Abstract Algebra. Math 6310. Bertram/Utah 2022-23.

More Modules, especially over a PID

An R-module M is *freely generated* by elements $w_1, ..., w_m \in M$ if:

$$f : R^m \to M;\ f(e_i) = w_i \text{ is an isomorphism}$$

Let R be a PID and M be a finitely generated R-module.

Proposition 1. If $M \subset R^n$ is a sub-module of a free module, then M is also free. In fact, there are elements $v_1, ..., v_n \in R^n$ and $d_1, ..., d_m \in R$ for $m \le n$ such that:

(i) The $v_1, ..., v_n$ freely generate R^n.

(ii) Each $d_i v_i \in M$ and the $d_1 v_1, ..., d_m v_m$ freely generate M

(iii) Each *invariant factor* d_i divides d_{i+1}. That is:

$$\langle d_m \rangle \subset \langle d_{m-1} \rangle \subset \cdots \subset \langle d_1 \rangle$$

Remark. When $R = k$ is a field, this is the statement that each subspace of k^n has a basis $v_1, ..., v_m \in k^n$ of vectors that extends to a basis $v_1, ..., v_n$ of k^n.

Proof. M is finitely generated since R is Noetherian, and a choice of generators $w_1, ..., w_l$ for M gives a matrix:

$$A : R^l \to R^n \text{ whose image is } M$$

with column vectors $w_1, ..., w_l$ and entries a_{ij}. If A only consists of:

$$a_{ii} = d_i \text{ for } i \text{ from 1 to } m \text{ with } d_1 | d_2 | \cdots | d_m$$

Then the Proposition holds with $v_i = e_i$ the standard basis of R^n and $w_i = d_i v_i$. The goal, then, is to diagonalize the matrix A with the use of automorphisms (invertible matrices) $C \in \mathrm{Aut}(R^l)$ and $B \in \mathrm{Aut}(R^n)$. If we can achieve the desired diagonal matrix as BAC, then the columns of B^{-1} are the vectors v_i we seek.

In fact, the entries of A already tell us what d_1 needs to be, namely:

$$\langle d_1 \rangle = \langle a_{ij} \rangle$$

a generator (R is a PID) of the ideal generated by all the entries of A. To this end, let's recall that row and column operations (switching rows/columns, adding a multiple of a row/column to another) are achieved by multiplication with such matrices B and C (of determinant 1). To this, we add one more operation:

Let $a, b \in R$ and suppose $\langle d \rangle = \langle a, b \rangle$, so that: $ax + by = d,\ a = dp,\ b = dq$ and so $xp + yq = 1$ for some $x, y, p, q \in R$. Then:

$$[a \ \ b] \cdot \begin{bmatrix} x & -q \\ y & p \end{bmatrix} = [d \ \ 0]$$

and the transpose:

$$\begin{bmatrix} x & y \\ -q & p \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$$

show how to apply 2×2 matrix (augmented by the identity) to modify a matrix A with elements $a = a_{ij}, b = a_{i,k}$ in the same row or $b = a_{kj}$ in the same column to get a new "improved" matrix A. Together with row and column operations, this allows one to obtain the desired diagonal form of BAC.

Definition. A matrix $D = BAC$ as above with the divisibility property $d_{1,1} | \cdots | d_{m,m}$ (and no other nonzero entries) is a *Smith normal form* for A.

Example. Suppose $M \subset \mathbb{Z}^2$ is generated by $(2,0)$ and $(0,3)$. Then:

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$$

multiplied on the left by

$$B_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

(to add the second row to the first) gives:

$$B_1 A = \begin{bmatrix} 2 & 3 \\ 0 & 3 \end{bmatrix}$$

which then may be multiplied on the right by:

$$C_1 = \begin{bmatrix} -1 & 2 \\ 1 & -3 \end{bmatrix}$$

to get

$$B_1 A C_1 = \begin{bmatrix} 1 & -5 \\ 3 & -9 \end{bmatrix}$$

and then multiplied on the left and right by:

$$B_2 = \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix} \text{ and } C_2 = \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix}$$

to clear the first row and column, to finally get

$$B_2 B_1 A C_1 C_2 = \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$$

and since:

$$B^{-1} = (B_2 B_1)^{-1} = \begin{bmatrix} -2 & -1 \\ 3 & 1 \end{bmatrix}$$

we get desired vectors:

$$v_1 = (-2,3) \text{ and } v_2 = (1,-1) \text{ with } v_1, 6v_2 = (-6,6) \text{ freely generating } M$$

As a corollary, we get the:

Invariant Factor Decomposition for Modules over a PID. If M is a finitely generated module over a PID R, then M is isomorphic to:

$$R/\langle d_1 \rangle \oplus \cdots \oplus R/\langle d_m \rangle \oplus R^r$$

for elements $d_1 | d_2 | \cdots | d_m \in R$.

