Primary Decomposition Project
Topics in Ring theory final project

Andrew Ma
May 7, 2014

Primary decomposition of ideals is the analog of prime factorization for integers and it is used as a tool for computations. In these notes I compiled most of the basic definitions and theorems (without proof) for the theory of primary decomposition of ideals that I found from online lecture notes. Additionally I mention the connections between primary decompositions and geometry and state the existence of algorithms for computing primary decompositions. These notes should only be considered an informal survey of this tool.

It should be added that these notes only deal with the theory for ideals. There is a theory of primary decomposition developed for Modules working more with the set of Associated Primes - which in my opinion makes the proofs much easier to follow. Please see Commutative Algebra by David Eisenbud [5] for an excellent presentation of this.

1 Primary Ideals and Primary Decomposition of Ideals

1.1 Basic Information on Primary Ideals

The following definitions come from Washington University online lecture notes [1]. Let $R$ be a commutative ring.

Definition 1. A proper ideal $I \in R$ is called primary if for any $xy \in I$ we have either $x \in I$ or $y \in \sqrt{I}$ (remark: $y \in \sqrt{I} \iff y^n \in I$ for some $n > 0$).

Lemma 1. An ideal $I$ is primary if and only if $R/I \neq 0$ and any zero divisor in $R/I$ is nilpotent.

Lemma 2. All prime ideals are primary.

Lemma 3. For a primary ideal $I$, $\sqrt{I}$ is prime.

Definition 2. If $I$ is a primary ideal such that $\sqrt{I} = p$ then $I$ is called $p$–primary.

Remark 1. Be careful
1. For a prime ideal, \( p^n \) might not be primary.

2. \( I \) being \( p \)-primary does not imply \( I = p^n \).

**Proposition 1.** If \( m \) is a maximal ideal then \( m^n \) is \( m \)-primary.

The next example and remark come from the Brandeis University [2].

**Example 1.** For \( R = \mathbb{Z} \), (4) is a primary ideal with \( \sqrt{(4)} = (2) \). Hence (4) is 2-primary.

This example is from Cheng-Chung University online lecture notes [3].

**Example 2.** Let \( R = k[x, y] \) and \( I = (x^2, y) \). Now \( \sqrt{I} = (x, y) \) because in general for ideals \( I, J \) there is the identity

\[
\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}
\]

Hence, \( I \) is an \((x, y)\)-primary ideal because \((x, y)\) is maximal ideal of \( R \).

**Lemma 4.** If \( I_1, \ldots, I_n \) are \( p \)-primary ideals then \( \bigcap_1^n I_i \) is a \( p \)-primary ideal.

**Example 3.** If \( R = \mathbb{Z} \) then an ideal \((a)\) is primary if and only if \( a = p^n \) for some prime \( p \). Further any ideal \( I \subset R \) may be written as the "product" (= intersection of primary ideals).

### 1.2 Primary Decomposition of Ideals

**Definition 3.** Given an ideal \( I \subset R \). The expression \( I = Q_1 \cap Q_2 \cap \ldots \cap Q_n \), where each \( Q_i \) is a primary ideal, is called a primary decomposition.

Recall that multiplication is thought of as ideal intersections.

**Example 4.** Ideal \((xy) \in k[x, y]\) has a primary decomposition \((xy) = (x) \cap (y)\).

**Theorem 1.1** (Existence). If \( R \) is a Noetherian ring then every ideal in \( R \) has a primary decomposition.

The following presented definitions and examples were drawn from a combination of Washington University lecture notes and [1] the book "A Singular Introduction to Commutative Algebra" [4].

**Definition 4.** A primary decomposition of \( I \), \( I = Q_1 \cap Q_2 \cap \ldots \cap Q_n \), is called irredundant (or equivalently minimal) if no \( Q_i \) can be omitted in the decomposition and \( \sqrt{Q_i} \neq \sqrt{Q_j} \) for all \( i \neq j \).

**Definition 5.** If \( I = Q_1 \cap Q_2 \cap \ldots \cap Q_n \) is an irredundant primary decomposition then the prime ideals \( p_i = \sqrt{Q_i} \) are the associated primes of \( I \). This set of primes is denoted \( \text{Ass}(I) \).

