1.9 Lecture 9: Finitely generated modules over a PID

A **principal ideal domain** (PID) is a commutative ring $\mathbb{A}$ such that

(a) (Cancellation law) If $a, b, c \in \mathbb{A}$ and $c \neq 0$ and $ac = bc$ then $a = b$,

(b) (Principal Ideals) If I is an ideal of $\mathbb{A}$ then there exists $m \in R$ such that
$$I = m\mathbb{A}, \qquad \text{where} \qquad m\mathbb{A} = \{cm \mid c \in \mathbb{A}\} = \mathbb{A}\text{-span}\{m\}.$$

Let $\mathbb{A}$ be a PID and let M be an $\mathbb{A}$-module. Let $B \subseteq M$. The **submodule generated by** S is
$$\mathbb{A}\text{-span}(B) = \{c_1b_1 + \cdots c_kb_k \mid k \in \mathbb{Z}_{>0},\ c_1, \ldots, c_k \in \mathbb{A},\ b_1, \ldots, b_k \in B\}.$$
The module M is **finitely generated** if there exists a finite set $B \subseteq M$ such that $M = \mathbb{A}\text{-span}(B)$.

Proposition 1.22. *Let $\mathbb{A}$ be a PID and let M be an $\mathbb{A}$-module given by generators*
$$\textit{generators} \qquad m_1, \ldots, m_s \in M \qquad \textit{and relations} \qquad \begin{matrix} a_{11}m_1 + \cdots + a_{1s}m_s = 0, \\ \vdots \\ a_{t1}m_1 + \cdots + a_{ts}m_s = 0. \end{matrix}$$
Let $P \in GL_t(\mathbb{A})$, $Q \in GL_s(\mathbb{A})$, $k = \min(s, t)$ and $d_1, \ldots, d_k \in \mathbb{A}$ such that
$$A = PDQ, \qquad \textit{where} \qquad D = \mathrm{diag}(d_1, \ldots, d_k).$$
Then M is presented by
$$\textit{generators} \quad b_1, \ldots, b_s \quad \textit{and relations} \qquad d_1b_1 = 0, \quad \ldots, \quad d_kb_k = 0.$$

Theorem 1.23. *Let $\mathbb{A}$ be a PID and let M be a finitely generated $\mathbb{A}$ module. Then there exist $k, \ell \in \mathbb{Z}_{\geq 0}$ and $d_1, \ldots, d_k \in \mathbb{A}$ such that*
$$M \cong \frac{\mathbb{A}}{d_1\mathbb{A}} \oplus \cdots \oplus \frac{\mathbb{A}}{d_k\mathbb{A}} \oplus \mathbb{A}^{\oplus \ell}$$

Special cases of $\mathbb{A}/d\mathbb{A}$ are
$$\frac{\mathbb{A}}{0\mathbb{A}} = \mathbb{A} \qquad \text{and} \qquad \text{if } u \in \mathbb{A}^\times \text{ then } \quad \frac{\mathbb{A}}{u\mathbb{A}} = \frac{\mathbb{A}}{\mathbb{A}} = 0.$$

Theorem 1.24. *(Chinese remainder theorem) Let $\mathbb{A}$ be a PID and let $d \in \mathbb{A}$.*
$$\textit{Assume} \qquad d = pq \qquad \textit{with} \qquad \gcd(p, q) = 1.$$
Then there exist $r, s \in A$ such that $1 = pr + qs$ and
$$\begin{matrix} \dfrac{\mathbb{A}}{d\mathbb{A}} & \xrightarrow{\sim} & \dfrac{\mathbb{A}}{p\mathbb{A}} \oplus \dfrac{\mathbb{A}}{q\mathbb{A}} \\ pr + pq\mathbb{A} & \mapsto & (0 + p\mathbb{A}, 1 + q\mathbb{A}) \\ qs + pq\mathbb{A} & \mapsto & (1 + p\mathbb{A}, 0 + q\mathbb{A}) \\ 1 + pq\mathbb{A} & \mapsto & (1 + p\mathbb{A}, 1 + q\mathbb{A}) \end{matrix} \qquad \textit{is an } \mathbb{A}\textit{-module isomorphism.}$$

Proof. . Let $r, s \in \mathbb{A}$ such that $pr + sq = 1$. Then
$$\begin{pmatrix} 1 & 0 \\ 0 & pq \end{pmatrix} = \begin{pmatrix} pr + qs & 0 \\ 0 & pq \end{pmatrix} = \begin{pmatrix} p & q \\ 0 & q \end{pmatrix} \begin{pmatrix} r & -q \\ s & p \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix} \begin{pmatrix} r & -q \\ s & p \end{pmatrix}$$
Using this and the method of proof of Proposition 1.22 gives
$$\frac{\mathbb{A}}{p\mathbb{A}} \oplus \frac{\mathbb{A}}{q\mathbb{A}} \cong \frac{\mathbb{A}}{1 \cdot \mathbb{A}} \oplus \frac{\mathbb{A}}{pq\mathbb{A}} = 0 \oplus \frac{\mathbb{A}}{pq\mathbb{A}} = \frac{\mathbb{A}}{pq\mathbb{A}}.$$
□

