Regular Chains (Theory)

Steffen Marcus, Marc Moreno Maza, Éric Schost and Paul Vrbik

April 12, 2011

Abstract

A self contained survey of the theory of regular chains.

Example Bank

Example 1 (From [**?**])**.** In this example, we define the ITERATED INITIALS of a polynomial $p \in \mathbf{P}_n$. These form a triangular set $\mathbf{iter}(p) \subset \mathbf{P}_n$ defined recursively by the rule $\mathbf{iter}(p) = \{p\} \bigcup \mathbf{iter}(\mathbf{init}(p))$ and $\mathbf{iter}(p) = \emptyset$ for $p \in k$. The polynomial $p = (x_2x_3 - 1)x_4 + x_2^2$ has iterated initials $\mathbf{iter}(p) = \{x_2, x_2x_3 - 1, p\}$.

Example 2 (From [**?**])**.** Let $n \geq 3$ and assume $k = \mathbb{Q}$ so that our polynomials are defined over the rational numbers. Define polynomials

$$\begin{aligned} p_1 &= x_1^4 - 5x_1^2 + 6, \\ p_2 &= (x_1^2 - 2)x_2^2 + (-2x_1^3 + 4x_1)x_2 + x_1^4 - 2x_1^2, \\ p_3 &= (x_1^2 - 2)x_3^4 + (x_2 - x_1)x_3^3 + (1 - x_1)x_3 + 1, \end{aligned}$$

and set $T_1 = \{p_1\}$ and $T_2 = \{p_1, p_2\}$. These are both triangular sets, but T_2 is not a regular chain. Consider the primary decomposition

$$\langle T_2 \rangle = \left\langle x_1^2 - 3, (x_2 - x_1)^2 \right\rangle \cap \left\langle x_1^2 - 2 \right\rangle$$

with respective associated primes $P_1 = \langle x_1^2 - 3, (x_2 - x_1) \rangle$ and $P_2 = \langle x_1^2 - 2 \rangle$. Notice also that $\langle x_1^2 - 2 \rangle$ is an associated prime of $\langle p_1 \rangle$. Since $\mathbf{init}(p_2)$ vanishies with respect to this ideal, T_2 is not a regular chain. It is straightforward to see how T_2 can be encoded by regular chains, since both $\{x_1^2 - 3, (x_2 - x_1)^2\}$ and $\{x_1^2 - 2\}$ are regular chains and P_1 and P_2 are the respective radicals of their saturation ideals. Finally, notice that $T_3 = \{x_1^2 - 3, (x_2 - x_1)^2, p_3\}$ is also a regular chain, and $\sqrt{\mathbf{Sat}(T_3)} = \langle x_1^2 - 3, x_2 - x_1, (x_3^2 - x_1)(x_3^2 + 1) \rangle$.

Example 3 (From [**?**])**.** Let $n = 4$ and take $T = \{x_1x_3 + x_2, x_2x_4 + x_1\}$. Then

$$\langle T \rangle = \langle x_1, x_2 \rangle \cap \langle x_1x_3 + x_2, -x_3x_4 + 1 \rangle ,$$

whereas

$$\mathbf{Sat}(T) = \langle x_1x_3 + x_2, -x_3x_4 + 1 \rangle ,$$

This is an example where $\mathbf{Sat}(T)$ is strictly larger than $\langle T \rangle$.

Example 4 (From [?])**.** Let $n = 3$ and set $T_1 = \{x_1x_2\}$ and $T_2 = \{x_1x_2, x_1x_3\}$. Then T_1 and T_2 are regular chains with $\mathbf{Sat}(T_1) = \langle x_2\rangle$ and $\mathbf{Sat}(T_2) = \langle x_2, x_3\rangle$.

Commutative Algebra

I am following [?] for most, if not all, of this. It's a text I am learning to love btw.

Notation. Denote by A an arbitrary commutative Noetherian ring. We will usually denote ideals in A by $I, J, \ldots$ which, since A is Noetherian, are finitely generated.