There is an equivalent definition of associated primes.
Proposition 2. A prime ideal $p$ is an associated prime $\iff$ there exists an $a \in R/p$ such that $p = \sqrt{\text{Ann}_R(a)}$ i.e. $p$ is a minimal prime over $\text{Ann}_R(a)$.

Example 5. For $I = (xy, xz, yz) \subset k[x, y, z]$ there is a primary decomposition $I = (x, y) \cap (x, z) \cap (y, z)$ and $\text{Ass}(I) = \{(x, y), (x, z), (y, z)\}$.

Example 6. For $I = \langle (y^2 - xz) \cdot (z^2 - x^2y), (y^2 - xz) \cdot z \rangle \subset k[x, y, z]$ there is an irredundant primary decomposition $I = (y^2 - xz) \cap (x^2, z) \cap (y, z^2)$ with $\text{Ass}(I) = \{(y^2 - xz), (x, z), (y, z)\}$.

Example 7. If $I = (f) \subset k[x_1, \ldots, x_n]$ is a principal ideal and $f = f_1^{n_1} \cdots f_s^{n_s}$ is the factorization of $f$ into irreducible factors, then

$$ I = (f_1^{n_1}) \cap \cdots \cap (f_s^{n_s}) $$

is the primary decomposition and $\text{Ass}(I) = \{(f_i) | 1 \leq i \leq s\}$ are the associated prime ideals.

Theorem 1.2 (1st Uniqueness theorem). For any irredundant primary decomposition of an ideal $I$ the corresponding set of associated primes is uniquely determined by $I$ i.e. $\text{Ass}(I)$ is unique.

More precisely, if $I = Q_1 \cap Q_2 \cap \ldots \cap Q_n = Q'_1 \cap Q'_2 \cap \ldots \cap Q'_m$ are two distinct irredundant primary decompositions then

$$ \{\sqrt{Q_1}, \ldots, \sqrt{Q_n}\} = \{\sqrt{Q'_1}, \ldots, \sqrt{Q'_m}\} $$

Example 8. For the ideal $I = (x^2, xy) \subset k[x, y]$ there are primary decompositions

$$ I = (x) \cap (x^2, y) = (x) \cap (x^2, y) $$

but the associated primes are $\text{Ass}(I) = \{(x), (x, y)\}$.

Definition 6. Given an irredundant primary decomposition $I = Q_1 \cap Q_2 \cap \ldots \cap Q_n$ with $\text{Ass}(I) = \{P_1, P_2, \ldots, P_n\}$ let $\text{minAss}(I) = \{P_1, P_2, \ldots, P_n\} \subseteq \text{Ass}(I)$ be the subset of primes which are minimal (with respect to containment) over $I$.

Call the $Q_i$ corresponding to the $P_i \in \text{minAss}(I)$ the isolated components (or minimal components) of the decomposition and the other primary ideals the embedded components.

Theorem 1.3 (2nd Uniqueness theorem). The isolated components of any irredundant primary decomposition of an ideal $I$ are determined by $I$.

More precisely, if $I = Q_1 \cap Q_2 \cap \ldots \cap Q_n = Q'_1 \cap Q'_2 \cap \ldots \cap Q'_m$ then

$$ \{Q_i | 1 \leq i \leq n, Q_i \leftrightarrow P_i \in \text{minAss}(I)\} = \{Q'_j | 1 \leq j \leq m, Q'_j \leftrightarrow P_j \in \text{minAss}(I)\} $$

so that if $k = |\text{minAss}(I)|$, then without loss of generality $Q_i = Q'_i$ for $1 \leq i \leq k$ in

$$ Q_1 \cap Q_2 \cap \ldots \cap Q_n = I = Q'_1 \cap Q'_2 \cap \ldots \cap Q'_m $$
Example 9. From previous example 8. For $I = (x^2, xy) \subset k[x, y]$ there are primary decompositions

$$I = \underbrace{(x)}_{\text{isolated comp.}} \cap \underbrace{(x^2, xy, y^2)}_{\text{embedded comp.}} = \underbrace{(x)}_{\text{isolated comp.}} \cap \underbrace{(x^2, y)}_{\text{embedded comp.}}$$

2 Connections to Geometry

Primary decomposition allows us to "decompose" an algebraic variety into its irreducible components.

