4.1 Primary Decompositions

— generalization of factorization of an integer as a product of prime powers.

— "unique factorization" of **ideals** in a large class of rings.

In $\mathbb{Z}$, a prime number p gives rise to a **prime ideal** $p\mathbb{Z}$; a prime power p^n gives rise to a **primary ideal** $p^n\mathbb{Z}$.

Call an ideal Q of a ring A **primary** if

(i) $Q \neq A$; and

(ii) For all $x, y \in A$,

$$xy \in Q \quad \Longrightarrow$$

$$x \in Q \quad \text{or} \quad y^n \in Q \qquad (\exists n \geq 1) \; .$$

Clearly

$$\boxed{\text{Every prime ideal is primary}}$$

(taking $n = 1$ in the definition).

Observation: Q is primary iff

A/Q is not trivial and every zero-divisor in A/Q is nilpotent.

Proof: $(\Longrightarrow)$ If Q is primary then certainly A/Q is not trivial,

and if $z + Q \in A/Q$ is a zero-divisor, then

$$zw + Q \;=\; (z+Q)(w+Q) \;=\; Q \qquad (\exists w \notin Q)$$

so $zw \in Q$, so $z^n \in Q$ for some $n \geq 1$

(since $w \notin Q$), yielding

$$(z+Q)^n \;=\; z^n \;+\; Q \;=\; Q\;,$$

proving $z + Q$ is nilpotent.

($\Longleftarrow$) Suppose A/Q is not trivial, and every zero-divisor in A/Q is nilpotent.

Certainly $Q \neq A$. Let $x, y \in A$ such that $xy \in Q$.

Either $x \in Q$ or $x \notin Q$. If $x \notin Q$ then

$$(y+Q)(x+Q) \;=\; yx+Q \;=\; Q \;,$$

so $y+Q$ is a zero-divisor, so

$$y^n+Q \;=\; (y+Q)^n \;=\; Q \qquad (\exists n \geq 1) \;,$$

so $y^n \in Q$, proving Q is primary.

Example: The primary ideals of $\mathbb{Z}$ are precisely

$$0\mathbb{Z} \qquad \text{and} \qquad p^i\mathbb{Z}$$

where p is prime and $i \geq 1$.

Proof: It is easy to check that $0\mathbb{Z}$ and $p^i\mathbb{Z}$ are primary for p prime and $i \geq 1$.

Suppose $Q \lhd \mathbb{Z}$ is primary. Then $Q = m\mathbb{Z}$ for some $m \in \mathbb{Z}^+$, and $m \neq 1$, since $Q \neq \mathbb{Z}$.

Suppose that $m \neq 0$ and m is not a prime power.

Then

$$m = p^i q$$

for some prime p , $i \geq 1$ and integer q such that $p \not| q$.

But then $p + m\mathbb{Z}$ is a zero-divisor of $\mathbb{Z}/m\mathbb{Z}$

and $p + m\mathbb{Z}$ is not nilpotent,

contradicting that $m\mathbb{Z}$ is primary and the previous Observation.

Hence $m = 0$ or m is a prime power.

Observe that $0\mathbb{Z}$ is prime and $p^i\mathbb{Z} = (p\mathbb{Z})^i$, so that

in $\mathbb{Z}$ all primary ideals are powers of prime ideals.

Observation: The contraction of a primary ideal is primary.

Proof: Let $f\ A \to B$ be a ring homomorphism and $Q \lhd B$ be primary. WTS $f^{-1}(Q)$ is primary.

Suppose $x, y \in A$ and $xy \in f^{-1}(Q)$.

Then

$$f(xy) \;=\; f(x)f(y) \;\in\; Q \;,$$

so

$$f(x) \in Q \qquad \text{or} \qquad \big[f(y)\big]^n \;=\; f(y^n) \;\in\; Q$$

for some $n \geq 1$, yielding

$$x \in f^{-1}(Q) \qquad \text{or} \qquad y^n \in f^{-1}(Q) \;,$$

proving $f^{-1}(Q)$ is primary, noting $f^{-1}(Q) \neq A$.

We relate prime and primary ideals using the radical operator:

Theorem: The radical of a primary ideal is the smallest prime ideal containing it.

Proof: Let $Q \lhd A$ be primary. By an early result, the radical of Q,

$$r(Q) = \{ a \in A \mid a^n \in Q \quad (\exists n \geq 1) \},$$

is the intersection of all the prime ideals containing Q. It suffices then to check that $r(Q)$ is prime.

