IV.D. Primary decomposition

Recall that in the passage from UFDs like $\mathbb{Z}[\sqrt{-1}]$ to general rings of integers $\mathcal{O}_K$, we were able to recover a version of unique factorization for *ideals*. For instance, in $\mathbb{Z}[\sqrt{-5}]$, while 6 factors non-uniquely into irreducibles, the corresponding principal ideal (6) factors uniquely into a product of (non-principal) primes like $(2, 1+\sqrt{-5})$. We would like to have a similar result for ideals in arbitrary Noetherian rings.

However, in the proof of IV.C.11, it was mentioned that in many Noetherian rings, ideals *don't* decompose as products of primes. Consider $I = (x^2, y) \subset \mathbb{C}[x,y]$; then $\mathrm{Rad}(I) \supseteq (x,y)$ by IV.C.5, while maximality of (x,y) and properness of $\mathrm{Rad}(I)$ (which e.g. doesn't contain 1) force equality. So the *only* prime ideal containing I is (x,y), of which I is clearly not a power. This suggests that we need to consider decompositions into a somewhat more general class of ideals.

There are problems even in the case of radical ideals. Consider $I = (x, yz) \subset \mathbb{C}[x,y,z]$; this is the intersection of the primes $P = (x,y)$ and $Q = (x,z)$. But it is not their product $PQ = (x^2, xy, xz, yz)$ (which is strictly smaller), and in fact it cannot be a product of primes at all (why?). So perhaps we should consider decomposing ideals as intersections instead of products.[3]

The larger class of ideals we will need is the following:

IV.D.1. DEFINITION. An ideal $Q \subsetneq R$ is **primary** if

$$ab \in Q \text{ and } a \notin Q \implies b^n \in Q \text{ for some } n.$$

(Equivalently: $ab \in Q$ and $b \notin \mathrm{Rad}(Q) \implies a \in Q$.)

IV.D.2. EXAMPLES. (i) In $R = \mathbb{Z}$, the primary ideals are the (p^t):

[3]We discussed intersections vs. products of ideals in commutative rings in [**Algebra I**, III.E.13(ii)], concluding that these are equal when the ideals are pairwise coprime. (Otherwise, there are easy counterexamples like $(p)(p) = (p^2) \subsetneq (p) = (p) \cap (p)$ in $\mathbb{Z}$.) One important case where ideals are automatically coprime is that of distinct maximal ideals $\mathfrak{m}, \mathfrak{m}'$, since their sum contains an element not in (say) $\mathfrak{m}$ hence must be the whole ring.

If $ab \in (p^t)$, then $ab = mp^t$; and if $p^t \nmid a$, then some power of p divides b by unique factorization in $\mathbb{Z}$. Hence a power of b is divisible by p^t. This shows that (p^t) is primary.

On the other hand, if $I = (m)$ with $m = \prod_{i=1}^{k} p_i^{t_i}$ (p_i distinct primes, $k > 1$), then taking $a = \prod_{i=2}^{k} p_i^{t_i}$ and $b = p_1^{t_1}$, no power of b is in I even though $a \notin I$ and $ab \in I$.

(ii) In $R = \mathbb{C}[x, y]$, $I = (x^2, y)$ is a primary ideal, whereas $P = (x, y)$ is prime. In fact, the latter is maximal since $R/P = \mathbb{C}$ is a field; while $x \notin I$ (but $x^2 \in I$) $\implies$ I not prime.

To see that I is primary, note that $fg \in I \implies fg = x^2F + yG$ ($F, G \in R$), and $f \notin I \implies f(0,0) \neq 0$ or $f(0,0) = 0 \neq f_x(0,0)$. It follows that $g(0,0) = 0$, hence $g(x,y) = xh_1(x,y) + yh_2(x,y)$ ($h_i \in R$) $\implies g^2 = x^2h_1^2 + y\{2xh_1h_2 + yh_2^2\} \in I$.

