In view of the uniqueness part of Theorem 35.31, we make the following definition.

Definition 35.12. Given a finitely generated module M over a PID A as in Theorem 35.31, the ideals $\mathfrak{a}_i = \alpha_i A$ are called the *invariant factors* of M. The generators α_i of these ideals (uniquely defined up to a unit) are also called the *invariant factors* of M.

Proposition 35.23 can be sharpened as follows:

Proposition 35.32. *Let F be a finitely generated free module over a PID A, and let M be any submodule of F. Then, M is a free module and there is a basis $(e_1, ..., e_n)$ of F, some $q \leq n$, and some nonzero elements $a_1, \ldots, a_q \in A$, such that $(a_1e_1, \ldots, a_qe_q)$ is a basis of M and a_i divides a_{i+1} for all i, with $1 \leq i \leq q-1$. Furthermore, the free module M' with basis $(e_1, \ldots, e_q)$ and the ideals $a_1A, \ldots, a_qA$ are uniquely determined by M; the quotient module M'/M is the torsion module of F/M, and we have an isomorphism*

$$M'/M \approx A/a_1A \oplus \cdots \oplus A/a_qA.$$

Proof. Since $a_i \neq 0$ for $i = 1, \ldots, q$, observe that

$$M' = \{x \in F \mid (\exists \beta \in A,\, \beta \neq 0)(\beta x \in M)\},$$

which shows that M'/M is the torsion module of F/M. Therefore, M' is uniquely determined. Since

$$M = Aa_1e_1 \oplus \cdots \oplus Aa_qe_q,$$

by Proposition 35.24 we have an isomorphism

$$M'/M \approx A/a_1A \oplus \cdots \oplus A/a_qA.$$

Now, it is possible that the first s elements a_i are units, in which case $A/a_iA = (0)$, so we can eliminate such factors and we get

$$M'/M \approx A/a_{s+1}A \oplus \cdots \oplus A/a_qA,$$

with $a_qA \subseteq a_{q-1}A \subseteq \cdots \subseteq a_{s+1}A \neq A$. By Proposition 35.30, $q-s$ and the ideals a_jA are uniquely determined for $j = s+1, \ldots, q$, and since $a_1A = \cdots = a_sA = A$, the q ideals a_iA are uniquely determined. ☐

The ideals $a_1A, \ldots, a_qA$ of Proposition 35.32 are called the *invariant factors of M with respect to F*. They *should not be confused* with the invariant factors of a module M.

It turns out that $a_1, \ldots, a_q$ can also be computed in terms of gcd's of minors of a certain matrix. Recall that if X is an $m \times n$ matrix, then a $k \times k$ minor of X is the determinant of any $k \times k$ matrix obtained by picking k columns of X, and then k rows from these k columns.