# M3P8 MASTERY MATERIAL: MODULES OVER PRINCIPAL IDEAL DOMAINS

## 1. Some basic definitions

**Definition 1.1.** Let $R$ be an integral domain. The *rank* of an $R$-module $M$ is the size of the largest $R$-linearly independent subset of $M$.

**Exercise 1.2.** Show that if $R$ is Noetherian and $M$ is a finitely generated $R$-module, then the rank of $M$ is finite. Show that the rank of the free $R$-module $R^n$ is $n$. (In particular, this agrees with our previous definition of a "free $R$-module of rank $n$".

**Exercise 1.3.** Show that if $R$ is an integral domain then the rank of any submodule $N$ of $M$ is less than or equal to the rank of $M$. Similarly, show that if $N$ is a quotient of $M$ then the rank of $N$ is less than or equal to the rank of $M$.

**Definition 1.4.** Let $R$ be an integral domain and let $M$ be an $R$-module. An element $m$ of $M$ is *torsion* if there exists a nonzero element $r$ of $R$ such that $rm = 0$. We say $M$ is *torsion-free* if there are no nonzero torsion elements on $M$.

**Exercise 1.5.** Show that if $R$ is an integral domain and $M$ is an $R$-module, then the torsion elements of $M$ form an $R$-submodule of $M$ (called the *torsion submodule* of $M$). Give an example of an integral domain $R$ and a finitely generated, torsion-free $R$-module $M$ such that $M$ is not a free $R$-module.

## 2. The classification

Henceforth let $R$ be a PID. Our goal is to classify finitely generated $R$-modules $M$. Fix such an $M$, and suppose that $M$ is generated by $n$ elements $m_1, \ldots, m_r$. There is then a surjection:

$$F \to M,$$

where $F$ is free $R$-module of rank $n$ with basis $e_1, \ldots, e_r$, which takes $e_i$ to $m_i$ for all $i$. If $N$ is the kernel of this surjection then we have an isomorphism of $M$ with the quotient $F/N$. Thus to classify finitely generated $R$-modules up to isomorphism, it sufficies to understand submodules $N$ of a free module $F$. We have:

**Theorem 2.1.** *Let $R$ be a PID and let $F$ be a free $R$-module of rank $r$. Let $N$ be a submodule of $F$. Then $N$ is free of rank $n \leq r$. Moreover, there exists a basis $e_1, \ldots, e_r$ of $F$, and nonzero elements $a_1, \ldots, a_n$ such that*

(1) $a_1|a_2|\dots|a_n$, *and*
(2) $a_1e_1, \dots, a_ne_n$ *is a basis for* $N$.

Before we prove this we explore some of the consequences of this result:

**Exercise 2.2.** Show that if $R$, $F$, and $N$ are as in the theorem, then we have an isomorphism:

$$F/N \cong R^{r-n} \oplus R/\langle a_1\rangle \oplus R/\langle a_2\rangle \oplus \cdots \oplus R/\langle a_n\rangle.$$

Conclude that every finitely generated $R$-module $M$ is isomorphic to

$$R^s \oplus R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_n\rangle$$

where $a_1, \dots, a_n$ is a sequence of nonzero elements of $R$ such that $a_1|a_2|\dots|a_n$, and $s$ is the rank of $M$.

This result is called the *classification of finitely generated modules over a PID*. A natural question to ask is how unique this classification is. Since the integer $s$ in the above theorem is equal to the rank of $M$, it does not depend on the choice of $F$ and $N$ as in the theorem. The elements $a_1, \dots, a_n$ are called the *invariant factors* of $M$. They are only well-defined up to multiplication by units, but one has:

**Exercise 2.3.** Let $M \cong R^s \oplus R/\langle a_1\rangle \oplus \cdots \oplus R/\langle a_n\rangle$ as in the previous exercise. Let $p$ be a prime of $R$ and $m$ an integer. Show that the number of $i$ such that $p^m$ divides $a_i$ is equal to the dimension $(\dim_{R/p} p^{m-1}M/p^mM) - s$. Conclude that up to multiplication by elements of $R^\times$, the invariant factors of $M$ depend only on $M$ and not on any of the choices made. (In particular, conclude that if $a_1, \dots, a_n$ and $b_1, \dots, b_m$ are such that $a_1|a_2|\dots|a_n$, $b_1|b_2|\dots|b_m$, and

$$R/\langle a_1\rangle \oplus R/\langle a_2\rangle \dots R/\langle a_n\rangle \cong R/\langle b_1\rangle \oplus R/\langle b_2\rangle \oplus \cdots \oplus R/\langle b_m\rangle,$$

then $n = m$ and $a_i$ is a unit times $b_i$ for all $i$.)

