sum of the cyclic factors whose elementary divisors are powers of p) is isomorphic to the p-primary submodule of M_2, since these are the submodules of elements which are annihilated by some power of p. We are therefore reduced to the case of proving that if two modules M_1 and M_2 which have annihilator a power of p are isomorphic then they have the same elementary divisors.

We proceed by induction on the power of p in the annihilator of M_1 (which is the same as the annihilator of M_2 since M_1 and M_2 are isomorphic). If this power is 0, then both M_1 and M_2 are 0 and we are done. Otherwise M_1 (and M_2) have nontrivial elementary divisors. Suppose the elementary divisors of M_1 are given by

$$\text{elementary divisors of } M_1\text{:}\ \underbrace{p, p, \dots, p}_{m \text{ times}},\ p^{\alpha_1}, p^{\alpha_2}, \dots, p^{\alpha_s},$$

where $2 \le \alpha_1 \le \alpha_2 \le \cdots \le \alpha_s$, i.e., M_1 is the direct sum of cyclic modules with generators $x_1, x_2, \dots, x_m, x_{m+1}, \dots, x_{m+s}$, say, whose annihilators are $(p), (p), \dots, (p)$, $(p^{\alpha_1}), \dots, (p^{\alpha_s})$, respectively. Then the submodule pM_1 has elementary divisors

$$\text{elementary divisors of } pM_1\text{:}\ p^{\alpha_1-1}, p^{\alpha_2-1}, \dots, p^{\alpha_s-1}$$

since pM_1 is the direct sum of the cyclic modules with generators $px_1, px_2, \dots, px_m$, $px_{m+1}, \dots, px_{m+s}$ whose annihilators are $(1), (1), \dots, (1), (p^{\alpha_1-1}), \dots, (p^{\alpha_s-1})$, respectively. Similarly, if the elementary divisors of M_2 are given by

$$\text{elementary divisors of } M_2\text{:}\ \underbrace{p, p, \dots, p}_{n \text{ times}},\ p^{\beta_1}, p^{\beta_2}, \dots, p^{\beta_t},$$

where $2 \le \beta_1 \le \beta_2 \le \cdots \le \beta_t$, then pM_2 has elementary divisors

$$\text{elementary divisors of } pM_2\text{:}\ p^{\beta_1-1}, p^{\beta_2-1}, \dots, p^{\beta_t-1}.$$

Since $M_1 \cong M_2$, also $pM_1 \cong pM_2$ and the power of p in the annihilator of pM_1 is one less than the power of p in the annihilator of M_1. By induction, the elementary divisors for pM_1 are the same as the elementary divisors for pM_2, i.e., $s = t$ and $\alpha_i - 1 = \beta_i - 1$ for $i = 1, 2, \dots, s$, hence $\alpha_i = \beta_i$ for $i = 1, 2, \dots, s$. Finally, since also $M_1/pM_1 \cong M_2/pM_2$ we see from (3) of the lemma above that $F^{m+s} \cong F^{n+t}$, which shows that $m + s = n + t$ hence $m = n$ since we have already seen $s = t$. This proves that the set of elementary divisors for M_1 is the same as the set of elementary divisors for M_2.

We now show that M_1 and M_2 must have the same invariant factors. Suppose $a_1 \mid a_2 \mid \cdots \mid a_m$ are invariant factors for M_1. We obtain a set of elementary divisors for M_1 by taking the prime power factors of these elements. Note that then the divisibility relations on the invariant factors imply that a_m is the product of the largest of the prime powers among these elementary divisors, a_{m-1} is the product of the largest prime powers among these elementary divisors once the factors for a_m have been removed, and so on. If $b_1 \mid b_2 \mid \cdots \mid b_n$ are invariant factors for M_2 then we similarly obtain a set of elementary divisors for M_2 by taking the prime power factors of these elements. But we showed above that the elementary divisors for M_1 and M_2 are the same, and it follows that the same is true of the invariant factors.

Corollary 10. Let R be a P.I.D. and let M be a finitely generated R-module.

(1) The elementary divisors of M are the prime power factors of the invariant factors of M.

(2) The largest invariant factor of M is the product of the largest of the distinct prime powers among the elementary divisors of M, the next largest invariant factor is the product of the largest of the distinct prime powers among the remaining elementary divisors of M, and so on.

Proof: The procedure in (1) gives *a* set of elementary divisors and since the elementary divisors for M are unique by the theorem, it follows that the procedure in (1) gives *the* set of elementary divisors. Similarly for (2).

Corollary 11. *(The Fundamental Theorem of Finitely Generated Abelian Groups)* See Theorem 5.3 and Theorem 5.5.

Proof: Take $R = \mathbb{Z}$ in Theorems 5, 6 and 9 (note however that the invariant factors are listed in reverse order in Chapter 5 for computational convenience).

The procedure for passing between elementary divisors and invariant factors in Corollary 10 is described in some detail in Chapter 5 in the case of finitely generated abelian groups.

Note also that if a finitely generated module M is written as a direct sum of cyclic modules of the form $R/(a)$ then the ideals (a) which occur are not in general unique unless some additional conditions are imposed (such as the divisibility condition for the invariant factors or the condition that a be the power of a prime in the case of the elementary divisors). To decide whether two modules are isomorphic it is necessary to first write them in such a standard (or *canonical*) form.

