ALTERNATE PROOF OF UNIQUENESS OF DECOMPOSITION OF MODULES OVER PIDS – MATH 536 SPRING

KARL SCHWEDE

We will give a presentation of the following theorem we proved in class. This slightly differs from the presentation in the book.

Theorem 0.1. *Suppose that R is a PID and suppose that*

$$M = R^{\oplus a_0} \oplus R/\langle p_1^{a_1}\rangle \oplus R/\langle p_2^{a_2}\rangle \oplus \ldots \oplus R/\langle p_n^{a_n}\rangle$$

and

$$M' = R^{\oplus b_0} \oplus R/\langle q_1^{b_1}\rangle \oplus R/\langle q_2^{b_2}\rangle \oplus \ldots \oplus R/\langle q_m^{b_m}\rangle$$

are R-modules with $a_0, b_0 \geq 0$ and the other $a_i, b_i > 0$ and the p_i and q_i prime elements. Then if $M \cong M'$ we have that $a_0 = b_0$ and the other terms in the direct sum are the same up to reordering (note that multiplying p_i by a unit doesn't change the ideal $\langle p_i^{a_i}\rangle$ and so such modifications are allowed – and ignored).

Proof. We notice that the rank of M is equal to a_0. To see this suppose that $p = \prod p_i^{a_i}$ then

$$pM = (pR)^{\oplus a_0} \oplus 0 \oplus \ldots \oplus 0 \cong R^{\oplus a_0}.$$

It follows easily then the terms in the non-free summands of R cannot contribute to a set being linearly independent and so the rank of M is a_0 and likewise the rank of M' is b_0. Hence since $M \cong M'$ we see that $a_0 = b_0$.

Next we claim that we can in fact assume that a_0 and b_0 are zero. Let

$$\text{torsion}(M) := \{x \in M \mid rx = 0 \text{ for some nonzero } r \in R\}.$$

Then in fact $\text{torsion}(M) \cong R/\langle p_1^{a_1}\rangle \oplus R/\langle p_2^{a_2}\rangle \oplus \ldots \oplus R/\langle p_n^{a_n}\rangle$ (nonzero elements in the free summands can't show up in the torsion part of M since R is an integral domain). Likewise $\text{torsion}(M') \cong R/\langle q_1^{b_1}\rangle \oplus R/\langle q_2^{b_2}\rangle \oplus \ldots \oplus R/\langle q_m^{b_m}\rangle$. Therefore if $M \cong M'$ we see that

$$R/\langle p_1^{a_1}\rangle \oplus R/\langle p_2^{a_2}\rangle \oplus \ldots \oplus R/\langle p_n^{a_n}\rangle \cong R/\langle q_1^{b_1}\rangle \oplus R/\langle q_2^{b_2}\rangle \oplus \ldots \oplus R/\langle q_m^{b_m}\rangle$$

hence we can assume that $a_0 = b_0 = 0$ as claimed.

Next we make a definition, for any $r \in R$ define $\text{Ann}_r(M) = \{x \in M \mid rx = 0\}$. We likewise define $\text{Ann}_{r^\infty}(M) = \{x \in M \mid r^k x = 0 \text{ for some } k \in \mathbb{Z}_{>0}\}$.

Claim 0.2. *If $p \in R$ (a PID) is irreducibile then* $\text{Ann}_{p^\infty}(M) = \bigoplus_{\langle p\rangle = \langle p_i\rangle} R/\langle p^{a_i}\rangle$

Proof of claim. It is an exercise left to the reader that $\text{Ann}_{p^\infty}(A \oplus B) \cong \text{Ann}_{p^\infty}(A) \oplus \text{Ann}_{p^\infty}(B)$. Assuming this observe that $Ann_{p^\infty}(R/\langle p^i\rangle) = R/\langle p^i\rangle$ since every element is killed by a power of p.