IV.D.3. PROPOSITION. *If Q is primary, then* $\mathrm{Rad}(Q)$ *is prime.*

PROOF. Given $ab \in \mathrm{Rad}(Q)$ and $a \notin \mathrm{Rad}(Q)$, we have (for some $n \in \mathbb{N}$) $a^n b^n = (ab)^n \in Q$ and $a^n \notin Q$. Since Q is primary, we have $(b^n)^m \in Q$ for some m, hence $b \in \mathrm{Rad}(Q)$. $\square$

Writing $P := \mathrm{Rad}(Q)$, we say that Q is ***P*-primary**.

IV.D.4. EXAMPLES. (i) In $\mathbb{Z}$, (27) is (3)-primary.

(ii) In $\mathbb{C}[x, y]$, (x^2, y) is (x, y)-primary.

(iii) If I is an ideal in a commutative ring R with $\mathrm{Rad}(I)$ a maximal ideal, then I is primary. Indeed, given $ab \in I$, with $b \notin \mathrm{Rad}(I)$, we have that (since $\mathrm{Rad}(I)$ is the *only* maximal ideal containing I) no maximal ideal contains both I and b. So $I + (b) = R \implies (a) = a(I + (b)) \subset I + (ab) = I \implies a \in I$.

(iv) In a ring of integers $\mathcal{O}_K$, any prime ideal is maximal (cf. I.M.28). So if an ideal $I \subset \mathcal{O}_K$ has prime radical $P := \mathrm{Rad}(I)$, then I is primary. Again, P is the only prime ideal containing/dividing I, and so by unique ideal factorization in $\mathcal{O}_K$, $I = P^k$ for some k.

IV.D.5. WARNING. The converse of IV.D.3 is *false*. For example, in $R = \mathbb{C}[x, y]$, $I = (xy, y^2)$ is not primary: $yx \in I$ and $y \notin I$, but no power of x is in I. However, $\mathrm{Rad}(I) = (xy, y) = (y)$ is prime.

In fact, even a power of a (non-maximal) prime ideal can fail to be primary (HW).

IV.D.6. PROPOSITION. *Given $Q, P \subset R$ ideals,*

$$Q \text{ is } P\text{-primary} \quad \Longleftrightarrow \quad \begin{cases} Q \subset P \subset \mathrm{Rad}(Q), \quad \textit{and} \\ \boxed{ab \in Q,\, a \notin Q \implies b \in P} (*) \end{cases}$$

PROOF. Note that the LHS is actually three statements: that P is prime, Q is primary, and $\mathrm{Rad}(Q) = P$.

$\underline{(\Longleftarrow)}$: By $(*)$, if $a, b \in Q$ and $a \notin Q$, then $b \in P \subset \mathrm{Rad}(Q)$ hence $b^n \in Q$; and so Q is primary. It remains to show that $\mathrm{Rad}(Q) \subset P$. Given $b \in \mathrm{Rad}(Q)$, let n be the minimal exponent for which $b^n \in Q$. If $n = 1$, then $b \in Q \subset P$ and we are done. If $n > 1$, then by minimality $b^{n-1} \notin Q$, while $b^{n-1}b = b^n \in Q$; and $(*)$ gives $b \in P$.

$\underline{(\Longrightarrow)}$: We have $Q \subset \mathrm{Rad}(Q) = P$; and if $ab \in Q$ and $a \notin Q$, then $b^n \in Q \implies b \in \mathrm{Rad}(Q) = P$. □

IV.D.7. LEMMA. *If $Q_1, \ldots, Q_n$ are P-primary ideals, then $\cap_i Q_i$ is P-primary.*

PROOF. Given $\mathrm{Rad}(Q_i) = P$ $(\forall i)$, by IV.C.7(ii) we already know that $\mathrm{Rad}(\cap_i Q_i) = \cap_i \mathrm{Rad}(Q_i) = \cap_i P = P$. (But we still have to show that $\cap_i Q_i$ is primary!) If $ab \in \cap_i Q_i$ but $a \notin \cap_i Q_i$, then for some i we have $a \notin Q_i$ (and $ab \in Q_i$) hence $b \in P$ by IV.D.6($\Longrightarrow$) for Q_i. Now applying IV.D.6($\Longleftarrow$) for $\cap_i Q_i$ shows the latter is indeed (P-)primary. □

We are now ready to introduce the more general notion of decomposition that we will seek.

