PROOF OF THE SMITH NORMAL FORM THEOREM

Most people find the proof of the Smith normal form theorem for Euclidean domains more intuitive than the case of a general PID. When I went to write them out, they actually came out very similar.

(99) **Proof of Smith normal form for Euclidean integral domains** Let R be a Euclidean integral domain with positive norm $N(\ )$. Let $X \in \mathrm{Mat}_{m\times n}(R)$. If $X = 0$, the Smith normal form theorem clearly holds for X, so assume otherwise. Let d be an element of smallest norm among all nonzero elements occurring as an entry in a matrix Y with $Y \sim X$. Let Y be a matrix with $Y \sim X$ and $Y_{11} = d$.

(a) Show that d divides Y_{i1} and Y_{1j} for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(b) Show that there is a matrix $Z \sim Y$ with $Z_{11} = d$ and $Z_{i1} = Z_{1j} = 0$ for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(c) Show that d divides Z_{ij} for all $2 \leq i \leq m$ and $2 \leq j \leq n$. (Hint: If not, find $W \sim Z$ with $W_{11} = d$ and $W_{1j} = Z_{ij}$.)
(d) Show that X is $\sim$-equivalent to a matrix of the form $\mathrm{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)})$ with $d_1|d_2|\cdots|d_{\min(m,n)}$.

(100) Consequence of the proof of Smith normal form for Euclidean integral domains: Define a stronger equivalence relation $\sim_E$ where $X \sim_E Y$ if $Y = UXV$ where U and V products of elementary matrices.

(a) Trace through your proof and check that you have shown, in a Euclidean integral domain, that every matrix is $\sim_E$-equivalent to a matrix of the form $\mathrm{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)})$ with $d_1|d_2|\cdots|d_{\min(m,n)}$.
(b) Let R be a Euclidean integral domain. Let $\mathrm{SL}_n(R)$ be the group of $n \times n$ matrices with entries in R and determinant 1. Show that $\mathrm{SL}_n(R)$ is generated by elementary matrices.

To do the case of a general PID, you'll need the following old problems:

(81) Let x and $y \in R$ Show that there is a matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with entries in R such that $ad - bc = 1$ and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \mathrm{GCD}(x, y) \\ 0 \end{bmatrix}.$$

(82) Let x and y be nonzero elements of R. Show that there are invertible 2×2 matrices U and V with

$$U \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} V = \begin{bmatrix} \mathrm{GCD}(x, y) & 0 \\ 0 & \mathrm{LCM}(x, y) \end{bmatrix}.$$

Here $\mathrm{LCM}(x, y) := \frac{xy}{\mathrm{GCD}(x,y)}$.

(101) Let R be a Noetherian ring (such as a PID) and let $\mathcal{D}$ be a nonempty subset of R. Show that there is an element $d \in \mathcal{D}$ which is "minimal with respect to division": More precisely, show that there is an element such that if $d' \in \mathcal{D}$ divides d, then d divides d' as well.

(102) **Proof of Smith normal form for PID's** Let R be a PID. Let $X \in \mathrm{Mat}_{m\times n}(R)$. Let $\mathcal{D}$ be the set of all entries occurring in any matrix Y with $Y \sim X$. Let d be as in Problem 101 for $\mathcal{D}$ and let Y be a matrix with $Y \sim X$ and $Y_{11} = d$.

(a) Show that d divides Y_{i1} and Y_{1j} for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(b) Show that there is a matrix $Z \sim Y$ with $Z_{11} = d$ and $Z_{i1} = Z_{1j} = 0$ for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(c) Show that d divides Z_{ij} for all $2 \leq i \leq m$ and $2 \leq j \leq n$.
(d) Show that X is $\sim$-equivalent to a matrix of the form $\mathrm{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)})$ with $d_1|d_2|\cdots|d_{\min(m,n)}$.