Finitely Generated Modules over a PID, I

A will throughout be a fixed PID. We will develop the structure theory for finitely generated A-modules.

Lemma 1 *Any submodule of a free A-module is itself free.* □

Lemma 2 *A torsion-free, finitely generated A-module is isomorphic to a submodule of a free module, hence is free.* □

Lemma 3 *If M is a finitely generated A-module and $T \subset M$ is its torsion submodule, then $M/T = F$ is a finitely generated torsion-free, hence free, A-module and one has a direct sum decomposition $M \cong T \oplus F$. Moreover, T is a finitely generated A-module.* □

We now need to analyze a finitely generated, torsion A-module, T. If $x \in T$, let $\operatorname{ord}(x) = \{a \in A \mid ax = 0\}$. By definition of torsion module, $\operatorname{ord}(x)$ is a non-zero ideal of A, and in our case a principal ideal. Let $\operatorname{ann}(T) = \{a \in A \mid ax = 0, \text{ for all } x \in T\}$, also an ideal of A.

Lemma 4 *If torsion A-module T is generated by $\{x_1, x_2, \ldots, x_s\}$ and if* $\operatorname{ord}(x_i) = (a_i)$, *then* $\operatorname{ann}(T) = (d) = \operatorname{lcm}(a_i)$.

Proof Since $a_i \mid d$, clearly $dx_i = 0$, for all i, hence $d \in \operatorname{ann}(T)$. Conversely, if $e \in \operatorname{ann}(T)$ then $ex_i = 0$, hence $a_i \mid e$ and consequently $d \mid e$. ■

Lemma 5 *Suppose T is a torsion A-module, $x, y \in T$. Let* $\operatorname{ord}(x) = (p)$, $\operatorname{ord}(y) = (q)$, $\gcd(p, q) = 1$. *Then* $\operatorname{ord}(x + y) = pq$.

Proof Certainly $pq(x + y) = 0$. If $d(x + y) = 0$, then $dqx = 0$, since $dqy = 0$. So $p \mid qd$ which implies $p \mid d$. Similarly, $q \mid d$. ■

Lemma 6 *Suppose T is a torsion A-module, $x, y \in T$. Let* $\operatorname{ord}(x) = (a)$, $\operatorname{ord}(y) = (b)$, $\operatorname{lcm}(a, b) = (d)$. *If $\langle x, y\rangle$ denotes the submodule of T generated by x and y, then $\langle x, y\rangle = \langle x', y'\rangle$, where* $\operatorname{ord}(x') = (d)$.

Proof One can write $d = pq$, where $a = pr$, $b = qs$, and $\gcd(p, q) = \gcd(r, s) = 1$. Just take p and q to be suitable products of powers of primes chosen according to the factorizations of a and b in A. Then, by Lemma 5, $x' = rx + sy$ has $\operatorname{ord}(x') = (d)$, since $\operatorname{ord}(rx) = (p)$ and $\operatorname{ord}(sy) = (q)$. Now write $1 = Rr - Ss \in A$ and let $y' = Sx + Ry$. The matrix with rows (r, s) and (S, R) has determinant 1, so it is easy to solve for x and y as linear combinations of x' and y'. Thus $\langle x, y\rangle = \langle x', y'\rangle$. ■

Lemma 7 *If torsion A-module T is generated by $\{x_1, x_2, \ldots, x_m\}$ and if* $\operatorname{ann}(T) = (d)$ *as in Lemma 4, then $T = \langle y_1, y_2, \ldots, y_m\rangle$, where* $\operatorname{ord}(y_1) = (d)$.

Proof An easy iteration of Lemma 6. First replace $\langle x_1, x_2\rangle$ by $\langle x_1', x_2'\rangle$ as in Lemma 6. Then replace $\langle x_1', x_3\rangle$ by $\langle x_1'', x_3'\rangle$, so that now $\operatorname{ord}(x_1'') = \operatorname{lcm}(x_1, x_2, x_3)$. Continue. ■

Lemma 8 *Suppose T is a finitely generated torsion A module, $y \in T$, and* $\operatorname{ord}(y) = \operatorname{ann}(T) = (d)$. *Let $T^* = T/\langle y\rangle$, $x^* \in T^*$,* $\operatorname{ord}(x^*) = (e)$. *Then there exist elements $x \in T$ projecting to $x^* \in T^*$, with* $\operatorname{ord}(x) = \operatorname{ord}(x^*) = (e)$.