Proof. Choose a surjection $f : R^n \to M$ and apply Proposition 1 to the **kernel**. Then:

$$M = R^n/K = R/d_1 R \oplus \cdots \oplus R/d_m R \oplus R^{n-m}$$

by the choice of basis $v_1, ..., v_n \in R^n$, with one caveat. If $d \in R$ is a unit, then $R/dR = 0$ is a superfluous factor, and we will leave those out.

Example. In the example above, $(\mathbb{Z} \oplus \mathbb{Z})/(2\mathbb{Z} \oplus 3\mathbb{Z}) = \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$.

Corollary. Every finitely generated abelian group is a product of cyclic groups.

Before we prove uniqueness of the collection of summands in the theorem, we make some remarks about finitely generated modules M over general commutative rings R with 1 to obtain an alternative decomposition to the invariant factors.

Definition. (a) Given an ideal $I \subset R$, then:

$$IM = \{\sum_{\text{finite}} a_i m_i \mid a_i \in I, m_i \in M\}$$

is the *product* R-module. When $I = \langle a \rangle$, the product is denoted aM.

(b) The *annihilator* of a module M is the largest ideal satisfying $IM = 0$, i.e.

$$\operatorname{Ann}(M) = \{a \in A \mid aM = 0\}$$

(c) M is *cyclic* if M has a single generator, in which case $M \cong R/\operatorname{Ann}(M)$.

Proposition 2. Let $S, T \subset M$ be submodules. Then:

$$0 \to S \cap T \xrightarrow{f} S \oplus T \xrightarrow{g} S + T \to 0$$

$$f(m) = (-m, m),\ g(s, t) = s + t$$

is a short exact sequence of R-modules.

The proof of this is left to the reader.

Corollary. If $S \cap T = 0$ and $S + T = M$, then $M \cong S \oplus T$.

Applying this to the invariant (cyclic) factors of a module M over a PID, we get:

Proposition 3. Let $d \in R$ (a PID), and let

$$d = p_1^{r_1} \cdots p_k^{r_k}$$

be a prime factorization of d, with $p_i \neq p_j$ for $i \neq j$. Then:

$$R/\langle d \rangle \cong R/\langle p_1^{r_1} \rangle \oplus \cdots \oplus R/\langle p_k^{r_k} \rangle$$

Proof. The result follows inductively once we show the following. If $a, b \in R$ share no common prime factor, then:

$$R/\langle ab \rangle \cong R/\langle a \rangle \oplus R/\langle b \rangle$$

This in turn follows from Proposition 2, via the two inclusions:

$$f : R/\langle a \rangle \hookrightarrow R/\langle ab \rangle;\ f(r + aR) = br + abR$$

and

$$g : R/\langle b \rangle \hookrightarrow R/\langle ab \rangle;\ f(r + bR) = ar + abR$$

The UFD property of a PID gives:

$$R/\langle a \rangle \cap R/\langle b \rangle = 0$$

and the PID property of a PID gives $1 = ax + by$ for some x, y since a, b, by virtue of sharing no common prime factor, do not lie in any common maximal ideal. Then $f(y + aR) + g(x + bR) = 1 + abR$ and so $R/\langle a \rangle + R/\langle b \rangle = R/\langle ab \rangle$ $\square$

This leads to a:

Primary Decomposition of Modules over a PID. Every finitely generated module M over a PID R is a direct sum:

$$M = \bigoplus R/\langle p_i^{r_i} \rangle$$

of cyclic R-modules $C_i = R/\langle p_i^{r_i} \rangle$ with *primary* annihiator ideals $\operatorname{Ann}(C_i) = \langle p_i^{r_i} \rangle$.

Proof. Apply Prop 3 to each summand of the invariant factor decomposition.