IV.D.8. DEFINITION. An ideal $I \subset R$ has a **primary decomposition** if $I = Q_1 \cap \cdots \cap Q_n$ with each Q_i primary. This decomposition is **reduced** if (i) no Q_i contains $\cap_{j \neq i} Q_j$ and (ii) the radicals $\mathrm{Rad}(Q_i)$ are all distinct. The prime ideals $P_i := \mathrm{Rad}(Q_i)$ are called the **associated primes** of the decomposition.

For brevity, I will use the abbreviations PD and RPD.

IV.D.9. PROPOSITION. *If an ideal I has a PD, then it has an RPD.*

PROOF. If (i) in IV.D.8 fails for some Q_i, i.e. $Q_i \supset \cap_{j \neq i} Q_j$, then removing Q_i does not change the full intersection. Assume we have made such removals, so that (i) holds.

To deal with (ii), suppose that (say) Q_1 and Q_2 are both P-primary (i.e. have the same radical). Without affecting the full intersection, we can replace them by $Q_1 \cap Q_2$, which is P-primary by IV.D.7. $\square$

The main result, to be proved below in a more general context, is:

IV.D.10. THEOREM. *Every* (*proper*) *ideal of a* (*commutative*) *Noetherian ring has an RPD, and this is unique up to reordering of factors provided the associated primes are all* ***isolated*** (*no P_i contains any P_j*).

In the event that some P_i contains one of the other associated primes, it is called an **embedded** prime, and then the corresponding Q_i in the decomposition is not unique (but P_i itself is), see IV.D.17 below.

IV.D.11. EXAMPLES. (i) Of course, the simplest example of an RPD is $(p_1^{n_1} \cdots p_k^{n_k}) = (p_1^{n_1}) \cap \cdots \cap (p_k^{n_k})$ in $R = \mathbb{Z}$, with associated primes (p_i).

(ii) If $R = \mathbb{C}[x, y]$, we can already get examples where the issue regarding embedded primes and non-uniqueness shows up: two RPDs for the ideal $I = (xy, y^2)$ are $(y) \cap (x, y^2)$ and $(y) \cap (x + y, y^2)$. Here the associated primes are (y) and (x, y), the latter being "embedded". (This terminology comes from what the ideal represents in geometrically, which is the x-axis "union" an extra copy of the origin, a so-called "embedded point".)

Primary modules.

IV.D.12. DEFINITION. Let M be an R-module. A proper submodule $A \subsetneq M$ is **primary** if

(IV.D.13)
$$r \in R,\ m \notin A,\ rm \in A \implies r^n M \subset A \text{ for some } n \in \mathbb{Z}_{>0}.$$

(Equivalently, $\mathrm{Rad}(\mathrm{ann}(M/A)) = \{r \in R \mid \exists \mu \in M/A \text{ s.t. } r\mu = 0\}$. That is, the elements a power of which annihilates M/A are the elements which kill *some* nonzero element of M/A.)

In the case where M is R viewed as an R-module, (IV.D.13) says exactly that A is a primary ideal. More generally:

IV.D.14. PROPOSITION. *If a proper submodule $A \subsetneq M$ is primary, then $Q_A := \{r \in R \mid rM \subset A\}$ $(= \mathrm{ann}(M/A))$ is a primary ideal.*

PROOF. First, $1 \notin Q_A \implies Q_A \neq R$; so Q_A is a proper ideal. Since

$$\begin{aligned} rs \in Q_A \text{ and } s \notin Q_A &\implies rsM \subset A \text{ and } sM \not\subset A \\ &\implies \exists m \in M \text{ s.t. } sm \notin A \text{ and } r(sm) \in A \\ &\underset{\text{(IV.D.13)}}{\implies} r^n \in Q_A, \end{aligned}$$

Q_A satisfies IV.D.1. □

IV.D.15. DEFINITION. (i) Suppose $A \subset M$ is primary, and put $P := \mathrm{Rad}(Q_A)$ $(= \mathrm{Rad}(\mathrm{ann}(M/A)))$; we say that A is ***P*-primary**.

