Subject : MATHEMATICS

Paper 1 : ABSTRACT ALGEBRA

Chapter 8 : Field Extensions

Module 2 : Minimal polynomials

Anjan Kumar Bhuniya
Department of Mathematics
Visva-Bharati; Santiniketan
West Bengal

Minimal polynomials

Learning Outcomes:	1. Algebraic and transcendental elements.
	2. Minimal polynomial of an algebraic element.
	3. Degree of the simple extension $K(c)/K$.

In the previous module we defined degree $[F : K]$ of a field extension F/K to be the dimension of F as a vector space over K. Though we have results ensuring existence of basis of every vector space, but there is no for finding a basis in general. In this module we set the theory a step forward to find $[F : K]$. The degree of a simple extension $K(c)/K$ is finite if and only if c is a root of some nonconstant polynomial $f(x)$ over K. Here we discuss how to find a basis and dimension of such simple extensions $K(c)/K$.

Definition 0.1. *Let F/K be a field extension. Then $c \in F$ is called an algebraic element over K, if there is a nonconstant polynomial $f(x) \in K[x]$ such that $f(c) = 0$, i.e. if there exists $k_0, k_1, \cdots, k_n \in K$ not all zero such that*

$$k_0 + k_1 c + \cdots + k_n c^n = 0.$$

Otherwise c is called a transcendental element over K.

Example 0.2. *1. $1, \sqrt{2}, 3\sqrt{5}, i$ etc are algebraic over $\mathbb{Q}$.*

2. e, π, e^e are transcendental over $\mathbb{Q}$. [For a proof that e is transcendental over $\mathbb{Q}$ we refer to the classic text Topics in Algebra by I. N. Herstein.]

The algebraic elements $\alpha \in \mathbb{C}$ over $\mathbb{Q}$ are of special interest for their importance in algebra, geometry, number theory, cryptography, etc..

Definition 0.3. *A complex number α is called an algebraic number if α is an algebraic element over $\mathbb{Q}$ that is, if there is a nonconstant polynomial $f(x)$ with rational coefficients such that*

$$f(\alpha) = 0.$$

Otherwise $\alpha \in \mathbb{C}$ is called a transcendental number.

Let $\alpha \in F$ be an algebraic element over K. Now we show that uniqueness can be imposed to the polynomials $f(x) \in K[x]$ such that $f(\alpha) = 0$ up to some restrictions.

Theorem 0.4. *Let F/K be a field extension and $\alpha \in F$ be algebraic over K. Then there is a unique monic polynomial $m(x) \in K[x]$ of least degree such that $m(\alpha) = 0$.*

Proof. Since α is algebraic over K, there is a nonconstant polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$. This implies that $P = \{f(x) \in K[x] \mid f(x)$ is nonconstant and $f(\alpha) = 0\}$ is nonempty and hence $N = \{\deg f(x) \mid f(x) \in P\}$ is a nonempty subset of $\mathbb{N}$. By the well-ordering principle of natural numbers, N has the least element, say n and correspondingly a polynomial $f(x) = k_0x^n + k_1x^{n-1} + \cdots + k_{n-1}x + k_n \in K[x]$ of degree n in P. Then $k_0 \neq 0$ and hence $m(x) = k_0^{-1}f(x)$ becomes a monic polynomial of the least degree n such that $m(\alpha) = 0$.

Suppose $p(x)$ is a monic polynomial of degree n and $p(\alpha) = 0$. Since K is a field, there are $q(x), r(x) \in K[x]$ such that $p(x) = m(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg m(x)$. If $\deg r(x) < \deg m(x)$, then $r(x)$ becomes a nonconstant polynomial such that $r(\alpha) = p(\alpha) - m(\alpha)q(\alpha) = 0$, which contradicts the choice of $m(x)$ as a polynomial of least degree such that $m(\alpha) = 0$. Thus $r(x) = 0$ and we have $p(x) = m(x)q(x)$ which implies that $\deg q(x) = 0$, i.e. $q(x) = k \in K$. Since both $p(x)$ and $m(x)$ are monic, $p(x) = km(x)$ implies that $k = 1$ and thus the uniqueness of $m(x)$ is established. □

Definition 0.5. *Let F/K be a field extension and $\alpha \in F$ algebraic over K. Then the unique monic polynomial $m(x) \in K[x]$ of least degree such that $m(\alpha) = 0$ is called the minimal polynomial of α over K.*

If $n = \deg m(x)$, then α is called algebraic of degree n over K.

Example 0.6. *Consider the extension $\mathbb{R}/\mathbb{Q}$. Then $x^2 - 3$ is the minimal polynomial of $\sqrt{3} \in \mathbb{R}$ over $\mathbb{Q}$. Thus $\sqrt{3}$ is algebraic of degree 2 over $\mathbb{Q}$.*

Example 0.7. *Let F/K be a field extension and c be algebraic over K of degree 5. We show that $K(c) = K(c^2)$.*

Let $m(x) = x^5 + k_4x^4 + k_3x^3 + k_2x^2 + k_1x + k_0$ be the minimal polynomial of c over K. Then c can not be a root of any polynomial of degree less than 5, and so $c^4 + k_3c^2 + k_1 \neq 0$. Then $c^5 + k_4c^4 + k_3c^3 + k_2c^2 + k_1c + k_0 = 0$ implies that $c = \frac{-k_0 - k_2c^2 - k_4c^4}{k_1 + k_3c^2 + c^4} \in K(c^2)$, and hence $K(c) \subseteq K(c^2)$. Again $c^2 \in K(c)$ implies that $K(c^2) \subseteq K(c)$. Thus $K(c) = K(c^2)$.

