STRUCTURE THEOREM OF FINITELY GENERATED MODULES OVER A PID

M. G. MAHMOUDI

Abstract. We present a proof of the structure theorem of finitely generated modules for a PID. The proof assumes the knowledge of exact sequences, free modules, projective modules, injective modules and basic facts about PID's.

Notation 1. For a left R-module M and $x \in M$, the (left) annihilator of x is defined by $\mathrm{Ann}(x) = \{r \in R : rx = 0\}$. This is a left ideal of R.

Lemma 2. *Let M be a left R-module. Then for every $x \in M$ we have an isomorphism of left R-modules $Rx \simeq R/\mathrm{Ann}(x)$.*

We use the following criterion for injectiveness:

Theorem 3. *A left R-module M is injective if and only if for every left ideal I of R and for every R-module homomorphism $f : I \to M$ there exists $q \in M$ such that $f(i) = iq$ for every $i \in I$.*

Notation 4. In a commutative ring R, the principal ideal generated by $a \in R$ is denoted by (a).

Definition 5. Let M be an module over an integral domain A. The torsion part $\mathrm{Tor}(M)$ of M is the submodule of M consisting of all elements $m \in M$ such that there exists a nonzero $a \in A$ such that $am = 0$.

Definition 6. A subset X of a left R-module M is called linearly independent (or just independent) if for every n and every distinct elements $x_1, \ldots, x_n \in X$, the relation $r_1x_1 + \cdots + r_nx_n = 0$ where $r_i \in R$ implies that $r_i = 0$ for each i.

Lemma 7. *Let A be an integral domain. Then for every nonzero $a \in A$, the principal ideal (a) is a free A-module of rank one.*

Lemma 8. *Let $M = Ra$ be a cyclic left R-module. Every submodule of I is of the form Ia for some left ideal I of R.*

Proof. Let $f : R \to Ra$ be the homomorphism of R-modules given by $f(r) = ra$. Since f is surjective, every submodule of Ra is of the form $f(I)$ for some left ideal I of R. □

Lemma 9. *Let A be a PID and let J be a nonzero ideal of A. Then A/J is an injective A/J-module.*

Proof. We may assume that $J = (a)$ for some nonzero $a \in A$. Let I/J be an ideal of A/J and let $f : I/J \to A/J$ be an A/J-module homomorphism. It suffices to check that there exists $q + J \in A/J$ such that $f(i + J) = (i + J)(q + J)$ for every $i \in I$. There exists $b \in A$ such that $I = (b)$. Since $J \subseteq I$ there exists $c \in A$ such that $a = bc$. Since $J \neq 0$, a is nonzero, thus $c \neq 0$. One can write $f(b+J) = (b' + J)$ for some $b' \in A$. We multiply both sides of $f(b + J) = (b' + J)$ by $c + J$ and use the fact that f is an A/J-module homomorphism. We obtain $0 + J = b'c + J$. Hence, $b'c \in J$, thus there exists $q \in A$ such that $b'c = aq$. Thus, $b'c = bcq$, which implies that $b' = bq$ (note that here we here use $c \neq 0$, this is the only place where $J \neq 0$ is used). We claim that for this c we have $f(i + J) = (i + J)(q + J)$ for every $i \in I$. One can write $i = rb$ for some $r \in A$. We have $f(i) = (r + J)f(b + J) = (r + J)(b' + J) = (r + J)(bq + J) = (rb + J)(q + J) = (i + J)(q + J)$. □

Date: December 24, 2020.

Theorem 10. *Let M be a free module of finite rank over a PID then every submodule N of M is free and* $\mathrm{rank}(N) \leq \mathrm{rank}(M)$*.*

Proof. Suppose that $\mathrm{rank}(M) = r < \infty$. Let $\{e_1, \ldots, e_r\}$ be a basis of M. If $r = 1$, then $M = Ae_1$. By Lemma 8, there exists an ideal I of A such that $N = Ie_1$. Since A is a PID, there exists $a \in I$ such that $I = (a)$. Hence, $N = Ie_1 = (a)e_1$. If $N = \{0\}$, N is a free submodule of N (with empty basis). If $N \neq \{0\}$ (hence $a \neq 0$), we claim that $\{ae_1\}$ is a basis of N. The element ae_1 generates N since $N = (a)e_1$. It suffices to check that $\{ae_1\}$ is an independent subset of N. If not, there exists a nonzero $r \in A$ such that $rae_1 = 0$. Since A is an integral domain, $ra \neq 0$. This is a contradiction since $\{e_1\}$ is an independent subset of M. Now assume that $r > 1$. For $i = 1, \ldots, r$, let $\pi_i : M \to A$ be the canonical projections

