Minimal Polynomial

By the Cayley-Hamilton Theorem, $\Delta_A(A)=0$, $\Delta_T(T)=0$ for a matrix A or linear operator T. Thus the set of nonzero polynomials with A (or T) as a zero is nonempty, and so there is one of lowest degree. Dividing this polynomial by its leading coefficient yields a monic polynomial of lowest degree with A (or T) as a zero.

Defn: Let A be a square matrix or T a linear operator. The minimal polynomial of A or T is the monic polynomial of lowest degree with A or T as a zero. The minimal polynomial is denoted $m(t)$ (or $m_A(t)$, $m_T(t)$, respectively).

Note: If $T: V \to V$ is a linear operator and S a basis for V, then for any polynomial $f(t)$, $f(T)=0$ if and only if $f([T]_S)=0$. Hence the minimal polynomial of T is the same as for $[T]_S$. Therefore the following results stated for matrices hold for linear operators as well.

We will also need the following fact about polynomials:

Division Algorithm: If $f(t), g(t)$ are polynomials over K with $g(t) \neq 0$, then there exist (unique) polynomials $Q(t)$, $R(t)$ over K such that

$$f(t) = Q(t)g(t) + R(t)$$

and either $R(t)=0$ or $\deg R(t) < \deg g(t)$.

If $R(t)=0$, so that $f(t) = Q(t)g(t)$, we say that $g(t)$ divides $f(t)$ or that $g(t)$ is a factor of $f(t)$.