Finitely generated modules over a PID

Lemma. Let R be a commutative ring with $1 \neq 0$. If $R^m \cong R^n$ as R-modules then $m = n$.

Proof. Let $\mathfrak{m} \subset R$ be a maximal ideal, and let $k = R/\mathfrak{m}$. Then $R^m \cong R^n$ implies that $k^m \cong R^m/\mathfrak{m} \cdot R^m \cong R^n/\mathfrak{m} \cdot R^n \cong k^n$ as k-modules; hence $m = n$. $\square$

Proposition 1. Let R be a PID. If $M \subset R^n$ is a submodule, then M is free of rank $\leqslant n$.

Proof. Induction on n, the case $n = 0$ being trivial. Assume $n \geqslant 1$ and the proposition is true in lower rank. Let $\pi\colon R^n \to R$ be the projection onto the last factor, write R^{n-1} for the kernel, and let $M' = M \cap R^{n-1}$. If $\pi(M) = 0$ then $M \subset R^{n-1}$ and we are done. As R is a PID, if $\pi(M) \neq 0$ then $\pi(M) \subset R$ is a principal ideal. Choose an element $\mu \in M$ such that $\pi(\mu)$ generates $\pi(M)$. By induction, there exists a basis $e_1, \ldots, e_r$ for M' as an R-module, with $r \leqslant n-1$. If $m \in M$, we have $\pi(m) = r \cdot \pi(\mu)$ for some $r \in R$, and then $m - r\mu \in M'$. Hence $e_1, \ldots, e_r, \mu$ generate M. They are also linearly independent, for $\sum c_i e_i + d\mu = 0$ implies $d = 0$ by applying π, and we already know that $e_1, \ldots, e_r$ are linearly independent. Hence in this case M is free of rank $r + 1 \leqslant n$. $\square$

If A is an $m \times n$ matrix with coefficients in R, we simply write $\mathrm{Coker}(A)$ for the cokernel of the map $R^n \to R^m$ given by A.

Corollary. Let M be a f.g. module over a PID R. Then there exists an $m \times n$ matrix A with coefficients in R, for some m and n, such that $M \cong \mathrm{Coker}(A)$.

Proof. As M is finitely generated, there exists a surjective map $p\colon R^m \to M$. By the proposition, there exists $n \leqslant m$ and an isomorphism $R^n \xrightarrow{\sim} \mathrm{Ker}(p)$. Then $M \cong \mathrm{Coker}(A)$, where A is the matrix of the composite map $R^n \to \mathrm{Ker}(p) \hookrightarrow R^m$. $\square$

In what follows, let R be a PID. Any two non-zero elements of R have a gcd that is well-determined up to multiplication by a unit: c is said to be a gcd of a and b if $(c) = (a, b)$. Note that, by definition, this implies that c can be written as $c = x \cdot a + y \cdot b$ for some x, $y \in R$.

Proposition 2. Let m and n be positive integers and $A = (a_{ij})$ an $m \times n$ matrix with coefficients in R. Then there exist $P \in \mathrm{GL}_m(R)$ and $Q \in \mathrm{GL}_n(R)$ such that $P \cdot A \cdot Q$ is a diagonal matrix $\mathrm{diag}(r_1, \ldots, r_t, 0, \ldots, 0)$ with non-zero $r_i \in R$ such that r_i divides r_{i+1} for $i = 1, \ldots, t-1$.

Note that "diag" here means an $m \times n$ diagonal matrix, so not necessarily square.

Proof. Let $E(A)$ be the set of all matrices of the form $P \cdot A \cdot Q$ with invertible P and Q. Note: if $B \in E(A)$ then $E(B) = E(A)$. Further, if $B \in E(A)$ then any matrix obtained from B by permuting rows and columns is again in $E(A)$. Also, any matrix obtained from B by elementary row or column operations is again in $E(A)$.

Let $V \subset R$ be the subset of all elements that occur as matrix coefficient in some matrix in $E(A)$. We may assume V contains non-zero elements, for otherwise $A = 0$ and there is nothing to prove. Let $\beta \in V$ be any non-zero element for which (β) is as large as possible. In other words:

there is no C in $E(A)$ that has a matrix coefficient c_{ij} that strictly divides β, i.e., for which $(\beta) \subsetneq (c_{ij})$. (Such an element β exists because R is a noetherian ring. Alternatively, use that R is a UFD.) Using row and column permutations we find that there exists a $B = (b_{ij}) \in E(A)$ such that $b_{1,1} = \beta$.

We claim that β divides all $b_{1,j}$ and all $b_{i,1}$. Indeed, suppose β does not divide some $b_{1,j}$. For simplicity of exposition, suppose it is $b_{1,2}$. Let c be a gcd of $\beta = b_{1,1}$ and $b_{1,2}$, and choose x, $y \in R$ such that $c = x \cdot \beta + y \cdot b_{1,2}$. Write $\beta = r \cdot c$ and $b_{1,2} = s \cdot c$, so that $1 = x \cdot r + y \cdot s$. Let $Q \in \mathrm{GL}_n(R)$ the matrix

$$Q = \begin{pmatrix} x & -s & & & \\ y & r & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

Then $B \cdot Q \in E(A)$ and as c is a matrix coefficient of $B \cdot Q$ we arrive at a contradiction with our choice of β. In a similar way we see that β divides all $b_{i,1}$. By row and column operations, this gives a matrix in $E(A)$ of the form

$$\begin{pmatrix} \beta & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_2 & \\ 0 & & & \end{pmatrix}$$

where A_2 is an $(m-1) \times (n-1)$ matrix.