[HINT: it is helpful to show that first show that for any $a, b \in R$, one has $b(R/\langle a\rangle) = \langle a, b\rangle/\langle a\rangle$. In particular if $\langle p^m, a\rangle = \langle p^{m-1}, a\rangle$ then $p^m(R/\langle a\rangle) = p^{m-1}(R/\langle a\rangle)$.]

There is another formulation of the classification that works "one prime at a time". Let $p_1, \dots, p_t$ be the primes of $R$ dividing $a_r$. For each $j$, write $a_j = u_j p_1^{k_{1j}} \dots p_t^{k_{tj}}$. Then the Chinese remainder theorem gives isomorphisms:

$$R/\langle a_j\rangle \cong \bigoplus_i R/\langle p_i^{k_{ij}}\rangle,$$

$$M \cong R^s \oplus \bigoplus_i \bigoplus_j R/\langle p_i^{k_{ij}}\rangle.$$

The powers $p_i^{k_{ij}}$ appearing here are called the *elementary divisors* of $M$; they give an alternative to the invariant factors as a way of describing the torsion of $M$. The submodule $\bigoplus_j R/\langle p_i^{k_{ij}}\rangle$ is called the $p_i$*-primary part* of $M$; it is the largest submodule of $M$ that is annihilated by a power of $p_i$.

It remains to prove Theorem 2.1. We will do this by induction on the rank $r$ of $F$. The case $r = 1$ is clear; in this case $F \cong R$ as $R$-modules and under any such isomorphism $N$ is an ideal of $R$. In particular either $N = \langle 0 \rangle$ or $N = \langle a \rangle$ for some nonzero element $a$ of $R$ and the theorem is clear.

Now suppose Theorem 2.1 holds for $F$ free of rank $r-1$, and fix $F$ free of rank $r$ with $N \subseteq F$. If $N = 0$ we can take $n = 0$, and $e_1, \ldots, e_r$ any basis of $F$. Suppose $N$ is nonzero.

We write $F \cong R^r$ and for $1 \leq i \leq r$, let $\pi_i$ be the projection of $R^r$ onto the $i$th coordinate, regarded as an $R$-linear map $\pi_i : F \to R$. Note that if $f \in F$ and $\pi_i(f) = 0$ for all $i$, then $f = 0$. In particular, since $N$ is nonzero, there exists a map $\Phi : F \to R$ such that $\Phi(F)$ is a nonzero ideal of $R$ (and we can even take $\Phi = \pi_i$ for some $i$).

Let $\Sigma$ be the set of ideals of $R$ of the form $\Phi(N)$ for some $\Phi : F \to R$. Let $I$ be a maximal element of $\Sigma$; that is, an element of $\Sigma$ that is not properly contained in any other element of $\Sigma$. The ideal $I$ is nonzero, so it is generated by a nonzero element $a_1$ of $R$. Since $I$ is an element of $\Sigma$, there exists a $\Phi : F \to R$ such that $\Phi(N) = I = \langle a_1 \rangle$; in particular there is an element $n$ of $N$ with $\Phi(n) = a_1$.

Now let $\Psi : F \to R$ be any $R$-linear map. Then $\Psi(N) = \langle d \rangle$ for some element $d$ of $R$. We next show:

**Exercise 2.4.** Show that $a_1$ divides $\Psi(n)$. [Hint: let $d'$ be the greatest common divisor of $\Phi(n)$ and $\Psi(n)$. By taking a suitable linear combinaton of $\Psi$ and $\Phi$, show that there exists an $R$-linear map $\Theta : F \to R$ such that $\Theta(n) = d'$. Use the maximality of $I$ to conclude that $\langle a_1 \rangle = \langle d' \rangle$, so that $a_1$ divides $\Psi(n)$].

**Exercise 2.5.** Show that there exists an element $e_1$ of $F$ such that $a_1 e_1 = n$. [HINT: use the previous exercise to show that $a_1$ divides $\pi_i(n)$ for all $i$, and show that there exists $e_1$ in $F$ with $\pi_i(e_1) = \frac{\pi_i(n)}{a_1}$ for all $i$.]

Since $a_1 e_1 = n$, we have $\Phi(a_1 e_1) = \Phi(n) = a_1$, so $\Phi(e_1) = 1$. In particular, $\Phi : F \to R$ is surjective, as is $\frac{1}{a_1}\Phi : N \to R$. We now need:

**Exercise 2.6.** Let $F$ be a finitely generated $R$-module and $\Phi : F \to R$ a surjective linear map. Show that $F$ is a free $R$-module of rank $r$ if, and only if, $\ker \Phi$ is a free $R$-module of rank $r-1$.

