Modules over a PID

Joel Antonio-Vásquez
hello@joelantonio.me

October 21, 2017

Definition. A domain is a commutative ring $\mathcal{R} \neq 0$, with identity, such that for any $x, y \neq 0 \in \mathcal{R}$ implies $xy \neq 0$.

Definition. Let I be a subset of a ring $\mathcal{R}$. Then I is called an ideal if for all $y \in \mathcal{R}$ and every $x \in I$ implies that $xy \in I$ and $yx \in I$.

Definition. A principal ideal domain (PID) is a domain in which every ideal is principal (i.e. an ideal generated by a single element).

Theorem 1. Let M over a PID $\mathcal{R}$. There is a unique decresing sequence of proper ideals

$$d_1 \supseteq \cdots \supseteq d_n$$

such that M is isomorphic to the sum of cyclic modules

$$M \cong \bigoplus_i \mathcal{R}/(d_i).$$

The d_is are called invariant factors of M.

Proof: Let φ be a $\mathcal{R}$-linear map such that can be determined by $\varphi(e_1) = f_1, \ldots, \varphi(e_n) = f_n$ where $e_1, \ldots, e_n$ is the basis of n-dimensional $\mathcal{R}$. Then $\varphi(e_j) = \sum_{i=1}^n c_{ij} e_i$, such that (c_{ij}) is the matrix presentation of φ with respect to the basis. Then

$$\varphi(\mathcal{R}) = \mathcal{R}\varphi(e_1) \oplus \cdots \oplus \mathcal{R}\varphi(e_n) = \mathcal{R}f_1 \oplus \cdots \oplus \mathcal{R}f_n,$$

by aligned bases of $\mathcal{R}$ and its module $\varphi(\mathcal{R})$, we can say that

$$\mathcal{R} = \mathcal{R}v_1 \oplus \cdots \oplus \mathcal{R}v_n, \qquad \varphi(R) = \mathcal{R}a_1 v_1 \oplus \cdots \oplus \mathcal{R}a_n v_n,$$

where a_is are nonzero integers. Then

$$\mathcal{R}/\varphi(R) \cong \bigoplus_i \mathcal{R}/a_i\mathcal{R}.$$

Obvioulsy, $\mathcal{R}/\varphi(R)$ is our M and claim follows. $\square$

As an useful comment, we can calculate the invariant factors with the Smith Normal Form (SNF) (see problem 1).

1 Submodules

We need to remember that no every module has a basis, that's because we use free module here.

Definition. A free module is a module with a basis.

Lemma 1. Let $\mathcal{R}$ be a n-dimensional module over a PID, then every $\mathcal{R}$-submodule of $\mathcal{R}$ is an ideal.

Proof: Let $x \neq 0 \in \mathcal{R}$, then for $\mathcal{R}x$ since all ideals in $\mathcal{R}$ are principal, it's clearly that $\mathcal{R}x \cong \mathcal{R}$ as $\mathcal{R}$-modules. □

Lemma 2. Let $\mathcal{R}$ be a commutative ring and M be an R-module. Let f be an $\mathcal{R}$-linear and onto map such that $f : M \longrightarrow \mathcal{R}$, then there is an $\mathcal{R}$-module isomorphism $h : M \cong \mathcal{R}^n \oplus \operatorname{Ker} f$ where $h(m) = (f(m), *)$, making f the first component of h.

Proof: Let $\mathcal{R}^n = \mathcal{R}e_1 \oplus \cdots \oplus \mathcal{R}e_n$ where $e_1, \ldots, e_n$ is the basis of $\mathcal{R}$, let $m_i \in M$ such that $f(m_i) = e_i$ then there is a map $g : \mathcal{R}^n \longrightarrow M$ such that

$$g(c_1e_1 + \cdots + c_ne_n) = c_1m_1 + \cdots + c_nm_n,$$

Now, we define the function $h : M \longrightarrow \mathcal{R}^n \oplus \operatorname{Ker} f$ such that $h(m) = (f(m), m - g(f(m)))$. □

Theorem 2. Let $M \subset \mathcal{R}$ be a free $\mathcal{R}$-module of rank n where $\mathcal{R}$ is a PID, then for any S submodule of M is free of rank $\leq n$.

Proof: The free $\mathcal{R}$-module is $\mathcal{R}^n$ by lemma **??**. By induction on n, let $S \subset \mathcal{R}^{n+1}$ be a submodule. We gonna show that S is free of rak $\leq n+1$. The a projection of direct sum $\phi : \mathcal{R} \oplus \mathcal{R}^n \longrightarrow \mathcal{R}^n$ (i.e. $\mathcal{R}^{n+1} = \mathcal{R} \oplus \mathcal{R}^n$), then $N = \phi(S) \subset \mathcal{R}^n$ is free of rank $\leq n$. Now, by lemma **??**

$$S \cong N \oplus \operatorname{Ker} \phi|_S,$$

so $N \oplus \operatorname{Ker} \phi|_S$ is free of rank $\leq n+1$, so S does. □

2 Cardinality

Definition. Let $\mathcal{R}$ be a module and let $x \in \mathcal{R}$, which is called a torsion element if there exists a nonzero $r \in \mathcal{R}$ such that $rx = 0$. If $rx \neq 0$ for all $r \neq 0 \in R$, then the element x is called a torsion-free.