Definition 1 (ideal quotient)**.** Let I, J be ideals in A. The IDEAL QUOTIENT of I by J is the ideal

$$I : J = \{a \in A : aJ \subset I\}.$$

Definition 2. An element $f \in A$ is regular modulo I if its canonical image in the quotient A/I is a regular element (meaning a nonzerodivisor).

Definition 3 (saturation)**.** Let I, J be ideals in A. The SATURATION of I with respect to J is the ideal

$$I : J^\infty = \bigcup_{n\geq 1}(I : J^n).$$

Remark 1. The ideal quotient gets its name because, for K an ideal, $IJ \subset K \Leftrightarrow I \subset (K : J)$. The saturation ideal gets its name from the notion of saturation for the localization of rings by multiplicative sets. That is, for S a multiplicative set of A, the localization of I at S is the set

$$_SI = \{a \in A | \exists s \in S, sa \in I\}.$$

and this set is sometimes also called the saturation of the ideal I with respect to S. When S is finitely generated by elements $s_1, \ldots, s_n$, and we set $f = \prod s_i$, then $_SI = I : f^\infty$.

Proposition 1. *The element $f \in A$ is regular modulo an ideal I if and only if*

$$I : f = I \text{ or } I : f^\infty = I.$$

Proof. Let $\bar{f}$ be the canonical image of f in $\mathbf{A}/I$. We first assume $I : f = I$ or $I : f^\infty = I$. If $I : f = I$, then the elements $a \in A$ such that $af \in I$ are precisely the elements of I. Take $a \in A$ such that $\overline{af} = \bar{0}$ in A/I. This is equivalent to $af \in I$ in A, so this part of this direction is immediate. If we don't have $I : f = I$, we instead have $I : f^\infty = I$. Again take $a \in A$ so that $\overline{af} = \overline{0}$. Then $af \in I$, and we need only multiply by a sufficiently high enough power of f to get $a \in I$. For the other direction, assume $\bar{f}$ is not a zero-divisor. Then $af^n \in I$ implies $\overline{af^n} = \bar{0}$, which in turn implies $\overline{af^{n-1}} = \bar{0}$. Continue reducing the exponent of $\bar{f}$ until we get $a \in I$. □

Proposition 2. *The ideal $I : J^\infty$ removes from any primary decomposition of I all P_i-primary components for whom J intersects P_i. In other words, $I : J^\infty$ is the intersection of the primary components for whom $P_i \cap J = \emptyset$.*

Proof. Given any primary ideal Q in A, $Q : J^\infty = Q$ if $J \cap \sqrt{Q} = \emptyset$ and $Q : J^\infty = A$ if $J \cap \sqrt{Q} \neq \emptyset$. (expand on this?) □

Definition 4 (annihilator)**.** For a nonzero $m \in A/I$, define the ANNIHILATOR of m to be the set

$$0 : m = \{a \in A | \overline{a}m = 0\}.$$

Similarly, define the annihilator of $B \subset A/I$ to be the set $0 : B = \left\{a \in A \,\middle|\, \overline{a}B = 0\right\}$.

Definition 5 (associated prime)**.** We say that a prime ideal P in A is an ASSOCIATED PRIME of the ideal I (or simply, $P \in \mathbf{Ass}_A(I)$) when there is an $m \in A/I$ such that $P = 0 : m$. That is,

$$P \in \mathbf{Ass}_A(I) \iff \exists m \in A/I \text{ s.t. } P = \left\{a \in A \,\middle|\, \overline{a}m = 0\right\}.$$

Definition 6 (primary)**.** An ideal I is said to be PRIMARY if $\mathbf{Ass}_A(I) = P$ contains only one prime ideal. We may refer to I as P-primary in order to differentiate between primary ideals with different associated primes.

Remark 2. Since A is noetherian, $\mathbf{Ass}_A(I)$ will always be a finite set. The minimal primes of I are a subset of the associated primes, and those that are not minimal are called embedded primes of I. In other words, an ideal $P \in \mathbf{Ass}_A(I)$ is an embedded prime of I if it properly contains another element of $\mathbf{Ass}_A(I)$. Also, the following gives an interesting connection between associated ideals and quotient ideals:

$$P \in \mathbf{Ass}_A(I) \Leftrightarrow I : (I : P) \subset P.$$

The intersection of two P-primary ideals is again P-primary.

