Graev, and A. V. Zelevinsky, *Holonomic systems of equations and series of hypergeometric type*, Dokl. Akad. Nauk SSSR **295** (1987), no. 1, 14–19.

[GKZ89] I. M. Gelfand, A. V. Zelevinsky, and M. M. Kapranov, *Hypergeometric functions and toric varieties*, Funktsional. Anal. i Prilozhen. **23** (1989), no. 2, 12–26. Correction in ibid, **27** (1993), no. 4, 91.

[Gil84] Robert Gilmer, *Commutative semigroup rings*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1984.

[Gri75] Pierre Antoine Grillet, *Primary semigroups*, Michigan Math. J. **22** (1975), no. 4, 321–336.

[Gri01] Pierre A. Grillet, *Commutative semigroups*, Advances in Mathematics, Kluwer Academic Publishers, London, 2001.

[Gri07] Pierre Antoine Grillet, *Commutative Actions*, Acta Sci. Math. (Szeged) **73** (2007), 91–112.

[GMW09] Alan Guo, Ezra Miller, and Michael Weimerskirch, *Potential applications of commutative algebra to combinatorial game theory*, in Kommutative Algebra, Oberwolfach reports **22** (2009), pp. 23–26.

[GM10] Alan Guo and Ezra Miller, *Lattice point methods for combinatorial games*, Advances in Applied Mathematics **46** (2010), 363–378. doi:10.1016/j.aam.2010.10.004 arXiv:math.CO/ 0908.3473

[GM11] Alan Guo and Ezra Miller, *Algorithms for lattice games*, 12 pages, submitted, 2011.

[GS] Daniel R. Grayson and Michael E. Stillman, *Macaulay 2, a software system for research in algebraic geometry*, Available at `http://www.math.uiuc.edu/Macaulay2/`.

[HM03] David Helm and Ezra Miller, *Bass numbers of semigroup-graded local cohomology*, Pacific J. Math. **209**, no. 1 (2003), 41–66.

[HM04] David Helm and Ezra Miller, *Algorithms for graded injective resolutions and local cohomology over semigroup rings*, J. Symbolic Comput. **39** (2005), 373–395. arXiv:math.CO/0309256

[HHHKR10] Jürgen Herzog, Takayuki Hibi, Freyja Hreinsdóttir, Thomas Kahle, and Johannes Rauh, *Binomial edge ideals and conditional independence statements*, Advances in Applied Mathematics **45** (2010), no. 3, 317–333.

[HS00] Serkan Hoşten and Jay Shapiro, *Primary decomposition of lattice basis ideals*, J. Symbolic Comput. **29** (2000), no. 4-5, 625–639, Symbolic computation in algebra, analysis, and geometry (Berkeley, CA, 1998).

[Ish87] Masa-Nori Ishida, *The local cohomology groups of an affine semigroup ring*, Algebraic geometry and commutative algebra in Honor of Masayaoshi Nagata, Vol. I, Kinokuniya, Tokyo, 1987, pp. 141– 153.

[ILL+07] Srikanth Iyengar, Graham Leuschke, Anton Leykin, Claudia Miller, Ezra Miller, Anurag Singh, and Uli Walther, *Twenty-four hours of local cohomology*, Graduate Studies in Mathematics, vol. 87, American Mathematical Society, Providence, RI, 2007.

[Kah10] Thomas Kahle, *Decompositions of Binomial Ideals*, AISM, **62** (2010), no 4, 727–745.

[Kah11] Thomas Kahle, *Binomials.m2 - Binomial ideals in Macaulay 2*, Available at `http://www.thomas-kahle.de/bpd`.

[MMW05] Laura Felicia Matusevich, Ezra Miller, and Uli Walther, *Homological methods for hypergeometric families*, J. Amer. Math. Soc. **18** (2005), no. 4, 919–941.

[Mil98] Ezra Miller, *Multiplicities of ideals in noetherian rings*, Beiträge zur Alg. und Geom. **39** (1998), no. 1, 47–51.

[Mil02] Ezra Miller, *Cohen–Macaulay quotients of normal semigroup rings via irreducible resolutions*, Math. Res. Lett. **9** (2002), no. 1, 117–128.

[Mil11a] Ezra Miller, *Theory and applications of lattice point methods for binomial ideals*, in Combinatorial Aspects of Commutative Algebra and Algebraic Geometry, Proceedings of the Abel Symposium held at Voss, Norway, 1–4 June 2009, Springer, 2011, pp. 99–154.

[Mil11b] Ezra Miller, *Affine stratifications from finite misère quotients*, submitted, 2011. arXiv: math.CO/1009.2199v2

[MS05] Ezra Miller and Bernd Sturmfels, *Combinatorial commutative algebra*, Graduate Texts in Mathematics, vol. 227, Springer-Verlag, New York, 2005.

[Noe21] Emmy Noether, *Idealtheorie in Ringbereichen*, Mathematische Annalen **83** (1921), no. 1, 24–66.

[Oje10] Ignacio Ojeda, *Binomial canonical decomposition of binomial ideals.* to appear in Comm. Algebra. arXiv:1003.1701

[Ort59] Vicente Ortiz, *Sur une certaine décomposition canonique d'un idéal en intersection d'idéaux primaires dans un anneau noethérien commutatif*, C. R. Acad. Sci. Paris **248** (1959), 3385–3387.

[Pla05] Thane E. Plambeck, *Taming the wild in impartial combinatorial games*, Integers **5** (2005), G5, 36 pp. (electronic)

[PS07] Thane E. Plambeck and Aaron N. Siegel, *Misère quotients for impartial games*, J. Combin. Theory, Ser. A **115** (2008), 593–622. arXiv:math.CO/0609825v5

[Ree40] David Rees, *On semi-groups*, Proc. Cambridge Philos. Soc. **36**, (1940), 387–400.

[SS10] Anne Shiu and Bernd Sturmfels, *Siphons in chemical reaction networks*, Bull. Math. Biol. **72** (2010), no. 6, 1448–1463.

[Sta96] Richard P. Stanley, *Combinatorics and commutative algebra*, second ed., Progress in Mathematics Vol. 41, Birkhäuser, Boston, MA, 1996.

[Vas98] Wolmer V. Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, Algorithms and Computation in Mathematics Vol. 2, Springer-Verlag, Berlin, 1998.

[Zie95] Günter M. Ziegler, *Lectures on polytopes*, Graduate Texts in Mathematics Vol. 152, Springer-Verlag, New York, 1995.

Isaac Newton Institute, 20 Clarkson Road, Cambridge, CB3 0EH, UK
E-mail address: `www.thomas-kahle.de`

Mathematics Department, Duke University, Durham, NC 27708
E-mail address: `www.math.duke.edu/~ezra`