(ii) A submodule $N \subset M$ has a **primary decomposition** if $N = A_1 \cap \cdots \cap A_n$ with each A_i primary. Writing $P_i := \mathrm{Rad}(Q_{A_i})$, this primary decomposition is **reduced** if the P_i are distinct and no A_i contains $A_1 \cap \cdots \cap \widehat{A_i} \cap \cdots \cap A_n$. The P_i are again called **associated primes**.

IV.D.16. PROPOSITION. *If N has a PD, then it has an RPD.*

PROOF. See the proof of IV.D.9. The main new point is that we need to know the intersection $A \cap B$ of two P-primary modules is a P-primary module. First note that $Q_{A\cap B} = Q_A \cap Q_B$, which is P-primary by IV.D.7 since Q_A and Q_B are. Now, given $rm \in A \cap B$ with $m \notin A \cap B$, we have $rm \in A$ and (say) $m \notin A$, hence (by (IV.D.13)) $r^n \in Q_A$ and thus $r \in \mathrm{Rad}(Q_A) = P = \mathrm{Rad}(Q_{A\cap B})$. But then we have a power $r^m \in Q_{A\cap B}$ whence $r^m M \subset A \cap B$. □

We are now ready to prove a uniqueness result for RPDs.

IV.D.17. THEOREM. (i) *Let* $N \subsetneq M$ *be an* R*-submodule with two RPDs* $A_1 \cap \cdots \cap A_k = N = A'_1 \cap \cdots \cap A'_\ell$*, with* A_i P_i*-primary and* A'_j P'_j*-primary. Then* $k = \ell$ *and, up to reordering,* $P_i = P'_i$ $(\forall i)$.

(ii) *If* P_i *is an isolated prime* (*i.e. contains no other* P_j)*, then in addition we get* $A_i = A'_i$.

PROOF. (i) We may assume that P_1 is maximal (under inclusion) in $\{P_1, \ldots, P'_\ell\}$. Suppose that no $P'_j = P_1$. Then $P_1 \not\subset P'_j$ $(\forall j)$; and $P_1 \not\subset P_i$ $(\forall i > 1)$ by definition (i.e. IV.D.15(ii)). So by the Prime Avoidance Lemma, $P_1 \not\subset P_2 \cup \cdots \cup P_k \cup P'_1 \cup \cdots \cup P'_\ell =: \mathsf{U}$.

Let $r \in P_1 \backslash (P_1 \cap \mathsf{U})$. Then $r^n M \subset A_1$ for some n and we set

$$N^* := \{x \in M \mid r^n x \in N\} \subset N.$$

If $k = 1$ then $N = A_1 \implies N^* = M \implies N = M$ yields a contradiction. If $k > 1$ then $A_2 \cap \cdots \cap A_k \subset N^*$ and $A'_1 \cap \cdots \cap A'_\ell \subset N^*$. I claim these inclusions are equalities. Consider $x \notin A_2 \cap \cdots \cap A_k$. By (IV.D.13), $r^n x \in A_{i\,(>1)}$ would imply $r^{mn} \in Q_{A_i}$ hence $r \in P_i$ (contradicting the choice of r), so $r^n x \notin A_2 \cap \cdots \cap A_k$ hence $r^n x \notin N$ and $x \notin N^*$. Conclude that $N^* = A_2 \cap \cdots \cap A_k$. Similarly one shows $N^* = A'_1 \cap \cdots \cap A'_\ell \,(= N)$. But then $A_2 \cap \cdots \cap A_k = N^* = N = A_1 \cap \cdots \cap A_k \subset A_1$ contradicts the definition of RPD.