Suppose that $x, y \in A$ and $xy \in r(Q)$. Then

$$x^m y^m = (xy)^m \in Q \qquad (\exists m \geq 1) .$$

But Q is primary, so

$$x^m \in Q \qquad \text{or} \qquad y^{mn} = (y^m)^n \in Q$$

for some $n \geq 1$. Hence $x \in r(Q)$ or $y \in r(Q)$.

This proves $r(Q)$ is prime, so therefore $r(Q)$ is the smallest prime ideal containing Q .

If P , $Q \lhd A$, P prime, Q primary and

$$P = r(Q)$$

then we say Q is P-**primary**.

e.g. If $A = \mathbb{Z}$ and p is prime then

$$r(p^i\mathbb{Z}) = p\mathbb{Z} ,$$

so $p^i\mathbb{Z}$ is $p\mathbb{Z}$-primary.

Exercise: Let A be a UFD (unique factorization domain) and let $x \in A$ be prime. Verify that all powers of xA are primary.

Hence $(x-\lambda)^n F[x]$ is a primary ideal of $F[x]$ where F is a field, $\lambda \in F$ and $n \geq 1$.

Exercise: Find a ring A and $I \lhd A$ such that I is **not** primary yet, for all $x, y \in A$,

$$xy \in I \quad \Longrightarrow \quad x^m \in I \text{ or } y^m \in I \ (\exists m \geq 1) \ .$$

We give an example to show that primary ideals need not be powers of prime ideals.

Example: Let $A = F[x,y]$ where F is a field and put

$$Q \;=\; \langle\, x \,,\; y^2 \,\rangle \;=\; Ax \,+\, Ay^2 \,.$$

Define

$$\phi \,:\, A \;\longrightarrow\; F[y] \,/\, \langle\, y^2 \,\rangle$$

by

$$p(x,y) \;\mapsto\; p(0,y) \,+\, \langle\, y^2 \,\rangle \,.$$

Then ϕ is easily seen to be an onto ring homomorphism and

$$\ker\phi \;=\; \{\, p(x,y) \;\in\; A \;\mid\; p(0,y) \;\in\; \langle\, y^2 \,\rangle \,\}\;.$$

Certainly x , $y^2 \in \ker\phi$, so $Q \subseteq \ker\phi$.

If $p(x,y) \in \ker\phi$ then

$$p(x,y) \;=\; p_1(y) \;+\; xp_2(x,y)$$

for some $p_1(y) \in F[y]$ and $p_2(x,y) \in F[x,y]$, so that

$$p_1(y) \;=\; p(0,y) \;\in\; \langle\, y^2 \,\rangle$$

so $p(x,y) \;\in\; \langle\, x \,,\; y^2 \,\rangle \;=\; Q$.

Thus $\ker\phi \;=\; Q$.

By the Fundamental Homomorphism Theorem,

$$A/Q \;\;\cong\;\; F[y] \,/\, \langle\, y^2 \,\rangle \;.$$

By the remark following the first exercise on page 667,

$$\langle\, y^2 \,\rangle \;=\; y^2 F[y] \;=\; \big(yF[y]\big)^2$$

is a primary ideal of $F[y]$,

so all zero-divisors of $F[y] \,/\, \langle\, y^2 \,\rangle$, and hence also of A/Q , are nilpotent. Thus

$$\boxed{\;Q \text{ is a primary ideal of } A\,.\;}$$

Further,

$$r(Q) \;=\; \langle\, x \,,\; y \,\rangle \;=\; Ax \;+\; Ay \,,$$

so

$$\bigl[r(Q)\bigr]^2 \;=\; (Ax)^2 \;+\; (Ay)^2 \;+\; (Ax)(A(y)$$

$$=\; Ax^2 \;+\; Ay^2 \;+\; Axy \,,$$

so

$$\boxed{\bigl[r(Q)\bigr]^2 \;\subset\; Q \;\subset\; r(Q) \,.}$$

Thus Q is not a power of its radical.

$$\boxed{\textbf{Claim: } Q \text{ is not a power of any prime ideal.}}$$

Proof: Suppose $Q = P^n$ for some prime ideal P and $n \geq 1$. Then

$$\big[r(Q)\big]^2 \subset Q \subseteq P \quad \text{and} \quad P^n = Q \subset r(Q) \, .$$

$$\boxed{\text{We check } P = r(Q) \, .}$$

If $\alpha \in P$ then $\alpha^n \in P^n \subseteq r(Q)$,

so $\alpha \in r(r(Q)) = r(Q)$.

If $\beta \in r(Q)$ then $\beta^2 \in \left[r(Q)\right]^2 \subseteq P$,

so $\beta \in P$, since P is prime.