Let $F' = \ker \Phi$ and $N' = N \cap F'$. The exercise shows that $F'$ is free of rank $r-1$. By the inductive hypothesis, $N'$ is free as an $R$-module, and there exists an basis $e_2, \ldots, e_r$ of $F'$, and elements $a_2, \ldots, a_n$ of $R$ with $a_2 | a_3 | \ldots | a_n$ such that $a_2 e_2, \ldots, a_n e_n$ is a basis for $N'$.

**Exercise 2.7.** Show that $e_1, \ldots, e_r$ is a basis of $F$, and that $a_1 e_1, \ldots, a_n e_n$ is a basis for $N$.

At this point it remains to show that $a_1$ divides $a_2$. Let $\Psi : F \to R$ be the unique linear map such that $\Psi(e_1) = 1$, $\Psi(e_2) = 1$, and $\Psi(e_i) = 0$ for $i > 2$.

**Exercise 2.8.** Show that $\Psi(N)$ contains the ideal generated by $a_1$ and $a_2$. Conclude that $a_1$ divides $a_2$. [HINT: use the maximality of $I$].

At this point the proof of Theorem 2.1 is complete.

## 3. Finitely generated Abelian groups

Since abelian groups are simply $\mathbb{Z}$-modules, and $\mathbb{Z}$ is a PID, we immediately obtain the classification of finitely generated abelian groups:

**Theorem 3.1.** *Let $A$ be a finitely generated abelian group. Then there is a unique integer $r$, and unique positive integers $a_1, \ldots, a_t$, with $a_1|a_2|\ldots|a_t$, such that there exists an isomorphism:*

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_t\mathbb{Z}.$$

**Exercise 3.2.** Let $m$ and $n$ be relatively prime integers and let $A$ be an abelian group of order $mn$. Show there exist unique subgroups $G$ and $H$ of $A$, of order $m$ and $n$ respectively. Show further that $A$ is isomorphic to the direct sum $G \oplus H$.

## 4. Linear transformations on finite dimensional vector spaces and $K[T]$-modules

A perhaps more surprising application of the theory of modules over PIDs is to linear algebra. Let $K$ be a field, let $V$ be a finite dimensional $K$-vector space, and let $L : V \to V$ be a $K$-linear map. We will study the map $L$ by relating it to a certain $K[T]$-module $M_L$ and applying the classification. As a consequence, we'll obtain an easy proof of the Jordan Canonical Form when $K$ is algebraically closed and even see how to generalize it to non-algebraically closed $K$!

The key point is that a linear map $L : V \to V$ lets us give $V$ the structure of a $K[T]$-module. The key idea is as follows: let $P(T) \in K[T]$ be the polnyomial $a_0 + a_1T + \cdots + a_dT^d$. Then we define a $K$-linear map $P(L) : V \to V$ by $P(L) = a_0 + a_1L + a_2L^2 + \cdots + a_dL^d$.

Define a $K[T]$-module $M_L$ as follows: the underlying set of $M_L$ is simply the vector space $V$. Addition on $M_L$ is given by addition in $V$. For any $v \in M_L$ and $P(T)$ in $K[T]$, we define $P(T) \cdot v = P(L)(v)$.

**Exercise 4.1.** Show that the multiplication law above makes $M_L$ into a $K[T]$-module as claimed. Show further that this module is a finitely generated, torsion $K[T]$-module. Show that there is a $K$-linear isomorphism of $M_L$ with $V$, and that under this isomorphism, "multiplication by $T$": $M_L \to M_L$ is simply the linear map $L : V \to V$.

Since $M_L$ is torsion, the classification shows there are polynomials $P_1(T), \ldots, P_t(T)$ such that $P_1(T)|P_2(T)|\ldots|P_t(T)$, and $M_L$ is isomorphic to the $K[T]$-module:

$$K[T]/\langle P_1(T)\rangle \oplus K[T]/\langle P_2(T)\rangle \oplus \cdots \oplus K[T]/\langle P_t(T)\rangle.$$

We can (and do) take the $P_i$ to be *monic*; they are then uniquely determined by $L$. For each $i$, let $d_i$ denote the degree of $P_i(T)$.

