Proposition 35.33. *Let F be a free module of finite dimension over a PID, $(u_1, \ldots, u_n)$ be a basis of F, M be a submodule of F, and $(x_1, \ldots, x_m)$ be a set of generators of M. If $a_1A, \ldots, a_qA$ are the invariant factors of M with respect to F as in Proposition 35.32, then for $k = 1, \ldots, q$, the product $a_1 \cdots a_k$ is a gcd of the $k \times k$ minors of the $n \times m$ matrix X_U whose columns are the coordinates of the x_j over the u_i.*

Proof. Proposition 35.23 shows that $M \subseteq a_1F$. Consequently, the coordinates of any element of M are multiples of a_1. On the other hand, we know that there is a linear form f for which a_1A is a maximal ideal and some $e' \in M$ such that $f(e') = a_1$. If we write e' as a linear combination of the x_i, we see that a_1 belongs to the ideal spanned by the coordinates of the x_i over the basis $(u_1, \ldots, u_n)$. Since these coordinates are all multiples of a_1, it follows that a_1 is their gcd, which proves the case $k = 1$.

For any $k \geq 2$, consider the exterior power $\bigwedge^k M$. Using the notation of the proof of Proposition 35.23, the module M has the basis $(a_1e_1, \ldots, a_qe_q)$, so $\bigwedge^k M$ has a basis consisting of elements of the form

$$a_{i_1}e_{i_1} \wedge \cdots \wedge a_{i_k}e_{i_k} = a_{i_1} \cdots a_{i_k}\, e_{i_1} \wedge \cdots \wedge e_{i_k},$$

for all sequences $(i_1, \ldots, i_k)$ such that $1 \leq i_1 < i_2 < \cdots < i_k \leq q$. However, the vectors $e_{i_1} \wedge \cdots \wedge e_{i_k}$ form a basis of $\bigwedge^k F$. Thus, the map from $\bigwedge^k M$ into $\bigwedge^k F$ induced by the inclusion $M \subseteq F$ defines an isomorphism of $\bigwedge^k M$ onto the submodule of $\bigwedge^k F$ having the elements $a_{i_1} \cdots a_{i_k}\, e_{i_1} \wedge \cdots \wedge e_{i_k}$ as a basis. Since a_j is a multiple of the a_i for $i < j$, the products $a_{i_1} \cdots a_{i_k}$ are all multiples of $\delta_k = a_1 \cdots a_k$, and one of these is equal to δ_k. The reasoning used for $k = 1$ shows that δ_k is a gcd of the set of coordinates of any spanning set of $\bigwedge^k M$ over any basis of $\bigwedge^k F$. If we pick as basis of $\bigwedge^k F$ the wedge products $u_{i_1} \wedge \cdots \wedge u_{i_k}$, and as generators of $\bigwedge^k M$ the wedge products $x_{i_1} \wedge \cdots \wedge x_{i_k}$, it is easy to see that the coordinates of the $x_{i_1} \wedge \cdots \wedge x_{i_k}$ are indeed determinants which are the $k \times k$ minors of the matrix X_U. ☐

Proposition 35.33 yields $a_1, \ldots, a_q$ (up to units) as follows: First, a_1 is a gcd of the entries in X_U. Having computed $a_1, \ldots, a_k$, let $b_k = a_1 \cdots, a_k$, compute $b_{k+1} = a_1 \cdots a_k a_{k+1}$ as a gcd of all the $(k+1) \times (k+1)$ minors of X_U, and then a_{k+1} is obtained by dividing b_{k+1} by b_k (recall that a PID is an integral domain).

We also have the following interesting result about linear maps between free modules over a PID.

Proposition 35.34. *Let A be a PID, let F be a free module of dimension n, F' be a free module of dimension m, and $f\colon F \to F'$ be a linear map from F to F'. Then, there exist a basis $(e_1, \ldots, e_n)$ of F, a basis $(e'_1, \ldots, e'_m)$ of F', and some nonzero elements $\alpha_1, \ldots \alpha_r \in A$ such that*

$$f(e_i) = \begin{cases} \alpha_i e'_i & \text{if } 1 \leq i \leq r \\ 0 & \text{if } r+1 \leq i \leq n, \end{cases}$$