Hence, indeed $P = r(Q)$, so

$$\boxed{P^2 \subset P^n \subset P}$$

which is impossible.

Thus Q is not a power of a prime ideal.

We now give an example to show that powers of prime ideals need not be primary.

Example: Let $A = F[x,y,z]$, where F is a field, and put

$$I = (xy - z^2)A \,,$$

$$B = A/I \,,$$

$$P = \langle\, x + I \,,\; z + I \,\rangle \,.$$

Claim: P is a prime ideal of B and P^2 is not primary.

Proof: We first show that P is prime by verifying that B/P is an integral domain.

Let $\phi : A \longrightarrow F[y]$ where

$$\phi \;:\; p(x,y,z) \;\mapsto\; p(0,y,0) \;.$$

It is easy to check that ϕ is an onto ring homomorphism.

Also $\phi(xy - z^2) = 0$, so $I \subseteq \ker \phi$.

Hence ϕ induces an onto ring homomorphism

$$\overline{\phi} \, : \, B = A/I \quad \longrightarrow \quad F[y]$$

where

$$\overline{\phi} \, : \, p(x, y, z) + I \quad \mapsto \quad p(0, y, 0) \ .$$

Clearly $x + I$ and $z + I$ lie in $\ker \overline{\phi}$, so

$$P \;\subseteq\; \ker \overline{\phi} \;.$$

Conversely, suppose

$$p(x,y,z) + I \;\in\; \ker \overline{\phi} \;,$$

and write

$$p(x,y,z) \;=\; p_1(y) \;+\; x\,p_2(x,y) \;+\; z\,p_3(x,y,z)$$

for some $p_1(y) \;\in\; F[y]$, $p_2(x,y) \;\in\; F[x,y]$ and

$p_3(x, y, z) \;\in\; F[x, y, z]$.

Then

$$p_1(y) \;=\; p(0, y, 0) \;=\; \overline{\phi}\big(p(x, y, z) + I\big) \;=\; 0 \;,$$

so

$$p(x, y, z) \;\in\; \langle\; x \;,\; z \;\rangle \;,$$

so

$$p(x, y, z) + I \;\in\; \langle\; x + I \;,\; z + I \;\rangle \;=\; P \;.$$

Thus $\ker \overline{\phi} = P$, so

$$B/P \cong F[y] \, .$$

Hence B/P is an integral domain, since $F[y]$ is, which proves

$$\boxed{P \text{ is a prime ideal.}}$$

We now show that P^2 is not primary.

Observe that

$$
\begin{aligned}
(x+I)(y+I) &= xy+I \\
&= xy-(xy-z^2)+I \\
&= z^2+I \;=\; (z+I)^2 \;\in\; P^2\,.
\end{aligned}
$$

Also

$$
P^2 \;=\; \langle\, x^2+I\,,\; xz+I\,,\; z^2+I\,\rangle\,.
$$

If P^2 is primary then $x + I \in P^2$ or

$$y^k + I = (y+I)^k \in P^2 \qquad (\exists k \geq 1)$$

so that

$$x \quad \text{or} \quad y^k \in \langle\, x^2\,,\ xz\,,\ z^2\,,\ xy - z^2 \,\rangle\ ,$$

which is impossible, by inspecting monomials in

$$\alpha\, x^2 + \beta\, xz + \gamma\, z^2 + \delta\,(xy - z^2)$$

for $\alpha, \beta, \gamma, \delta \in A$.

Thus

$$\boxed{P^2 \text{ is not a primary ideal,}}$$

and the Claim is proved.

Despite the previous example we have:

Theorem: If $Q \lhd A$ and $r(Q)$ is maximal, then Q is primary.

In particular, all powers of a maximal ideal M are M-primary.

Proof: Suppose Q , M are ideals of A , where M is maximal and $M = r(Q)$.

By an early result about radicals of ideals (the theorem on page 220),

M is the intersection of all prime ideals of A containing Q ,

so M is the unique prime ideal of A containing Q , that is,

$$\boxed{M/Q \text{ is the unique prime ideal of } A/Q\ .}$$

Every nonunit of a ring is contained in a maximal ideal (the corollary on page 93, a result using Zorn's Lemma),

so every nonunit of A/Q is contained in M/Q .

But all elements in M have powers lying in Q, so

$$\boxed{\text{every nonunit of } A/Q \text{ is nilpotent.}}$$

Zero-divisors are nonunits, so

$$\boxed{\text{every zero-divisor in } A/Q \text{ is nilpotent.}}$$

By an earlier Observation (page 657),

$$\boxed{Q \ \text{ is primary.}}$$

If now M is any maximal ideal of A then

$$r(M^n) \ = \ M \qquad\qquad (\forall n \geq 1)$$

by an exercise (on page 217),

so, by what we have just proved, M^n is primary, so M-primary,

and the Theorem is proved.