Uniqueness. The torsion submodule $T \subset M$ of a finitely generated module M over a PID is uniquely determined, and from an invariant factor decomposition, we obtain:

$$T \cong R/\langle d_1 \rangle \oplus \cdots \oplus R/\langle d_m \rangle \text{ and } M/T \cong R^r$$

Since the *rank* of a free R-module is well-defined, this gives the uniqueness of the number of free cyclic modules in the decomposition. Moreover, the smallest ideal (most divisible d_m) is also easily determined via:

$$\text{Ann}(T) = \langle d_m \rangle$$

but for the other factors, we will turn to the primary decomposition. In light of the well-definedness of the rank r of the free part, we may as well restrict our attention to torsion finitely generated R-modules T.

Proposition 4. The cyclic summands $R/\langle p_i^{r_i} \rangle$ of a primary decomposition of T uniquely determine the cyclic summands of an invariant factor decomposition of T.

Proof. For each prime p appearing in the primary decomposition, lay out the summands in increasing order of the power of p in a single row:

$$R/\langle p \rangle \oplus \cdots \oplus R/\langle p^2 \rangle \oplus \cdots \oplus R/\langle p^{r_p} \rangle \oplus \cdots$$

Right justify the rows for the distinct primes and use Proposition 3 to multiply the prime powers in the columns to obtain each $R/\langle d_i \rangle$. Thus, for example,

$$R/\langle d_m \rangle = R/\langle p_1^{r_{p_1}} p_2^{r_{p_2}} \cdots \rangle$$

This procedure is the (unique!) inverse to the factoring procedure. $\square$

Remark. It is an inverse only in the sense that number of cyclic modules of each type in each decomposition are determined by each other. There are quite a few automorphisms of T (e.g. reordering the prime factors of the same type) that negates any attempt to assign a canonical decomposition of either type. We only can record the number of summands of each type.

Example. $T = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ converts to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and then back again, but the order of the $\mathbb{Z}/3\mathbb{Z}$ factors in the return trip could be reversed, resulting in a nontrivial automorphism of T. In particular, the subgroup $\mathbb{Z}/6\mathbb{Z} \subset T$ is not canonically defined.

We now prove the uniqueness of the summands of the primary decomposition. To do this (and because it is a useful tool for studying modules), we introduce the *localization* of an R-module M for a general commutative ring R with 1. This requires us to make some improvements to our earlier definition since now we cannot avoid the issue of zero divisors (annihilators) in our multiplicative set.

Localization 2.0. Let R be a commutative ring with 1 (possibly not a domain) let $S \subset R$ be a multiplicative subset and let M be an R-module. Then:

$$S^{-1}R = \{\frac{r}{s} \mid r \in D,\ s \in S\}/\sim \text{ and } S^{-1}M = \{\frac{m}{s} \mid m \in M,\ s \in S\}/\sim$$

where

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \text{ if and only if } \exists s \in S \text{ such that } s(r_1 s_2 - r_2 s_1) = 0$$

and

$$\frac{m_1}{s_1} \sim \frac{m_2}{s_2} \text{ if and only if } \exists s \in S \text{ such that } s(m_1 s_2 - m_2 s_1) = 0$$

Then $\sim$ is an equivalence relation and $S^{-1}R$ is a commutative ring with $1 \neq 0$ and $S^{-1}M$ is an $S^{-1}R$-module. The morphisms:

$$i : R \to S^{-1}R \text{ and } i : M \to S^{-1}M$$

are not necessarily injective in this setting, though, since:

$$i(r) = 0 \Leftrightarrow sr = 0 \text{ for some } s \in S \text{ and } i(m) = 0 \Leftrightarrow sm = 0 \text{ for some } s \in S$$

Example. If $R = \mathbb{Z}$ and $M = \mathbb{Z}/6\mathbb{Z}$ and $S = \{1, 2, 4, 8, ...\}$, then:

$$R \subset S^{-1}R = \{\frac{a}{2^n} \mid a \text{ is odd}\} \cup \{0\}$$

and

$$M \to S^{-1}M = \mathbb{Z}/3\mathbb{Z} \text{ has kernel } 3M \text{ with } \frac{1}{2} \cdot m = 2m$$

Let $p, q \in R$ be two prime elements in a PID.