1.9.1 Proof sketches

Proposition 1.25. *Let $\mathbb{A}$ be a PID and let M be an $\mathbb{A}$-module given by generators*

$$\text{generators} \qquad m_1, \ldots, m_s \in M \qquad \text{and relations} \qquad \begin{matrix} a_{11}m_1 + \cdots + a_{1s}m_s = 0, \\ \vdots \\ a_{t1}m_1 + \cdots + a_{ts}m_s = 0, \end{matrix}$$

Let $P \in GL_t(\mathbb{A})$, $Q \in GL_s(\mathbb{A})$, $k = \min(s,t)$ and $d_1, \ldots, d_k \in \mathbb{A}$ such that

$$A = PDQ, \qquad \text{where} \qquad D = \mathrm{diag}(d_1, \ldots, d_k).$$

Then M is presented by

$$\text{generators} \quad b_1, \ldots, b_s \quad \text{and relations} \qquad d_1b_1 = 0, \ldots, d_kb_k = 0.$$

Proof. For $i \in \{1, \ldots, s\}$ let

$$b_i = Q_{i1}m_1 + \cdots + Q_{is}m_s, \qquad \text{so that} \qquad m_j = (Q^{-1})_{j1}b_1 + \cdots + (Q^{-1})_{js}b_s,$$

for $j \in \{1, \ldots, s\}$. Thus generators (m) can be written in terms of generators (b) and vice versa. Since

$$\sum_j a_{ij}m_j = \sum_{j,k} a_{ij}Q^{-1}_{jk}b_k = \sum_k P_{ik}d_kb_k = 0$$

then the relations (m) can be derived from the relations (b). Since

$$d_kb_k = \sum_{i,j,l} (P^{-1})_{kj}a_{jl}(Q^{-1})_{lk}b_k = \sum_{i,j,l} (P^{-1})_{kj}a_{jl}m_l = 0,$$

then the relations (b) can be derived from the relations (m). □

Theorem 1.26. *Let $\mathbb{A}$ be a PID and let M be a finitely generated $\mathbb{A}$ module. Then there exist $k, \ell \in \mathbb{Z}_{\geq 0}$ and $d_1, \ldots, d_k \in \mathbb{A}$ such that*

$$M \cong \frac{\mathbb{A}}{d_1\mathbb{A}} \oplus \cdots \oplus \frac{\mathbb{A}}{d_k\mathbb{A}} \oplus \mathbb{A}^{\oplus \ell}$$

Proof. Since M is finitely generated there exist $s \in \mathbb{Z}_{>0}$ and $m_1, \ldots, m_s \in M$ such that

$$M = \mathbb{A}\text{-span}\{m_1, \ldots, m_s\}, \qquad \text{Define} \quad \begin{matrix} \mathbb{A}^{\oplus s} & \xrightarrow{\Phi} & M \\ e_i & \longmapsto & m_i \end{matrix} \quad \text{and let} \qquad K = \ker(\Phi).$$

Since $\mathbb{A}$ satisfies ACC and $\mathbb{A}^{\oplus s}$ is a finitely generated $\mathbb{A}$-module then

$$\text{the } \mathbb{A}\text{-submodule } K \text{ is finitely generated.}$$

So there exist $t \in \mathbb{Z}_{>0}$ and

$$a_1 = (a_{11}, \ldots, a_{1s}), \quad \ldots \quad a_t = (a_{t1}, \ldots, a_{ts}) \qquad \text{in } \mathbb{A}^{\oplus s} \qquad \text{such that} \qquad K = \mathbb{A}\text{-span}\{a_1, \ldots, a_t\}.$$

Since

$$M \cong \frac{\mathbb{A}^{\oplus s}}{K}$$

then M is presented by

$$\text{generators} \qquad m_1, \ldots, m_s \in M \qquad \text{and relations} \qquad \begin{matrix} a_{11}m_1 + \cdots + a_{1s}m_s = 0, \\ \vdots \\ a_{t1}m_1 + \cdots + a_{ts}m_s = 0, \end{matrix}$$

Then use the previous proposition to produce the isomorphism $M \cong \frac{\mathbb{A}}{d_1\mathbb{A}} \oplus \cdots \oplus \frac{\mathbb{A}}{d_k\mathbb{A}} \oplus \mathbb{A}^{\oplus \ell}$. □