Definition. Let M be f.g. free R-module. We will say that $\underline{M \text{ has rank } n}$ if M has a basis of cardinality n.

Warning: In general rank may not be well defined. It is well defined, though, if R is a field (exchange lemma from basic linear algebra) or R is a commutative domain (to be proved later). The rank of M (when well defined) will be denoted by $\mathrm{rk}(M)$.

7. Modules over PID, part I. Structure of submodules

Theorem 7.1 (structure of submodules of f.g. free modules over PID)**.** *Let R be a PID, M a f.g. free R-module and N a submodule of M. Then there exist*

(i) *a basis $\{y_1, \ldots, y_n\}$ of M and*
(ii) *nonzero elements $a_1, \ldots, a_m \in R$ with $m \leq n$ s.t.*
 (1) *$\{a_1y_1, \ldots, a_my_m\}$ is a basis of N*
 (2) *$a_1 \mid a_2 \mid \ldots \mid a_m$.*

Furthermore, the integers n and m are uniquely determined and $a_1, \ldots, a_m$ are uniqely determined up to multiplication by units.

Corollary 7.2. *If R is a PID, M a f.g. free R-module and N a submodule of M, then N is free and $\mathrm{rk}(N) \leq \mathrm{rk}(M)$.*

7.1. Some preparations.

Observation 7.3. *Let R be any ring, M an R-module, $\{u_1, \ldots, u_k\}$ and $\{w_1, \ldots, w_l\}$ ordered tuples of elements of M. Assume that $\{u_1, \ldots, u_k\}$ is a generating set of M. Then for any $1 \leq i \leq l$ we can write $w_i = \sum_{j=1}^{k} b_{ij}u_j$ for some $b_{ij} \in R$. Equivalently,* $\begin{pmatrix} w_1 \\ \vdots \\ w_l \end{pmatrix} = B \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$ *for some matrix $B = (b_{ij}) \in Mat_{l\times k}(R)$.*

Lemma 7.4. *Let $R, M, \{u_1, \ldots, u_n\}, \{w_1, \ldots, w_n\}$ and B satisfy the assumptions of Observation 7.3. Suppose that $B \in GL_n(R)$. The following hold:*

(a) *$\{w_1, \ldots, w_n\}$ is a generating set of M*
(b) *Assume in addition that $\{u_1, \ldots, u_n\}$ is a basis of M. Then $\{w_1, \ldots, w_n\}$ is also a basis of M.*

Proof. (a) Since $B \in GL_n(R)$, we have $\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = B^{-1} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$. Therefore, the submodule generated by $\{w_1, \dots, w_n\}$ contains $u_1, \dots, u_n$ and hence is equal to M.
(b) Assume that $\{w_1, \dots, w_n\}$ is linearly dependent, so there exist $r_1, \dots, r_n \in R$, not all 0, s.t. $\sum r_i w_i = 0$ or $\begin{pmatrix} r_1 & \dots & r_n \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = 0$ and hence

$$\begin{pmatrix} r_1 & \dots & r_n \end{pmatrix} B \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = 0.$$

Since $u_1, \dots, u_n$ are linearly independent, we must have $\begin{pmatrix} r_1 & \dots & r_n \end{pmatrix} B = \begin{pmatrix} 0 & \dots & 0 \end{pmatrix}$. Multiplying by B^{-1}, we get $\begin{pmatrix} r_1 & \dots & r_n \end{pmatrix} = \begin{pmatrix} 0 & \dots & 0 \end{pmatrix}$, so each $r_i = 0$. □

Theorem 7.5 (Smith Normal Form)**.** *Let R be a PID, $k, n \in \mathbb{N}$ and $A \in Mat_{k \times n}(R)$. Then A can be written as $A = CDB$ where $B \in GL_n(R)$, $C \in GL_k(R)$ and $D \in Mat_{k \times n}(R)$ is equal to* $\begin{pmatrix} \begin{matrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & a_m \end{matrix} & 0 \\ 0 & 0 \end{pmatrix}$ *for some $m \le \min\{n, k\}$ and nonzero $a_1, \dots, a_m$ with $a_1 \mid a_2 \mid \dots \mid a_m$. The matrix D is called the <u>Smith Normal Form</u> of A. Its entries $a_1, \dots, a_m$ are uniquely determined up to multiplication by units.*

Lemma 7.6. *Let R be a Noetherian ring and M a f.g. R-module. Then any submodule of M is finitely generated.*

Proof. This will be assigned as a homework problem. □

7.2. **Proof of the existence part of Theorem 7.1.**

Proof. Let $\{x_1, \dots, x_n\}$ be a basis of M and let $\{u_1, \dots, u_k\}$ be some finite generating set of N (it exists by Lemma 7.6). Then u_i's are R-linear combinations of x_j's, so there is a matrix $A \in Mat_{k \times n}(R)$ s.t. $\begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Put A into Smith normal form, that is, write $A = CDB$ where $C \in GL_k(R)$, $B \in GL_n(R)$ and $D = diag_{k \times n}(a_1, \dots, a_m)$ with $a_1 \mid \dots \mid a_m$.

Now let $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = C^{-1} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$. By Lemma 7.4 $\{y_1, \ldots, y_n\}$ is a basis of M and $\{v_1, \ldots, v_k\}$ is a generating set for N. Note that

$$\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = C^{-1}A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \underbrace{C^{-1}AB^{-1}}_{D} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} =$$

$$\begin{pmatrix} \begin{matrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & a_m \end{matrix} & \text{\Large 0} \\ \text{\Large 0} & \text{\Large 0} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} a_1 y_1 \\ \vdots \\ a_m y_m \\ 0 \\ \vdots \end{pmatrix}.$$

Thus $v_i = a_i y_i$ for $1 \leq i \leq m$ and $v_i = 0$ for $i > m$. Since $\{v_1, \ldots, v_k\}$ is a generating set for N, $\{v_1, \ldots, v_m\}$ is also a generating set for N.
It remains to show that $v_1, \ldots, v_m$ are linearly independent. If $\sum\limits_{i=1}^{m} r_i v_i = 0$, then $\sum\limits_{i=1}^{m} (r_i a_i) y_i = 0$. Since $\{y_i\}$ are linearly independent, this implies that $r_i a_i = 0$ for all i and hence each $r_i = 0$ (for R is a domain). This finishes the proof of the existence part of Theorem 7.1. □

7.3. **What is next?** Note that the proof of the existence part of Theorem 7.1 used only the existence (not the uniqueness) of the Smith Normal Form. Also note that the uniqueness part of Theorem 7.1 does not obviously follow from the uniqueness of the Smith Normal Form; on the contrary, as the above argument shows, the converse is true: the uniqueness part of Theorem 7.1 implies the uniqueness of the Smith Normal Form. This observation will be a part of our general argument for a complete proof of Theorem 7.1, Smith Normal Form Theorem as well as two versions of the classification theorem for finitely generated modules over PIDs – invariant factors (IF) form and elementary divisors (ED) form.

In Lecture 8 we will prove existence of the Smith Normal Form, which by the above argument implies the existence part of Theorem 7.1. This will easily imply the existence part of the classification theorem in IF form which, in turn, will imply the existence part of the classification theorem in ED form.

The uniqueness parts of these four theorems will be established in reverse order (in Lecture 9). First we will prove the uniqueness part of the classification theorem in ED form, then deduce the uniqueness part of the classification theorem in IF form. This will imply the uniqueness part of Theorem 7.1 which finally implies the uniqueness of the Smith Normal Form (we have already proved the last implication).