to be the trivial homomorphism shows that $(0) \in \Sigma$. By Corollary 2, Σ has at least one maximal element i.e., there is at least one homomorphism ν of M to R so that the principal ideal $\nu(N) = (a_\nu)$ is not properly contained in any other element of Σ. Let $a_1 = a_\nu$ for this maximal element and let $y \in N$ be an element mapping to the generator a_1 under the homomorphism ν: $\nu(y) = a_1$.

We now show the element a_1 is nonzero. Let $x_1, x_2, \ldots, x_n$ be any basis of the free module M and let $\pi_i \in \operatorname{Hom}_R(M, R)$ be the natural projection homomorphism onto the i^{th} coordinate with respect to this basis. Since $N \neq \{0\}$, there exists an i such that $\pi_i(N) \neq 0$, which in particular shows that Σ contains more than just the trivial ideal (0). Since (a_1) is a maximal element of Σ it follows that $a_1 \neq 0$.

We next show that this element a_1 divides $\varphi(y)$ for every $\varphi \in \operatorname{Hom}_R(M, R)$. To see this let d be a generator for the principal ideal generated by a_1 and $\varphi(y)$. Then d is a divisor of both a_1 and $\varphi(y)$ in R and $d = r_1a_1 + r_2\varphi(y)$ for some $r_1, r_2 \in R$. Consider the homomorphism $\psi = r_1\nu + r_2\varphi$ from M to R. Then $\psi(y) = (r_1\nu + r_2\varphi)(y) = r_1a_1 + r_2\varphi(y) = d$ so that $d \in \psi(N)$, hence also $(d) \subseteq \psi(N)$. But d is a divisor of a_1 so we also have $(a_1) \subseteq (d)$. Then $(a_1) \subseteq (d) \subseteq \psi(N)$ and by the maximality of (a_1) we must have equality: $(a_1) = (d) = \psi(N)$. In particular $(a_1) = (d)$ shows that $a_1 \mid \varphi(y)$ since d divides $\varphi(y)$.

If we apply this to the projection homomorphisms π_i we see that a_1 divides $\pi_i(y)$ for all i. Write $\pi_i(y) = a_1b_i$ for some $b_i \in R$, $1 \leq i \leq n$ and define

$$y_1 = \sum_{i=1}^{n} b_ix_i.$$

Note that $a_1y_1 = y$. Since $a_1 = \nu(y) = \nu(a_1y_1) = a_1\nu(y_1)$ and a_1 is a nonzero element of the integral domain R this shows

$$\nu(y_1) = 1.$$

We now verify that this element y_1 can be taken as one element in a basis for M and that a_1y_1 can be taken as one element in a basis for N, namely that we have

(a) $M = Ry_1 \oplus \ker\nu$, and

(b) $N = Ra_1y_1 \oplus (N \cap \ker\nu)$.

To see (a) let x be an arbitrary element in M and write $x = \nu(x)y_1 + (x - \nu(x)y_1)$. Since

$$\begin{aligned}\nu(x - \nu(x)y_1) &= \nu(x) - \nu(x)\nu(y_1)\\ &= \nu(x) - \nu(x)\cdot 1\\ &= 0\end{aligned}$$

we see that $x - \nu(x)y_1$ is an element in the kernel of ν. This shows that x can be written as the sum of an element in Ry_1 and an element in the kernel of ν, so $M = Ry_1 + \ker\nu$. To see that the sum is direct, suppose ry_1 is also an element in the kernel of ν. Then $0 = \nu(ry_1) = r\nu(y_1) = r$ shows that this element is indeed 0.

For (b) observe that $\nu(x')$ is divisible by a_1 for every $x' \in N$ by the definition of a_1 as a generator for $\nu(N)$. If we write $\nu(x') = ba_1$ where $b \in R$ then the decomposition we used in (a) above is $x' = \nu(x')y_1 + (x' - \nu(x')y_1) = ba_1y_1 + (x' - ba_1y_1)$ where the second summand is in the kernel of ν and is an element of N. This shows that

$N = Ra_1y_1 + (N \cap \ker \nu)$. The fact that the sum in (b) is direct is a special case of the directness of the sum in (a).

We now prove part (1) of the theorem by induction on the rank, m, of N. If $m = 0$, then N is a torsion module, hence $N = 0$ since a free module is torsion free, so (1) holds trivially. Assume then that $m > 0$. Since the sum in (b) above is direct we see easily that $N \cap \ker \nu$ has rank $m - 1$ (cf. Exercise 3). By induction $N \cap \ker \nu$ is then a free R-module of rank $m - 1$. Again by the directness of the sum in (b) we see that adjoining a_1y_1 to any basis of $N \cap \ker \nu$ gives a basis of N, so N is also free (of rank m), which proves (1).