EXERCISES

1. Let M be a module over the integral domain R.
   (a) Suppose x is a nonzero torsion element in M. Show that x and 0 are "linearly dependent." Conclude that the rank of Tor(M) is 0, so that in particular any torsion R-module has rank 0.
   (b) Show that the rank of M is the same as the rank of the (torsion free) quotient $M/\text{Tor}M$.
2. Let M be a module over the integral domain R.
   (a) Suppose that M has rank n and that $x_1, x_2, \ldots, x_n$ is any maximal set of linearly independent elements of M. Let $N = Rx_1 + \ldots + Rx_n$ be the submodule generated by $x_1, x_2, \ldots, x_n$. Prove that N is isomorphic to R^n and that the quotient M/N is a torsion R-module (equivalently, the elements $x_1, \ldots, x_n$ are linearly independent and for any $y \in M$ there is a nonzero element $r \in R$ such that ry can be written as a linear combination $r_1x_1 + \ldots + r_nx_n$ of the x_i).
   (b) Prove conversely that if M contains a submodule N that is free of rank n (i.e., $N \cong R^n$) such that the quotient M/N is a torsion R-module then M has rank n. [Let $y_1, y_2, \ldots, y_{n+1}$ be any $n+1$ elements of M. Use the fact that M/N is torsion to write r_iy_i as a linear combination of a basis for N for some nonzero elements $r_1, \ldots, r_{n+1}$ of R. Use an argument as in the proof of Proposition 3 to see that the r_iy_i, and hence also the y_i, are linearly dependent.]

3. Let R be an integral domain and let A and B be R-modules of ranks m and n, respectively. Prove that the rank of $A \oplus B$ is $m+n$. [Use the previous exercise.]

4. Let R be an integral domain, let M be an R-module and let N be a submodule of M. Suppose M has rank n, N has rank r and the quotient M/N has rank s. Prove that $n = r + s$. [Let $x_1, x_2, \dots, x_s$ be elements of M whose images in M/N are a maximal set of independent elements and let $x_{s+1}, x_{s+2}, \dots, x_{s+r}$ be a maximal set of independent elements in N. Prove that $x_1, x_2, \dots, x_{s+r}$ are linearly independent in M and that for any element $y \in M$ there is a nonzero element $r \in R$ such that ry is a linear combination of these elements. Then use Exercise 2.]

5. Let $R = \mathbb{Z}[x]$ and let $M = (2, x)$ be the ideal generated by 2 and x, considered as a submodule of R. Show that $\{2, x\}$ is not a basis of M. [Find a nontrivial R-linear dependence between these two elements.] Show that the rank of M is 1 but that M is not free of rank 1 (cf. Exercise 2).

6. Show that if R is an integral domain and M is any nonprincipal ideal of R then M is torsion free of rank 1 but is not a free R-module.

7. Let R be any ring, let $A_1, A_2, \dots, A_m$ be R-modules and let B_i be a submodule of A_i, $1 \le i \le m$. Prove that
$$(A_1 \oplus A_2 \oplus \cdots \oplus A_m)/(B_1 \oplus B_2 \oplus \cdots \oplus B_m) \cong (A_1/B_1) \oplus (A_2/B_2) \oplus \cdots \oplus (A_m/B_m).$$

8. Let R be a P.I.D., let B be a torsion R-module and let p be a prime in R. Prove that if $pb = 0$ for some nonzero $b \in B$, then $\mathrm{Ann}(B) \subseteq (p)$.

9. Give an example of an integral domain R and a nonzero torsion R-module M such that $\mathrm{Ann}(M) = 0$. Prove that if N is a finitely generated torsion R-module then $\mathrm{Ann}(N) \neq 0$.

10. For p a prime in the P.I.D. R and N an R-module prove that the p-primary component of N is a submodule of N and prove that N is the direct sum of its p-primary components (there need not be finitely many of them).

11. Let R be a P.I.D., let a be a nonzero element of R and let $M = R/(a)$. For any prime p of R prove that
$$p^{k-1}M/p^kM \cong \begin{cases} R/(p) & \text{if } k \le n \\ 0 & \text{if } k > n, \end{cases}$$
where n is the power of p dividing a in R.

12. Let R be a P.I.D. and let p be a prime in R.
    (a) Let M be a finitely generated torsion R-module. Use the previous exercise to prove that $p^{k-1}M/p^kM \cong F^{n_k}$ where F is the field $R/(p)$ and n_k is the number of elementary divisors of M which are powers p^α with $\alpha \ge k$.
    (b) Suppose M_1 and M_2 are isomorphic finitely generated torsion R-modules. Use (a) to prove that, for every $k \ge 0$, M_1 and M_2 have the same number of elementary divisors p^α with $\alpha \ge k$. Prove that this implies M_1 and M_2 have the same set of elementary divisors.

13. If M is a finitely generated module over the P.I.D. R, describe the structure of $M/\mathrm{Tor}(M)$.

14. Let R be a P.I.D. and let M be a torsion R-module. Prove that M is irreducible (cf. Exercises 9 to 11 of Section 10.3) if and only if $M = Rm$ for any nonzero element $m \in M$ where the annihilator of m is a nonzero prime ideal (p).

15. Prove that if R is a Noetherian ring then R^n is a Noetherian R-module. [Fix a basis of R^n. If M is a submodule of R^n show that the collection of first coordinates of elements of M is a submodule of R hence is finitely generated. Let $m_1, m_2, \dots, m_k$ be elements of M