Primary ideals

Some rings, such as $\mathbb{Z}$ and $k[x_1, \ldots, x_n]$ where k is a field, are **unique factorisation domains**, meaning every element x can be factored uniquely (up to reordering and multiplication by units) as a product

$$x = p_1 p_2 \cdots p_k$$

with p_i irreducible ring elements.

For most rings A, this is not the case:

Example.
- In $\mathbb{Z}[i\sqrt{5}] = \mathbb{Z}[x]/(x^2+5)$, we have $6 = 2 \cdot 3 = (1+i\sqrt{5})(1-\sqrt{5})$, where $2, 3, 1+i\sqrt{5}$ and $1-i\sqrt{5}$ are all irreducible.
- Let k be a field. In the ring $A = k[x,y]/(y^2 - x^3 + x)$, we have
$$y^2 = y \cdot y = x(x-1)(x+1),$$
and y, x, $(x-1)$, $(x+1)$ are all irreducible.

The best we can hope for in general is some kind of factorisation of *ideals*. A reasonable way to formalise this turns out to be that of factoring into **primary ideals**.

Definition. An ideal $\mathfrak{a} \subseteq A$ is primary if $\mathfrak{a} \neq (1)$, and $fg \in \mathfrak{a}$ implies either $f \in \mathfrak{a}$ or $g^n \in \mathfrak{a}$ for some $n \geq 1$.

Remark. Equivalently, $\mathfrak{a} \subsetneq A$ is primary if $fg \in \mathfrak{a}$ implies $f \in \mathfrak{a}$ or $g \in \sqrt{\mathfrak{a}}$.

Lemma. *An ideal $\mathfrak{a} \subseteq A$ is primary if and only if $A/\mathfrak{a} \neq 0$, and every 0-divisor in $A/\mathfrak{a}$ is nilpotent.*

Proof. Use that $f \in \mathfrak{a}$ is equivalent to $f + \mathfrak{a} = 0$ in $A/\mathfrak{a}$, and $g^n \in \mathfrak{a}$ for some n is equivalent to $g + \mathfrak{a}$ being nilpotent in $A/\mathfrak{a}$. □

Example. Every prime ideal is primary.

Example. In $\mathbb{Z}$, the primary ideals are (0) and (p^i) for p a prime.

Example. Let A be a unique factorisation domain and let $x \in A$ be irreducible. Then (x^n) is primary: If $fg \in (x^n)$, then x^n divides fg. This means in the irreducible factorisations $f = p_1 \ldots p_l$ and $g = q_1 \ldots q_m$, the factor x (up to units) must appear n times. If x divides g, then $g^n \in (x^n)$, and if not, then x^n must divide f.

Proposition. *If $\mathfrak{a}$ is primary, then $\sqrt{\mathfrak{a}}$ is prime.*

Proof. Assume $fg \in \sqrt{\mathfrak{a}}$. Then there's some n such that $f^n g^n \in \mathfrak{a}$, so that either $f^n \in \mathfrak{a}$, or there's some m such that $(g^n)^m \in \mathfrak{a}$. In either case one of f and g must lie in $\sqrt{\mathfrak{a}}$, so $\sqrt{\mathfrak{a}}$ is prime. □

Definition. We say that $\mathfrak{a}$ is **$\mathfrak{p}$-primary** if $\sqrt{\mathfrak{a}} = \mathfrak{p}$.

Remark. It is not true that $\sqrt{\mathfrak{a}}$ prime implies $\mathfrak{a}$ primary.

Let $\mathfrak{a} = (xy, y^2) \subseteq k[x,y]$. Then $y \in \sqrt{\mathfrak{a}}$, so $(y) \subseteq \sqrt{\mathfrak{a}}$. As $\sqrt{\mathfrak{a}}$ is the intersection of all prime ideals containing $\mathfrak{a}$, we have $\sqrt{\mathfrak{a}} \subseteq (y)$, so $\sqrt{\mathfrak{a}} = (y)$. Now $\mathfrak{a}$ is not primary, since $yx \in \mathfrak{a}$, but $x \notin \sqrt{\mathfrak{a}}$.

