5. Modules over a PID

I spent one more day to finish the uniqueness part of the structure theorem for f.g. modules over a PID. First I reviewed properties of the rank.

5.1. **rank.**

Recall that if R is any domain, $Q(R)$ is a field. So, for any R-module M, we can define the *rank* of M to be

$$rM = \dim_{Q(R)} M \otimes Q(R).$$

We know that $Q(R) = S^{-1}R$ is a flat R-module. Therefore, any short exact sequence of R-modules

$$0 \to A \to B \to C \to 0$$

gives a short exact sequence of vector spaces

$$0 \to Q(R) \otimes A \to Q(R) \otimes B \to Q(R) \otimes C \to 0.$$

Lemma 5.1. *If $0 \to A \to B \to C \to 0$ is a short exact sequence of vector spaces over a field F then*

(1) $B \cong A \oplus C$
(2) $\dim B = \dim A + \dim C$.

Proof. This follows from the fact that all modules over fields are free and thus projective. □

Theorem 5.2. *If $0 \to A \to B \to C \to 0$ is a short exact sequence of f.g. R-modules where R is any domain, then*

$$r(B) = r(A) + r(C).$$

5.2. **$\mathfrak{p}$-rank.**

Suppose that $\mathfrak{p} \subseteq R$ is a prime ideal. Then $R/\mathfrak{p}$ is a domain. So, modules over $R/\mathfrak{p}$ have rank.

Definition 5.3. Define the $\mathfrak{p}$-*rank* of an R-module M to be the rank of the $R/\mathfrak{p}$-module

$$R/\mathfrak{p} \otimes M = M/\mathfrak{p}M.$$

This is the dimension of the vector space

$$Q(R/\mathfrak{p}) \otimes M.$$

Example 5.4. Let $R = \mathbb{Z}$ and

$$M = \mathbb{Z}/20 \oplus \mathbb{Z}/8.$$

The prime number $p = 5$ is irreducible and thus generates a prime ideal $\mathfrak{p} = (5) = 5\mathbb{Z}$. Here $R/\mathfrak{p} = \mathbb{Z}/5$ is a field.

The 5-rank of M is the dimension of the vector space:

$$\begin{aligned} \mathbb{Z}/5 \otimes M \quad &= \mathbb{Z}/5 \otimes (\mathbb{Z}/20 \oplus \mathbb{Z}/8) \\ &= (\mathbb{Z}/5 \otimes \mathbb{Z}/20) \oplus (\mathbb{Z}/5 \otimes \mathbb{Z}/8) \\ &= \mathbb{Z}/(5,20) \oplus \mathbb{Z}/(5,8) \\ &= \mathbb{Z}/5 \end{aligned}$$

which is 1. In the first step we used the distributivity of tensor product over direct sum. In the second step we used the rule that

$$M \otimes R/(p) = M/pM.$$

So,

$$\mathbb{Z}/5 \otimes \mathbb{Z}/20 = \frac{\mathbb{Z}}{5\mathbb{Z} + 20\mathbb{Z}} = \frac{\mathbb{Z}}{5\mathbb{Z}}$$

and

$$\mathbb{Z}/5 \otimes \mathbb{Z}/8 = \frac{\mathbb{Z}}{5\mathbb{Z} + 8\mathbb{Z}} = \frac{\mathbb{Z}}{\mathbb{Z}} = 0$$

Similarly, the 2-rank of M is the dimension over $\mathbb{Z}/2$ of

$$\mathbb{Z}/2 \otimes M = \mathbb{Z}/2 \otimes (\mathbb{Z}/20 \oplus \mathbb{Z}/8) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

which is 2. For all other prime numbers p, the p-rank of M is zero.

With this example we decided that we could state without proof the general formula.

Proposition 5.5.

(1) *Suppose* $R = \mathbb{Z}$ *and*

$$M = \bigoplus_{i=1}^{k} \mathbb{Z}/n_i.$$

Then the p*-rank of* M *is the number of indices* i *so that* $p|n_i$.

(2) *More generally, suppose that* R *is a PID and*

$$M = \bigoplus_{i=1}^{k} R/(p_i^{n_i})$$

where $p_i \in R$ *are irreducible. Then the* p*-rank of* M *is the number of indices* i *so that* $p = p_i$.

We will use the following observation.

