Stacked basis theorem: If R is a PID, M is an R-module which is free of rank n, and $N \subseteq M$ is a sub-module, then: i) $\exists\ 0 \leq m \leq n$ s.t. N is a free R-module of rank m.

ii) $\exists$ a basis $x_1, \dots, x_n \in M$, $a_1, \dots, a_m \in R \setminus \{0\}$ s.t.

$a_1 x_1, a_2 x_2, \dots, a_m x_m$ is a basis for N

and $a_1 | a_2 | \cdots | a_m$.

Pf. of stacked basis thm for the case when R is an ED:

$$M \cong R^n \overset{\text{(lemma)}}{\Longrightarrow} \text{rank of } N \text{ is } m \leq n.$$

If $x_1, \dots, x_n$ any basis for M and if $y_1, \dots, y_m$ is any generating set for N then

$$\vec{y} = A\vec{x} \text{ for some } A \in M_{m \times n}(R).$$

Goal: Use elem. row & col. ops. to pick a basis and gen. set for which

$$\vec{y} = \left(\begin{array}{cccc|c} a_1 & 0 & \cdots & 0 & \\ 0 & \ddots & & \vdots & \\ \vdots & & \ddots & 0 & 0 \\ 0 & \cdots & 0 & a_m & \end{array} \right) \vec{x}$$

where $a_1 | a_2 | \cdots | a_m$.

Explanation:

i) What do elem. row. ops. on A do?

- switching two rows of A $\Leftrightarrow$ interchanging y_i & y_j
- replace ith row by ith row $+ a \cdot (j$th row$)$ $\Leftrightarrow$ replacing y_i by $y_i + a y_j$.

ii) What do elem. col. ops. on A do?

- switching two cols. of A $\Leftrightarrow$ interchanging x_i & x_j

- replace ith col. by ith col. + $a\cdot$(jth col.) $\Leftrightarrow$ replacing x_i by $x_i + a x_j$.

i.e. row & col. ops. allow us to change the basis for M and the gen. set. for N.

Now: $A = (a_{ij})_{\substack{1\le i\le m \\ 1\le j\le n}}$

Notes:
- PID $\Rightarrow$ existence of gcd
- ED $\Rightarrow$ "Euclidean algorithm" to compute gcd

Let $a_1' = \gcd(a_{ij} \mid 1\le i\le m,\ 1\le j\le n)$.

Use row and col. ops.:

successive column ops. the fact that we are in a ED

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \longrightarrow \begin{pmatrix} (a_{11},\dots,a_{1n}) & * & * & \cdots & * \\ * & * & & & \vdots \\ \vdots & & & \ddots & \\ * & & \cdots & & * \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} (a_{11},\dots,a_{1n}) & 0 & \cdots & 0 \\ * & * & \cdots & * \\ \vdots & & \ddots & \\ * & * & & * \end{pmatrix}$$

(successive row ops.)

$$\longrightarrow \begin{pmatrix} a_1' & * & \cdots & * \\ 0 & * & & * \\ \vdots & & \ddots & \\ 0 & * & & * \end{pmatrix}$$

Now: if a_1' doesn't divide all entries of 1st row, repeat to get a new value of a_1'. Each time we repeat this process, the Euclidean function of a_1' decreases.

This allows us to conclude that eventually we will obtain a matrix of the form

$$\to \begin{pmatrix} a_1' & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

Repeat on the bottom right block to obtain

$$\begin{pmatrix} a_1' & 0 & \cdots & 0 \\ 0 & a_2' & 0 \cdots & 0 \\ 0 & 0 & * \cdots & * \\ \vdots & \vdots & \vdots \ddots & \vdots \\ 0 & 0 & * & * \end{pmatrix} \to \cdots \to \left(\begin{array}{ccc|c} a_1' & & O & \\ & a_2' & & O \\ O & & \ddots & \\ & & a_m' & \end{array}\right)$$

(Note: $\operatorname{rank} N = m \Rightarrow a_i' \neq 0 \quad \forall\ 1 \leq i \leq m$)

Next, add all rows to 1st row and use col ops:

$$\left(\begin{array}{cccc|c} a_1' & a_2' & \cdots & a_m' & \\ & a_2' & & O & O \\ O & & \ddots & a_m' & \end{array}\right) \to \left(\begin{array}{cccc|c} \overset{=\gcd(a_1',\ldots,a_m')}{a_1} & * & \cdots & * & \\ * & * & \cdots & * & O \\ \vdots & \vdots & \ddots & \vdots & \\ * & * & \cdots & * & \end{array}\right)$$

$$\to \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

(this time, a_1 does divide everything)

Finally, let $a_2 = \gcd$(all entries of bottom right matrix);

$$\longrightarrow \begin{pmatrix} a_1 & 0 & \cdots & & 0 \\ 0 & a_2 & e_2 & & 0 \\ \vdots & 0 & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & * & \cdots & * \end{pmatrix} \xrightarrow{\text{(repeat)}} \left(\begin{array}{ccc|c} a_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & a_m & \end{array}\right)$$

$a_1 \mid a_2 \mid \cdots \mid a_m$. $\blacksquare$

A few other notes: In general in a PID there may not be a nice algorithm to compute gcds. However, Bezout's lemma still holds, a PID is a UFD, and computing the gcd of two elems cannot increase the # of prime factors of the numbers. Using this fact, the argument above can be made to work for PIDs, but it is no longer constructive. See proof of <u>Smith Normal form</u> for more details.

Exs:

1) Suppose R is a PID, let K be its field of fractions, and L/K a finite extension of fields. Prove that every finitely generated R-submodule of L is free of rank at most $[L:K]$.

Suppose $\{x_1, \dots, x_\ell\}$ is an R-gen. set for M. Then it is R-lin. ind.

Claim: $\{x_1, \dots, x_\ell\}$ is K-lin. ind.

Pf of claim: If $\sum_{i=1}^{\ell} \underbrace{\frac{p_i}{q_i}}_{=\alpha_i} x_i = 0$ for some $\frac{p_i}{q_i} \in K$ $(p_i, q_i \in R)$ then clear denoms: $q = q_1 \cdots q_\ell$,

$\sum_{i=1}^{\ell} (q\alpha_i) x_i = 0$, $q\alpha_i \in R \Rightarrow q\alpha_i = 0 \ \forall i$

$\Rightarrow \alpha_i = 0 \ \forall i$. $\blacksquare$

Extend $x_1, \dots, x_\ell$ to a K-basis $\{x_1, \dots, x_n\}$ for L, let M' be the R-module gen by $x_1, \dots, x_n$.

$\{x_1, \dots, x_n\}$ is K-lin. ind $\Rightarrow$ R lin. ind.

$\Rightarrow M'$ is a free R-module of rank n

(stacked basis thm)

$\Rightarrow M$ is a free R-module of rank $\leq n$.