Proposition. *If $\mathfrak{m} \subset A$ is maximal, and $\sqrt{\mathfrak{a}} = \mathfrak{m}$, then $\mathfrak{a}$ is primary.*

Proof. The ring $A/\mathfrak{a}$ has the property that the nilradical $\sqrt{(0)} = \mathfrak{m}/\mathfrak{a}$ is a maximal ideal. Since the nilradical is the intersection of all prime ideals, we must have that $\mathfrak{m}/\mathfrak{a}$ is the unique prime ideal of $A/\mathfrak{a}$. Every element outside of $\mathfrak{m}/\mathfrak{a}$ is then a unit, so every 0-divisor lies in $\mathfrak{m}/\mathfrak{a} = \sqrt{(0)}$, which means $\mathfrak{a}$ is primary. □

Definition. A **primary decomposition** of an ideal $\mathfrak{a} \subseteq A$ is an expression

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

with the $\mathfrak{q}_i$ primary. It is said to be **minimal** if

(1) the primes $\sqrt{\mathfrak{q}_i}$ are distinct, and
(2) if there is no i such that

$$\mathfrak{q}_i \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \cdots \cap \mathfrak{q}_n.$$

Remark. A nonminimal primary decomposition easily gives a minimal one. If $\sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}_j}$, just replace $\mathfrak{q}_i$ and $\mathfrak{q}_j$ by $\mathfrak{q}_i \cap \mathfrak{q}_j$, which is primary by the lemma below.
If

$$\mathfrak{q}_i \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \cdots \cap \mathfrak{q}_n,$$

just remove $\mathfrak{q}_i$.

Lemma. *If $\mathfrak{q}, \mathfrak{q}'$ are $\mathfrak{p}$-primary, then so is $\mathfrak{q} \cap \mathfrak{q}'$.*

Proof. We have $\sqrt{\mathfrak{q} \cap \mathfrak{q}'} = \sqrt{\mathfrak{q}} \cap \sqrt{\mathfrak{q}'} = \mathfrak{p} \cap \mathfrak{p} = \mathfrak{p}$. Suppose for a contradiction that $fg \in \mathfrak{q} \cap \mathfrak{q}'$ but $f \notin \mathfrak{q} \cap \mathfrak{q}'$ and $g \notin \mathfrak{p}$. Then WLOG we have $f \notin \mathfrak{q}$, which is a contradiction since $fg \in \mathfrak{q}$ and $\mathfrak{q}$ is $\mathfrak{p}$-primary. □

Example. Let $n = p_1^{e_1} \dots p_j^{e_j}$ with the p_i distinct primes. Then

$$(n) = (p_1^{e_1}) \cap \cdots \cap (p_j^{e_j}),$$

is a minimal primary decomposition, and this is the unique minimal primary decomposition of (n).

Example. In the ring $\mathbb{Z}[i\sqrt{5}]$, one can check that (6) is written as an intersection

$$(6) = (2) \cap (3, 1 - i\sqrt{5}) \cap (3, 1 + i\sqrt{5})$$

The ideal (2) is $(2, 1 - i\sqrt{5})$-primary, and $(3, 1 \pm i\sqrt{5})$ are prime ideals.

Example. The ideal $(xy) \subseteq k[x, y]$ admits a minimal primary decomposition $(xy) = (x) \cap (y)$, which is also unique.

Primary decompositions in Noetherian rings

Theorem (Lasker–Noether theorem)**.** *Let A be a Noetherian ring, and let $\mathfrak{a} \subseteq A$ be an ideal. Then $\mathfrak{a}$ admits a primary decomposition, i.e. we can write*

$$\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$$

with $\mathfrak{q}_i$ primary ideals.

We prove this in two steps. We say an ideal is **irreducible** if it cannot be written as a finite intersection of strictly bigger ideals. The first step is

Lemma. *Let A be a Noetherian ring, and let $\mathfrak{a} \subseteq A$ be an ideal. Then we can write $\mathfrak{a}$ as a finite intersection of irreducible ideals.*

Proof. Assume there is an ideal which is not an intersection of finitely many irreducible ideals. Since A is Noetherian we can take a maximal such ideal, call it $\mathfrak{a}$. The ideal $\mathfrak{a}$ is not itself irreducible, hence we can write $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ with $\mathfrak{a} \subsetneq \mathfrak{b}, \mathfrak{c}$. But now since $\mathfrak{a}$ is maximal, we can write $\mathfrak{b}$ and $\mathfrak{c}$ as finite intersections of irreducible ideals, so the same holds for $\mathfrak{a}$, a contradiction. □

Lemma. *Let A be a Noetherian ring, and let $\mathfrak{a}$ be irreducible. Then $\mathfrak{a}$ is primary.*

Proof. Passing to $A/\mathfrak{a}$, we may assume that $\mathfrak{a} = (0)$, and we want to show that (0) is primary.