Definition 7 (irreducible ideal)**.** An ideal I is IRREDUCIBLE if it is not the intersection of two other ideals in which it is properly contained.

Proposition 3.

Theorem 1 (Lasker-Noether theorem [**?**], [**?**], Theorem 3.1.1)**.** *Every ideal is a finite intersection of irreducible ideals. Every irreducible ideal is primary. Thus any ideal I can be represented as a finite intersection of primary ideals*

$$I = J_1 \cap \cdots \cap J_n.$$

Such a representation is not necessarily unique, but can be minimized by removing redundant primary ideals and intersecting P-primary ideals for each associated prime P. This forms a minimal primary decomposition with a uniquely defined number of components, one for each associated prime ideal.

Definition 8 (dimension)**.** We define the *dimension* of A to be the supremum of the lengths of chains of prime ideals in A. The dimension of I is then defined to be the dimension of the quotient ring R/I. When I is prime, we can localize away from I and define the codimension of I to be dimension of the local ring A_I (when I is not prime, just take the minimum codimension over all primes containing I).

Definition 9 (unmixed and equidimensional)**.** We call I *equidimensional* if all its minimal primes have equal codimension. Further, we call I *unmixed dimensional* if it is equidimensional and has no embedded primes, that is, all associated primes are the same codimension.

Definition 10. A REGULAR SEQUENCE on A is a sequence of elements $a_1, \ldots, a_r \in A$ such that the ideal $\langle a_1, \ldots, a_r \rangle$ is proper and for each i the canonical image of a_{i+1} in $A/\langle a_1, \ldots, a_i \rangle$ is a nonzerodivisor.

Remark 3. Assume I is an ideal of codimension m. What we would like is not only a minimal primary decomposition $I = J_1 \cap \cdots \cap J_n$, but even more, such a composition grouped into equidimensional collections of the primary ideals. Implicitly, this is not complicated. Given any minimal primary decomposition, intersect those primary components of the same codimension, producing equidimensional ideals I_i of codimension i. In general, we can produce a representation

$$I = I_m \cap \cdots \cap I_{\dim(A)}.$$

Using some (rather complicated) homological algebra and local cohomology, this can be accomplished explicitly rather than implicitly in any Gorenstein ring A by reversing the process and first computing a decomposition into equidimensional components l_i. The process is as follows:

1. Decompose I into equidimensional ideals $I = I_m \cap \cdots \cap I_{\dim(A)}$ whose associated primes are also associated primes of I.

2. Decompose the corresponding radicals into minimal primary decompositions

$$\sqrt{I_i} = \bigcap_j J_{i,j}.$$

3. Set $K_{i,j} = I_i : (I_i : J_{i,j}^{\infty})$. Then the desired minimal primary decomposition is

$$I = \bigcap_{i,j} K_{i,j}.$$

The major difficulty is explicitly computing the I_i in step 1. This is solved by using regular systems, in particular, by the following criterion for unmixedness:

Proposition 4 ([**?**] Corollary 3.2.2)**.** *Assume A is Gorenstein and I is codimension m, with $\mathbf{x} = \{x_1, \ldots, x_m\} \subset I$. Then I is unmixed dimensional if and only if $I = \langle \mathbf{x} \rangle : (\langle \mathbf{x} \rangle : I)$.*

1 Introduction

We start by asking a rudimentary question:

Question 1. What does it mean to solve a system of polynomials? To be more precise, let $\mathbf{k}$ be a field, and denote by K it's algebraic closure. Given a subset $F = \{f_0, \ldots, f_m\}$ of $\mathbf{k}[x_1, \ldots, x_n]$, what does it mean to "usefully" encode the set of points in K^n where the f_i's vanish simultaneously?