By induction, we find that $E(A)$ contains a matrix $\mathrm{diag}(\beta, r_2, \ldots, r_t, 0, \ldots, 0)$ with r_i dividing r_{i+1}. It only remains to be shown that β divides r_2. For this, choose x, $y \in R$ such that $c = x \cdot \beta + y \cdot r_2$ is a gcd of β and r_2. Then it follows from the identity

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \cdot \begin{pmatrix} \beta & 0 \\ 0 & r_2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} = \begin{pmatrix} \beta & 0 \\ c & r_2 \end{pmatrix}$$

that $E(A)$ contains a matrix in which c occurs as coefficient. By our choice of β we must have $(\beta) = (c)$, which means that $\beta | r_2$. $\square$

Theorem. Let R be a PID. Let M be a f.g. module over R. Then there exist integers $r, t \geqslant 0$ and a chain of ideals $R \neq I_1 \supseteq I_2 \supseteq \cdots \supseteq I_t \neq (0)$, all uniquely determined, such that

$$M \cong R^r \oplus R/I_1 \oplus \cdots \oplus R/I_t$$

as R-modules.

Proof. The existence follows from the Corollary to Proposition 1 together with Proposition 2; here we note that if $B = P \cdot A \cdot Q$ then $P \colon R^m \xrightarrow{\sim} R^m$ induces an isomorphism $\mathrm{Coker}(A) \xrightarrow{\sim} \mathrm{Coker}(B)$.

For the uniqueness, suppose $M = R^r \oplus R/I_1 \oplus \cdots \oplus R/I_t$ and $N = R^\rho \oplus R/J_1 \oplus \cdots \oplus R/J_u$ are isomorphic, where we assume $R \neq I_1 \supseteq I_2 \supseteq \cdots \supseteq I_t \neq (0)$ and $R \neq J_1 \supseteq J_2 \supseteq \cdots \supseteq J_u \neq (0)$. Then $R/I_1 \oplus \cdots \oplus R/I_t = \mathrm{Tors}(M)$ is isomorphic to $R/J_1 \oplus \cdots \oplus R/J_u = \mathrm{Tors}(N)$ and $R^r \cong M/\mathrm{Tors}(M) \cong N/\mathrm{Tors}(N) \cong R^\rho$. The latter already implies that $r = \rho$. It remains to treat the case $r = \rho = 0$. If $m \in M$, its annihilator $\mathrm{ann}(m) = \{r \in R \mid rm = 0\}$ is an ideal of R, and I_1 is the largest proper ideal of R that occurs among these ideals. This characterizes I_1, and hence $I_1 = J_1$. If $\mathfrak{m}$ is a maximal ideal containing I_1 then t is the dimension of $M/\mathfrak{m}M$ over the residue field $R/\mathfrak{m}$; this characterizes t, and hence $t = u$.

Let $\mathscr{M}$ be the set of all maximal ideals of R. Every non-zero ideal $I \subset R$ can be written in a unique way as $I = \prod_{\mathfrak{p} \in \mathscr{M}} \mathfrak{p}^{v_\mathfrak{p}(I)}$ with exponents $v_\mathfrak{p}(I) \geqslant 0$ that are 0 for almost all $\mathfrak{p}$. By how we have chosen the I_i and J_i, we have $v_\mathfrak{p}(I_i) \leqslant v_\mathfrak{p}(I_{i+1})$ and $v_\mathfrak{p}(J_i) \leqslant v_\mathfrak{p}(J_{i+1})$ for all $\mathfrak{p} \in \mathscr{M}$ and $i = 1, \ldots, t-1$. If $I_q \neq J_q$ for some q, choose q maximal with this property. There exists $\mathfrak{p} \in \mathscr{M}$ with $v_\mathfrak{p}(I_q) \neq v_\mathfrak{p}(J_q)$, and by symmetry we may assume $v_\mathfrak{p}(I_q) > v_\mathfrak{p}(J_q)$. If P is an R-module and $a \geqslant 0$ then $\mathfrak{p}^a \cdot P/\mathfrak{p}^{a+1} \cdot P$ is a vector space over the residue field $k = R/\mathfrak{p}$. Moreover, in case $P = R/I$ for some non-zero ideal I we find that $\mathfrak{p}^a \cdot P/\mathfrak{p}^{a+1} \cdot P$ is zero if $v_\mathfrak{p}(I) < a$ and is 1-dimensional over k if $v_\mathfrak{p}(I) \geqslant a$. Therefore, if we take $a = v_\mathfrak{p}(I_q)$ then we find that $\dim_k\bigl(\mathfrak{p}^a \cdot M/\mathfrak{p}^{a+1} \cdot M\bigr) > \dim_k\bigl(\mathfrak{p}^a \cdot N/\mathfrak{p}^{a+1} \cdot N\bigr)$; contradiction. This shows that $I_q = J_q$ for all q. $\square$