We will assume that (0) is not primary, and then show that it is not irreducible. Since (0) is not primary, there exist $x, y \in A$ such that $xy = 0$, but $x \neq 0$ and y is not nilpotent. Consider then the sequence of ideals in A given by

$$\operatorname{Ann}(y) \subseteq \operatorname{Ann}(y^2) \subseteq \cdots .$$

Since A is Noetherian, this stabilises, so there is an N such that for $n \geq N$, we have $\operatorname{Ann}(y^n) = \operatorname{Ann}(y^N)$. Consider now the ideals (y^N) and $\operatorname{Ann}(y^N)$. Since y is not nilpotent, we have $(y^N) \neq (0)$. And since $x \in \operatorname{Ann}(y) \subseteq \operatorname{Ann}(y^N)$, we have $\operatorname{Ann}(y^N) \neq (0)$.

Main claim: $(y^N) \cap \operatorname{Ann}(y^N) = (0)$, which contradicts (0) being irreducible. *Proof of claim:* An element in the intersection has the form ay^N for some $a \in A$. It further satisfies

$$ay^N y^N = ay^{2N} = 0.$$

But then $a \in \operatorname{Ann}(y^{2N}) = \operatorname{Ann}(y^N)$, so $ay^N = 0$. □

Example. We have seen the ideal $(xy, y^2) \subset k[x, y]$ is not primary. It is contained in (y), which is a prime ideal, hence primary. It is also contained in $(x^2, xy, y^2) = (x, y)^2$. The ideal (x^2, xy, y^2) is (x, y)-primary since $\sqrt{(x, y)^2} = (x, y)$ is maximal ("radical maximal implies primary").

Now we claim

$$(xy, y^2) = (y) \cap (x^2, xy, y^2).$$

This follows from saying what it means for a polynomial to lie in each ideal, namely

$$(xy, y^2) = \{\sum a_{ij} x^i y^j \mid a_{i0} = 0 \text{ and } a_{01} = 0\}$$

$$(y) = \{\sum a_{ij} x^i y^j \mid a_{i0} = 0\}$$

$$(x^2, xy, y^2) = \{\sum a_{ij} x^i y^j \mid a_{00} = a_{10} = a_{01} = 0\}.$$

The intersection above is a minimal primary decomposition since

(1) $\sqrt{(y)} \neq \sqrt{(x, y)^2}$, and
(2) neither of the ideals (y) and (x^2, xy, y^2) are contained in the other.

The primary decomposition of (xy, y^2) is *not* unique, in particular we also have minimal decompositions

$$(xy, y^2) = (y) \cap (y^2, xy, x^n)$$

for any $n \geq 1$, or

$$(xy, y^2) = (y) \cap (y^2, x + ay)$$

for any $a \in k$.

Recall $(\mathfrak{a} : x) = \{y \in A \mid yx \in \mathfrak{a}\}$.

Theorem (Uniqueness 1)**.** *Let $\mathfrak{a}$ be a decomposable ideal, with minimal decomposition*

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i.$$

The prime ideals $\sqrt{\mathfrak{q}_i}$ are precisely the prime ideals which can be written as $\sqrt{(\mathfrak{a} : x)}$.

Corollary. *Every minimal primary decomposition of $\mathfrak{a}$ gives the same set of prime ideals.*

Definition. The ideals of the form $\sqrt{\mathfrak{q}_i}$ are the prime ideals **associated with** $\mathfrak{a}$.

Proof of Uniqueness theorem. The proof requires two reasonably simple lemmas.

