Minimal polynomial, naturally

rapha • 25 Apr 2025

Let K/F be a field extension and pick any element $\alpha \in K$. There is a morphism $\mathrm{ev}_{K,\alpha}$ or more briefly ev_α, defined as the composition

$$F[x] \hookrightarrow K[x] \twoheadrightarrow K[x]/(x-\alpha) \xrightarrow{\cong} K.$$

In other words, $\mathrm{ev}_\alpha : F[x] \to K$ is a map of rings that does the obvious thing: it takes some polynomial $p(x)$ and evaluates it at the element α inside of K.

Because $F[x]$ is a principal ideal domain, the kernel of this map may be written as (m_α) for some polynomial $m_\alpha \in F[x]$. We can further assume this polynomial is monic, since whether it is or not won't affect the resulting ideal. We say that an element $\alpha \in K$ is **algebraic over** F if, and only if, the polynomial m_α is not zero. Otherwise, the element α is said to be **transcendental over** F. In other words, an element is transcendental if, and only if, the evaluation at that element is an injective ring homomorphism.

Usually, people define an algebraic element as an element such that there exists a non-zero polynomial which, when evaluated at that element, is zero; an element is then transcendental when it is not algebraic. It's not hard to show that my definitions and the usual definitions are equivalent, so I'm not going to prove it here. The main reason for introducing my alternative definition is because it gives a context in which the minimal polynomial naturally appears as the kernel of an obvious map. Keep reading for the details.

For the rest of this article we suppose that α is algebraic over F, and thus the polynomial m_α is non-zero (recall that we also supposed it is monic). This non-zero polynomial is called the **minimal polynomial of** α. Because $F[x]/(m_\alpha)$ is (identified with) a subring of K, and because K is a field and thus an integral domain, the ring $F[x]/(m_\alpha)$ is also an integral domain. Hence, the ideal (m_α) is prime, so the non-zero polynomial m_α must be *irreducible*. Moreover, suppose $(m_\alpha) = (m')$ for some other non-zero monic irreducible polynomial m'. In particular, $m_\alpha \in (m')$, so there exists some polynomial u such that $m_\alpha = um'$. By irreducibility, u is a unit, so m_α and m' have the same degree, let's call it $d \in \mathbb{N}$. Equality of polynomials means they have the same coefficients at every

degree; in particular, the coefficient at x^d of m_α is 1, while for um' it is u. This forces $u = 1$, so $m_\alpha = m'$. This justifies my usage of the word “the” when I defined *the* minimal polynomial.

I think this point of view on the minimal polynomial makes its properties clearer, and the importance of m_α is better felt. For instance, with the “usual” definition, it’s not so hard to show that if p is a polynomial such that $p(\alpha) = 0$, then m_α divides p. However, using my definition, this fact is immediate and needs almost no proof, since $p(\alpha) = 0$ exactly means that p is in the kernel of the evaluation map, which is (m_α).