The polynomials $P_i(T)$ contain information about $L$. To make this more precise we need to recall some facts from linear algebra:

**Exercise 4.2.** Show that the set $I_L := \{P(T) \in K(T) : P(L) = 0\}$ is a nonzero ideal of $K[T]$.

The unique monic generator $Q(T)$ of $I_L$ is called the *minimal polynomial* of $L$. We have $Q(L) = 0$, and if $P(T)$ is any polynomial with $P(L) = 0$, then $Q(T)$ divides $P(T)$. (Note, however, that unlike minimal polynomials of elements of field extensions, the minimal polynomial of a linear map: $V \to V$ need *not* be irreducible.)

**Exercise 4.3.** Show that the dimension of $V$ is equal to $d_1 + d_2 + \cdots + d_t$, and that $P_t(T)$ is the minimal polynomial of $L$.

Since $M_L$ is naturally isomorphic to $V$ as $K$-vector spaces, we can find a $K$-basis for $V$ by finding a $K$-basis for $M_L$. Even better, since our isomorphism of $M_L$ with $V$ carries "multiplication by $T$" to $L$, the matrix of $L$ with respect to the basis for $V$ is *the same* as the matrix of "multiplication by $T$" on $M_L$ with respect to the corresponding basis of $M_L$. By choosing a nice basis of $M_L$, we can thus find a basis for $V$ that gives a nice matrix for $L$!

For instance, the $K[T]$-module $K[T]/\langle P_i(T)\rangle$ has as a basis $1, T, T^2, \ldots, T^{d_i-1}$. With respect to this basis, "multiplication by $T$" has as its matrix:

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_{0i} \\ 1 & 0 & 0 & \ldots & 0 & -a_{1i} \\ 0 & 1 & 0 & \ldots & 0 & -a_{2i} \\ 0 & 0 & 1 & \ldots & 0 & -a_{3i} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{d_i-1,i} \end{pmatrix}$$

where $P_i(T) = a_{0i} + a_{1i}T + \cdots + a_{d_i-1,i}T^{d_i-1} + T^{d_i}$. (Recall that this matrix is called the *companion matrix* for $P_i(T)$).

If we let $M_i$ denote the compation matrix for $P_i(T)$, then (with respect to the above chosen basis for each summand $K[T]/\langle P_i(T)\rangle$ of $M_L$) the matrix of "multiplication by $T$" on $M_L$ is "block diagonal", with blocks $M_1, M_2, \ldots, M_t$. That is, we have:

**Theorem 4.4.** *There exists a basis for $V$ such that the map $L : V \to V$ has matrix:*

$$\begin{pmatrix} M_1 & 0 & 0 & \ldots & 0 \\ 0 & M_2 & 0 & \ldots & 0 \\ 0 & 0 & M_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & M_t \end{pmatrix}$$

*where $M_i$ is the companion matrix of the $i$th invariant factor for $M_L$.*

This matrix is called a *rational canonical form* for $L$; it exists for *any* $L$, over *any* field $K$, and is uniquely determined by $L$. In particular, given any $n$ by $n$ matrix $A$ with cofficients in $K$, there is a unique matrix in rational canonical form that is conjugate to $A$ by an element of $\mathrm{G}L_n(K)$.

Now let us assume $K$ is algebraically closed; in particular every irreducible monic polynomial in $K[T]$ is of the form $T-\lambda$ for some $\lambda \in K$. By factoring each $P_i(T)$ into irreducibles, we find that there is a finite collection of elements $\lambda_1, \ldots, \lambda_r$ of $K$, and for each $\lambda_i$ a nondecreasing sequence $n_{i1}, \ldots, n_{it}$ of nonnegative integers such that

$$P_j(T) = \prod_i (T-\lambda_i)^{n_{ij}}.$$

We thus obtain an isomorphism:

$$M_L \cong \prod_i \prod_j K[T]/\langle (T-\lambda_i)^{n_{ij}} \rangle.$$

The module $K[T]/\langle (T-\lambda)^n \rangle$ has as a basis $(T-\lambda)^{n-1}, (T-\lambda)^{n-2}, \ldots, (T-\lambda), 1$.

**Exercise 4.5.** Show that the matrix of "multiplication by $T$" on $K[T]/\langle (T-\lambda)^n \rangle$ with respect to this basis is the "Jordan block of size $n$ and eigenvalue $\lambda$"; that is, the matrix:

$$\begin{pmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ldots & 0 \\ 0 & 0 & \lambda & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & \lambda \end{pmatrix}.$$

Conclude that when $K$ is algebraically closed and $L$ is any linear map $V \to V$, there exists a basis of $V$ such that the matrix of $L$ is in Jordan canonical form (that is, is block diagonal with each block a Jordan block.