Minimum Polynomial

Definition: Algebraic

Let K/F be a field extension and $\alpha \in K$. To say that a is *algebraic* over F means that $\exists\, f(x) \in F[x]$ such that $f(x) \not\equiv 0$ and $f(\alpha) = 0$.

To say that K/F is algebraic means $\forall\, \alpha \in K, \alpha$ is algebraic.

Definition: Minimum Polynomial

Let K/F be a field extension and $\alpha \in K$ be algebraic over F. The *minimal polynomial* of α over F, denoted $m_\alpha(x)$ or $m_{\alpha,F}(x)$, is a monic polynomial $f(x) \in F[x]$ of minimal degree such that $f(\alpha) = 0$.

Theorem

Let K/F be a field extension and $\alpha \in K$ be algebraic over F:

1). $m_{\alpha,F}(x)$ exists in $F[x]$.

2). $m_{\alpha,F}(x)$ is irreducible in $F[x]$.

3). $m_{\alpha,F}(x)$ is unique in $F[x]$.

4). $\forall\, f(x) \in F[x], f(\alpha) = 0 \implies m_{\alpha,F}(x) \mid f(x)$ in $F[x]$.

Proof

Since α is algebraic over F, and by the well-ordering principle, $m_{\alpha,f}(x)$ must exist.

ABC: $m_{\alpha,F}(x)$ is not irreducible in $F[x]$
$\exists\, g(x), h(x) \in F(x)$ such that $g(x)$ and $h(x)$ are not units in $F[x]$ and $m_{\alpha,F}(x) = g(x)h(x)$
But then $\deg(g(x)), \deg(h(x)) < \deg(m_{\alpha,F}(x))$
Also $g(\alpha) = 0$ or $h(\alpha) = 0$, violating the minimality of $m_{\alpha,F}(x)$ - contradiction.

Therefore $m_{\alpha,F}(x)$ is irreducible in $F[x]$.

Assume $f(x) \in F[x]$ such that $f(\alpha) = 0$
By the division algorithm: $f(x) = q(x)m_{\alpha,F}(x) + r(x)$ and $\deg(r(x)) < \deg(m_{\alpha,F}(x))$
$f(\alpha) = q(\alpha)m_{\alpha,F}(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = 0 + r(\alpha) = r(\alpha) = 0$
So by the minimality of $m_{\alpha,F}(x)$ it must be the case that $r(x) = 0$

Therefore $m_{\alpha,F}(x) \mid f(x)$ in $F[x]$.

Assume $f(x)$ is also a minimal polynomial
$f(x) \mid m_{\alpha,F}(a)$ and $m_{\alpha,F}(a) \mid f(x)$
So $m_{\alpha,F}(x)$ and $f(x)$ are associates
But $m_{\alpha,F}(x)$ and $f(x)$ are monic and so $m_{\alpha,F}(x) = f(x)$

Therefore $m_{\alpha,F}(x)$ is unique in $F[x]$.

Theorem

Let K/F be a field extension:

$[K : F] = n$ is finite $\implies K/F$ is algebraic.

Proof

Assume $\alpha \in K$
Consider $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$
This set has $n + 1$ vectors and thus the set must be F-linearly dependent
So there exists coefficients $c_k \in F$ not all zero such that:

$$\sum_{k=0}^{n} c_k \alpha^k = 0$$

Let $f(x) = \sum_{k=0}^{n} c_k x^k \in F[x]$
$f(\alpha) = 0$
So α is algebraic over F

Therefore K/F is algebraic.

Thus, all simple extensions by an algebraic α are algebraic.

Theorem

Let α be algebraic over F:

$$F(\alpha) = F[\alpha]$$

Proof

Assume $\frac{f(\alpha)}{g(\alpha)} \in F(\alpha)$ where $f(x), g(x) \in F[x]$ and $g(\alpha) \neq 0$

There exists irreducible $m_{\alpha,F}(x) \in F[x]$
So the GCD of $m_{\alpha,F}(x)$ and $g(x)$ is 1
But $F[x]$ is a PID and so $h(x)g(x) + w(x)m_{\alpha,F}(x) = 1$ for some $h(x), w(x) \in F[x]$
$h(\alpha)g(\alpha) + w(\alpha)m_{\alpha,F}(\alpha) = h(\alpha)g(\alpha) + w(\alpha) \cdot 0 = h(\alpha)g(\alpha) = 1$
$h(\alpha) = \frac{1}{g(\alpha)}$
$\frac{f(\alpha)}{g(\alpha)} = f(\alpha)h(\alpha) \in F[\alpha]$

Assume $f(\alpha) \in F[\alpha]$

$f(a) = \sum_{k=0}^{n} c_k \alpha^k \in F(a)$

Theorem

Let K/F be a field extension and $\alpha \in K$ be algebraic over F with minimal polynomial $m_{\alpha,F}(x)$ such that $\deg(m_{\alpha,F}(x)) = n$:

1). $[F(\alpha) : F] = n$

2). $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an F-basis for $F(a)$

Proof

ABC: $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is linearly dependent
So there exists $c_k \in F$ not all zero such that:

$$\sum_{k=0}^{n-1} c_k \alpha^k = 0$$

Let $f(x) = \sum_{k=0}^{n-1} c_k x^k$
$\deg(f(x)) = n - 1$ and $f(\alpha) = 0$, thus violating the minimality of $m_{\alpha,F}(x)$

Therefore $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is linearly independent.

Assume $\beta \in F(\alpha)$
$\beta \in F[\alpha]$
$\beta = f(\alpha)$ for some $f(x) \in F[x]$
$f(x) = q(x)m_{\alpha,F}(x) + r(x)$ where $\deg(r(x)) < n$
$f(\alpha) = q(\alpha)m_{\alpha,F}(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = 0 + r(\alpha) = r(\alpha)$
Thus $\beta = \sum_{k=0}^{m} c_k \alpha^k$ for some $m < n$

Therefore $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ spans $F(\alpha)$

Therefore $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an F-basis for $F(a)$ and $[F(\alpha) : F] = n$.