Definition. Let T be a module, we say that T is called a torsion-free module, if every element of T is a torsion-free module.

Definition. Let T be a finitely torsion module over the PID $\mathcal{R}$. By theorem **??**, we write $T \cong R/(d_1) \oplus \cdots \oplus R/(d_m)$, then the $\mathcal{R}$-cardinality of T to be the ideal

$$\operatorname{card}_{\mathcal{R}}(T) = (d_1d_2 \ldots d_m).$$

Theorem 3. Let T_1 and T_2 be two finitely generated torsion $\mathcal{R}$-modules, then

$$\text{card}_{\mathcal{R}}(T_1 \oplus T_2) = \text{card}_{\mathcal{R}}(T_1)\text{card}_{\mathcal{R}}(T_2).$$

Proof: We combine cyclic decompositions of T_1 and T_2 and then get $T_1 \oplus T_2$. $\square$

If we pick $x_1, \ldots, x_n$ the generating set for a torsion-free module T as an $\mathcal{R}$-module, then we have a linear map $f : \mathcal{R}^n \longrightarrow T$ where $f(e_i) = x_i$ for the basis $e_1, \ldots, e_n$ of $\mathcal{R}^n$ such there exists a linearly indepedent sequence $y_1, \ldots, y_n$ of T such that $y_j = \sum_{i=1}^n a_{ij} x_i$ with $a_{ij} \in \mathcal{R}$. By zorn's lemma, there is a linearly independent subset of T with maximal size $t_1, \ldots, t_d$ such that $\sum_{j=1}^d At_j \cong T^d$. Then we can get an isomorphism map

$$T \to aT \hookrightarrow \sum_{j=1}^{d} Tt_j \to A^d,$$

for a linearly dependent set $x, t_1, \ldots, t_d$ and a nontrivial linear realtion $ax + \sum_{i=1}^d a_i t_i = 0$ with $a \neq 0$. Now, we can say the following

Lemma 3. Let T be a finitely generated torsion-free module over a PID $\mathcal{R}$ such that $T \neq 0$, then there is an embedding $T \hookrightarrow \mathcal{R}^d$ for some $d \geq 1$ such that the image of T intersects each standard coordinate axis of $\mathcal{R}^d$.

Now, we use the above lemma to formulate the next theorem

Theorem 4. Let $\mathcal{R}$ be a PID, then every finitely generated torsion-free $\mathcal{R}$-module is a free $\mathcal{R}$-module.

Proof: By lemma **??**, there is a module that embeds a finite free $\mathcal{R}$-module, then it's finite free too by theorem **??**. $\square$

As last, we have the following theorem

Theorem 5. Let $\mathcal{R}$ be a PID, every finitely $\mathcal{R}$-module has the form $F \oplus T$ where F is a finite free $\mathcal{R}$-module and T is a finitely generated torsion $\mathcal{R}$-module. Moreover, $T \cong \bigoplus_j \mathcal{R}/(a_j)$ with a nonzero a_j.

Proof: Let T be a finitely generated $\mathcal{R}$-module, with generators $x_1, \ldots, x_n$. We define $f : \mathcal{R}^n \longrightarrow T$ by $f(e_i) = x_i$. We know that

$$\mathcal{R}^n/N \cong \left(\bigoplus_{j}^{m} \mathcal{R}/(a_j) \right) \oplus \mathcal{R}^{n-m},$$

for some $m \leq n$, a quotient $\mathcal{R}^n/N$ and nonzero a_js. The direct sum of the $A/(a_j)$'s is a torsion module and $\mathcal{R}^{n-m}$ is a finite free $\mathcal{R}$-module. $\square$

3 Problems

1. Describre, as a direct sum of cyclic groups, the cokernel $\varphi : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ given by left multiplication by the matrix

$$\begin{bmatrix} 30 & 9 & 18 \\ 15 & 6 & 6 \\ 18 & 3 & 27 \end{bmatrix}.$$

(Hint: use SNF)

2. Let M be a finitely generated $\mathcal{R}$-module with submodules $S \subset N$ such that M/N is a torsion module. Show that

$$[M : N]_{\mathcal{R}} = [M : S]_{\mathcal{R}}[S : N]_{\mathcal{R}}.$$

3. Let $\mathcal{R}$ be a PID. Show that a finitely generated $\mathcal{R}$-module M is a torsion module iff there is some $r \neq 0$ in $\mathcal{R}$ such that $r\mathcal{R} = 0$.

4. Does theorem **??** works for any kind of module? (Hint: First think with free modules and after try with non-free modules).

5. What does SNF give us? (Hint: see SNF)

4 Further Links

- Keith Conrad's notes on Modules over a PID: `http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/modulesoverPID.pdf`

- Prasad Senesi's notes on Modules over a Principal Ideal Domain: `http://math.ucr.edu/~prasad/PID%20mods.pdf`