We now study "decompositions" of ideals as intersections of primary ideals.

Lemma: Let P be a prime ideal and $Q_1 , \ldots , Q_n$ be P-primary ideals. Then

$$Q = \bigcap_{i=1}^{n} Q_i$$

is also P-primary.

Proof: By an exercise (page 216),

$$r(Q) \;=\; \bigcap_{i=1}^{n} r(Q_i) \;=\; \bigcap_{i=1}^{n} P \;=\; P \;,$$

so it just remains to check Q is primary.

Suppose $x, y \in A$ and $xy \in Q$. Then

$$xy \;\in\; Q_i \qquad (\forall i) \;.$$

If $x \in Q$ then we are done.

If $x \notin Q$ then $x \notin Q_j$ for some j, so

$$y^n \in Q_j \qquad (\exists n \geq 1) ,$$

since Q_j is primary, so

$$y \in r(Q_j) = P ,$$

yielding

$$y^m \in Q \qquad (\exists m \geq 1) ,$$

since $r(Q) = P$, proving Q is P-primary.

Lemma: Let P be prime, Q be P-primary and $x \in A$. Then

(i) $x \in Q \implies (Q : x) = A$;

(ii) $x \notin Q \implies (Q : x)$ is P-primary;

(iii) $x \notin P \implies (Q : x) = Q$.

Proof: (i) If $x \in Q$ then $Ax \subseteq Q$, since $Q \lhd A$, so $(Q : x) = A$.

(iii) Suppose $x \notin P$. Certainly $Q \subseteq (Q : x)$. Consider $y \notin Q$. If $xy \in Q$ then

$$x^k \in Q \qquad (\exists k \geq 1)$$

since Q is primary, so

$$x \in r(Q) = P ,$$

contradicting that $x \notin P$. Hence

$$xy \notin Q \quad \text{, so} \qquad y \notin (Q : x) \text{ .}$$

Thus $(Q : x) \subseteq Q$, so equality holds, and (iii) is proved.

(ii) Suppose $x \notin Q$.

If $y \in (Q : x)$ then $xy \in Q$, so

$$y^k \in Q \qquad (\exists k \geq 1)$$

(because $x \notin Q$ and Q is primary), so

$$y \in r(Q) = P \ .$$

Thus

$$Q \subseteq (Q : x) \subseteq P \, ,$$

yielding

$$P = r(Q) \subseteq r(Q : x) \subseteq r(P) = P \, .$$

Hence

$$\boxed{r(Q : x) = P \, ,}$$

so it suffices to check that $(Q : x)$ is primary.

Certainly $1 \notin (Q : x)$, so $(Q : x) \neq A$.

Suppose $a, b \in A$ and $ab \in (Q : x)$.

$$\boxed{\begin{gathered} \text{WTS} \quad a \in (Q : x) \\ \text{or } b^k \in (Q : x) \text{ for some } k \geq 1 . \end{gathered}}$$

Suppose $b^k \notin (Q : x)$ for all $k \geq 1$.

Then

$$b \notin r(Q : x) = P .$$

But $abx \in Q$, so

$$ax \in Q \qquad \text{or} \qquad b^\ell \in Q \qquad (\exists \ell \geq 1) \, .$$

$$\boxed{\text{In the latter case, } b \in r(Q) = P \text{, contradicting that } b \notin P \, .}$$

Hence $ax \in Q$, so $a \in (Q : x)$.

This completes the proof that $(Q : x)$ is P-primary.

A **primary decomposition** of $I \lhd A$ is an expression as a finite intersection of primary ideals:

$$I = \bigcap_{i=1}^{n} Q_i \qquad (*)$$

An equation of the form $(*)$ may not exist:

Exercise: Exhibit an ideal of a ring which possesses no primary decomposition.

Call the decomposition $(*)$ **minimal** if

(i) $r(Q_1)$, ... , $r(Q_n)$ are distinct; and

(ii) $(\forall i = 1, \ldots, n)$ $\qquad Q_i \not\supseteq \bigcap_{j \neq i} Q_j$.

Observation: Any primary decomposition may be replaced by a minimal one.

Proof: Consider a primary decomposition

$$I = \bigcap_{i=1}^{n} Q_i \; .$$

If $r(Q_{i_1}) = \ldots = r(Q_{i_k}) = P$, then,

by an earlier Lemma (page 688),

$$Q = \bigcap_{j=1}^{k} Q_{i_j}$$

is also P-primary, so we may replace

$$Q_{i_1} \ , \ \ldots \ , \ Q_{i_k} \ \text{ by } \ Q$$

in the decomposition.

