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 is equal to the rank of M seen as a matrix of $\mathrm{Frac}(A)$.

Existence, a special case: A is an euclidean domain

Assume A is euclidean, as it 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, some coefficient of M and $d(M)$ are associated.

There are two cases:

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

Up to elementary row operations, we may assume $M_{1,1}$ is such that $v(M_{1,1}) = t(M)$. We must have $M_{1,1} \mid M_{i,j}$ for any i, j. 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 form $\begin{pmatrix} M_{1,1} & 0 & \dots & 0 \end{pmatrix}$, 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).

Existence, 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 $\{a_1, \dots, a_s\}$.

We postpone the proof, and focus on deducing the main result. We argue by induction on the size of the matrix.

Let $C = \begin{pmatrix} C_1 \\ \vdots \\ C_n \end{pmatrix}$ be a column vector (row vector is analogous). Since A is a PID, we can find a Bezout identity, that is coefficients $a_1, \dots, a_n$ such that $a_1C_1 + \dots a_nC_n = d$ with d a gcd of the coefficients of C. The a_i's are setwise coprime, and by the lemma we can find a $n \times n$ invertible matrix Q whose first line is $\begin{pmatrix} a_1 & \dots & a_n \end{pmatrix}$. It follows that $d = (QC)_{1,1}$ divides all the coefficients on the first column, and by the now usual row operations we get a first column of

the form $\begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. This handles the base case.

Now let $M \in \mathcal{M}_{n,m}(A)$, and proceed as in the base case with the first column of M. The d may not divide the coefficients on the first line, and we must do the same thing by right-multiplying by a matrix P so that the first line is of the form $\begin{pmatrix} d' & 0 & \dots & 0 \end{pmatrix}$, but now the first column is not "clean" anymore. But we have still have $d' \mid d$ and iterating this process we get a sequence (d_n) such that $d_{n+1} \mid d_n$. Since A is noetherian, it must stabilize at some rank k and then, by setting $p_1 = d_k$ we can simplify the first row/column to get a matrix of the form.

$$\begin{pmatrix} p_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{pmatrix}$$

Through the induction hypothesis applied to N and block multiplications we get the equivalent matrix

$$\begin{pmatrix} p_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & p_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & 0 & \ddots & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & p_r & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

with $p_2 \mid \dots \mid p_r$. To get p_1 dividing p_2, we add the second line to the first and repeat the process as above. Since the new p_2 may not divide p_3, we repeat the procedure until we reach p_r. We are done.

Back to the lemma. We argue by induction once again. The case $s = 1$ is obvious. Assume the result is true for some $s - 1 \geq 1$. Let N be a $(s-1) \times (s-1)$ matrix satisfying the induction hypothesis applied to $a_2, \dots, a_s$. Let d be the determinant of N and let $x, y \in A$ so that $a_1 x + dy = d'$ where d' is a gcd of $\{a_1, \dots, a_s\}$. Consider the matrix

$$\begin{pmatrix} a_1 & & & \\ 0 & & N & \\ \vdots & & & \\ (-1)^{s-1} y & (-1)^s \frac{a_2 x}{d} & \dots & (-1)^s \frac{a_s x}{d} \end{pmatrix}$$

Developing the determinant along the first column proves that the determinant is equal to d', as desired.

Uniqueness

The statement we must prove is also that the r-tuple $(d_1, \ldots, d_r)$ is unique up to multiplication by units. To do that, we define the quantity $\delta_k(M)$ as the *gcd* of all the $k \times k$ minors of M. We will prove

> For any matrix P and any k, $\delta_k(M)$ divides $\delta_k(PM)$

It will follow that $\delta_k(M)$ and $\delta_k(PMQ)$ are associated whenever P, Q are invertible. In Smith normal form, we easily see that $\delta_k(M) = d_1 \ldots d_k$ when $k \leq r$ and then $\delta_k(M) = 0$ when $k > r$, and thus we can recover the invariant factors intrisically.

To show the proposition, observe that the lines of PM are linear combinations of the lines of M, and using n-linearity of the determinant, the result follows.

References (clickable)

The general case and uniqueness

The euclidean case