Proposition 35.36. *Two $m \times n$ matrices X and Y are equivalent iff they have the same invariant factors.*

If X is the matrix of a linear map $f \colon F \to F'$ with respect to some basis $(u_1, \ldots, u_n)$ of F and some basis $(u'_1, \ldots, u'_m)$ of F', then the columns of X are the coordinates of the $f(u_j)$ over the u'_i, where the $f(u_j)$ generate $f(F)$, so Proposition 35.33 applies and yields the following result:

Proposition 35.37. *If X is a $m \times n$ matrix or rank r over a PID A, and if $\alpha_1 A, \ldots, \alpha_r A$ are its invariant factors, then α_1 is a gcd of the entries in X, and for $k = 2, \ldots, r$, the product $\alpha_1 \cdots \alpha_k$ is a gcd of all $k \times k$ minors of X.*

There are algorithms for converting a matrix X over a PID to the form $X = QDP^{-1}$ as described in Proposition 35.35. For Euclidean domains, this can be achieved by using the elementary row and column operations $P(i, k)$, $E_{i,j;\beta}$, and $E_{i,\lambda}$ described in Chapter 8, where we require the scalar λ used in $E_{i,\lambda}$ to be a unit. For an arbitrary PID, another kind of elementary matrix (containing some 2×2 submatrix in addition to diagonal entries) is needed. These procedures involve computing gcd's and use the Bezout identity to mimic division. Such methods are presented in D. Serre [156], Jacobson [98], and Van Der Waerden [179], and sketched in Artin [7]. We describe and justify several of these methods in Section 36.5.

Proposition 35.32 has the following two applications.

First, consider a finitely presented module M over a PID given by some $m \times n$ matrix R. By Proposition 35.35, the matrix R can be diagonalized as $R = QDP^{-1}$ where D is a diagonal matrix. Then, we see that M has a presentation with m generators and r relations of the form

$$\alpha_i e_i = 0,$$

where $\alpha_i \neq 0$ and $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_r$.

For the second application, let F be a free module with basis $(e_1, \ldots, e_n)$, and let M be a submodule of F generated by m vectors $v_1, \ldots, v_m$ in F. The module M can be viewed as the set of linear combinations of the columns of the $n \times m$ matrix also denoted M consisting of the coordinates of the vectors $v_1, \ldots, v_m$ over the basis $(e_1, \ldots, e_n)$. Then by Proposition 35.35, the matrix R can be diagonalized as $R = QDP^{-1}$ where D is a diagonal matrix. The columns of Q form a basis $(e'_1, \ldots, e'_n)$ of F, and since $RP = QD$, the nonzero columns of RP form the basis $(a_1 e'_1, \ldots, a_q e'_q)$ of M.

When the ring A is a Euclidean domain, Theorem 36.18 shows that P and Q are products of elementary row and column operations. In particular, when $A = \mathbb{Z}$, in which cases our $\mathbb{Z}$-modules are abelian groups, we can find P and Q using Euclidean division.

If $A = \mathbb{Z}$, a finitely generated submodule M of $\mathbb{Z}^n$ is called a *lattice*. It is given as the set of integral linear combinations of a finite set of integral vectors.