Proof First, $e \mid d$, since $dT = (0)$ implies $dT^* = (0)$. Choose some element $z \in T$ which projects to $x^* \in T^*$. Then $ez \in \langle y \rangle$, say $ez = fy$. Now, $0 = dz = (d/e)(ez) = (df/e)y$. Since $\operatorname{ord}(y) = (d)$, conclude $e \mid f$. Let $x = z - (f/e)y$. Then x projects to x^* and $ex = ez - fy = 0$, as desired. ∎

Lemma 9 *If T is a finitely generated nonzero torsion A-module then $T \cong A/(d_1) \oplus A/(d_2) \oplus \cdots \oplus A/(d_m)$, where the d_i are neither 0 nor units in A and $d_1 \mid d_2 \mid \cdots \mid d_{m-1} \mid d_m$. Note that necessarily $(d_m) = \operatorname{ann}(T)$ here.*

Proof Induction based on Lemma 8. Say $T = \langle y_1, \ldots, y_m \rangle$, with m as small as possible and with $\operatorname{ord}(y_m) = (d) = \operatorname{ann}(T)$. If $m = 1$, there is nothing to prove, T is cyclic. Otherwise, let $T^* = T/\langle y_m \rangle$. Now, T^* can be generated by $m - 1$ elements (but no fewer than $m - 1$). By induction, we can assume Lemma 9 holds for T^*. Applying Lemma 8 to each cyclic generator in a direct sum decomposition for T^* gives a splitting of the exact sequence $(0) \to \langle y_m \rangle \to T \to T^* \to (0)$, which establishes Lemma 9 for T. ∎

Theorem 1 *If M is a finitely generated A module then*

$$M \cong F \oplus T \cong A^n \oplus A/(d_1) \oplus A/(d_2) \oplus \cdots \oplus A/(d_m)$$

where the d_i are neither 0 nor units in A and $d_1 \mid d_2 \mid \cdots \mid d_{m-1} \mid d_m$. Moreover, the rank n and the ideals (d_i) with the indicated divisibility properties are uniquely determined by M. The least number of generators of T is m and the least number of generators of M is $m + n$.

(The interpretation of $n = 0$ is that $M = T$ is a torsion module, and the interpretation of $m = 0$, that is no d_is, is that $M = F$ is a free module.)

Proof The existence statement just collects the conclusions of Lemmas 3 and 9. The rank, n, of F is invariant since $F \cong M/T$, which is independent of decomposition. Suppose p is a prime which divides d_1. Then M/pM is a vector space over the field $A/(p)$ of dimension $n + m$. This proves $n + m$ is independent of the decomposition and also proves M cannot be generated by fewer than $n + m$ elements. Similarly, T/pT has dimension m as vector space over $A/(p)$, so T cannot be generated by fewer than m elements.

The uniqueness of the ideals (d_i) can be proved in different ways. Here is a nice characterization of (d_i). For $e \in A$, the module eT can be generated by $m - i$ elements if and only if d_i divides e. Thus, d_i is the gcd of all such elements e. The idea is, multiply all the summands of one decomposition by e. You get something isomorphic to another sum of cyclic modules

$$A/(e_1) \oplus A/(e_2) \oplus \cdots \oplus A/(e_m)$$

with $e_i \mid e_{i+1}$. Precisely, $e_i = d_i/\gcd(e, d_i)$. The number of non-zero summands here is therefore the least number of generators of eT. But a term disappears if and only if d_i divides e. Another proof of uniqueness of the (d_i) can be based on Theorem 2 below, which presents an alternate version of the structure theorem.∎

Finitely Generated Modules over a PID, II

An alternate approach to the structure of a torsion module over a PID A uses first a decomposition into p-primary summands, for primes $p \in A$, and then an analysis of a p-primary module. In general, if $a \in A$ is a nonzero element and T is a torsion A-module, set $T_a = \{x \in T \mid a^n x = 0, \text{ for some } n \geq 0\}$. T is p-primary for a prime p if $T = T_p$. Note $T_p = T_q$ if $q = p^s$.

Lemma 10 *If* $\gcd(a,b) = 1$, *then* $T_a \cap T_b = (0)$.

Proof If $x \in T_a \cap T_b$ and $a^n x = b^m x = 0$, write $1 = ua^n + vb^m \in A$. Then $x = 1x = (ua^n + vb^m)x = 0$. ■

Lemma 11 *If* $\gcd(a,b) = 1$, *then* $T_{ab} \cong T_a \oplus T_b$. *If* $a, b, c, \ldots, k$ *are finitely many pairwise relatively prime elements of A, for example, powers of distinct primes, then* $T_{ab\cdots k} = T_a \oplus \cdots \oplus T_k$.

