Primary Decomposition

Nathan Ordansky

December 15, 2008

1 Introduction

The fundamental theorem of arithmetic states that every integer $z > 1$ can be written

$$z = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

where p_i is a prime for $1 \leq i \leq k$ and $\alpha i \geq 1$. Then, in terms of ideals of the ring $\mathbb{Z}$, we can write

$$(z) = (p_1^{\alpha_1}) \cap \cdots \cap (p_k^{\alpha_k}).$$

In this paper, we will begin generalize this decomposition idea for any ideal of any (Noetherian) ring. The reason we concentrate on Noetherian rings is becuase the ring $k[x_1, \ldots, x_n]$ is Noetherian for any field k and our application of choice for these ideas is algebraic geometry.

(Note from the author: What follows is taken from section 15.2 of *Abstract Algebra* by Dummit and Foote. I have presented the material in a slightly different way and filled in details where necessary. I regret not motivating this paper more and not going deeper in to the topic, though I hope to do so in the future.)

2 Radicals

Before beginning our discussion of primary ideals, we first recall (or perhaps introduce) a few defnitions and properties regarding the radical of an ideal.

Definition 2.1. Let I be an ideal in a commutative ring R.

(i) The **radical** of I, deoted rad I, is the set

$$\text{rad } I = \{f \in I : f^n \in I \text{ for some } n\}.$$

(ii) We say that I is a **radical ideal** if $I = \text{rad } I$.

(iii) The radical of the zero ideal, rad (0), is called the **nilradical** of R.

The proofs of the following facts are not all that difficult and have probably been seen before by the reader, so we leave them out.

Properties 2.2.

(1) rad I is the intersection of all prime ideals in R containing I. In particular, the nilradical is the intersection of all of the prime ideals in R.

(2) Prime (and hence maximal) ideals are radical.

(3) For ideals $I_1, \ldots, I_k$, we have

$$\text{rad}\left(\bigcap_{i=1}^{k} I_i\right) = \bigcap_{i=1}^{k} (\text{rad } I_i).$$

3 Primary Ideals

We now define a new class of ideals, primary ideals. As we see presently, these ideals have some nice properties.

Definition 3.1. A proper ideal Q of a commutative ring R is said to be **primary** if $ab \in Q$ and $a \notin Q$ implies that $b^n \in Q$ for some positive integer n. That is, Q is primary if

$$ab \in Q,\, a \notin Q \implies b \in \text{rad } Q.$$

Remark 3.2. Notice that if P is a prime ideal of a commutative ring R with $ab \in P$ and $a \notin P$, then $b \in P$. Thus, prime ideals are primary.

Proposition 3.3. *Let R be a commutative ring with 1 and let $Q \subseteq R$ be an ideal.*

(1) Q is primary if and only if every zero divisor in R/Q is nilpotent.

(2) If Q is primary, then rad Q is a prime ideal. In this case, rad Q is the unique smallest prime ideal containing Q.

(3) If rad Q is a maximal ideal, then Q is primary.

(4) Suppose M is a maximal ideal and $M^n \subseteq Q \subseteq M$ for some $n \geq 1$. Then Q is primary and rad $Q = M$.

Proof. To prove (1), First suppose that Q is primary and let $a + Q \in R/Q$ be a zero divisor. Then there is a $b + Q \neq 0 + Q$ such that $ab + Q = 0 + Q$. So $ab \in Q$ and $b \notin Q$, meaning $a^n \in Q$ for some n. Thus, $a^n + Q = 0 + Q$, meaning $a + Q$ is nilpotent.

To prove the converse, assume all zero divisors in R/Q are nilpotent and let $ab \in Q$ with $a \notin Q$. Then $ab + Q = 0 + Q$, which implies that $b + Q$ is a zero divisor in R/Q. Thus, $b+Q$ is nilpotent, which means $b^n \in Q$ for some n, making Q primary.

To prove (2), let $ab \in \text{rad } Q$. Then $(ab)^k = a^k b^k \in \text{rad } Q$, meaning either $a^k \ inQ$ or $(b^k)^n \in Q$ since Q is primary. Thus, either $a \in \text{rad } Q$ or $b \in \text{rad } Q$, making rad Q prime. The fact that it is the smallest prime ideal containing Q comes from property (1) of 2.2 above.