We are forced by these contradictions to admit that $P_1 = P'_j$ for some j, say $j = 1$. Using $A_2 \cap \cdots \cap A_k = N^* = A'_2 \cap \cdots \cap A'_\ell$ we reduce by induction to the base case $k = 1$.

In the $k = 1$ case, if $\ell > 1$ a symmetric argument shows each $P'_{j>1}$ must equal something on the other side, and P_1 is the only possibility. But then $P'_2 = P_1 = P'_1$ contradicts the definition of RPD again, and so $\ell = 1$.

(ii) Suppose P_1 is isolated, and A_1, A'_1 are P_1-primary. For each $j \geq 2$, $\exists r_j \in P_j \backslash (P_j \cap P_1) \implies t := r_2 \cdots r_k \in (P_2 \cap \cdots \cap P_k) \backslash (P_1 \cap \cdots \cap P_k)$. Since A_j [resp. A'_j] is P_j-primary, $\exists$ n_j [resp. m_j] with $t^{n_j} M \subset A_j$ [resp. $t^{m_j} M \subset A'_j$] for $j \geq 2$. Put $n := \max(\{n_j, m_j\}_{j=2}^{k})$, and define $\tilde{N} := \{x \in M \mid t^n x \in N\}$.

I claim that $A_1 = \tilde{N}$. Given $x \in A_1$, we have $t^n x \in A_1 \cap \cdots \cap A_k = N \implies x \in \tilde{N}$. Conversely, $x \in \tilde{N} \implies t^n x \in N \subset A_1$. Since A_1 is P_1-primary and $t \notin P_1$, we have $t^m M \not\subset A_1$ $(\forall m \geq 0)$. Now if $x \notin A_1$, then (since A_1 is primary) $t^n x \in A_1 \implies t^{nq} M \subset A_1$, a contradiction. So $x \in A_1$ and the claim is proved.

Similarly, we get $A_1' = \tilde{N}$. So $A_1' = A_1$ and we are done. $\square$

Turning to the existence of RPDs, we recall that finitely-generated modules over a Noetherian ring, including the ring itself, satisfy the ACC. In particular, IV.D.10 follows immediately from the next result together with IV.D.17.

IV.D.18. THEOREM. *If M satisfies the ACC, then every $N \subsetneq M$ has an RPD.*

PROOF. Say $\mathbb{S} := \{N \subset M \mid N \text{ has no PD}\}$ is nonempty. The ACC yields an upper bound for each chain, hence a maximal $N \in \mathbb{S}$. Since N is certainly non-primary, there exist $r \in R$ and $m \in M \backslash N$ such that $rm \in N$ and $r^n M \not\subset N$ $(\forall n \in \mathbb{N})$.

Define an ascending chain by $M_n := \{x \in M \mid r^n x \in N\}$; in particular, $M_0 = N$ and $M_1 \ni m$. By the ACC, this chain stabilizes at (say) k. Set $\tilde{N} := \{x \in M \mid x = r^k y + z \text{ for some } y \in M, z \in N\}$. Clearly $N \subset M_k \cap \tilde{N}$.

Conversely, given $x \in M_k \cap \tilde{N}$, we have $x = r^k y + z$ and also $r^k x \in N$, hence

$$r^{2k} y = r^k (r^k y) = r^k (x - z) = r^k x - r^k z \in N$$

$\implies y \in M_{2k} = M_k \implies r^k y \in N \implies x = r^k y + z \in N$. So $M_k \cap \tilde{N} = N$.

Now since $m \in M_k \backslash N$ and $r^k M \not\subset M$, we have $N \subsetneq M_k \subsetneq M$ and $N \subsetneq \tilde{N} \subsetneq M$. By maximality of N in $\mathbb{S}$, $\tilde{N}$ and M_k must have PDs. But then their intersection (namely N) does, by concatenating the PDs, a contradiction. So $\mathbb{S} = \emptyset$ and IV.D.16 adds the final touch. $\square$

Krull intersection theorem.

We conclude with an application of primary decomposition. This will require a couple of lemmas.

