35.5 Finitely Generated Modules over a PID; Invariant Factor Decomposition

There are several ways of obtaining the decomposition of a finitely generated module as a direct sum of cyclic modules. One way to proceed is to first use the Primary Decomposition Theorem and then to show how each primary module M_p is the direct sum of cyclic modules of the form $A/(p^n)$. This is the approach followed by Lang [109] (Chapter III, section 7), among others. We prefer to use a proposition that produces a particular basis for a submodule of a finitely generated free module, because it yields more information. This is the approach followed in Dummitt and Foote [54] (Chapter 12) and Bourbaki [26] (Chapter VII). The proof that we present is due to Pierre Samuel.

Proposition 35.23. *Let F be a finitely generated free module over a PID A, and let M be any submodule of F. Then, M is a free module and there is a basis $(e_1, ..., e_n)$ of F, some $q \leq n$, and some nonzero elements $a_1, \ldots, a_q \in A$, such that $(a_1e_1, \ldots, a_qe_q)$ is a basis of M and a_i divides a_{i+1} for all i, with $1 \leq i \leq q-1$.*

Proof. The proposition is trivial when $M = \{0\}$, thus assume that M is nontrivial. Pick some basis $(u_1, \ldots, u_n)$ for F. Let $L(F, A)$ be the set of linear forms on F. For any $f \in L(F, A)$, it is immediately verified that $f(M)$ is an ideal in A. Thus, $f(M) = a_hA$, for some $a_h \in A$, since every ideal in A is a principal ideal. Since A is a PID, any nonempty family of ideals in A has a maximal element, so let f be a linear map such that a_hA is a maximal ideal in A. Let $\pi_i \colon F \to A$ be the i-th projection, i.e., π_i is defined such that $\pi_i(x_1u_1 + \cdots + x_nu_n) = x_i$. It is clear that π_i is a linear map, and since M is nontrivial, one of the $\pi_i(M)$ is nontrivial, and $a_h \neq 0$. There is some $e' \in M$ such that $f(e') = a_h$.

We claim that, for every $g \in L(F, A)$, the element $a_h \in A$ divides $g(e')$.

Indeed, if d is the gcd of a_h and $g(e')$, by the Bézout identity, we can write

$$d = ra_h + sg(e'),$$

for some $r, s \in A$, and thus

$$d = rf(e') + sg(e') = (rf + sg)(e').$$

However, $rf + sg \in L(F, A)$, and thus,

$$a_hA \subseteq dA \subseteq (rf + sg)(M),$$

since d divides a_h, and by maximality of a_hA, we must have $a_hA = dA$, which implies that $d = a_h$, and thus, a_h divides $g(e')$. In particular, a_h divides each $\pi_i(e')$ and let $\pi_i(e') = a_hb_i$, with $b_i \in A$.

Let $e = b_1u_1 + \cdots + b_nu_n$. Note that

$$e' = \pi_1(e')u_1 + \cdots + \pi_n(e')u_n = a_hb_1u_1 + \cdots + a_hb_nu_n,$$