$$a_1e_1 + \cdots + a_re_r \mapsto a_i.$$

If for some i, $\pi_i(N) = 0$, then we have $N \subseteq \oplus_{j\neq i} Ae_j$. Since $\oplus_{j\neq i} Ae_j$ is a free A-module of rank $r - 1$, the conclusion follows from induction. Hence assume that $\pi_i(N)$ is a nonzero ideal of A for all i. Since A is a PID, there exists a nonzero $a_i \in A$ such that $\pi_i(N) = (a_i)$. Now consider that exact sequence

$$0 \to \ker(\pi_i|_N) \to N \xrightarrow{\pi_i|_N} \pi_i(N) \to 0,$$

where $\pi_i|_N$ denotes the restriction of π_i to N. By Lemma 7, $\pi_i(N) = (a_i)$ is a free A-module, hence a projective A-module. It follows that $N \simeq \pi_i(N) \oplus \ker(\pi_i|_N)$. Since $\ker(\pi_i|_N) \subseteq \ker(\pi_i) = \oplus_{j\neq i} Ae_j$ and $\oplus_{j\neq i} Ae_j$ is a free A-module of rank $r-1$, by induction $\ker(\pi_i|_N)$ is a free A-module of rank $\leq r - 1$. Since $\pi_i(N) = (a_i)$ is a free A-module of rank 1, the relation $N \simeq \pi_i(N) \oplus \ker(\pi_i|_N)$ implies that N is a free A-module of rank at most r. □

Theorem 11. *Let A be a PID. Then every finitely generated torsion-free module M over A is free.*

Proof. Let $X = \{e_1, \ldots, e_n\}$ be a generating set for M. Let $Y = \{f_1, \ldots, f_m\}$ be a maximal linearly independent subset of X. Hence, the submodule $N = Af_1 + \cdots + Af_m$ is a free A-module. By maximality of Y, for every i, the subset $Y \cup \{e_i\}$ is linearly dependent. Hence, there exists a nonzero $a_i \in A$ such that $a_ie_i \in N$. Let $a = \prod_{i=1}^n a_i \in A$ which is nonzero since A is an integral domain. The fact that $\{e_1, \ldots, e_n\}$ is a generating set for M and $a_ie_i \in N$ for each i, imply that $aM \subseteq N$. Since M is torsion-free, the A-module homomorphism $f : M \to N$ given by $f(x) = ax$ is injective. Hence $M \simeq \mathrm{image}(f)$. This means that M is isomorphic to a submodule of N. Since N is a free A-module, Theorem 10 implies that M is a free A-module as well. □

Corollary 12. *Let A be a PID and let M be left A-module which can be generated by n elements. Then every submodule N of M can be generated by at most n elements.*

Proof. Let $\{e_1, \ldots, e_n\}$ be a generating set for M. Let F be a free A-module generated by n elements $\{x_1, \ldots, x_n\}$ and let $\phi : F \to M$ be the surjection induced by $\phi(x_i) = e_i$. The submodule $\phi^{-1}(N)$ is a free module of rank at most n by Theorem 10. In particular $\phi^{-1}(N)$ can be generated by at most n elements. It follows that $N = \phi(\phi^{-1}(N))$ can be generated by at most n elements as well. □

Proposition 13. *Let M be a finitely generated module over a PID. Then*
(i) $M/\mathrm{Tor}(M)$ *is a free module of finite rank.*
(ii) $M \simeq \mathrm{Tor}(M) \oplus M/\mathrm{Tor}(M)$*, in particular both* $\mathrm{Tor}(M)$ *and* $M/\mathrm{Tor}(M)$ *are direct summands of M.*

Proof. Since $M/\mathrm{Tor}(M)$ is torsion-free and finitely generated, (i) follows from Theorem 11. For (ii) consider the exact sequence

$$0 \to \mathrm{Tor}(M) \to M \to M/\mathrm{Tor}(M) \to 0$$

By (i), $M/\mathrm{Tor}(M)$ is free, hence projective, thus (ii) follows. □

Theorem 14. *Let A be a PID. Let M be a finitely generated torsion module over A. Then M can be written as a direct sum of finitely many cyclic modules. In other words, there exist $x_1, \ldots, x_n$ in M such that $M = \oplus_{i=1}^n Ax_i$.*

Proof. For the case where $M = 0$, we may take $n = 1$ and $x_1 = 0$. Hence, we may assume that $M \neq 0$. Let $x_1, \ldots, x_n$ be e generating set for M. Since M is torsion, there exists nonzero $a_i \in A$ such that $a_i x_i = 0$ for every i. Let $p_1, \ldots, p_m$ be all primes appearing in the decomposition of $a_1 a_2 \cdots a_n$. For every prime $p \in A$, let M_p be the p-torsion part of M, i.e.,

$$M_p = \{x \in M : \exists n \geq 0, \ p^n x = 0\}.$$

We claim that $M = \oplus_{i=1}^m M_{p_i}$. Consider an element $x \in M$. Since M is torsion, there exist nonnegative integers $\alpha_1, \ldots, \alpha_m$ such that $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} x = 0$. By the Bézout theorem there exist $c_1, \ldots, c_m \in A$ such that $\sum c_i d_i = 1$ where

$$d_i = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}}{p_i^{\alpha_i}}.$$