For (3), first note that the image of rad Q in the quotient ring R/Q is the nilradical, so we have the situation where $Q = (0)$ and the nilradical $M = \text{rad } Q = \text{rad } (0)$ is a maximal ideal. Since the nilradical is contained in every prime ideal (by (1) of 2.2), M is only prime ideal of R/Q, meaning it is also the only maximal ideal of R/Q. So if d were a zero divisor, then (d) would be a proper ideal. Thus, we must have $(d) \subseteq M$, meaning $d \in M$. So $d^n \in (0)$ in R/Q for some n, which implies that d is nilpotent in R/Q.

Finally, for (4), suppose that $M^n \subseteq Q \subseteq M$. Then $Q \subseteq M$ implies that $\text{rad } Q \subseteq \text{rad } M = M$ (the last inequality is by (2) of 2.2). But the fact that $M^n \subseteq Q$ means that $M \subseteq \text{rad } Q$, so we have $M = \text{rad } Q$ and Q is primary by (3). □

Remark 3.4.

- Notice that we have that the definitions of "prime ideal" and "primary ideal" are basically equivalent "modulo the radical of the primary ideal".
- Recall that we have the following definitions:
  - If $J = (f_1, \ldots, f_m)$ is an ideal in $k[x_1, \ldots, x_n]$, then
  $$V(J) = \{a = (a_1, \ldots, a_n) \in \mathbb{A}^n : f_1(a) = \ldots = f_m(a) = 0\} \text{ and}$$
  - for any closed subset X of $\mathbb{A}^n$,
  $$I(X) = \{f \in k[x_1, \ldots, x_n] : f(a) = 0 \text{ and } a = (a_1, \ldots, a_n) \in X\}.$$

  If $J = (f_1, \ldots, f_m)$ and $X = V(J)$, then $I(X) = \text{rad } J$. We say that X is irreducible if and only if the coordinate ring of X,
  $$k[X] = k[x_1, \ldots, x_n]/I(X),$$
  is an integral domain. Thus, since rad J is prime when J is primary, closed subsets of affine space given by primary ideals are irreducible.

Definition 3.5. If Q is a primary ideal of a ring R, then the prime ideal $P = \text{rad } Q$ is called the **associated prime** to Q and we say that Q is P-**primary**.

The following proposition will be helpful in the next section.

Proposition 3.6. *If Q_1 and Q_2 are both P-primary ideals, then $Q_1 \cap Q_2$ is a P-primary ideal.*

Proof. Note first that $P = \text{rad } Q_1 = \text{rad } Q_2$, so we have:

$$P = \text{rad } Q_1 \cap Q_2 = \text{rad } (Q_1 \cap Q_2)$$

where the last equality is from property (3) of 2.2. Now we must show that $Q_1 \cap Q_2$ is indeed primary. But this is straight forward since

$$\begin{aligned} ab \in Q_1 \cup Q_2 \text{ with } a \notin Q_1 \cup Q_2 &\implies a \notin Q_i \text{ for } i = 1 \text{ or } i = 2 \\ &\implies b^n \in Q_i \text{ for some } n \text{ since } Q_i \text{ is primary} \\ &\implies b + Q \text{ is nilpotent in } R/Q_i. \end{aligned}$$

Now (1) of proposition 3.3 says we are done. □

4 Primary Decomposition in Noetherian Rings

Now we present the Primary Decomposition Theorem for Noetherian Rings, often called the Lasker-Noether Decomposition Theorem. Before we get to the theorem, though, we introduce another kind of ideal, the irreducible ideal. The properties of irreducible ideals are the key ingredients in proving our theorem.

For the whole of this section, let R be a Noetherian ring.

Definition 4.1. A proper ideal I of R is *irreducible* if

$$I = J \cup K \text{ implies either } I = J \text{ or } I = K \text{ for ideals } J \text{ and } K.$$

Lemma 4.2. *Every proper ideal in R is a finite intersection of irreducible ideals.*

Proof. Let $\mathcal{S}$ be the collection of ideals of R which cannot be written as a finite intersection of irreducible ideals. If $\mathcal{S} \neq \emptyset$, then there is a maximal element I in S since R is Noetherian. Then I is reducible; that is, $I = J \cap K$ for ideals J and K distinct from I. But then $I \subsetneq J$ and $I \subsetneq K$, which implies that neither J nor K is an element of $\mathcal{S}$ since I is maximal in $\mathcal{S}$. So both J and K can be written as finite intersections of irreducible ideals. But this would imply that I could be written as the finite intersection of irreducible ideals, a contradiction. Thus, we must have $\mathcal{S} = \emptyset$. □

Definition 4.3. Let I be an ideal of R.

