where $p_1, \ldots, p_n$ are the invariant factors of $\mathrm{Im}(X1 - \overline{f})$ with respect to $E[X]$. Since $E_f \approx E[X]/\mathrm{Im}(X1 - \overline{f})$, by the uniqueness part of Theorem 35.31 and because the polynomials are monic, we must have $p_i = q_i$, for $i = 1, \ldots, n$. Therefore, we proved the following crucial fact:

Proposition 36.11. *For any linear map $f\colon E \to E$ over a K-vector space E of dimension n, the similarity invariants of f are equal to the invariant factors of $\mathrm{Im}(X1 - \overline{f})$ with respect to $E[X]$.*

Proposition 36.11 is the key to computing the similarity invariants of a linear map. This can be done using a procedure to convert $XI - M$ to its *Smith normal form*. Propositions 36.11 and 35.37 yield the following result.

Proposition 36.12. *For any linear map $f\colon E \to E$ over a K-vector space E of dimension n, if $(q_1, \ldots, q_n)$ are the similarity invariants of f, for any matrix M representing f with respect to any basis, then for $k = 1, \ldots, n$ the product*

$$d_k(X) = q_1(X) \cdots q_k(X)$$

is the gcd of the $k \times k$-minors of the matrix $XI - M$.

Note that the matrix $XI - M$ is none other than the matrix that yields the characteristic polynomial $\chi_f(X) = \det(XI - M)$ of f.

Proposition 36.13. *For any linear map $f\colon E \to E$ over a K-vector space E of dimension n, if $(q_1, \ldots, q_n)$ are the similarity invariants of f, then the following properties hold:*

(1) If $\chi_f(X)$ is the characteristic polynomial of f, then

$$\chi_f(X) = q_1(X) \cdots q_n(X).$$

(2) The minimal polynomial $m(X) = q_n(X)$ of f divides the characteristic polynomial $\chi_f(X)$ of f.

(3) The characteristic polynomial $\chi_f(X)$ divides $m(X)^n$.

(4) E is cyclic for f iff $m(X) = \chi_f(X)$.

Proof. Property (1) follows from Proposition 36.12 for $k = n$. It also follows from Theorem 36.6 and the fact that for the companion matrix associated with q_i, the characteristic polynomial of this matrix is also q_i. Property (2) is obvious from (1). Since each q_i divides q_{i+1}, each q_i divides q_n, so their product $\chi_f(X)$ divides $m(X)^n = q_n(X)^n$. The last condition says that $q_1 = \cdots = q_{n-1} = 1$, which means that E_f has a single summand. $\square$

Observe that Proposition 36.13 yields another proof of the Cayley–Hamilton Theorem. It also implies that a linear map is nilpotent iff its characteristic polynomial is X^n.