It follows that $x = \sum c_i d_i x$. But $c_i d_i x \in M_{p_i}$ since $p_i^{\alpha_i} c_i d_i x = 0$. It follows that $M = \sum_{i=1}^m M_{p_i}$. To show that this sum is a direct sum, let $y_i \in M_{p_i}$ with

$$y_1 + \cdots + y_m = 0 \tag{1}$$

We may assume that $p_i^{\alpha_i} y_i = 0$ for some $\alpha_i \geq 0$. We have to show that $y_i = 0$ for every i. In fact, multiply the relation (1) by d_k as defined above. It follows that $d_k y_k = 0$. Now multiply the relation $\sum c_i d_i = 1$ by y_k, considering the fact that $d_i y_k = 0$ for $i \neq k$, we obtain $y_k = 0$. Hence, it suffices to prove the result for the case where $M = M_p$ for some prime p. Note that each M_{p_i} is a quotient module of M, hence finitely generated.

We thus may assume that M is a p-torsion module for some prime p in A, i.e., we may assume that for every $x \in M$, there exists $k \geq 0$ such that $p^k x = 0$. Since M is finitely generated, we may assume that there exists $k \geq 0$ such that $p^k x = 0$ for all $x \in M$. We may take this k minimum. We prove the result by induction on the number n of generators of M. If $n = 1$, then M is cyclic and the conclusion is immediate. Let $\{x_1, \ldots, x_n\}$ be a generating set for M. By the minimality of k, there exists i such that $p^{k-1} x_i \neq 0$. Without loss of generality, we may assume that $i = 1$, that is $p^{k-1} x_1 \neq 0$. We claim that $\mathrm{Ann}(x_1) = (p^k)$. Since $p^k x_1 = 0$ we have $(p^k) \subseteq \mathrm{Ann}(x_1)$. Conversely, let $a \in \mathrm{Ann}(x_1)$, i.e., $ax_1 = 0$. We also have $p^k x_1 = 0$. Let p^r (where $1 \leq r \leq k$) be the gcd of a and p^k. From the relations $ax_1 = 0$ and $p^k x_1 = 0$ we obtain $p^r x_1 = 0$. But r cannot be smaller than k, because $p^{k-1} x_1 \neq 0$. It follows that the gcd of a and p^k is p^k, thus p^k divides a. It follows that $a \in (p^k)$, hence $\mathrm{Ann}(x_1) \subseteq (p^k)$. Now put $J := (a) = \mathrm{Ann}(x_1)$. We have $JM = 0$, hence M is an A/J-module. Now consider the exact sequence $0 \to Ax_1 \to M \to M/Ax_1 \to 0$ of A/J-modules. Since $Ax_1 \simeq A/J$ and by Lemma 9, A/J is an injective A/J-module, we can write $M \simeq Ax_1 \oplus M/Ax_1$ as A/J-modules. Thus, $M \simeq Ax_1 \oplus M/Ax_1$ as A-modules. But M/Ax_1 can be generated by the cosets of $x_2, \ldots, x_n$ in M/Ax_1. Hence, by induction, M/Ax_1 is a direct sum of cyclic modules. It follows that M is a direct sum of cyclic modules. □

Theorem 15 (Structure theorem of finitely generated modules over a PID)**.** *Let A be a PID and let M be a finitely generated A-modules. Then there exist $m, n \geq 0$ and elements $x_1, \ldots, x_n \in M$ such that $M \simeq (\oplus_{i=1}^m A) \oplus Ax_1 \oplus \cdots \oplus Ax_n$.*

Proof. By Proposition 13, $M \simeq \mathrm{Tor}(M) \oplus M/\mathrm{Tor}(M)$. By Theorem 11, $M/\mathrm{Tor}(M)$ is free hence isomorphic to $\oplus_{i=1}^m A$ for some $m \geq 0$. By Theorem 14, $\mathrm{Tor}(M)$ is isomorphic to $Ax_1 \oplus \cdots \oplus Ax_n$ for some $x_1, \ldots, x_n \in M$ and the result is proved. □

M. G. Mahmoudi, mmahmoudi@sharif.ir, Department of Mathematical Sciences, Sharif University of Technology, P. O. Box 11155-9415, Tehran, Iran. Fax: (+98) (21) 6616-5117