Proposition 5. Let $S = R - qR$. Then:

(a) $D = S^{-1}R$ is a DVR with maximal ideal $\mathfrak{m}$ (i.e. R is a Dedekind domain)

(b) $S^{-1}(R/q^rR) = D/\mathfrak{m}^r$.

(c) $S^{-1}(R/p^rR) = 0$ if p is not associated to q.

Proof. The maximal ideal $\mathfrak{m} \subset D$ is $S^{-1}qR$, generated by $q/1$, so D is a DVR and the ideals in D are the powers $\mathfrak{m}^r = (q^r/1)D = S^{-1}q^rR$.

If $\langle p\rangle \neq \langle q\rangle$, then $p^r \in S$ and $p^r(1 - 0) = 0 \in R/p^rR$ so $1 = 0$ in $S^{-1}(R/p^rR)$.

This only leaves (b), which is the interesting assertion that:

$$S^{-1}R/S^{-1}q^rR = S^{-1}(R/q^rR)$$

which we leave to the reader in its general form.

Proposition 6. If $M \subset N$ are R-modules and $S \subset R$ is a multiplicative set, then:

$$S^{-1}N \subset S^{-1}M \text{ and } (S^{-1}N)/(S^{-1}M) \cong S^{-1}(N/M)$$

Proof. Exercise.

Proof of Uniqueness. Via localizing as in Proposition 5 for each prime q in turn, it suffices to show that if D is a DVR and

$$T = (D/\mathfrak{m})^{r_1} \oplus \cdots \oplus (D/\mathfrak{m}^n)^{r_n}$$

then $r_1, ..., r_n$ are determined. Note that $D/\mathfrak{m}$ is a field k, and:

$$0 = \mathfrak{m}^n/\mathfrak{m}^n \subset \mathfrak{m}^{n-1}/\mathfrak{m}^n \subset \cdots \subset \mathfrak{m}/\mathfrak{m}^n \subset D/\mathfrak{m}^n$$

is a composition series, in which each successive quotient:

$$(\mathfrak{m}^{i-1}/\mathfrak{m}^n)/(\mathfrak{m}^i/\mathfrak{m}^n) \cong \mathfrak{m}^{i-1}/\mathfrak{m}^i \cong k$$

(by the third isomorphism theorem). Thus, as a k-vector space, $D/\mathfrak{m}^n$ has rank n. Now we work by induction, multiplying T by powers of $\mathfrak{m}$:

$$\mathfrak{m}^{n-1}T \cong (\mathfrak{m}^{n-1}/\mathfrak{m}^n)^{r_n} = k^{r_n}$$

so r_n is determined by T alone. Next,

$$\mathfrak{m}^{n-2}T \cong (\mathfrak{m}^{n-2}/\mathfrak{m}^{n-1})^{r_{n-1}} \oplus (\mathfrak{m}^{n-2}/\mathfrak{m}^n)^{r_n} = V$$

has dimension $r_{n-1} + 2r_n$ as a vector space over k, so r_{n-1} is determined, etc. □

Next, we apply this to the problem of finding "canonical forms" of a matrix.

An Application to Linear Algebra. Recall the following:

Definition. Two $n \times n$ matrices $A_1, A_2 : k^n \to k^n$ are *similar* if there is an invertible matrix $B : k^n \to k^n$ such that $A_2 = BA_1B^{-1}$.

Remark. Similarity of matrices is an equivalence relation. If V is a vector space of dimension n and $f : V \to V$ is a linear map. Then a choice of basis $k^n \cong V$ determines a matrix representation $A : k^n \cong V \xrightarrow{f} V \cong k^n$, and the matrices for two distinct choices of basis are similar via the *change of basis* matrix B.

Recall also:

Definition. Two fundamental polynomials associated to a matrix A are:

(i) The characteristic polynomial of A

$$\chi_A(t) = \det(tI_n - A) = t^n - \mathrm{tr}(A)t^{n-1} + \cdots + (-1)^n \det(A) \in k[t] \text{ and}$$

(ii) The minimal polynomial (ideal) of $f : V \to V$:

$$\{P(t) \in k[t] \mid 0 = P(f) : V \to V\} \subset k[t]$$

in which constants $c \in k$ are converted to scalar multiplication $c : V \to V$ and multiplication (e.g. $t \cdot t$) is converted to composition (e.g. $f \circ f$) and the minimal polynomial $\mu_f(t)$ is the unique monic generator of this ideal.