Lemma (AM, Prop. 1.11)**.** *If $\mathfrak{p}$ is a prime ideal, and $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n \subset A$ are prime ideals such that*

$$\mathfrak{p} \subseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n,$$

then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some i. If moreover

$$\mathfrak{p} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n,$$

then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

To motivate the second one, note that if

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i,$$

then

$$\sqrt{(\mathfrak{a} : x)} = \sqrt{(\cap \mathfrak{q}_i : x)} = \sqrt{\cap (\mathfrak{q}_i : x)} = \bigcap_{i=1}^{n} \sqrt{(\mathfrak{q}_i : x)},$$

so we need to analyse $(\mathfrak{q}_i : x)$.

Lemma. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Then*

$$\sqrt{(\mathfrak{q} : x)} = \begin{cases} \mathfrak{p} & \text{if } x \notin \mathfrak{q} \\ (1) & \text{if } x \in \mathfrak{q} \end{cases}$$

Proof. If $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = (1)$.

If $x \notin \mathfrak{q}$ and $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$. Since $\mathfrak{q}$ is primary, this implies that $y^n \in \mathfrak{q}$ for some n, so $y \in \mathfrak{p}$. Conversely, if $x \notin \mathfrak{q}$ and $y \in \mathfrak{p}$, then for some $n \geq 1$ we have

$$y^n \in \mathfrak{q} \Rightarrow xy^n \in \mathfrak{q} \Rightarrow y^n \in (\mathfrak{q} : x) \Rightarrow y \in \sqrt{(\mathfrak{q} : x)}.$$

□

Now to prove the Uniquness theorem, assume that $\mathfrak{a} = \cap \mathfrak{q}_i$ is a minimal primary decomposition and that $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Now assume that $\mathfrak{p} = \sqrt{\mathfrak{a} : x)}$ is a prime ideal – we must show that $\mathfrak{p} = \mathfrak{p}_i$ for some i. We have, using Lemma 2, that

$$\mathfrak{p} = \bigcap_{i=1}^{n} \sqrt{(\mathfrak{q}_i : x)} = \mathfrak{p}_{i_1} \cap \mathfrak{p}_{i_2} \cap \cdots \cap \mathfrak{p}_{i_k},$$

where the set $\{i_1, \ldots, i_k\}$ is the set of i for which $x \notin \mathfrak{q}_i$. Using Lemma 1, then $\mathfrak{p} = \mathfrak{p}_{i_j}$ for some j.

We must also show that for every prime ideal $\mathfrak{p}_i$, we can find an $x \in A$ such that $\mathfrak{p}_i = \sqrt{(\mathfrak{a} : x)}$. Taking $x \in \mathfrak{q}_j$ for all $j \neq i$ but $x \notin \mathfrak{q}_i$ (which is possible since the decomposition is minimal), we get that $\sqrt{(\mathfrak{a} : x)} = \mathfrak{p}_i$. □

Example. The ideal $(xy, y^2) \subset k[x, y]$ can be given minimal primary decompositions

$$(xy, y^2) = (x^2, xy, y^2) \cap (y) = (x^n, xy, y^2) \cap (y).$$

The associated primes are $\sqrt{(x^2, xy, y^2)} = (x, y)$ and $\sqrt{(y)} = (y)$, and for each $n \geq 1$ we have that $\sqrt{(x^n, xy, y^2)} = (x, y)$.

Definition. The set of prime ideals associated with $\mathfrak{a}$ is partially ordered with respect to inclusion, i.e. $\mathfrak{p} \leq \mathfrak{p}'$ if $\mathfrak{p} \subseteq \mathfrak{p}'$.

The minimal elements of this set are called the **isolated** or **minimal** prime ideals associated with $\mathfrak{a}$, while the other ones are called **embedded**.

Example. In the decomposition $(y^2, xy) = (x^2, xy, y^2) \cap (y)$, the we have $(y) \subsetneq (x, y)$, so (y) is an isolated prime ideal, while (x, y) is embedded.