In particular, we have the following proposition borrowed from Washington University [1].

Proposition 3. Given an ideal $I$ there is a one-to-one correspondence

$$\text{Isolated components of } I \leftrightarrow \text{Irreducible components of } V(I)$$

Moreover the embedded components correspond to algebraic sets which are "embedded" in $V(I)$.

The next two examples can be found in section 3.8 of Eisenbud [5].

Example 10 (Isolated components). Let $I$ be a radical ideal. If $I = \bigcap_j I_j$ is an irredun- dant primary decomposition then each $I_j$ is a prime ideal minimal over $I$. Thus each $I_j$ is an isolated component and by the proposition $V(I) = \bigcup_j V(I_j)$ so that $V(I)$ is seen as the union of irreducible components.

Example 11 (Embedded components). Suppose $I = I_1 \cap I_2$ is a primary decomposition where $I_1$ is an embedded component. Then the associated prime $\sqrt{I_1}$ is not minimal over $I$. Hence $\exists P$ a minimal prime s.t. $I \subset P \subset \sqrt{I_1}$. Then passing the variety we get $V(I) \supset V(P) \supset V(\sqrt{I_1}) = V(I_1)$ and we see that $I_1$ is "embedded" into the variety $V(P)$

2.1 Geometric Pictures to Ideals

Here is an example from ”A Singular Introduction” [4]

![Fig. 4.1. The zero-set of $(xy, xc, yc)$](image)
Example 12 (3-axis). Recall Example 5 with
\[ I = (xy, xz, yz) \subset k[x, y, z] \]
where \( V(I) \) is the union of the 3 axis. There is a primary decomposition
\[ I = (x, y) \cap (x, z) \cap (y, z) \]
Clearly this is an irredundant primary decomposition and
\[ \text{minAss}(I) = \{(x, y), (x, z), (y, z)\} \]
and so each component of the decomposition is an isolated component. Each \( V(x, y), V(x, z), \) and \( V(y, z) \) appears as one of the axis i.e. \( V(I) = V(x, y) \cup V(x, z) \cup V(y, z) \).

The next example is a situation where the geometric intuition is used to motivate the calculation of a complicated primary decomposition. The next example was part of a question posted on Math Stack Exchange and answered by Jim Belk.

Example 13 (Unusual 2-axis). Let \( I = (xy, x - yz) \). One can observe that \( V(I) \) is the union of the \( y \) and \( z \) axis. Thus we can expect a primary decomposition of \( I = I_1 \cap I_1 \)
where
\[ \sqrt{I_1} = (x, y) \quad \text{and} \quad \sqrt{I_2} = (x, z) \]
Now, note that \( I = (y^2, x - yz) \) because \( xy - y^2z = y(x - yz) \). Factoring \( y^2z \) gets
\[ I = (y^2, x - yz) = (y^2, x - yz) \cap (z, x - yz) \]
It can be checked that \( (y^2, x - yz) \) is primary and \( (z, x - yz) = (x, z) \) is prime so that \( I_1 = (y^2, x - yz) \) corresponds to the \( z \) axis and \( I_2 = (x, z) \) corresponds to the \( y \) axis.

Finally we have an interesting example taken from "A Singular Introduction to Commutative Algebra" [4].
Example 14 (Infinite elliptic cone). Recall example 6 with
\[ I = \langle (y^2 - xz) \cdot (z^2 - x^2y), (y^2 - xz) \cdot z \rangle \subset k[x, y, z] \]
and irredundant primary decomposition
\[ I = (y^2 - xz) \cap (x^2, z) \cap (y, z^2) \text{ with } \text{minAss}(I) = \{ (y^2 - xz), (x, z) \} \]
so that the isolated components are \((y^2 - xz), (x^2, z)\) and we can see that \(V(I)\) is the union of the infinite elliptic cone, \(V(y^2 - xz)\), with the \(y\)-axis, \(V(x^2, z)\).

The primary ideal \((y, z^2)\) corresponds to an algebraic set embedded in \(V(I)\).