The minimal polynomial of similar matrices is clearly the same since it does not depend upon the choice of basis of V! The characteristic polynomial of similar matrices is also the same since the determinant is a multiplicative function, and so:

$$\det(BAB^{-1}) = \det(B)\det(A)\det(B^{-1}) = \det(B)\det(A)\det(B)^{-1} = \det(A)$$

and $\chi_A(t) = \det(tI_n - A) = \det(B(tI_n - A)B^{-1}) = \det(tI_n - BAB^{-1})$. This means we are justified in reindexing the characteristic polynomial by f:

$$\chi_f(t) = \chi_A(t) \text{ for any matrix representation } A \text{ of } f$$

Note. The trace of similar matrices is also the same, but trace is not multiplicative! Instead, the basic identity satisfied by trace is: $\mathrm{tr}(AB) = \mathrm{tr}(BA)$.

And now for the punchline:

Observation. The choice of a k-linear endomorphism of a k-vector space:

$$f : V \to V$$

is equivalent to promoting V to a (torsion) $k[t]$-module V_f via:

$$t \cdot v = f(v) \text{ for } v \in V$$

Rational Canonical Form. Decompose the $k[t]$-module V_f into invariant factors:

$$V_f \cong k[t]/\langle d_1(t)\rangle \oplus \cdots \oplus k[t]/\langle d_m(t)\rangle \text{ with } d_1(t)|d_2(t)|\cdots|d_m(t)$$

Each summand is a vector space V_i of dimension $n_i = \deg(d_i)$ and

$$n = \sum_{i=1}^{m} n_i$$

and each summand is a (cyclic) $k[t]$-module, corresponding to the linear map:

$$f_i : V_i \to V_i \text{ with } f_i(v) = t \cdot v$$

This means that if we choose the basis $\mathcal{B} = \{1, t, \cdots, t_{n_i - 1}\}$ for V_i and if:

$$d_i(t) = t^{n_i} + c_{n_i - 1} t^{n_i - 1} + \cdots + c_1 t + c_0$$

then the matrix representing f_i in the basis $\mathcal{B}$ is:

$$A_i = \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ & & \vdots & & \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{bmatrix}$$

This is one of the *rational canonical blocks* of f in rational canonical form.

A straightforward calculation gives:

$$\chi_{f_i}(t) = \chi_{A_i}(t) = d_i(t) \text{ and } \chi_f(t) = \prod \chi_{f_i}(t) = \prod d_i(t)$$

On the other hand, the minimal ideal is the annihilator of the module.

$$\mathrm{Ann}(V_f) = \langle d_m(t) \rangle$$

and so in particular, we get the:

Cayley-Hamilton Theorem: The characteristic polynomial of f satisfies

$$\chi_f(f) = 0$$

i.e. χ_f is in the minimal polynomial ideal $\langle d_m(t) \rangle$ of f.

Jordan Canonical Form. Assume k is *algebraically closed* so the primes

$$p_i \subset k[t] \text{ are } p_i = \langle x - \lambda_i \rangle \text{ for } \lambda_i \in k$$

Then the primary decomposition of V_f has the form:

$$V_f = \bigoplus k[t]/\langle (x - \lambda_i)^{n_i} \rangle = \bigoplus V_{g_i}$$

(maybe with repeating “eigenvalues” λ_i). For each summand, choose the basis:

$$\mathcal{B} = \{(t - \lambda_i)^{n_i - 1}, ..., (t - \lambda_i), 1\}$$

for V_{g_i} with $g_i(v) = t \cdot v$. Then the matrix representing g_i in this basis is:

$$A_i = \begin{bmatrix} \lambda_i & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_i & \cdots & 0 & 0 \\ & & & \vdots & & \\ 0 & 0 & 0 & \cdots & \lambda_i & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_i \end{bmatrix}$$

which is one of the *Jordan blocks* of f in Jordan canonical form.

Definition. f is *semi-simple* if it is diagonal in Jordan canonical form, i.e. if all the primary summands of V_f are of the form $k[t]/\langle x - \lambda \rangle$.

Example. The following two matrices are similar:

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -3 \\ 0 & 1 & 3 \end{bmatrix}$$

passing from Jordan block to rational canonical block for $V_f = k[t]/\langle (t - 1)^3 \rangle$.