Problem (Problem 2)**:** Let R be a PID. For an R-module M, denote by $d(M)$ the minimal number of generators of M.

(a) Prove that if M is a finitely generated R-module, and N is a submodule of M, then $d(N) \leq d(M)$.

(b) Let $a \in R$ be a nonzero non-unit. Find (with proof) the number of submodules of R/aR in terms of the prime decomposition of a.

Solution:

(a) Let $\{v_1, \dots, v_n\}$ be a minimal generating set for M. Via the surjection $R^n \to M$ taking $(r_1, \dots, r_n) \mapsto \sum_{i=1}^n r_i v_i$, we observe that $M \cong R^n/G$ for some submodule G of R^n. Since N is a submodule of M, it follows from the fourth isomorphism theorem that N corresponds to a submodule of R^n containing G, which we will call N'; since N' is a submodule of a free module, it is free with rank $m \leq n$, and N' surjects onto N so that $d(N) \leq d(N') \leq n = d(M)$.

(b) Without loss of generality, let $a = p_1^{d_1} \cdots p_t^{d_t}$ be the prime decomposition for a, where $d_i \in \mathbb{N}$. From the Chinese Remainder Theorem, we have

$$R/(a) \cong R/\left(p_1^{d_1}\right) \oplus \cdots \oplus R/\left(p_t^{d_t}\right).$$

Observe that any submodule of $R/(a)$ is in correspondence with an ideal containing a (by the fourth isomorphism theorem). These ideals are precisely the ideals of products of prime powers that are less than or equal to a. Since, given $p_i^{d_i}$, there are $0, \dots, d_i$ potential options for the power of p_i, so that there are $(d_1 + 1) \cdots (d_t + 1)$ submodules in $R/(a)$.

Problem (Problem 3)**:**

(a) Let R be a PID, M a finitely generated R-module, and

$$M = \left(\bigoplus_{i=1}^{\ell} R/(a_i) \right) \oplus R^s$$

its invariant factor decomposition. Prove that $d(M) = m + s$.

(b) Again let R be a PID. Let F be a free R-module of rank n with basis $e_1, \dots, e_n$, N the submodule of F generated by some elements $v_1, \dots, v_n \in F$, and let $A \in \mathrm{Mat}_n(F)$ be the matrix such that

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}.$$

Find a simple condition on the entries of A which holds if and only if $d(F/N) = n$.

Solution:

(a) Let p be a prime dividing a_1. Now, we observe that

$$\begin{aligned} M/pM &\cong \frac{\left(\bigoplus_{i=1}^m R/(a_i)\right) \oplus R^s}{\left(\bigoplus_{i=1}^m p(R/(a_i))\right) \oplus (pR)^s} \\ &\cong (R/(p))^{m+s}. \end{aligned}$$

Now, since R is a PID, any prime ideal is maximal, meaning that $d(M') = m + s$ is the dimension of $M' = (R/(p))^{m+s}$. Since M' is a quotient of M, it follows that $d(M) \geq m + s$.

Yet, since the set $\{e_i \mid 1 \leq i \leq m + s\}$ generates M as an R-module (where each e_i denotes the tuple with 1 at position i and 0 elsewhere), it follows that $d(M) \leq m + s$, so that $d(M) = m + s$.

(b) Observe that F/N is a finitely generated module over R, and that the invariant factors for $M \cong F/N$ emerge from the Smith normal form for A (as discussed in the proof of the classification in invariant

factors form). Therefore, we may write

$$M = \bigoplus_{i=1}^{\ell} R/(a_i) \oplus R^k.$$

Now, if $k + \ell = n$, then it follows that none of the ideals (a_i) are equal to R (as else their quotient would be equal to 0), implying that the Smith normal form of A does not admit any units.

Similarly, if $a_1 | \cdots | a_\ell$ are the invariant factors in the Smith normal form of A, then following the proof in the classification in invariant factors form, we find that

$$F/N \cong \bigoplus_{i=1}^{\ell} R/(a_i) \oplus R^{n-\ell},$$

where none of the $R/(a_i)$ are the zero ring. Thus, it follows that $d(F/N) = \ell + (n - \ell) = n$.

Problem (Problem 4)**:** Let M be a module over the integral domain R.

(a) Suppose that M has rank n, and that $x_1, \ldots, x_n$ is any maximal set of linearly independent elements of M. Let $N = \langle x_1, \ldots, x_n \rangle$ be the submodule generated by $x_1, \ldots, x_n$. Prove that N is isomorphic to R^n and that the quotient M/N is a torsion R-module.

(b) Prove conversely that if M contains a submodule N that is free of rank n such that the quotient M/N is a torsion R-module, then M has rank n.