Continuing if necessary we can guarantee that (i) holds. If (ii) is violated then we may omit ideals until (ii) is satisfied without changing the overall intersection.

Call an ideal **decomposable** if it has a primary decomposition.

First Uniqueness Theorem: Let I be a decomposable ideal and let $(*)$ be a minimal primary decomposition. Put

$$P_i = r(Q_i) \qquad \text{for } i = 1, \ldots, n \, .$$

Then

$$\{ \, P_1 \, , \, \ldots \, , \, P_n \, \} \;=\; \{ \, \text{prime ideals } P \;\mid\; (\exists x \in A) \quad P \;=\; r(I : x) \, \} \, .$$

The set $\{ P_1 , \ldots , P_n \}$ in the conclusion of the Theorem is independent of the particular minimal decomposition chosen for I, and can also be restated as follows:

> Regarding A/I as an A-module,
>
> $$\{ P_1 , \ldots , P_n \}$$
>
> is precisely the set of prime ideals which occur as radicals of annihilators of elements of A/I .

We say that the prime ideals P_1 , ... , P_n **belong to** I or are **associated to** I .

> In particular, I is primary iff I has exactly one associated prime ideal.

The minimal elements of P_1 , ... , P_n with respect to $\subseteq$ are called **minimal** or **isolated** prime ideals belonging to I ;

the nonminimal ones are called **embedded** prime ideals.

Proof of the First Uniqueness Theorem: Let $x \in A$. Then, by earlier exercises (pages 208 and 216),

$$r(I : x) \;=\; r\Big(\bigcap_i Q_i \;:\; x\Big) \;=\; r\Big(\bigcap_i (Q_i \;:\; x)\Big)$$

$$=\; \bigcap_i r(Q_i \;:\; x) \;=\; \bigcap_{i\,,\,x \notin Q_i} P_i \;,$$

in the last step, by (i) and (ii) of the Lemma on page 691.

Thus, if $r(I : x)$ is prime, then, by (i) of the Theorem on page 194,

$$r(I : x) \in \{ P_i \mid x \notin Q_i \} .$$

This proves

$$\boxed{\begin{aligned} &\left\{ \text{prime } P \mid (\exists x \in A) \quad P = r(I : x) \right\} \\ &\qquad\qquad \subseteq \quad \{ P_1 , \ldots , P_n \} . \end{aligned}}$$

Conversely, let $i \in \{1, \ldots, n\}$.

Because the primary decomposition is minimal,

$$\exists \; x_i \; \in \; \Big(\bigcap_{j \neq i} Q_j\Big) \backslash Q_i \; .$$

Observe first that if $y \;\in\; (Q_i : x_i)$ then $yx_i \;\in\; Q_i$, so

$$yx_i \;\in\; Q_i \;\cap\; \Big(\bigcap_{j \neq i} Q_j\Big) \;=\; I$$

so

$$y \;\in\; (I : x_i) \; .$$

Thus

$$(Q_i : x_i) \subseteq (I : x_i) \subseteq (Q_i : x_i)$$

since $I \subseteq Q_i$

so $(I : x_i) = (Q_i : x_i)$. Hence

$$r(I : x_i) = r(Q_i : x_i) = P_i ,$$

by (ii) of the Lemma on page 691, and the Theorem is proved.

$$\boxed{\text{Note: primary components need not be unique.}}$$

Example: Let $A = F[x,y]$ where F is a field and put

$$I = \langle x^2 , xy \rangle = x^2 A + xyA = x(xA + yA) .$$

Observe that

$$\boxed{I = \langle x \rangle \cap \langle x , y \rangle^2 \qquad (*)}$$

and

$$\boxed{\quad I \;=\; \langle\, x \,\rangle \cap \langle x^2 \,,\, y \,\rangle \qquad\qquad (**) \quad}$$

Certainly $\langle x \rangle = xA$ is primary (in fact prime, since x is prime in A).

Also $\langle\, x \,,\, y \,\rangle$ is maximal in A

(case $n = 2$ in example (3) on page 121)

so $\langle\, x \,,\, y \,\rangle^2$ is primary (by Theorem on page 684).

Also $\langle\, x^2\,,\, y\,\rangle$ is primary (by the Example on page 668 with x , y interchanged).

