The primary decomposition of modules over a ring.

Let R be a ring and M an R module. Then the ***annihilator*** of M in R is

$$\operatorname{Ann}(M) = \{r \in R : rx = 0 \text{ for all } x \in M\}$$

Problem 1. Show $\operatorname{Ann}(M)$ is an ideal of R. □

If R is a PID, then all ideals of R are principal and thus $\operatorname{Ann}(M) = \langle h \rangle$ for some $h \in R$.

Proposition 1. *Let V be a finite dimensional vector space over the field $\mathbb{F}$ and let $A\colon V \to V$ be a linear map. Make V into a module over the polynomial ring $\mathbb{F}[x]$ by*

$$f(x) \cdot v = f(A)v.$$

(We denote this $\mathbb{F}[x]$ module by V_A.) Then

$$\operatorname{Ann}(V_A) = \langle h(x) \rangle$$

where $h(x) = \min_A(x)$ is the minimal polynomial of A.

Problem 2. Prove this. □

Definition 2. Let M be an R module and $r \in R$ then the ***annihilator*** of r in M is

$$M(r) := \{x \in M : Rx = 0\}. \qquad \square$$

Problem 3. With the set up of Proposition 1 for $f(x) \in \mathbb{F}[x]$ show

$$V_A(f(x)) = \ker f(A).$$

That is the annihilator of $f(x)$ in V_A is just the kernel of the linear map $f(A)$. □

Theorem 3. *Let R be a PID and M a R module such that* $\operatorname{Ann}(M) \neq 0$. *Then*

$$\operatorname{Ann}(M) = \langle h \rangle$$

for some $0 \neq h \in R$. As PIDs are UFDs we can factor h into prime powers

$$h = p_1^{n_1} p_1^{n_2} \cdots p_k^{n_k}.$$

Then, with the notation of Definition 2 M splits as a direct sum

$$M = M(p_1^{n_1} \oplus M(p_1^{n_2}) \oplus \cdots \oplus M(p_k^{n_k}).$$

*This is the **primary decomposition** of M.*

Problem 4. Prove this along the following lines (this proof is going to look very much like one of the proofs of the Chinese remainder theorem, with is the motivation both for the theorem and its proof). First, to simplify notation, let

$$q_j = p_j^{n_j}.$$

Then

$$\operatorname{Ann}(M) = \langle h \rangle = \langle q_1 q_2 \cdots q_k \rangle.$$

For $1 \le j \le k$ let

$$h_j = \frac{h}{q_j} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_k = \prod_{i \in \{1,2,\dots,k\} \setminus \{j\}} q_i$$

(a) Show that if $i \ne j$, then

$$h_i h_j x = 0$$

for all $x \in M$.

(b) Show

$$\gcd(h_1, h_2, \dots, h_k) = 1.$$

(c) Show that there are $f_1, f_2, \dots, f_k \in R$ such that

$$f_1 h_1 + f_2 h_2 + \cdots + f_k q_k = 1.$$

(d) Define maps $E_j \colon M \to M$ as mutiplication by $f_f h_j$. That is

$$E_j(x) = f_j h_j x.$$

Show

(i) $E_1 + E_2 + \cdot E_k = I$ (where I is the identity on M.)

(ii) $E_j^2 = E_j$ (that is each E_j are idempotents.)

(iii) $E_i E_j = 0$ for $i \ne j$.

(e) Let $M_j := E_j M = \{E_j x : x \in M\}$ and show

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_k.$$

(f) Finish by showing

$$M_j = M(q_j).$$

Hint: If $x \in M_j$, then for some $x' \in M$ we have $x = E_j x' = f_j h_j x'$ and use $q_j h_j = h$ and $hy = 0$ for all y to see $q_j x = 0$. Therefore $M_j \subseteq M(q_j)$.

If $x \in M(q_j)$ then $q_j x = 0$ and use this to show $q_i x = 0$ for $i \ne j$. Then

$$x = 1x = (f_1 h_1 + f_2 h_2 + \cdots + f_k q_k)x = f_j h_j x = E_j x \in M_j.$$

Whence $M(q_j) \subseteq M_j$. □

Here are some examples that show how this is useful in concrete settings.

Problem 5. Let $A \colon V \to V$ be a linear map on the finite dimensional vector space V. Show that if the minimal polynomial of o A is $x^3 - x$, then

$$V = \{v : Av = -v\} \oplus \{v : Av = 0\} \oplus \{v : Av = v\}.$$ □

Problem 6. Let $A \colon V \to V$ be a linear map on a finite dimensional vector space. Assume the minimal polynomial of A is of the from

$$h(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_k)$$

for distinct elements $\lambda_1, \dots, \lambda_k$ of the field of scalars. Show this implies

$$V = \bigoplus_{j=1}^{k} \ker(A - \lambda_j I)$$

which in turn implies A is diagonalizable. □

Problem 7. Let $A\colon V \to V$ be a linear map over the complex numbers $\mathbb{C}$ where V is finite dimensional. Then the minimal polynomial of A factors as a product of powers of linear factors:

$$\min_A(x) = \prod_{j=1}^{k} (x-\lambda_j)^{n_j}.$$

Show

$$V = \bigoplus_{j=1}^{k} \ker\left((A-\lambda_j I)^{n_j}\right).$$

(In some derivations of the Jordan canonical form this is one of the main steps.) □

This can all be generalize a good deal.