Corollary 5.6. *The* p*-rank of a cyclic module is either 0 or 1.*

5.3. ***p*-primary modules.** Now suppose that R is a PID and p is a fixed irreducible element. Suppose that M is f.g. p-primary. Then

$$M = \bigoplus_{i=1}^{k} R/(p^{n_i}).$$

The p-rank of M is the number of summands k. We want to find a formula for the numbers n_i. In order to do this, we asked: *What is the p-rank of $p^m M$?*

We took one summand $R/(p^n)$ and noted that the annihilator of this module is (p^n) and $p^m \in (p^n)$ if and only if $m \geq n$. Therefore, $p^m R/(p^n) = 0$ if and only if $m \geq n$. If $m < n$ then $p^m R/(p^n)$ is nonzero and cyclic. Being p-primary, this makes its p-rank equal to 1. So:

$$p\text{-rank}\,(p^m R/(p^n)) = \begin{cases} 1 & \text{if } m < n \\ 0 & \text{if } m \geq n \end{cases}$$

So, the p-rank of

$$p^m M = \bigoplus_{i=1}^{k} p^m R/(p^{n_i})$$

is equal to the number of indices i for which $n_i > m$. Now we have enough invariants to show that the formula given in the structure theorem for f.g. modules over a PID is unique.

Example 5.7. Suppose that $R = \mathbb{Z}$ and $M = \mathbb{Z}^5 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}/27$.

(1) First, take the rank: $\mathbb{Q} \otimes M = \mathbb{Q}^5$. So, $rM = 5$.

(2) The 2-rank of M is $5 + 1 = 6$ since

$$\mathbb{Z}/2 \otimes M = M/2M = (\mathbb{Z}/2)^5 \oplus \mathbb{Z}/(2,6) \oplus \mathbb{Z}/(2,27) = (\mathbb{Z}/2)^6.$$

(3) This implies that M has one cyclic 2-primary summand $\mathbb{Z}/2^n$. To find n we compute the 2-ranks of $2M, 4M$, etc. until we reach 5. But

$$2M = (2\mathbb{Z})^5 \oplus 2\mathbb{Z}/6\mathbb{Z} \oplus 2\mathbb{Z}/27 \cong \mathbb{Z}^5 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/27$$

which has 2-rank 5. So, we see that the 2-primary summand of M is $\mathbb{Z}/2$.

(4) The 3-rank of M is $5 + 2 = 7$ since

$$\mathbb{Z}/3 \otimes M = M/3 = (\mathbb{Z}/3)^5 \oplus \mathbb{Z}/(3,6) \oplus \mathbb{Z}/(3,27) = (\mathbb{Z}/3)^7.$$

(5) So, M has 2 cyclic 3-primary summands. We need to calculate the 3-ranks of $3M, 9M$, etc.

$$3M = (3\mathbb{Z})^5 \oplus 3\mathbb{Z}/6 \oplus 3\mathbb{Z}/27 \cong \mathbb{Z}^5 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/9.$$

$$9M \cong \mathbb{Z}^5 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3.$$

$$27M \cong \mathbb{Z}^5 \oplus \mathbb{Z}/2.$$

So, $M, 3M, 9M, 27M$ have 3-rank 7,6,6,5 respectively. We stop when we reach the rank of M which is 5. These numbers show that the 3-primary part of M is $\mathbb{Z}/3 \oplus \mathbb{Z}/3^3$.

(6) For all other primes p, the p-rank of M is 5. So, the decomposition of M is

$$M = \mathbb{Z}^5 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/3^3.$$

Example 5.8. Suppose that M is a finitely generated abelian group with $rM = 2$, 2-rank of $M, 2M, 4M, 8M, 16M$ equal to $5, 5, 4, 3, 2$ and 3-rank of $M, 3M, 9M$ equal to $4, 4, 2$ and p-rank of M equal to 2 for all other primes. Then

$$\begin{aligned} M &\cong \mathbb{Z}^2 \oplus (\mathbb{Z}/4)^2 \oplus \mathbb{Z}/8 \oplus \mathbb{Z}/16 \oplus (\mathbb{Z}/9)^2 \\ &\cong \mathbb{Z}^2 \oplus \mathbb{Z}/144 \oplus \mathbb{Z}/72 \oplus \mathbb{Z}/8 \oplus (\mathbb{Z}/4)^2. \end{aligned}$$

(In this order each denominator divides the previous one.)

Theorem 5.9. *In the decomposition of a finitely generated module over a PID:*

$$M \cong R^r \oplus \bigoplus R/(p_i^{n_i})$$

the numbers r and pairs (p_i, n_i) are uniquely determined up to reordering and can be determined from the rank of M and the p-rank of M, pM, p^2M, etc. for each irreducible p.