(i) I has a **primary decomposition** if it may be written as a finite intersection of primary ideals. That is, if:

$$I = \bigcap_{i=1}^{m} \text{ where } Q_i \text{ is a primary ideal for all } i.$$

(ii) The primary decomposition above is said to be **minimal** and the Q_i are the **primary components** of I if

  (a) $Qi \not\supseteq \cap_{i\neq j} Q_j$ for all i and

  (b) rad $Q_i \neq$ rad Q_j for all $i \neq j$.

Theorem 4.4. *(Primary Decomposition Theorem for Noetherian Rings) Every proper ideal I in R has a minimal primary decomposition.*

Proof. First, suppose that I does have a primary decomposition, say $I = \bigcap_{i=1}^{m} Q_i$. We will show that it must be minimal. First, notice that if any $Q_i \supseteq \cap_{i\neq j} Q_j$, we can simply remove Q_i since it will not change the intersection. Thus, the primary decomposition of I satisfies (a) in definition 4.3 (ii) above. Next, we recall proposition 3.5. Notice that, in particular, it implies that any finite intersection of P-primary ideals is a P-primary ideal. Therefore, if $Q_{i_1}, \ldots, Q_{i_k}$ all belong to the same prime P, call their intersection M_1, a P-primary ideal. We may continue in this way so that each M_r is P-primary and rad $M_r \neq$ rad M_s for $r \neq s$. Therefore, we can write $I = \bigcap_{j=1}^{\ell} M_j = \bigcap_{i=1}^{m} Q_i$ to satisfy (b) in definition 4.3 (ii).

Now we show that I must in fact have a primary decomposition. We saw in lemma 4.2 that I has a decomposition as the intersection of finitely many irreducible ideals, so if we can show that every irreducible ideal is prime, we will be done. We do so presently.

Let Q be an irreducible ideal in R and suppose $ab \in Q$ with $b \notin Q$. Consider the ideal

$$A_n = \{r \in R : ra^n \in Q\} \subseteq R$$

and notice that $A_1 \subseteq A_2 \subseteq \ldots$. But since R is Noetherian, we must have

$$A_n = A_{n+1} = \ldots \text{ for some } n > 0.$$

Now define the ideals $I = (a^n) + Q$ and $J = (b) + Q$ of R and note that both I and J contain Q, so that $I \cap J \supseteq Q$. We claim that $I \cap J = Q$, so we must prove the reverse inclusion. To do this, let $y \in I \cap J$, so $y = ra^n + q$ for some $r \in R$ and $q \in Q$. Note next that $ab \in Q$, so $aJ \in Q$, so $ay \in Q$. Then we have $ra^{n-1} = ay - aq \in Q$, which means $r \in A_{n+1} = A_n$. But $r \in A_n$ implies that $ra^n \in Q$, meaning $y \in Q$. So we have $I \cap J = Q$. But Q is irreducible, so either $Q = I$ or $Q = J$. But $b \notin Q$, so $Q \neq J$. Thus, we must have $Q = I$. So since $a^n \in I = Q$, Q must be primary. □

Remark 4.5. This theorem implies that if we have an ideal J in R, we can write it rad J as the intersection of prime ideals. In other words, if $I(X) = J$ for some affine closed set X, a primary decomposition of J gives X as the intersection of irreducibles.

We finish by presenting the following definitions:

Definition 4.6. Let R be a Noetherian ring and $I \subseteq R$ an ideal.

(i) The associated prime ideals in any primary decomposition of I are called the **associated prime ideals of** I.

(ii) If an associated prime ideal P of I does not contain any other associated prime ideal of I, then P is called an **isolated prime ideal**.

(iii) An associated prime ideals P of I that contains at least one other associated prime ideal of I is called an **embedded prime ideal**.

Remark 4.7. These definitions give us the following facts:

- In general, the primary decomposition of an ideal I is not unique. However, it is unique if I is a radical ideal, which is true if and only if the primary components of a minimal primary decomposition of I are all prime ideals. In particular, any radical ideal in $k[\mathbb{A}^n]$ can be written as a finite intersection of prime ideals.

- The irreducible components of $V(I)$ are the zero sets of the isolated primes for I.

The details of this discussion will be saved for a later date.