Perhaps, as in algebraic geometry, one would be satisfied to decompose the variety

$$\mathbf{V}(F) = \left\{ p \in K^n \;\middle|\; f_i(p) = 0, \forall f_i \in F \right\}$$

into its irreducible components. However (in addition to being computationally infeasible []), this decomposition may not help with the actual construction of points in the affine space.

Switching to the algebraic approach from the geometric. We may try to manipulate $\langle F \rangle$ directly, by say, finding its Gröbner basis with respect to the lexical ordering. Elimination theory ensures that we get another, equivalent ideal $\langle G \rangle = \langle F \rangle$ with a crucial property. The generators of $\langle g_1, \ldots, g_n \rangle = \langle G \rangle$ have mutually different largest variable (e.g. $g_1 \in \mathbf{k}[x_1], g_2 \in \mathbf{k}[x_1, x_2], \ldots$) meaning (in the "nicest" zero-dimensional case) that we can solve for x_1, back substitute and solve for x_2, and repeat for all x_i. Of course complications arise when the solutions are of higher dimension; but surely this is an attractive quality for our "useful encoding".

2 First Examples

Check out the example on the second page of [**?**]. That is a really nice example, and sort of a baby of the type of examples I am thinking about for this section.

3 Algebraic Preliminaries

Remark 4. among all the obvious things for this section, I am particularly interested in building a clear understanding of the equidimensionality result of the theory. In particular, we should be able to explain how saturations are unmixed dimensional (not just equidimensional), and what that ends up meaning. We should also try to build an algebraic understanding of Mark's definition of 'strongly equidimensional', which is something I still haven't found in the literature.

4 Regular Chains

4.1 Triangular Sets

Let $\mathbf{k}$ be a field, and $x_n \succ x_{n-1} \succ \cdots \succ x_1$ be n ordered variables over the monomial ordering $\succ$. For each $i = 1, \ldots, n$, define $\mathbf{P}_i = \mathbf{k}[x_1, \ldots, x_n]$ to be the ring of multivariate polynomials in the variables $x_1, \ldots, x_n$ with coefficients in $\mathbf{k}$ (we also set $\mathbf{P}_0 = \mathbf{k}$). Let $p \in \mathbf{P}_n$ be a non-constant polynomial.

Let $\mathbf{mvar}(p)$ denote the $\succ$-largest x_i such that $\mathbf{deg}(p, x_i) > 0$ (which, for the purposes of this paper, will always correspond to the $>$-largest i).

Let us call such a set of polynomials with mutually different largest variable a TRIANGULAR SET.

Definition 11 (Triangular-Set)**.** A subset T of $\mathbf{P}_n$ is a TRIANGULAR SET if there is no $t \in T$ such that $t \in \mathbf{k}$. And, for all pairs, $p, q \in T$ with $p \neq q$ we have $\mathbf{mvar}(p) \neq \mathbf{mvar}(q)$.

Example 5. $T = \{x_1 - x - 1^2, x_2^2 - x_1, x_1 x_3^2 - 2x_2 x_3 + 1, (x_2 x_3 - 1)x_4 + x_2^2\} \subset \mathbf{P}_4$ is a triangular set because

$$\begin{aligned} (x_2 x_3 - 1)x_4 + x_2^2 &\in \mathbf{k}[x_1, x_2, x_3, x_4] \\ x_1 x_3^2 - 2x_2 x_3 + 1 &\in \mathbf{k}[x_1, x_2, x_3] \\ x_2^2 - x_1 &\in \mathbf{k}[x_1, x_2] \\ x_1 - x - 1^2 &\in \mathbf{k}[x_1] \end{aligned}$$

(the triangular shape of the polynomial rings as they are written above was the inspiration for the name "triangular" set).

So, addressing the original question. Suppose that we can take any variety $\mathbf{V}(F)$ and find *some* (i.e. non-unique) set of triangular sets $\{T_1, \ldots, T_k\}$ such that $\mathbf{V}(T_1) \cup \cdots \cup \mathbf{V}(T_k) = \mathbf{V}(F)$. This a good start but is still (quite) incomplete. Consider the following example.

