CLASS 26, APRIL 22ND: ASSOCIATED PRIMES

Today, we will return to the question of how to express a generic ideal in terms of prime ideals. The first step in this direction is to study the associated primes, or assassins, of an ideal, which might as well be defined for modules:

Definition 26.1. If M is an R-module, $\mathfrak{p} \in \mathrm{Spec}(R)$ is said to be **associated to** M, or an **associated prime of** M, or an **assassin of** M, if there exists an injective module homomorphism $R/\mathfrak{p} \hookrightarrow M$, i.e. $R/\mathfrak{p}$ is a submodule of M.

We (unflatteringly) call the set of Associated primes $\mathrm{Ass}(M)$.

Proposition 26.2. *Every $\mathfrak{p} \in \mathrm{Ass}(M)$ has the property that $\mathrm{Ann}(M) \subseteq \mathfrak{p}$. Additionally, $\mathfrak{p} \in \mathrm{Ass}(M)$ if and only if there exists $m \in M$ such that $\mathrm{Ann}(m) = \mathfrak{p}$.*

Proof. The second result implies the first, since $\mathrm{Ann}(M) = \bigcap_{0\neq m\in M} \mathrm{Ann}(m)$.

$\Rightarrow$: Suppose $\mathfrak{p} \in \mathrm{Ass}(M)$. Then $R/\mathfrak{p} \hookrightarrow M$. Consider the image of $1+\mathfrak{p}$ and call it m. Then it is immediate that $\mathrm{Ann}(m) = \mathfrak{p}$ by injectivity of the map.

$\Leftarrow$: Of course, if $\mathrm{Ann}(m) = \mathfrak{p}$, then we can construct the injective map

$$R/\mathfrak{p} \to M : 1 \mapsto m$$

$\square$

Example 26.3. If $n = p_1^{e_1} \cdots p_l^{e_l}$, then we can easily conclude that

$$\mathrm{Ass}(Z/n\mathbb{Z}) = \{\langle p_1\rangle, \dots, \langle p_l\rangle\}$$

This comes by considering the elements

$$m_i = p_1^{e_1} \cdots p_i^{e_i-1} \cdots p_l^{e_l} \in \mathbb{Z}/n\mathbb{Z}$$

for various i, which clearly has annihilator $\langle p_i\rangle$. Note that by our previous analysis we can conclude the following cool result:

$$\sqrt{\langle n\rangle} = \langle p_1\rangle \cap \cdots \cap \langle p_l\rangle = \bigcap_{\mathfrak{p}\in\mathrm{Ass}(\mathbb{Z}/n\mathbb{Z})} \mathfrak{p}$$

We will later see how deeply this connection goes. But first, we move onto the properties of $\mathrm{Ass}(M)$.

Proposition 26.4.
(a) *If $x \in M$ has $\mathrm{Ann}(x) = \mathfrak{p} \in \mathrm{Spec}(R)$, then every non-zero R-multiple of x, say $y = rx$, has $\mathrm{Ann}(y) = \mathfrak{p}$ as well. Thus $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$*
(b) *A maximal element of $\mathcal{S} = \{\mathrm{Ann}(m) \mid 0 \neq m \in M\}$ is prime, and thus in $\mathrm{Ass}(M)$.*
(c) *If R is Noetherian, then $M \neq 0$ implies $\mathrm{Ass}(M) \neq \emptyset$.*
(d) *Given a SES $0 \to M' \to M \to M'' \to 0$, we have that*

$$\mathrm{Ass}(M') \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$$

Proof.
(a) x is the image of 1 for some $R/\mathfrak{p} \hookrightarrow M$. As a result, since $R/\mathfrak{p}$ is a domain, y has image r which is a non-zero divisor. Thus $\mathrm{Ann}(y) = \mathfrak{p}$.
(b) Assume $\mathrm{Ann}(m)$ is maximal in $\mathcal{S}$. Suppose $x \cdot y \in \mathrm{Ann}(m)$, but $x, y \notin \mathrm{Ann}(m)$. Then $x \cdot m \neq 0$, and is annihilated by y. Therefore, $\mathrm{Ann}(m) \subsetneq \mathrm{Ann}(xm)$, contradicting maximality.