Solution:

(a) Let $\pi \colon R^n \to N$ be the projection onto N given by $(r_1, \ldots, r_n) \mapsto \sum_{i=1}^n r_i x_i$. We observe that this projection is surjective by the definition of N, and it is injective since $\{x_1, \ldots, x_n\}$ are linearly independent (hence the only way for the sum to equal zero is for each of the r_i to equal zero). Thus, N is isomorphic to R^n.

Now, suppose toward contradiction that M/N is not torsion. That is, there is some nonzero $x+N \in M/N$ such that $rx + N \neq 0$ for all $0 \neq r \in R$. This gives that $rx \notin N$ for all $0 \neq r \in R$, so if we have

$$0 = \sum_{i=1}^{n} r_i x_i + rx,$$

then upon taking quotients, we have that $r = 0$, and since the set $\{x_1, \ldots, x_n\}$ are linearly independent, we must have that each of the r_i are equal to zero, which would imply that x was independent of $\{x_1, \ldots, x_n\}$, contradicting maximality. Therefore, M/N is torsion.

(b) Suppose M contains a submodule N of rank n such that M/N is torsion. Suppose $\{y_1, \ldots, y_{n+1}\}$ are any $n+1$ elements of M. From our work above, we see that an equivalent result is that for any $y \in M$, we have some $0 \neq r \in R$ such that ry can be written as a linear combination of the maximally linearly independent set $\{x_1, \ldots, x_n\}$. For each i, we do this, yielding

$$r_i y_i = \sum_{j=1}^{n} a_{ij} x_j.$$

This gives that we may write the collection $\{r_1 y_1, \ldots, r_{n+1} y_{n+1}\}$ as a collection of $n+1$ vectors in $N \cong R^n$, meaning that we get a linear dependence relation

$$s_1 r_1 y_1 + \cdots + s_{n+1} r_{n+1} y_{n+1} = 0$$

with not all $s_i = 0$ since R is an integral domain. Therefore, we have that the collection $\{y_1, \ldots, y_{n+1}\}$ is linearly dependent, so M necessarily has rank n.

Problem (Problem 5)**:** Let R be a PID, M a finitely generated free R-module, and N a submodule of M. Prove that the following are equivalent:

(i) any basis of N can be extended to a basis of M;

(ii) some basis of N can be extended to a basis of M;

(iii) M/N is free;

(iv) M/N is torsion-free.

Solution: We will show (i) implies (ii) implies (iii) implies (i), and separately show (iii) holds if and only if (iv) holds.

First, the implication (i) implies (ii) follows from the fact that any submodule of a free module is free, meaning that it admits a basis, which by the assumption in (i) means said basis can be extended to one for M.

Now, suppose there is a basis $\{y_1, \dots, y_m\}$ of N that can be extended to a basis $\{y_1, \dots, y_n\}$ of M. Upon taking quotients, we observe that the set $\{y_{m+1} + N, \dots, y_n + N\}$ generates M/N since the full basis generates M. Furthermore, we have

$$\sum_{k=m+1}^{n} a_k(y_k + N) = \left(\sum_{k=m+1}^{n} a_k y_k \right) + N,$$

which equals zero in M/N if and only if the sum is contained in N, but that would contradict the linear independence of the set $\{y_1, \dots, y_n\}$, meaning that M/N is free.

Suppose now that M/N is free with basis $\{x_1 + N, \dots, x_\ell + N\}$, and let $\{y_1, \dots, y_m\}$ be a basis for N. We claim that $\{y_1, \dots, y_m, x_1, \dots, x_\ell\}$ is a basis for M. To see that it is generating, observe that if $v \in M$ is any element, then we may write

$$v + N = \left(\sum_{k=1}^{\ell} a_k x_k \right) + N,$$

and

$$v - \left(\sum_{k=1}^{\ell} a_k x_k \right) = \sum_{i=1}^{m} b_i y_i,$$

so that

$$v = \sum_{i=1}^{m} b_i y_i + \sum_{k=1}^{\ell} a_k x_k.$$

For linear independence, we let

$$\sum_{i=1}^{n} b_i y_i + \sum_{k=1}^{\ell} a_k x_k = 0.$$

Taking quotients, we observe that we have

$$\left(\sum_{k=1}^{\ell} a_k x_k \right) + N = 0,$$

implying that the sum $\sum_{k=1}^{\ell} a_k x_k \in N$, but this can only happen if $a_1, \dots, a_k = 0$. Therefore, we get

$$\sum_{i=1}^{m} b_i y_i = 0,$$

meaning that $b_1, \dots, b_m = 0$ since the y_i form a basis. Notice that this expression is well-defined since any two x_k differ by an element of N, which may then be absorbed into the linear combination of the y_i. This gives (i).

Finally, we let $P = M/N$. Since P is a finitely generated module over R, it admits an invariant factors decomposition

$$P = \bigoplus_{i=1}^{\ell} R/(a_i) \oplus R^s.$$

Observe that P has non-trivial invariant factors if and only if it has torsion, meaning that P is free if and only if it is torsion-free.