Finally, we prove (2) by induction on n, the rank of M. Applying (1) to the submodule $\ker \nu$ shows that this submodule is free and because the sum in (a) is direct it is free of rank $n - 1$. By the induction assumption applied to the module $\ker \nu$ (which plays the role of M) and its submodule $\ker \nu \cap N$ (which plays the role of N), we see that there is a basis $y_2, y_3, \ldots, y_n$ of $\ker \nu$ such that $a_2y_2, a_3y_3, \ldots, a_my_m$ is a basis of $N \cap \ker \nu$ for some elements $a_2, a_3, \ldots, a_m$ of R with $a_2 \mid a_3 \mid \cdots \mid a_m$. Since the sums (a) and (b) are direct, $y_1, y_2, \ldots, y_n$ is a basis of M and $a_1y_1, a_2y_2, \ldots, a_my_m$ is a basis of N. To complete the induction it remains to show that a_1 divides a_2. Define a homomorphism φ from M to R by defining $\varphi(y_1) = \varphi(y_2) = 1$ and $\varphi(y_i) = 0$, for all $i > 2$, on the basis for M. Then for this homomorphism φ we have $a_1 = \varphi(a_1y_1)$ so $a_1 \in \varphi(N)$ hence also $(a_1) \subseteq \varphi(N)$. By the maximality of (a_1) in Σ it follows that $(a_1) = \varphi(N)$. Since $a_2 = \varphi(a_2y_2) \in \varphi(N)$ we then have $a_2 \in (a_1)$ i.e., $a_1 \bigm| a_2$. This completes the proof of the theorem.

Recall that the left R-module C is a *cyclic* R-module (for any ring R, not necessarily commutative nor with 1) if there is an element $x \in C$ such that $C = Rx$. We can then define an R-module homomorphism

$$\pi : R \to C$$

by $\pi(r) = rx$, which will be surjective by the assumption $C = Rx$. The First Isomorphism Theorem gives an isomorphism of (left) R-modules

$$R/\ker \pi \cong C.$$

If R is a P.I.D., $\ker \pi$ is a principal ideal, (a), so we see that the cyclic R-modules C are of the form $R/(a)$ where $(a) = \mathrm{Ann}(C)$.

The cyclic modules are the simplest modules (since they require only one generator). The existence portion of the Fundamental Theorem states that any finitely generated module over a P.I.D. is isomorphic to the direct sum of finitely many cyclic modules.

Theorem 5. *(Fundamental Theorem, Existence: Invariant Factor Form)* Let R be a P.I.D. and let M be a finitely generated R-module.

(1) Then M is isomorphic to the direct sum of finitely many cyclic modules. More precisely,

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

for some integer $r \geq 0$ and nonzero elements $a_1, a_2, \ldots, a_m$ of R which are not units in R and which satisfy the divisibility relations

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

(2) M is torsion free if and only if M is free.
(3) In the decomposition in (1),

$$\mathrm{Tor}(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m).$$

In particular M is a torsion module if and only if $r = 0$ and in this case the annihilator of M is the ideal (a_m).

Proof: The module M can be generated by a finite set of elements by assumption so let $x_1, x_2, \ldots, x_n$ be a set of generators of M of minimal cardinality. Let R^n be the free R-module of rank n with basis $b_1, b_2, \ldots, b_n$ and define the homomorphism $\pi : R^n \to M$ by defining $\pi(b_i) = x_i$ for all i, which is automatically surjective since $x_1, \ldots, x_n$ generate M. By the First Isomorphism Theorem for modules we have $R^n/\ker\pi \cong M$. Now, by Theorem 4 applied to R^n and the submodule $\ker\pi$ we can choose another basis $y_1, y_2, \ldots, y_n$ of R^n so that $a_1y_1, a_2y_2, \ldots, a_my_m$ is a basis of $\ker\pi$ for some elements $a_1, a_2, \ldots, a_m$ of R with $a_1 \mid a_2 \mid \cdots \mid a_m$. This implies

$$M \cong R^n/\ker\pi = (Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m).$$

To identify the quotient on the right hand side we use the natural surjective R-module homomorphism

$$Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n \to R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$$

that maps $(\alpha_1y_1, \ldots, \alpha_ny_n)$ to $(\alpha_1 \bmod (a_1), \ldots, \alpha_m \bmod (a_m), \alpha_{m+1}, \ldots, \alpha_n)$. The kernel of this map is clearly the set of elements where a_i divides α_i, $i = 1, 2, \ldots, m$, i.e., $Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m$ (cf. Exercise 7). Hence we obtain

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

If a is a unit in R then $R/(a) = 0$, so in this direct sum we may remove any of the initial a_i which are units. This gives the decomposition in (1) (with $r = n - m$).

Since $R/(a)$ is a torsion R-module for any nonzero element a of R, (1) immediately implies M is a torsion free module if and only if $M \cong R^r$, which is (2). Part (3) is immediate from the definitions since the annihilator of $R/(a)$ is evidently the ideal (a).

We shall shortly prove the uniqueness of the decomposition in Theorem 5, namely that if we have

$$M \cong R^{r'} \oplus R/(b_1) \oplus R/(b_2) \oplus \cdots \oplus R/(b_{m'})$$

for some integer $r' \geq 0$ and nonzero elements $b_1, b_2, \ldots, b_{m'}$ of R which are not units with

$$b_1 \mid b_2 \mid \cdots \mid b_{m'},$$

then $r = r'$, $m = m'$ and $(a_i) = (b_i)$ (so $a_i = b_i$ up to units) for all i. It is precisely the divisibility condition $a_1 \mid a_2 \mid \cdots \mid a_m$ which gives this uniqueness.