Proposition. *The isolated prime ideals of $\mathfrak{a}$ are exactly the prime ideals minimal over $\mathfrak{a}$, i.e. the prime ideals $\mathfrak{p}$ such that there is no prime ideal $\mathfrak{p}'$ with $\mathfrak{a} \subseteq \mathfrak{p}' \subsetneq \mathfrak{p}$.*

Proof. Let $\mathfrak{r}_1, \ldots, \mathfrak{r}_k$ be the prime ideals which are minimal over $\mathfrak{a}$, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the prime ideals associated with $\mathfrak{a}$, ordered in such a way that $\mathfrak{p}_i$ is isolated for $i = 1, \ldots, m$ and embedded for $i = m+1, \ldots, n$. The claim to be shown is

$$\{\mathfrak{r}_1, \ldots, \mathfrak{r}_k\} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}.$$

We first show the inclusion $\subseteq$: Let $\mathfrak{p} = \mathfrak{r}_j \supseteq \mathfrak{a}$ be a minimal prime ideal containing $\mathfrak{a}$, and assume $\mathfrak{a} = \cap \mathfrak{q}_i$ is a minimal primary decomposition. We have

$$\mathfrak{a} \subseteq \mathfrak{p} \Rightarrow \sqrt{\mathfrak{a}} = \cap \sqrt{\mathfrak{q}_i} = \cap \mathfrak{p}_i \subseteq \mathfrak{p}.$$

This implies by the lemma above that for some i, $\mathfrak{p}_i \subseteq \mathfrak{p}$. But $\mathfrak{p}$ being minimal over $\mathfrak{a}$ then implies that $\mathfrak{p}_i = \mathfrak{p}$. Hence every prime ideal minimal over $\mathfrak{a}$ is an isolated prime ideal for $\mathfrak{a}$.

Now for the inclusion $\supseteq$, let $\mathfrak{p}_i$ be an isolated prime ideal of $\mathfrak{a}$. Assume for a contradiction that $\mathfrak{p}_i$ is not minimal over $\mathfrak{a}$, then there will be some minimal prime ideal $\mathfrak{p}'$ such that $\mathfrak{a} \subseteq \mathfrak{p}' \subsetneq \mathfrak{p}_i$ (this requires a Zorn's lemma argument). But by the above we know $\mathfrak{p}'$ is associated with $\mathfrak{a}$, so then $\mathfrak{p}_i$ is not isolated, giving a contradiction. □

Example. In our decompositions of $(y^2, xy) \subset k[x, y]$, we will always have two components, of which one is (y) and the other could be (x^2, xy, x^n) for any n. Our uniqueness statement from today says that at least $\sqrt{(y)} = (y)$ and $\sqrt{(x^2, xy, y^n)} = (x, y)$ will be the same for any primary decomposition.

Theorem. *Assume A admits a primary decomposition of (0), and let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be the associated prime ideals of (0). Then*

$$\{x \in A \mid x \text{ is a 0-divisor}\} = \bigcup_{i=1}^{n} \mathfrak{p}_i$$

Proof. Let

$$(0) = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

be a minimal primary decomposition, with $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$.

Assume $y \notin \mathfrak{p}_i$ for any i, and that $xy = 0$. Then $\mathfrak{q}_i$ being primary implies that $x \in \mathfrak{q}_i$, and since this holds for all i, we have $x \in \cap \mathfrak{q}_i = (0)$, so $x = 0$. This means y is not a 0-divisor, proving the $\subseteq$ inclusion of the theorem.

For the inclusion $\supseteq$, assume $y \in \mathfrak{p}_i$ for some i. There is some $x \in A$ such that

$$\sqrt{\mathrm{Ann}(x)} = \sqrt{((0) : x)} = \mathfrak{p}_i.$$

This means there is some n such that $y^n \in \mathrm{Ann}(x)$, which means there is some n such that $y^n x = 0$. Taking n_0 to be the minimal such n, we have $y^{n_0-1}x \neq 0$, and $y(y^{n_0-1}x) = y^{n_0}x = 0$, which means y is a 0-divisor. □

Example. In the ring $A = k[x, y]/(xy, y^2)$, the ideal (0) has a primary decomposition

$$(0) = (\bar{x}^2, \bar{x}\bar{y}, \bar{y}^2) \cap (\bar{y}),$$

with $\bar{x}$ and $\bar{y}$ the images of x and y in A. The associated primes ideals of (0) are $(\bar{x}, \bar{y})$ and $(\bar{y})$, and so the set of 0-divisors in A is

$$(\bar{x}, \bar{y}) \cup (\bar{y}) = (\bar{x}, \bar{y}) \subset A.$$