The goal is to show the following result

> (Smith normal form) Let A be a principal ideal domain. Any matrix $M \in \mathcal{M}_{n,m}(A)$ is equivalent to a matrix of the form
>
> $$\begin{pmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & d_r & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$
>
> with $d_1|\dots|d_r$. Moreover, the d_i's are unique up to multiplication by a unit.

Remark: It is clear that r is uniquely determined, as it equal to the rank of M seen as a matrix of $\mathrm{Frac}(A)$.

A special case: A is an euclidean domain

This is the case when $A = \mathbb{Z}$ or $A = k[X]$ with k a field. When that happens, everything may be done in a purely algorithmic fashion.

Let v be the euclidean map of A. Also, let $t(M) = \min_{M_{i,j} \neq 0} v(M_{i,j})$ and $d(M)$ an arbitrary gcd of the coefficients of M. Since $d(M)|M_{i,j}$ for any i, j, we have $v(d(M)) \leq t(M)$, and in case of equality, $t(M)$ and $d(M)$ are associated.

There are two cases:

Case 1, if $v(d(M)) = t(M)$:

We must have $t(M) \mid M_{i,j}$ for any i, j. Up to elementary row operations, we may assume $dM_{1,1}$ is such that $v(M_{1,1}) = t(M)$. Let $(L_i)_{1 \leq i \leq n}$ be the lines of M. The elementary row operations $L_i \leftarrow L_i - \dfrac{M_{1,i}}{M_{1,1}} L_1$ transform the first column to the form $\begin{pmatrix} M_{1,1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ while not changing that $M_{1,1}$ divides all the coefficients of the new matrix. Similar column operations give a first line of the first $\begin{pmatrix} M_{1,1} & 0 & \dots & 0 \end{pmatrix}$, and the matrix can now be written as

$$\begin{pmatrix} M_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{pmatrix}$$

with $M_{1,1}$ dividing all the coefficient of N. Induction finishes up the proof.

Case 2, if $v(d(M)) < t(M)$:

As before, we may assume $v(M_{1,1}) = t(M)$ for the sake of clarity.

There is once again two cases:

Case 2.1, there is some coefficient in the first line/column that's not divisible by $M_{1,1}$:

Without loss of generality, assume it's "line" and not "column", i.e there is some $i > 1$ such that $M_{1,1} \nmid M_{i,1}$. Euclidean division gives $M_{i,1} = qM_{1,1} + r$ with $v(r) < v(M_{1,1})$ and $r \neq 0$. The row operation $L_i \leftarrow L_i - qL_1$ gives rise to a new matrix N, and $t(N) \leq r < t(M)$. Iterating, we are reduced to the case $v(d(M)) = t(M)$.

Case 2.2, we know $M_{1,1}$ divides all the coefficients in the first line/column, and then by the same operations as in the case 1), we are reduced to a matrix of the form

$$\begin{pmatrix} M_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{pmatrix}$$

There is, by hypothesis, some coefficient of N that's not divisible by $M_{1,1}$. By adding the corresponding line to the first line, we are back to the case 2.1).

The general case

We cannot do everything through euclidean division and elementary operations anymore. The replacement is the following lemma.

> For any $a_1, \dots, a_s \in A$, there is a square matrix M whose first line is $\begin{pmatrix} a_1 & \dots & a_s \end{pmatrix}$ and whose determinant is a gcd of $\{a_1, \dots, a_s\}$.

TODO

References (clickable)

The general case

The euclidean case