1.8 Lecture 8: Reduction to diagonal for PIDs: Smith normal form

Let $\mathbb{F}$ be a field. The set of **monic polynomials with coefficients in** $\mathbb{F}$ is

$$\mathbb{F}[x]_{\mathrm{monic}} = \{x^\ell + c_{\ell-1}x^{\ell-1} + \cdots + c_1 x + c_0 \mid c_0, \ldots, c_{\ell-1} \in \mathbb{F}\} \cup \{0\}.$$

Theorem 1.20. *(Smith normal form) Let $t, s \in \mathbb{Z}_{>0}$.*

(a) Let $A \in M_{t\times s}(\mathbb{Z})$ and let $r = \min(t,s)$. Then there exist $P \in GL_t(\mathbb{Z})$ and $Q \in GL_s(\mathbb{Z})$ and $d_1, \ldots, d_r \in \mathbb{Z}_{\ge 0}$ such that $d_1\mathbb{Z} \supseteq d_2\mathbb{Z} \supseteq \cdots \supseteq d_k\mathbb{Z}$ and

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

(b) 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

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

(a) Let $\mathbb{A}$ be a PID and identify $\mathbb{A}/\mathbb{A}^\times$ with a specific choice of a set of representatives of the elements of $\mathbb{A}/\mathbb{A}^\times$. Let $A \in M_{t\times s}(\mathbb{A})$ and let $r = \min(t,s)$. Then there exist $P \in GL_t(\mathbb{A})$ and $Q \in GL_s(\mathbb{A})$ and $d_1, \ldots, d_r \in \mathbb{A}/\mathbb{A}^\times$ such that $d_1\mathbb{A} \supseteq d_2\mathbb{A} \supseteq \cdots \supseteq d_k\mathbb{A}$ and

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

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

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

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

Let $\mathbb{A}$ be a PID.

- The **group of units of** $\mathbb{A}$ is

$$\mathbb{A}^\times = \{c \in \mathbb{A} \mid \text{there exists } b \in \mathbb{A} \text{ with } bc = cb = 1\}.$$

- The **set of $\mathbb{A}^\times$-orbits in** $\mathbb{A}$ is

$$\mathbb{A}/\mathbb{A}^\times = \{d\mathbb{A}^\times \mid d \in \mathbb{A}\}, \qquad \text{where} \quad d\mathbb{A}^\times = \{dc \mid c \in \mathbb{A}^\times\}.$$

HW: Let $J \subseteq \mathbb{A}$. Show that J is an ideal of $\mathbb{A}$ if and only if J is an $\mathbb{A}$-submodule of $\mathbb{A}$.

HW:. Show that

$$\begin{array}{ccccc} \{\text{ideals of } \mathbb{Z}\} & \leftrightarrow & \mathbb{Z}/\mathbb{Z}^\times & \leftrightarrow & \mathbb{Z}_{\ge 0} \\ m\mathbb{Z} & \leftarrow\!\shortmid & \{m, -m\} & \leftarrow\!\shortmid & m \end{array} \qquad \text{are bijections}$$

and

$$\begin{array}{ccccc} \{\text{ideals of } \mathbb{F}[x]\} & \leftrightarrow & \mathbb{F}[x]/\mathbb{F}[x]^\times & \leftrightarrow & \mathbb{F}[x]_{\mathrm{monic}} \\ f(x)\mathbb{F}[x] & \leftarrow\!\shortmid & \{cf(x) \mid c \in \mathbb{F}^\times\} & \leftarrow\!\shortmid & f(x) \end{array} \qquad \text{are bijections.}$$

HW: Let $\mathbb{A}$ be a PID. For the $d \in \mathbb{A}$, the $\mathbb{A}^\times$**-orbit of** d is $d\mathbb{A}^\times = \{dc \mid c \in \mathbb{A}^\times\}$. Show that

$$\begin{array}{ccc} \{\text{ideals of } \mathbb{A}\} & \leftrightarrow & \mathbb{A}/\mathbb{A}^\times \\ d\mathbb{A} & \leftarrow\!\shortmid & d\mathbb{A}^\times \end{array} \qquad \text{is a bijection.}$$

1.8.1 An example of reduction to diagonal over $\mathbb{Z}$

Let

$$x_1(c) = \begin{pmatrix} 1 & c & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad L_1(c) = \begin{pmatrix} 1 & 0 & 0 \\ c & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad y_1(c) = \begin{pmatrix} c & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and

$$x_2(c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \qquad L_2(c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & c & 1 \end{pmatrix}, \qquad y_2(c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

Each of these matrices has determinant ± 1 and is an element of $GL_3(\mathbb{Z})$. Then

$$\begin{aligned}
\begin{pmatrix} 11 & -4 & 7 \\ -1 & 2 & 1 \\ 3 & 0 & 3 \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3 & 1 \end{pmatrix} \begin{pmatrix} 11 & -4 & 7 \\ -1 & 2 & 1 \\ 0 & 6 & 6 \end{pmatrix} \\
&= L_2(3) \begin{pmatrix} -11 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 2 & 1 \\ 0 & 18 & 18 \\ 0 & 6 & 6 \end{pmatrix} \\
&= L_2(3) y_2(-11) \begin{pmatrix} -1 & 0 & 1 \\ 0 & 18 & 18 \\ 0 & 6 & 6 \end{pmatrix} \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= L_2(3) y_2(-11) \begin{pmatrix} -1 & 1 & 0 \\ 0 & 18 & 18 \\ 0 & 6 & 6 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} x_1(-2) \\
&= L_2(3) y_2(-11) \begin{pmatrix} -1 & 0 & 0 \\ 0 & 18 & 18 \\ 0 & 6 & 6 \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} y_2(0) x_1(-2) \\
&= L_2(3) y_2(-11) \begin{pmatrix} -1 & 0 & 0 \\ 0 & 18 & 0 \\ 0 & 6 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} x_1(-1) y_2(0) x_1(-2) \\
&= L_2(3) y_2(-11) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 18 & 0 \end{pmatrix} x_2(1) x_1(-1) y_2(0) x_1(-2) \\
&= L_2(3) y_2(-11) y_2(0) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix} x_2(1) y_2(0) x_1(-1) y_2(0) x_1(-2) \\
&= L_2(3) y_2(-11) y_2(0) L_2(3) \begin{pmatrix} -1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix} y_2(0) x_2(1) y_2(0) x_1(-1) y_2(0) x_1(-2)
\end{aligned}$$

Letting $P = L_2(3)y_2(-11)y_2(0)L_2(3)$ and $Q = y_2(0)x_2(1)y_2(0)x_1(-1)y_2(0)x_1(-2)$ then

$$P, Q \in GL_3(\mathbb{Z}) \text{ and } \qquad \begin{pmatrix} 11 & -4 & 7 \\ -1 & 2 & 1 \\ 3 & 0 & 3 \end{pmatrix} = P \begin{pmatrix} -1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix} Q$$

and $\mathbb{Z} = -1 \cdot \mathbb{Z} \supseteq 6\mathbb{Z} \supseteq 0\mathbb{Z} = \{0\}$