On the other hand if $q \in R$ is an irreducible element such that $\langle p\rangle \neq \langle q\rangle$ then we assert that $\text{Ann}_{p^\infty}(R/\langle q^i\rangle) = 0$. Indeed consider the coset $x + \langle q^i\rangle$ and suppose that $p^k(x + \langle q^i\rangle) = p^k x + \langle q^i\rangle = 0 + \langle q^i\rangle$. Then $p^k x \in \langle q^i\rangle$. This implies that $q|p^k x$ and since $\langle p\rangle \neq \langle q\rangle$ we see that $q|x$. Hence $x + \langle q^i\rangle$ is the zero coset as asserted.

Applying our this to each term in the direct sum consecutively proves the claim. $\square$

We return to the main proof.

By applying the claim to both M and M' we may assume that all the p_is also appear as q_js and vice versa. We may also assume that all the p_i and q_i are equal to the same irreducible element p. Hence we may assume that

$$M = R/\langle p^{a_1}\rangle \oplus \ldots \oplus R/\langle p^{a_n}\rangle$$

and

$$M' = R/\langle p^{b_1}\rangle \oplus \ldots \oplus R/\langle p^{b_m}\rangle.$$

Consider now $\mathrm{Ann}_p(M) = \{x \in M \mid px = 0\}$.

Claim 0.3. $\mathrm{Ann}_p(M) \cong \bigoplus_{i=1}^n (R/\langle p\rangle)$

Proof of claim. We will again leave it to the reader to show that the formation of $\mathrm{Ann}_p(M)$ commutes with direct sums. Hence it remains to show that $\mathrm{Ann}_p(R/\langle p^a\rangle) \cong R/\langle p\rangle$. Note that

$$\mathrm{Ann}_p(R/\langle p^a\rangle) = \{r + \langle p^a\rangle \mid r \in R, pr \in p^a\} = \{p^{a-1}s + \langle p^a\rangle \mid s \in R\}.$$

Consider the map $\phi : R \longrightarrow \{p^{a-1}s + \langle p^a\rangle \mid s \in R\}$ which sends $s \mapsto p^{a-1}s + \langle p^a\rangle$. The kernel of ϕ is clearly $\langle p\rangle$ and ϕ is surjective so by the first isomorphism theorem $\mathrm{Ann}_p(R/\langle p^a\rangle) \cong R/\langle p\rangle$. This proves the claim. $\square$

It follows that $\mathrm{Ann}_p(M)$ is a n-dimensional $R/\langle p\rangle$-vector space. Hence applying the claim to M' we see that

$$m = n. \tag{0.3.1}$$

Next for each integer $k > 0$ consider

$$p^kM \text{ and } p^kM'$$

We claim that

Claim 0.4. $p^kM \cong \oplus_{a_i>k} R/\langle p^{a_i-k}\rangle$

Proof of claim. We leave it to the reader to check that $p^k(A \oplus B) \cong (p^kA) \oplus (p^kB)$ and so we only need to verify the case that $M = R/\langle p^a\rangle$. If $a \leq k$ then $p^k(x + \langle p^a\rangle) = p^kx + \langle p^a\rangle = 0 + \langle p^a\rangle$. Hence $p^kM = 0$. On the other hand, if $a > k$ then it is easy to see that

$$p^kM = \{p^kr + \langle p^a\rangle \mid r \in R\}.$$

Consider the map $\phi : R \longrightarrow p^kM$ which sends $r \mapsto p^kr + \langle p^a\rangle$. This obviously surjects onto p^kM and so we simply observe what the kernel is. It is those r such that $p^kr \in \langle p^a\rangle$ which is exactly those r which are divisible by p^{a-k}. Hence $\ker\phi = \langle p^{a-k}\rangle$. The the first isomorphism theorem shows that $p^kM = p^k(R/\langle p^a\rangle) \cong R/\langle p^{a-k}\rangle$ which proves the claim. $\square$

Fix an integer k and consider p^kM. The number of summands in p^kM (which is a constant by (0.3.1)) is equal to $\#\{a_i \mid a_i > k\}$. Since $p^aM \cong p^aM'$ we see that

$$\#\{a_i \mid a_i > k\} = \#\{b_i \mid b_i > k\}$$

By applying this for successive values of k we see immediately that

$$\#\{a_i \mid a_i = k\} = \#\{b_i \mid b_i = k\}$$

for all values of k. This is enough to conclude the theorem. $\square$