3.8 Tutorial 3: NEW MAST30005 Semester 1: Last week's theorems

Last week we covered the following theorems. Write careful proofs of each.

Proposition 3.15. *Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$. The following are equivalent*

(a) $f(x)$ is irreducible in $\mathbb{F}[x]$, *(b) $f(x)\mathbb{F}[x]$ is a maximal ideal,* *(c) $\frac{\mathbb{F}[x]}{f(x)\mathbb{F}[x]}$ is a field.*

Proposition 3.16. *Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if*

$$\begin{array}{ll} & \text{either } f(x) = \pm p, \text{ where } p \text{ is a prime integer,} \\ \text{or} & f(x) \text{ is a primitive polynomial and } f(x) \text{ is irreducible in } \mathbb{Q}[x]. \end{array}$$

Proposition 3.17. *Let $f(x) \in \mathbb{Z}[x]$ and let $p \in \mathbb{Z}_{>0}$ be prime. Let $\overline{f(x)}$ denote the image of $f(x)$ in $\mathbb{F}_p[x]$.*

$$\text{If } \deg(\overline{f(x)}) = \deg(f(x) \text{ and } \overline{f(x)} \text{ is irreducible in } \mathbb{F}_p[x]$$

$$\text{then } f(x) \text{ is irreducible in } \mathbb{Z}[x].$$

Theorem 3.18. *(Smith normal form) Let $t, s \in \mathbb{Z}_{>0}$. Let $A \in M_{t\times s}(\mathbb{F}[x])$ and let $r = \min(t, s)$. Then there exist $P \in GL_t(\mathbb{F}[x])$ and $Q \in GL_s(\mathbb{F}[x])$ and $d_1, \ldots, d_r \in \mathbb{F}[x]_{\mathrm{monic}}$ such that $d_1\mathbb{F}[x] \supseteq d_2\mathbb{F}[x] \supseteq \cdots \supseteq d_k\mathbb{F}[x]$ and*

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

Theorem 3.19. *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*

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

3.8.1 Proof sketches

Proposition 3.20. *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

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

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 3.21. *Let $\mathbb{A}$ be a PID and let M be a finitely generated $\mathbb{A}$ module. Then there exist $k,\ell\in\mathbb{Z}_{\ge0}$ 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

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

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