Example 6. Example where back substitution breaks everything.

Clearly, we need some additional restrictions to get the "nice" back substitution we desire (see §**??**).

4.2 Existence of Triangular Decompositions

Before we try to impose special behaviour of our triangular decompositions it is prudent to investigate that they actually exist for all arbitrary (finite) subsets of $\mathbf{P}_n$.

Theorem 2. *For any finite subset F of $\mathbf{P}_n$ there exists triangular sets $T_1, \ldots, T_n$ such that*

$$\mathbf{V}(F) = \mathbf{V}(T_1) \cup \cdots \cup \mathbf{V}(T_n).$$

Proof. There is some (super complicated) constructional proof by Wu, or by Changbo, or by MMM in MEGA. □

4.3 Nice Properties of Triangular Sets

Informal breakdown

1. Each T_i encodes a (strongly?) equidimensional subset of $\mathbf{V}(F)$ and all the components of $\mathbf{V}(F)$ get encoded (trivial by existence).
2. the set of things that reduce to zero modulo T is $\left\{p \in \mathbf{P}_N \,\middle|\, \text{prem}(p, T) = 0\right\}$ and is also a subset of $\text{sat}(T)$.
3. Euclids algorithm in n-dimensions

4.4 "Well-behaved" Back Substitution

Informal breakdown

1. Initially reduced triangular sets make sure leading coefficients don't vanish
   (a) need pseudo-remainders
2. $\sqrt{\langle T \rangle} : h = \sqrt{\text{sat}(T)}$, h is the pr
3. The "regular zeros of T" $(\mathbf{V}(T) - \mathbf{V}(h))$.

The problem with Example **??** is that the "leading coefficient" of $f_?$ vanishes. This section introduces the necessary restrictions on triangular sets to eliminate this "degenerate" case, towards our ultimate goal of "usefully" encoding the solution space of an arbitrary F.

Definition 12 (Initial)**.** For a polynomial $p \in \mathbf{k}[x_1, \ldots, x_m]$ with $\mathbf{mvar}(p) = x_m$, we denote $\mathbf{init}(p)$ to be the leading coefficient (in the usual sense) of p when it is regarded as a univariate polynomial from $(\mathbf{k}[x_1, \ldots, x_{m-1}])[x_m]$ (i.e. a polynomial in x_m with coefficients from $\mathbf{k}[x_1, \ldots, x_{m-1}]$).

Definition 13 (Regular Zero)**.** A point $a \in \mathbf{V}(T)$ is called a REGULAR ZERO of T if for every $p \in T$ we have that $\mathbf{init}(p)$ does not vanish when evaluated at a. Denote by $\mathbf{W}(T)$ the set of regular zeroes.

Example 7. Of an initial.

We can guarantee an initial will not vanish by moving to some residue ring where that initial is regular (i.e. not a zero divisor). Alternatively, this condition is equivalent to ensuring our polynomials are monic in some special field of fractions—but, more on this later. First, recall the following definitions.

Remark 5. I think the best idea of what we mean by well-behaved back substitution is as it is described in [**?**]. That is, for any algebraic variable x_i, the extension of generic zeros from $T^-_{x_i}$ to $T^-_{x_{i+1}}$. In particular, the way Hubert describes it, the definition of a regular chain gives us exactly the property that all associated primes of $\mathbf{Sat}(T^-_{x_{i+1}})$ are given exactly as the "cutbacks" of the associated primes of $\mathbf{Sat}(T)$. Said better, $\mathrm{Ass}(\mathbf{Sat}(T^-_{x_{i+1}}) = \{P \cap \mathbf{P}_i | P \in \mathrm{Ass}(\mathbf{Sat}(T))\}$. The important statements are Proposition 5.8 and examples 4.6 and 5.9 in Hubert's paper.

4.5 Regular Chains

5 Primitive Regular Chains

6 Decompositions

6.1 On Kalkbrenner Decompositions

6.2 On Lazard Decompositions

7 Other Applications