In particular, if we apply Theorem 36.19 to a matrix M of the form $M = XI - A$, where A is a square matrix, then $\det(XI - A) = \chi_A(X)$ is never zero, and since $XI - A = QDP^{-1}$ with P, Q invertible, all the entries in D must be nonzero and we obtain the following result showing that the similarity invariants of A can be computed using elementary operations.

Theorem 36.20. *If A is an $n \times n$ matrix over the field K, then there exist some invertible $n \times n$ matrices P and Q, where P and Q are products of elementary matrices with entries in $K[X]$, and a $n \times n$ matrix D of the form*

$$D = \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & q_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & q_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & q_m \end{pmatrix}$$

for some nonzero monic polynomials $q_i \in k[X]$ of degree ≥ 1, such that

(1) $q_1 \mid q_2 \mid \cdots \mid q_m$,

(2) $q_1, \ldots q_m$ are the similarity invariants of A, and

(3) $XI - A = QDP^{-1}$.

The matrix D in Theorem 36.20 is often called *Smith normal form* of A, even though this is confusing terminology since D is really the Smith normal form of $XI - A$.

Of course, we know from previous work that in Theorem 36.19, the $\alpha_1, \ldots, \alpha_r$ are unique, and that in Theorem 36.20, the $q_1, \ldots, q_m$ are unique. This can also be proved using some simple properties of minors, but we leave it as an exercise (for help, look at Jacobson [98], Chapter 3, Theorem 3.9).

The rational canonical form of A can also be obtained from Q^{-1} and D, but first, let us consider the generalization of Theorem 36.19 to PID's that are not necessarily Euclidean rings.

We need to find a "norm" that assigns a natural number $\sigma(a)$ to any nonzero element of a PID A, in such a way that $\sigma(a)$ decreases whenever we return to Step 2a and Step 2b. Since a PID is a UFD, we use the number

$$\sigma(a) = k_1 + \cdots + k_r$$

of prime factors in the factorization of a nonunit element

$$a = up_1^{k_1} \cdots p_r^{k_r},$$