IV.D.19. LEMMA. *Let M be a finitely generated R-module, and $I :=$ $\mathrm{ann}(M) \subset R$. Then M is Noetherian* [*resp. Artinian*] $\iff$ *R/I is Noetherian* [*resp. Artinian*].

PROOF. $\underline{(\Longleftarrow)}$: Because I annihilates M, M may be regarded also as an R/I-module. Since R/I satisfies the ACC [resp. DCC], so does M as R/I-module (by IV.B.8). As R-submodules are also R/I-submodules, they also satisfy the ACC [resp. DCC].

$\underline{(\Longrightarrow)}$: Writing $M = \sum_{j=1}^{n} Rm_j$ (by finite generation), we have $I = \cap_{j=1}^{n} \mathrm{ann}(Rm_j) =: \cap_{j=1}^{n} I_j$. Consider the natural R-module homomorphisms

$$R/I \overset{\theta}{\hookrightarrow} \times_{j=1}^{n} R/I_j \overset{\cong}{\to} \oplus_{j=1}^{n} Rm_j.$$

As submodules of M, the R/I_j satisfy the ACC [resp. DCC]. Hence, so does the submodule R/I of their direct sum (cf. IV.B.7). $\square$

IV.D.20. LEMMA. *Let $P \subset R$ be a prime ideal, M a Noetherian R-module, and $N \subset M$ a P-primary submodule. Then there exists $m \in \mathbb{N}$ such that $P^m M \subset N$.* (*In particular, any P-primary ideal in a Noetherian ring contains some power of P.*)

PROOF. Set $I := \mathrm{ann}(M)$ and $\bar{R} := R/I$, so that M, N may be viewed as $\bar{R}$-modules. We have

$$I \subset \mathrm{ann}(M/N) \subset P = \mathrm{Rad}(\mathrm{ann}(M/N)).$$

Clearly N is a $\bar{P}$-primary $\bar{R}$-submodule, and $\bar{P}$ consists of the elements of $\bar{R}$ some power of which kills M/N (knocks M into N).

Now M Noetherian $\overset{\text{IV.D.19}}{\Longrightarrow}$ $\bar{R}$ Noetherian $\overset{\text{IV.C.11}}{\Longrightarrow}$ $\bar{P}$ finitely generated $\Longrightarrow$ $\bar{P} = (\bar{p}_1, \ldots, \bar{p}_s)$. So (for each i) $\exists n_i \in \mathbb{N}$ such that $\bar{p}_i^{n_i} M \subset N$. Setting $m = n_1 + \cdots + n_s$, we have $\bar{P}^m M \subset N$ hence $P^m M \subset N$. $\square$

IV.D.21. KRULL INTERSECTION THEOREM (v. 1). *Given an ideal* $I \subset R$ *and a Noetherian R-module* M*, set* $N = \cap_{n \geq 1} I^n M$*. Then* $IN = N$*.*

PROOF. If $IN = M$, then $M = IN \subset N \implies N = M = IN$. So we may assume $IN \neq M$, and let $IN = N_1 \cap \cdots \cap N_s$ be a RPD with associated primes $P_1, \ldots, P_s$.

Suppose $I \subset P_i$ (for some i); then IV.D.20 $\implies P_i^m M \subset N_i$ (for some m) $\implies N = \cap_{n \geq 1} I^n M \subset I^m M \subset P_i^m M \subset N_i$.

On the other hand, if $I \not\subset P_i$, then let $r \in I \backslash (I \cap P_i)$. If $N \not\subset N_i$, then $\exists v \in N \backslash (N \cap N_i)$; and since $rv \in IN \subset N_i$, $v \notin N_i$, and N_i is primary, we must have $r^n M \subset N_i$ (for some n) hence $r \in P_i$. This contradiction means that $N \subset N_i$.

So either way, $N \subset N_i$. Since i was arbitrary, $N \subset \cap_i N_i = IN$ hence $N = IN$. □

It will be easier to see what this means (at least for local rings) in "v. 2", after we prove Nakayama's theorem in the next section.