9. Classification of finitely generated modules over PID.

Today we will prove two forms of the classification theorem for finitely generated modules over PIDs (stated below) – IF (invaraint factors) and ED (elementary divisors). We shall also establish the uniqueness parts of the submodule theorem (Theorem 7.1) and SNF Theorem (the existence parts of which we have already proved).

Our general scheme of the proof will be as follows:

$$\textbf{Existence}: \quad \boxed{\text{SNF Thm}} \quad \overset{1}{\Longrightarrow} \quad \text{submod. Thm} \quad \overset{2}{\Longrightarrow} \quad \text{IF class.} \quad \overset{3}{\Longrightarrow} \quad \text{ED class.}$$

$$\textbf{Uniqueness}: \quad \text{SNF Thm} \quad \overset{6}{\Longleftarrow} \quad \text{submod. Thm} \quad \overset{5}{\Longleftarrow} \quad \text{IF class.} \quad \overset{4}{\Longleftarrow} \quad \boxed{\text{ED class.}}$$

We shall prove the two boxed statements as well as implicatios (1)-(6). Note that the first boxed statement (existence part of SNF Theorem) has already been proved in Lecture 8 and implications 1 and 6 have been established in Lecture 7.

Theorem 9.1 (Classification in IF form)**.** *Let R be a PID and M a f.g. R-module. Then*

$$M \cong R/a_1R \oplus \ldots \oplus R/a_mR \oplus R^s$$

where $a_1, \ldots, a_m$ are nonzero non-units and $a_1 \mid \ldots \mid a_m$. The integers s and m are uniquely determined and $a_1, \ldots, a_m$ are uniquely determined up to multiplication by units.

Proof: IF, existence ($\overset{2}{\Longrightarrow}$). Let $\{x_1, \ldots, x_n\}$ be a finite generating set for M. Let $F = R^n$ (the standard free R-module of rank n), and denote its standard basis by $\{e_1, \ldots, e_n\}$.

Let $\varphi : F \to M$ be the unique R-module homomorphism such that $\varphi(e_i) = x_i$. Then φ is surjective, and thus $M \cong F/N$ where $N = \operatorname{Ker} \varphi$.

By Theorem 7.1 applied to the pair (F, N) there exist a basis $\{y_1, \ldots, y_n\}$ of F and nonzero elements $a_1, \ldots, a_l$ with $l \leq n$ and $a_1 \mid \ldots \mid a_l$ such that $\{a_1y_1, \ldots, a_ly_l\}$ is a basis of N. Then

$$F = Ry_1 \oplus \ldots \oplus Ry_n \text{ and } N = Ra_1y_1 \oplus \ldots \oplus Ra_ly_l,$$

and therefore [1]

$$F/N \cong Ry_1/Ra_1y_1 \oplus \ldots \oplus Ry_l/Ra_ly_l \oplus R^{n-l}.$$

[1] Here we use the fact that the i^{th} summand in the decomposition of N lies inside the i^{th} summand in the decomposition of F

It is clear that $Ry_i/Ra_iy_i \cong R/a_iR$ and $Ry_i \cong R$ as R-modules. If a_i is a unit for some i, then $R/a_iR = \{0\}$. Removing these trivial summands, we obtain the desired decomposition. □

Remark: This proof also establishes implication $\overset{5}{\Longleftarrow}$ (check details).

Theorem 9.2 (Classification in ED form)**.** *Let R be a PID and M a f.g. R-module. Then*

$$M \cong R/p_1^{\alpha_1}R \oplus \ldots \oplus R/p_k^{\alpha_k}R \oplus R^s$$

where $p_1, \ldots, p_k$ are primes (not necessarily distinct) and each $\alpha_i > 0$. The integers s and k are uniquely determined, and the elements $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ are uniquely determined up to permutation and multiplication by units.

Proof: ED, existence ($\overset{3}{\Longrightarrow}$). Since we already have IF decomposition, it is enough to show that for each $a \in R$ the cyclic module R/aR has ED decomposition. Write a as a product of prime powers $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}u$ where $p_1, \ldots, p_k$ are pairwise non-associate and u is a unit.

By the Chinese Remainder Theorem $R/aR \cong R/p_1^{\alpha_1}R \oplus \ldots \oplus R/p_k^{\alpha_k}R$ as rings, and an explicit isomorphism if given by $r + aR \mapsto (r + p_1^{\alpha_1}R, \ldots, r + p_k^{\alpha_1}R)$. But this map is clearly R-linear, and hence also an isomorphism of R-modules. □

Proof: ED, uniqueness. Suppose that $M \cong R/p_1^{\alpha_1}R \oplus \ldots \oplus R/p_k^{\alpha_k}R \oplus R^s$.
Step 1: Recovering s (from M). Let F be the field of fractions of R. What can we say about $F \otimes_R M$ as F-vector space? Note that

(i) $F \otimes_R (A \oplus B) \cong F \otimes_R A \oplus F \otimes_R B$ as F-modules (generalization of Proposition 4.3)

(ii) $F \otimes_R R \cong F$ as F-modules (generalization of Example 4.4)

(iii) $F \otimes_R (R/p_i^{\alpha_i}R) = \{0\}$ (torsion $\otimes$ divisible)

Thus, $F \otimes_R M \cong F^s$. By basic linear algebra a vector space over a field has a well defined dimension. Thus, $s = \dim_F(F \otimes_R M)$ is determined by M.
Step 2: Recovering primes and primary components. WOLOG we can assume that for any i, j either $p_i = p_j$ or p_i and p_j are non-associate.
For each prime $p \in R$ define

$$T_p(M) = \{m \in M : p^t m = 0 \text{ for some } t \in \mathbb{N}\}$$

It is easy to see that $T_p(M) \cong \oplus_{p_i=p} R/p^{\alpha_i}R$ if $p = p_j$ for some j and $T_p(M) = \{0\}$ if p is not associate to any p_j's. Thus M uniquely determines the primes involved in ED decomposition, and for each such prime M determines the sum of all summands involving that prime. This reduces the problem to ED decompositions with a single prime involved.

Step 3: The case of a single prime. Fix a prime p, and assume that

$$M \cong R/p^{\beta_1}R \oplus \ldots \oplus R/p^{\beta_l}R.$$

We want to recover β_i's from M. We shall argue by induction on $\sum \beta_i$.

Observe that $pM \cong R/p^{\beta_1 - 1}R \oplus \ldots \oplus R/p^{\beta_l - 1}R$. Thus, by induction we recover all β_i which are ≥ 2. It remains to show that the number of β_i's equal to 1 is determined by M, for which it is enough to show that l (the total number of β's) is determined by M.

But notice that $M/pM \cong (R/pR)^l$. Since M/pM is a field, we get that $l = \dim_{R/pR}(M/pM)$ is determined by M. □

To finish our combined proof of four theorems it remains to check implication $\overset{4}{\Longleftarrow}$. Given a PID R, there is a natural bijection

$$\boxed{\text{equiv. classes of possible IF decompositions}} \longleftrightarrow \boxed{\text{equiv. classes of possible ED decompositions}}$$

which preserves isomorphism class of modules (we described this bijection in the case of abelian groups in Algebra-I, and the general case is similar). Thus, if some f.g. R-module had two non-equivalent IF decompositions, it also would have had two non-equivalent ED decompositions. This proves $\overset{4}{\Longleftarrow}$.