The Minimal Polynomial Theorem

Lemma. *Let E be an extension of a field F and $a \in E$. Suppose $m(x), f(x) \in F[x]$, $m(x)$ is irreducible over F, $m(a) = 0$, and $f(a) = 0$. Then $m(x)$ must divide $f(x)$.*

Proof. If $m(x)$ does not divide $f(x)$, since $m(x)$ is irreducible, the GCD of $m(x)$ and $f(x)$ must be 1, which implies that there exist polynomials $g(x), h(x) \in F[x]$ such that

$$g(x)f(x) + h(x)m(x) = 1. \tag{1}$$

Plugging in $x = a$, we see that $0 = 1$; contradiction. $\square$

Theorem (The Minimal Polynomial Theorem)**.** *Let E be an extension of a field F, let $a \in E$ be algebraic over F, and suppose $m(x) \in F[x]$ is monic.*

Then the following are equivalent:

1. *$m(x)$ is irreducible over F and $m(a) = 0$.*
2. *$m(x)$ is a nonzero polynomial of smallest possible degree such that $m(a) = 0$.*
3. *For $n = \deg m(x)$, $\left\{1, a, \dots, a^{n-1}\right\}$ is a basis for $F(a)$ as a vector space over F and $m(a) = 0$.*
4. *$[F(a):F] = \deg m(x)$ and $m(a) = 0$.*
5. *$F(a) \approx F[x]/\langle m(x)\rangle$ and $m(a) = 0$.*

Furthermore, if any (and therefore all) of the above conditions hold, then for any $f(x) \in F[x]$ such that $f(a) = 0$, we have that $m(x)$ divides $f(x)$ in $F[x]$.

If any (and therefore all) of the equivalent conditions in the Theorem hold, we call $m(x)$ the *minimal polynomial of a over F*. Note that the requirement that $m(x)$ be monic is just so we can call $m(x)$ "the" minimal polynomial of a; more generally, a polynomial has properties (1)–(5) if and only if it is a nonzero scalar multiple of the minimal polynomial.

Proof. (1) $\Rightarrow$ (2): Suppose $m(x)$ is irreducible over F, $f(x) \in F[x]$, $\deg f(x) < \deg m(x)$, and $f(a) = 0$. By the Lemma, $m(x)$ divides $f(x)$, and since $\deg f(x) < \deg m(x)$, we must have $f(x) = 0$.

(2) $\Rightarrow$ (3): Suppose $m(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$. Since $m(a) = 0$, we have that

$$a^n = -c_{n-1}a^{n-1} - \cdots - c_0, \tag{2}$$

which means that any polynomial in a of degree $\geq n$ can be reduced to a polynomial in a of degree $< n$. In other words, the set $\left\{1, a, \dots, a^{n-1}\right\}$ spans $F(a)$ as a vector space over F.

On the other hand, suppose that for some $b_i \in F$, we have that

$$b_{n-1}a^{n-1} + \cdots + b_1 a + b_0 = 0. \tag{3}$$

In that case, $g(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ is a polynomial of degree strictly less than n such that $g(a) = 0$. However, since the smallest possible degree of a nonzero polynomial that has a as a zero is $\deg m(x) = n$, we must have that $g(x) = 0$, or in other words, that each of the $b_i = 0$. It follows that $\left\{1, a, \ldots, a^{n-1}\right\}$ is linearly independent, and therefore, that $\left\{1, a, \ldots, a^{n-1}\right\}$ is a basis for $F(a)$ as a vector space over F.

(3) $\Rightarrow$ (4): By definition, $[F(a) : F]$ is the dimension of $F(a)$ as a vector space over F, which is equal to the number of vectors in any basis.

(4) $\Rightarrow$ (5): Suppose $[F(a) : F] = \deg m(x) = n$, and let I be the principal ideal $\langle m(x) \rangle$ of $F[x]$. Define a map $\varphi : F[x]/I \to F(a)$ by the formula

$$\varphi(f(x) + I) = f(a). \tag{4}$$

Note that φ is well-defined because if g is another representative of the coset $f(x) + I$, we have that $g(x) = f(x) + q(x)m(x)$ for some $q(x) \in F[x]$, which means that

$$g(a) = f(a) + q(a)m(a) = f(a). \tag{5}$$

Since substitution is a homomorphism, it also follows that φ is a homomorphism.

So now suppose $f(x) + I \in \ker \varphi$, where $f(x) \in F[x]$ is a polynomial of degree $< n$. In that case, since $f(a) = 0$ and $\left\{1, a, \ldots, a^{n-1}\right\}$ is linearly independent, we must have that $f(x) = 0$, which means that φ is one-to-one. Furthermore, since $\left\{1, a, \ldots, a^{n-1}\right\}$ spans $F(a)$, φ is onto, and so $F(a) \approx F[x]/\langle m(x) \rangle$.

(5) $\Rightarrow$ (1): Since $F(a)$ is a field and $F(a) \approx F[x]/\langle m(x) \rangle$, $m(x)$ must be irreducible.

Finally, suppose conditions (1)–(5) all hold. In that case, if $f(x) \in F[x]$ and $f(a) = 0$, by the Lemma, $m(x)$ must divide $f(x)$. The theorem follows. $\square$