(c) The Noetherian property implies that any ascending chain
$$\mathrm{Ann}(m_1) \subseteq \mathrm{Ann}(m_2) \subseteq \cdots$$
must stabilize, providing an upper bound. Thus a maximal element in $\mathcal{S}$ of part (b) exists by Zorn's Lemma, and is therefore associated to M.

(d) If $\mathfrak{p} \in \mathrm{Ass}(M')$ composing yields $R/\mathfrak{p} \hookrightarrow M' \hookrightarrow M$, showing $\mathfrak{p} \in \mathrm{Ass}(M)$. Suppose $R/\mathfrak{p} \subseteq M$. Then we have that either $R/\mathfrak{p} \cap M' = 0$, in which case $R/\mathfrak{p} \hookrightarrow M''$. Alternatively, $R/\mathfrak{p} \cap M' \neq 0$. If x is in this intersection, then $\mathrm{Ann}(x) = \mathfrak{p}$ by part (a), showing $\mathfrak{p} \in \mathrm{Ass}(M')$.

□

Corollary 26.5. *If R is Noetherian, then for an R-module M,*
$$\{\textit{zero divisors of } M\} = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$$

Proof. This follows since zero divisors must be in some $\mathrm{Ann}(m)$ and by (b) of Proposition 26.4. For the reverse inclusion, each $\mathfrak{p}$ is the annihilator of some element by Proposition 26.2. □

Example 26.6. Let I be a radical ideal of a Noetherian domain R. Then
$$I = \sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$$
for some primes $\mathfrak{p}_i \in \mathrm{Spec}(R)$. Then we can form an exact sequence
$$0 \to I \to R \to R/I \to 0$$
by Proposition 26.4 (d), we know that
$$\mathrm{Ass}(I) \subseteq \mathrm{Ass}(R) \subseteq \mathrm{Ass}(I) \cup \mathrm{Ass}(R/I)$$
However, R being a domain implies $\mathrm{Ann}(r) = 0$ for every $r \neq 0$, so the only associated prime is 0 itself. However, since $R/I \hookrightarrow R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n$, we see $\mathrm{Ass}(R/I) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. It is harder to get equality here, but in the case of the Chinese Remainder Theorem (i.e. each $\mathfrak{p}_i, \mathfrak{p}_j$ is coprime, c.f. Theorem 26.7), the above inclusion is actually an isomorphism! Thus it is easy to construct an example ($I = \mathfrak{p}_i$) where
$$\mathrm{Ass}(R) \subsetneq \mathrm{Ass}(I) \cup \mathrm{Ass}(R/I)$$

Theorem 26.7 (Chinese Remainder Theorem)**.** *If $I_1, \ldots, I_n$ are pairwise coprime ideals (i.e. $I_i + I_j = R$ for each $i \neq j$), and $I = I_1 \cap \cdots \cap I_n$, then*
$$R/I \cong R/I_1 \times \cdots \times R/I_n$$

Proof. The map $R \to R/I_1 \times \cdots \times R/I_n : r \mapsto (r + I_1, \ldots, r + I_n)$ has kernel I. It only goes to show that it is also surjective.

I proceed by induction. If $n = 2$, then we can choose $a \in I_1$ and $b \in I_2$ such that $a + b = 1$. Then considering $r_2 a + r_1 b \in R$, we have that its image is
$$(r_1, r_2) \equiv (r_1 a + r_1 b, r_2 a + r_2 b) \equiv (r_2 a + r_1 b, r_2 a + r_1 b) \equiv (r_1 b, r_2 a) \pmod{I_1 \times I_2}$$
For the induction, it only goes to note that $I_1 \cap \cdots \cap I_{n-1}$ is coprime to I_n. Taking $a_i + b_i = 1$ for $a_i \in I_i$ and $b_i \in I_n$ for $i = 1, \ldots, n-1$, we can conclude
$$1 = 1^{n-1} = \prod_i (a_i + b_i) \in a_1 \cdots a_n + I_n \subseteq I_1 \cap \cdots \cap I_{n-1} + I_n$$
as desired! □