is a basis of M, since the sums are direct, and $e' = a_1e_1 = a_he$. It remains to show that a_1 divides a_2. Consider the linear map $g\colon F \to A$ such that $g(e_1) = g(e_2) = 1$, and $g(e_i) = 0$, for all i, with $3 \leq i \leq n$. We have $a_h = a_1 = g(a_1e_1) = g(e') \in g(M)$, and thus $a_hA \subseteq g(M)$. Since a_hA is maximal, we must have $g(M) = a_hA = a_1A$. Since $a_2 = g(a_2e_2) \in g(M)$, we have $a_2 \in a_1A$, which shows that a_1 divides a_2. $\square$

We need the following basic proposition.

Proposition 35.24. *For any commutative ring A, if F is a free A-module and if $(e_1, \ldots, e_n)$ is a basis of F, for any elements $a_1, \ldots, a_n \in A$, there is an isomorphism*

$$F/(Aa_1e_1 \oplus \cdots \oplus Aa_ne_n) \approx (A/a_1A) \oplus \cdots \oplus (A/a_nA).$$

Proof. Let $\sigma\colon F \to A/(a_1A) \oplus \cdots \oplus A/(a_nA)$ be the linear map given by

$$\sigma(x_1e_1 + \cdots + x_ne_n) = (\overline{x}_1, \ldots, \overline{x}_n),$$

where $\overline{x}_i$ is the equivalence class of x_i in A/a_iA. The map σ is clearly surjective, and its kernel consists of all vectors $x_1e_1 + \cdots + x_ne_n$ such that $x_i \in a_iA$, for $i = 1, \ldots, n$, which means that

$$\mathrm{Ker}\,(\sigma) = Aa_1e_1 \oplus \cdots \oplus Aa_ne_n.$$

Since $M/\mathrm{Ker}\,(\sigma)$ is isomorphic to $\mathrm{Im}(\sigma)$, we get the desired isomorphism. $\square$

We can now prove the existence part of the structure theorem for finitely generated modules over a PID.

Theorem 35.25. *Let M be a finitely generated nontrivial A-module, where A a PID. Then, M is isomorphic to a direct sum of cyclic modules*

$$M \approx A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_m,$$

where the $\mathfrak{a}_i$ are proper ideals of A (possibly zero) such that

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_m \neq A.$$

More precisely, if $\mathfrak{a}_1 = \cdots = \mathfrak{a}_r = (0)$ and $(0) \neq \mathfrak{a}_{r+1} \subseteq \cdots \subseteq \mathfrak{a}_m \neq A$, then

$$M \approx A^r \oplus (A/\mathfrak{a}_{r+1} \oplus \cdots \oplus A/\mathfrak{a}_m),$$

where $A/\mathfrak{a}_{r+1} \oplus \cdots \oplus A/\mathfrak{a}_m$ is the torsion submodule of M. The module M is free iff $r = m$, and a torsion-module iff $r = 0$. In the latter case, the annihilator of M is $\mathfrak{a}_1$.