Observe that

$$r\big(\langle\, x\,\rangle\big) \;=\; \langle\, x\,\rangle$$

and

$$r\big(\langle\, x\,,\, y\,\rangle^2\big) \;=\; r\big(\langle\, x^2\,,\, y\,\rangle\big) \;=\; \langle\, x\,,\, y\,\rangle\;.$$

> Thus $(*)$ and $(**)$ are two different minimal primary decompositions of I .

The prime ideals belonging to I are $\langle\, x \,\rangle$ and $\langle\, x\,,\, y \,\rangle$, and $\langle\, x \,\rangle \subset \langle\, x\,,\, y \,\rangle$, so

$$\boxed{\begin{array}{c} \langle\, x \,\rangle \text{ is isolated, and} \\ \langle\, x\,,\, y \,\rangle \text{ is embedded.} \end{array}}$$

Nevertheless, the primary ideal $\langle\, x \,\rangle$ is common to both decompositions.

Later we see that primary components whose radicals are **isolated** prime ideals are unique.

Theorem: Let $I \lhd A$ be decomposable, and let P be a prime ideal of A containing I.

Then P contains an isolated prime ideal belonging to I.

Corollary: The isolated prime ideals belonging to a decomposable ideal I are precisely the minimal elements in the poset of all prime ideals containing I.

Proof of the Theorem: Let $I = \bigcap_i Q_i$ be a minimal primary decomposition, and put

$$P_i = r(Q_i) \qquad (\forall i) .$$

Then

$$P = r(P) \supseteq r(I) = \bigcap_i r(Q_i) = \bigcap_i P_i ,$$

so $P \supseteq P_j$ for some j, by (i) of the Theorem on page 194, and the proof is complete.

We next discuss how notions involving primary ideals interact with taking fractions, and then apply our results to obtain a second uniqueness theorem.

Lemma: Let S be a multiplicatively closed subset of A , P a prime ideal and Q a P-primary ideal. Then

(i) $S \cap P \neq \emptyset \implies S^{-1}Q = S^{-1}A$;

(ii) $S \cap P = \emptyset \implies S^{-1}Q$ is $S^{-1}P$-primary and $(S^{-1}Q)^{\mathsf{c}} = Q$.

Here contraction is with respect to $a \mapsto a/1$ for $a \in A$.

Proof: (i) If $x \in S \cap P$ then

$$x^n \in S \cap Q \qquad (\exists n \geq 1)$$

so $S^{-1}Q$ contains $(1/x^n)(x^n/1) = 1/1$, so $S^{-1}Q = S^{-1}A$.

(ii) Suppose $S \cap P = \emptyset$. By **(4)** of the Theorem on page 617,

$$S^{-1}P \text{ is prime,}$$

and, by **(3)** of the same Theorem,

$$Q^{\mathsf{ec}} \;=\; \bigcup_{s\in S} (Q : s)\ .$$

But, for each $s \in S$, $s \notin P$, so, by (iii) of the Lemma on page 691,

$$(Q : s) \;=\; Q$$

so we deduce that

$$Q^{\mathsf{ec}} \;=\; Q\ .$$

Also, by the Claim on page 613,

$$Q^{\mathsf{e}} = S^{-1}Q ,$$

so

$$(S^{-1}Q)^{\mathsf{c}} = Q^{\mathsf{ec}} = Q .$$

Further, since S^{-1} commutes with taking radicals (part **(5)** of the Theorem on page 617),

$$r(S^{-1}Q) = S^{-1}(r(Q)) = S^{-1}P .$$

It remains therefore just to check $S^{-1}Q$ is primary.

Suppose $x, y \in A$, $s, t \in S$ and

$$(x/s)\,(y/t) \quad \in \quad S^{-1}Q \ .$$

Then

$$(xy)/(st) \quad = \quad z/u \qquad\qquad (\exists z \in Q \ , \ u \in S)$$

so

$$(xyu - zst)\,v \quad = \quad 0 \qquad\qquad (\exists v \in S)$$

so

$$xyuv \quad = \quad zstv \quad \in \quad Q \ .$$

If $x \in Q$ then $x/s \in S^{-1}Q$, and we are done.

Suppose $x \notin Q$. Then, since Q is primary,

$$y^n(uv)^n = (yuv)^n \in Q \qquad (\exists n \geq 1) .$$

If $y^n \notin Q$ then, again since Q is primary,

$$(uv)^{mn} = \left((uv)^n\right)^m \in Q \qquad (\exists m \geq 1) ,$$

so

$$(uv)^{mn} \in S \cap Q \subseteq S \cap P = \emptyset ,$$

which is impossible.

Hence $y^n \in Q$, so

$$(y/t)^n = y^n / t^n \in S^{-1}Q .$$

This proves $S^{-1}Q$ is primary, and hence $S^{-1}P$-primary. This completes the proof of the Lemma.