Proposition 4. *Let R be ring and M an R-module. Assume there are ideals $Q_1, Q_2, \ldots, Q_k$ of R such that*

$$Q_1 \cap Q_2 \cap \cdots \cap Q_k \subseteq \operatorname{Ann}(M)$$

and that the ideal are pairwise relatively prime in the sense that

$$Q_i + Q_j = R$$

for all $i \neq j$. Set

$$M(Q_j) := \{x \in M : qx = 0 \textit{ for all } q \in Q_j\}.$$

Then

$$M = M(Q_1) \oplus M(Q_2) \oplus \cdots \oplus M(Q_k).$$

Problem 8. Prove this. *Hint:* Note as $Q_1 + Q_i = R$ for $i \geq 2$ we have that there are $q_{1i} \in Q_1$ and $q_i \in Q_i$ with

$$1 = q_{1i} + q_i$$

Then

$$1 = 1^{k-1} = \prod_{i=2}^{k} (q_{1i} + q_i).$$

For example if $k = 4$ this is

$$\begin{aligned} 1 &= (q_{12}+q_2)(q_{13}+q_3)(q_{14}+q_4) \\ &= \Big(q_{12}q_{13}q_{14} + q_2q_{13}q_{14} + q_{12}q_3q_{14} + q_{12}q_{13}q_4 \\ &\qquad + q_2q_3q_{14} + q_2q_{13}q_4 + q_{12}q_3q_4 \Big) + q_2q_3q_4 \end{aligned}$$

where each of the terms in the parenthesis has a factor that is in Q_1 and thus the sum of the terms in the parenthesis is in Q_1. The term $q_{12}q_{13}q_{14}$ is in the intersection $Q_2 \cap Q_3 \cap Q_4$. Thus we have

$$1 = \hat{q}_1 + e_1, \quad \text{with } \hat{q}_1 \in Q_1 \text{ and } e_1 \in (Q_2 \cap Q_3 \cap Q_4).$$

In the general case we expand $\prod_{i=2}^{k}(q_{1i}+q_i)$ to get 2^{k-1} terms all but one of which have a factor which is in Q_1 and the remaining term is the product $q_2q_3\cdots q_k$ which is in $Q_2\cap Q_2\cap Q_k$. Therefore we can write

$$1=\hat{q}_1+e_1 \quad \text{with } \hat{q}_1\in Q_1 \text{ and } e_1\in(Q_2\cap Q_3\cap\cdots\cap Q_k).$$

Interchanging the roles of 1 and j we can find $\hat{q}_j$ and e_j with

$$1=\hat{q}_j+e_j \quad \text{with } \hat{q}_j\in Q_j \text{ and } e_j\in \bigcap_{i\in\{1,2,\dots,k\}\setminus\{j\}} Q_i.$$

Use this and $Q_1\cap Q_2\cap\cdots Q_k\subseteq \operatorname{Ann}(M)$ to show

$$\begin{aligned} e_1+e_2+\cdots+e_k &\equiv 1 \mod \operatorname{Ann}(M)\\ e_ie_j &\equiv 0 \mod \operatorname{Ann}(M) \quad \text{for } i\neq j\\ e_j^2 &\equiv e_j \mod \operatorname{Ann}(M)\end{aligned}$$

Set

$$M_j=\{e_jx : x\in M\}$$

and show splits M as a direct sum

$$M=M_1\oplus M_2\oplus\cdots\oplus M_k.$$

To finish show

$$M_j=M(Q_j).$$

In outline here is how this goes for $j=1$. First note $e_1\in Q_2\cap Q_2\cdots Q_k$. So if $q\in Q_1$, then $qe_1\in Q_1\cap Q_2\cap\cdots\cap Q_k\subseteq \operatorname{Ann}(M)$. Therefore if $y=e_1x\in M_1$ and $q\in Q_1$ we see $qy=qe_1x=0$. This shows $M_1\subseteq M(Q_1)$.

If $x\in M(Q_1)$, then for each $i>1$ we have $e_i\in Q_1$ and thus $e_ix=0$. Whence

$$x=e_1x+e_2x+\cdots e_kx=e_1x+0+\cdots+0=e_1x\in M_1$$

which shows $M(Q_1)\subseteq M_1$. □