Proof After Lemma 10, we only need to show $T_{ab} = T_a + T_b$. If $(ab)^n x = 0$, then $a^n x \in T_b$ and $b^n x \in T_a$. Write $1 = vb^n + ua^n \in A$. Then $x = 1x = (vb^n)x + (ua^n)x \in T_a + T_b$. The second statement is a simple induction, starting with two elements, a and $(bc\cdots k)$. ■

Remark 1 Lemma 11 can be viewed as a generalization of the Chinese Remainder Theorem in the case of PIDs. Namely, if $T = A/(ab)$, with $\gcd(a,b) = 1$, then it is easy to see $T_a \cong A/(a)$ and $T_b \cong A/(b)$. For example, the map "multiply by b," $A/(a) \to A/(ab) = T$, is injective and has image equal to T_a. □

Lemma 12 *For all torsion modules,* $T \cong \oplus_{p\ prime} T_p$.

Proof Any $x \in T$ belongs to T_d for some d, since T is a torsion module. Factor d into a product of distinct prime powers. Lemma 11 shows T_d is the direct sum of the T_p over the primes p which divide d. This shows every element of T is a finite sum of elements of the p-primary modules T_p. Uniqueness of such an expression is an easy consequence of Lemma 10. ■

Theorem 2 *If* T_p *is a finitely generated nonzero p-primary torsion module, then*

$$T_p \cong A/(p^{e_1}) \oplus A/(p^{e_2}) \oplus \cdots \oplus A/(p^{e_m}),$$

where $0 < e_1 \leq e_2 \leq \cdots \leq e_m$. *The exponents* e_j *are uniquely determined by* T_p. *The integer m is the least number of generators of* T_p.

Proof Follow the proof of Lemma 9 for the existence of such a decomposition. Given such a decomposition, obviously m is the dimension of T/pT as vector space over $A/(p)$, where we have abbreviated T_p by T. Furthermore, the dimension of pT/p^2T over $A/(p)$ is the number of e_j which are greater than 1. In general, the dimension of $p^iT/p^{i+1}T$ is the number of e_j which are greater than i. These dimensions are invariant, and determine the e_j, hence the e_j are uniquely determined by T_p. ■

Remark 2 The reason for claiming that this is somehow an alternate proof of the structure theorem is that Lemmas 4, 5, 6, and 7 are irrelevant or trivial for a p-primary module, since orders of elements of T_p are always powers of p. Those Lemmas are replaced by Lemmas 10, 11, and 12 here. Then one repeats Lemma 8, and its inductive consequence Lemma 9 for T_p. Also, the uniqueness part is more elementary here. □

Theorem 1 presents one normal form for a finitely generated torsion A-module T. The ideals $(d_j) \subset A$ of Theorem 1 that successively divide each other are called the **invariant factors** of T. Lemma 12 and Theorem II present a second normal form for T. The powers (p^{e_j}) which occur in the formula for T_p in Theorem 2, including the number of times each occurs, as p varies over prime divisors of $\text{ann}(T) = (d)$, are called **elementary divisors** of T.

It is quite easy to go back and forth between the invariant factor form and the elementary divisor form. Thus, one really wouldn't need to give both proofs. However, the various Lemmas in the separate proofs have some independent interest. Here is how the translation goes. Use the Chinese Remainder Theorem to convert an invariant factor formula for T, as in Theorem 1, to elementary divisor form. That is, if $d_i = \prod_j p_{ij}^{f_{ij}}$ is the factorization of d_i into distinct prime powers, then $A/(d_i) \cong \oplus_j A/(p_{ij}^{f_{ij}})$. Conversely, given the elementary divisor form of Theorem 2 for each T_p, p prime, reconstruct the invariant factors d_i as follows. The last $(d_m) = \text{ord}(T)$ must be the product of all the highest prime powers seen in the elementary divisor formulas for all the T_p. Then remove one cyclic summand of T corresponding to each of these highest prime powers, and look at the remaining summands. Apply the same recipe to these summands to construct d_{m-1}. Namely, d_{m-1} must be the product of the highest remaining prime powers. Continue this algorithm to find all the d_i. Examining these two translations, recovering each normal form from the other, reveals that a uniqueness result for either normal form implies uniqueness for the other normal form. Thus, uniqueness of the invariant factors follows from the rather clean proof of uniqueness of the elementary divisors.