Theorem: Primary ideals of A which avoid S are in a one-one correspondence with primary ideals in $S^{-1}A$ under the map

$$Q \mapsto S^{-1}Q .$$

Proof: Put

$$\mathcal{P}_1 \;=\; \{ \text{ primary ideals } Q \text{ of } A \;\mid\; Q \cap S \;=\; \emptyset \;\}$$

and

$$\mathcal{P}_2 \;=\; \{ \text{ primary ideals of } S^{-1}A \;\} \,.$$

Let

$$\Phi \;:\; \mathcal{P}_1 \;\longrightarrow\; \mathcal{P}_2 \,, \qquad Q \;\mapsto\; S^{-1}Q$$

$$\Psi \;:\; \mathcal{P}_2 \;\longrightarrow\; \mathcal{P}_1 \,, \qquad I \;\mapsto\; I^{\,\mathsf{c}} \,.$$

Then Ψ is sensibly defined, because if $I \in \mathcal{P}_2$ then I^{c} is primary (by the Observation on page 662), and $I^{\mathsf{c}} \cap S = \emptyset$

(because if $x \in I^{\mathsf{c}} \cap S$ then

$$1/1 = (1/x)(x/1) \in I$$

so that $I = S^{-1}A$, contradicting that $I \neq S^{-1}A$).

Further, if $Q \in \mathcal{P}_1$ then $S \cap r(Q) = \emptyset$

(for if $x \in S \cap r(Q)$ then some power of x lies in $S \cap Q$, contradicting that $S \cap Q = \emptyset$), so that, by part (ii) of the previous Lemma, $S^{-1}Q$ is primary, so that Φ is sensibly defined, and

$$\Psi\Phi(Q) \;=\; \Psi(S^{-1}Q) \;=\; (S^{-1}Q)^{\mathsf{c}} \;=\; Q\ .$$

If $I \in \mathcal{P}_2$ then $I = I^{\mathsf{ce}}$, since all ideals of $S^{-1}A$ are extended (see page 616), so

$$\Phi\Psi(I) \;=\; S^{-1}(I^{\mathsf{c}}) \;=\; I^{\mathsf{ce}} \;=\; I\ ,$$

since extension is the same as application of S^{-1} (see page 613).

Hence Φ and Ψ undo each other, so, in particular, Φ is a bijection and the Theorem is proved.

Notation: If $J \lhd A$, write

$$\boxed{S(J) \;=\; J^{\mathsf{ec}} \;=\; \{\, a \in A \mid a/1 \,\in\, S^{-1}J \,\}\,.}$$

Hence, if $Q \lhd A$ is primary and $Q \cap S = \emptyset$ then, from the previous proof:

$$S(Q) \;=\; \Psi\Phi(Q) \;=\; Q\,.$$

In what follows, S is a multiplicatively closed subset of A and $I \lhd A$ has a minimal primary decomposition

$$I = \bigcap_i Q_i ,$$

and we put $P_i = r(Q_i) \quad (\forall i)$. We suppose further that the ideals have been arranged so that, for some m where $1 \leq m \leq n$,

$$S \cap P_i = \emptyset \qquad (\forall i = 1, \ldots, m) ;$$
$$S \cap P_j \neq \emptyset \qquad (\forall j = m+1, \ldots, n) .$$

Theorem: We have the following minimal primary decompositions:

$$S^{-1}I \;=\; \bigcap_{i=1}^{m} S^{-1}Q_i$$

and

$$S(I) \;=\; \bigcap_{i=1}^{m} Q_i \;.$$

Proof: Observe that

$$S^{-1}I \;=\; \bigcap_{i=1}^{n} S^{-1}Q_i \;=\; \bigcap_{i=1}^{m} S^{-1}Q_i \qquad (*)$$

since S^{-1} commutes with intersection, and since $S^{-1}Q_j = S^{-1}A$ for $j \geq m+1$ by part (i) of the previous Lemma.

But also

$$S^{-1}Q_i \quad \text{is} \quad S^{-1}P_i\text{-primary}$$

for all $i = 1, \ldots, m$, by part (ii) of that Lemma, and further

$$S^{-1}P_1 \ , \ \ldots \ , \ S^{-1}P_m \quad \text{are distinct,}$$

since $P_1 \ , \ \ldots \ , \ P_m$ are distinct prime ideals which avoid S (applying part (iv) of the Theorem on page 617).