2.2 Ideals to Geometric Pictures
Section 3.8 of Commutative Algebra (by David Eisenbud) gives a method of taking any ideal of a polynomial ring and drawing a geometric picture of it. His explanation was so good that I decided it would be best if I simply referenced this rather than attempt to restate the discussion here.

2.3 Relation to Schemes
It should be mentioned that primary decomposition also gives a way of piecing apart schemes into irreducible subschemes in a manner very similar to how this is done for varieties. Discussions of this can be easily found on math stack exchange.

3 Algorithms for Computing Primary Decompositions
In research, most people compute primary decompositions with the aid of an algebraic solver such as MacCauley2 or Singular. As such, there is an algorithm for computing primary decompositions of a general ideal in a polynomial ring. The details of Singular’s algorithm for this is several pages long and detailed in the book ”A Singular Introduction to Commutative Algebra”.

3.1 A Simple Algorithm for Monomial Ideals
In the case of monomial ideals of polynomial ring there is a straightforward algorithm to compute a primary decomposition.

For the sake of demonstrating an algorithm, I will present the monomial ideal decomposition algorithm, as outlined in exercise 3.6, 3.7, and 3.8 in Eisenbud’s Commutative Algebra with a View Toward Algebraic Geometry [5].

Definition 7. Let \( k \) be a field. In the polynomial ring \( k[x_1, \ldots, x_r] \) a monomial is a product of the variables \( x_i \). A monomial ideal is an ideal generated by monomials.
Example 15. In $k[x_1, x_2] x_1 x_2$ is a monomial but $x_1 + x_2$ is not.

Claim 1 (Exercise 3.6). Given a monomial ideal $I \subset R = k[x_1, \ldots, x_r]$ we have the following properties:

1. $I$ is prime $\iff$ $I$ is generated by a subset of the variables
2. $I$ is irreducible $\iff$ $I$ is generated by powers of some of the variables
3. $I$ is radical $\iff$ $I$ is generated by square-free (or multilinear) monomials
4. $I$ is primary $\iff$ $I$ contains a power of each of a certain subset of variables and generated by elements involving no further variables.

Proof. Many of these characterizations are easy enough to see so I will only leave some remarks.

For (1) use the property that an ideal $I$ is prime $\iff R/I$ is an integral domain.

For (2) note that for an ideal generated by a product, $(x_i x_j)$, we have $(x_i x_j) = (x_i) \cap (x_j)$. Then for the general case of $I = (f, g)$ where $f, g$ are monomials we can reduce to the one generator case by passing to the quotient $R/(f)$.

For (3) use the fact that an ideal $I$ is radical $\iff R/I$ contains no nilpotent elements and see that nilpotents will exist in $R/I$ if and only there $I$ contains a power of a variable.

For (4) use the equivalent definition that an ideal $I$ is primary if $R/I \neq 0$ and all zero-divisors of $R/I$ are nilpotent.

Claim 2 (Exercise 3.8). There exists an algorithm for computing an irreducible decomposition, and thus a primary decomposition, of a monomial ideal $I$.

I will provide the algorithm without proof.

Algorithm 1: Factor

\begin{algorithm}
\begin{aligned}
\textbf{Data:} & \text{ A monomial ideal } I = (m_1, \ldots, m_n) \text{ where } m_i \text{ are monomial generators.} \\
\text{begin} & \\
& \text{ if } \exists \text{ a minimal generator, } m_j, \text{ which may be factored into relatively prime parts } m_j = m'_j m''_j \text{ then} \\
& \quad I = (I \cup m'_j) \cap (I \cup m''_j) \\
& \quad = (m_1, \ldots, m_{j-1}, m'_j, m_{j+1}, \ldots, m_n) \cap (m_1, \ldots, m_{j-1}, m''_j, m_{j+1}, \ldots, m_n) \\
& \quad \text{Let } I_1 = (m_1, m_2, \ldots, m_{j-1}, m'_j, m_{j+1}, \ldots, m_n) \text{ and let } \\
& I_2 = (m_1, m_2, \ldots, m_{j-1}, m''_j, m_{j+1}, \ldots, m_n) \\
& \quad \text{return} \text{ Factor}(I_1) \cap \text{ Factor} (I_2) \\
\text{end} \\
\end{aligned}
\end{algorithm}

7
References