Hence, contracting both sides of $(*)$,

$$S(I) \ = \ (S^{-1}I)^{\mathsf{c}} \ = \ \bigcap_{i=1}^{m} (S^{-1}Q_i)^{\mathsf{c}}$$

so

$$S(I) \;=\; \bigcap_{i=1}^{m} S(Q_i) \;=\; \bigcap_{i=1}^{m} Q_i \qquad (**)$$

since the "operator" S fixes each Q_i .

Certainly $(**)$ is a minimal primary decomposition.

If, for some $i \in \{ 1 , \ldots , m \}$,

$$S^{-1}Q_i \quad \supseteq \quad \bigcap_{j \neq i \, , \, 1 \leq j \leq m} S^{-1}Q_j$$

then

$$
\begin{aligned}
Q_i &= \left(S^{-1}Q_i\right)^{\mathsf{c}} \supseteq \bigcap_{j\neq i\,,\,1\leq j\leq m} \left(S^{-1}Q_j\right)^{\mathsf{c}} \\
&= \bigcap_{j\neq i\,,\,1\leq j\leq m} Q_j\ ,
\end{aligned}
$$

which contradicts the minimality of $(**)$.

Hence $(*)$ is also a minimal primary decomposition, and the Theorem is proved.

Consider a decomposable ideal I and put

$$\Pi = \{ \text{ prime ideals belonging to } I \} .$$

Call a subset Γ of Π **isolated** if

$$\boxed{\begin{gathered}(\forall P \in \Gamma)\,(\forall P' \in \Pi) \\ P' \subseteq P \quad \Longrightarrow \quad P' \in \Gamma \qquad (\dagger)\end{gathered}}$$

In particular,

$$\boxed{\text{if } P \in \Pi \text{ is isolated then } \{P\} \text{ is isolated.}}$$

Suppose Γ is isolated and put

$$\boxed{S = A \setminus \Big(\bigcup_{P\in\Gamma} P\Big) = \bigcap_{P\in\Gamma} (A\setminus P)\,.}$$

Then S is multiplicatively closed (being the intersection of multiplicatively closed subsets).

For each $P' \in \Pi$, clearly

$$P' \in \Gamma \implies P' \cap S = \emptyset \, ,$$

and further, by $(\dagger)$,

$$P' \notin \Gamma \implies (\forall P \in \Gamma) \; P' \not\subseteq P \, ,$$

so, by part (ii) of the Theorem on page 195,

$$P' \notin \Gamma \quad \Longrightarrow \quad P' \not\subseteq \bigcup_{P \in \Gamma} P \quad \Longrightarrow \quad P' \cap S \neq \emptyset \,.$$

Thus

$$\boxed{\quad P' \in \Gamma \qquad \Longleftrightarrow \qquad P' \cap S = \emptyset \qquad (\ddagger) \quad}$$

We can now deduce another uniqueness theorem.

Let I be decomposable and P_1 , ... , P_n be the prime ideals belonging to I

(which by the First Uniqueness Theorem are independent of the decomposition).

Suppose $m \leq n$ and $\Gamma = \{ P_1 , \ldots , P_m \}$ is isolated.

Second Uniqueness Theorem: For any two minimal primary decompositions

$$I = \bigcap_{i=1}^{n} Q_i = \bigcap_{i=1}^{n} Q_i'$$

where $r(Q_i) = r(Q_i') = P_i \qquad (\forall i)$
we have

$$\bigcap_{i=1}^{m} Q_i = \bigcap_{i=1}^{m} Q_i' \,.$$

Proof: By (‡) applied to

$$S = A \setminus (P_1 \cup \ldots \cup P_m)$$

we have, for each $i = 1, \ldots, n$,

$$P_i \cap S = \emptyset \qquad \Longleftrightarrow \qquad i \leq m \ ,$$

so, by the previous Theorem,

$$\bigcap_{i=1}^{m} Q_i = S(I) = \bigcap_{i=1}^{m} Q_i' \ ,$$

and we are done.

Call a primary component Q of a primary decomposition **isolated** if $r(Q)$ is isolated,

(in which case $\{ r(Q) \}$ is isolated),

and **embedded** otherwise.

Thus, taking $m = 1$ in the previous Theorem, we get

Corollary: The isolated primary components of a primary decomposition of a given ideal are unique.

Example: Put $A = F[x,y]$ where F is a field. Then

$$\langle\, x^2\,,\; xy\,\rangle \;\;=\;\; \langle\, x\,\rangle \;\cap\; \langle\, x\,,\; y\,\rangle^2$$

$$=\;\; \langle\, x\,\rangle \;\cap\; \langle\, x^2\,,\; y\,\rangle$$

are minimal primary decompositions, and because $\langle\, x\,\rangle$ is isolated, the corollary predicts that it must be common to both.