Though the above proof for the existence and uniqueness of the minimal polynomial $m(x)$ is intrinsic still it does not suggest any working method for finding the minimal polynomial. Now we show that irreducibility may be an efficient equivalent criterion for our practical purpose.

First let us prove the following lemma which is a direct consequence of the leastness of the minimal polynomial $m(x)$ in degree such that $m(\alpha) = 0$:

Lemma 0.8. *Let F/K be a field extension and $\alpha \in F$ algebraic over K. Then for every $f(x) \in K[x]$, $f(\alpha) = 0$ implies that $m(x) \mid f(x)$.*

Proof. By the Division Algorithm, there are $q(x), r(x) \in K[x]$ such that $f(x) = m(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg m(x)$. If $\deg r(x) < \deg m(x)$, then $r(x)$ becomes a nonconstant polynomial such that $r(\alpha) = p(\alpha) - m(\alpha)q(\alpha) = 0$, which contradicts the choice of $m(x)$ as a polynomial of least degree such that $m(\alpha) = 0$. Thus $r(x) = 0$ and we have $f(x) = m(x)q(x)$ which implies that $m(x) \mid f(x)$. □

If $f(x)$ is a nonconstant polynomial such that $f(\alpha) = 0$, then the above lemma shows that some factor of $f(x)$ is the minimal polynomial of α. Thus if we have some irreducible polynomial $p(x)$ such that $p(\alpha) = 0$, then this must be the monic polynomial up to a unit multiple, that is $m(x) = up(x)$. Since $K[x]$ is a UFD, there are irreducible polynomials $p_1(x), p_2(x), \cdots, p_m(x) \in K[x]$ such that $f(x) = p_1(x)p_2(x)\cdots p_m(x)$. Then $f(\alpha) = 0$ implies that $p_1(\alpha)p_2(\alpha)\cdots p_m(\alpha) = 0$ and hence $p_i(\alpha) = 0$ for some i. Thus we have an irreducible polynomial $p_i(x)$ having a root α. Now we show that irreducibility is enough to characterize minimal polynomials.

Theorem 0.9. *Let F/K be a field extension and $\alpha \in F$ algebraic over K. Then $m(x) \in K[x]$ is the minimal polynomial of α over K if and only if it is a monic irreducible polynomial such that $m(\alpha) = 0$.*

Proof. First assume that $m(x) \in K[x]$ is the minimal polynomial of α over K. Suppose $m(x) = u(x)v(x)$, $u(x), v(x) \in K[x]$. Then $m(\alpha) = 0$ implies that either $u(\alpha) = 0$ or $v(\alpha) = 0$. If $u(\alpha) = 0$, then $\deg u(x)$ can never be less than $\deg m(x)$ and hence $\deg u(x) = \deg m(x)$. This implies that $\deg v(x) = 0$ and hence $v(x)$ is a unit. Similarly $v(\alpha) = 0$ implies that $u(x)$ is a unit. Thus $m(x)$ is irreducible.

Conversely, consider a monic and irreducible polynomial $p(x) \in K[x]$ such that $p(\alpha) = 0$. Then $p(x) = m(x)q(x)$. Then the irreducibility of $p(x)$ implies that either $m(x)$ is a unit or $q(x)$ is a unit. Since $m(x)$ is nonconstant, it is not a unit. Thus $q(x)$ is a unit. Since both $p(x)$ and $m(x)$ are monic we have $q(x) = 1$. Thus $p(x) = m(x)$. □

Now we characterize algebraic elements and simple extensions generated by the algebraic elements.

Corollary 0.10. *Let F/K be a field extension and $\alpha \in F$. Then α is algebraic over K if and only if $K[\alpha] = K(\alpha)$. Moreover in this case, $K[\alpha] = K(\alpha) \simeq K[x]/ < m(x) >$.*

Proof. First assume that α is algebraic over K. Define $\psi : K[x] \longrightarrow K[\alpha]$ by: for every $f(x) \in K[x]$,

$$\psi(f(x)) = f(\alpha).$$

Then ψ is an onto homomorphism. Now

$$\begin{aligned} \ker \psi &= \{f(x) \in K[x] \mid f(\alpha) = 0\} \\ &= \{f(x) \in K[x] \mid m(x) \mid f(x)\} \\ &= < m(x) > \end{aligned}$$

implies, by the First Isomorphism Theorem, that $K[x]/ < m(x) > \simeq K[\alpha]$. Since $m(x)$ is irreducible, it follows that $K[x]/ < m(x) >$ is a field forcing $K[\alpha]$ to be a field. Hence $K[\alpha] = K(\alpha)$.

Conversely, suppose that $K[\alpha] = K(\alpha)$. That $\alpha = 0$ is algebraic follows directly. Let $\alpha \neq 0$. Since $K(\alpha)$ is a field, $\alpha^{-1} \in K(\alpha) = K[\alpha]$ and hence $\alpha^{-1} = k_0 + k_1\alpha + \cdots + k_n\alpha^n$ for some $k_i \in K$, where $k_i, i = 0, 1, 2, \cdots, n$ are not all zero. Then $k_n\alpha^{n+1} + k_{n-1}\alpha^n + \cdots + k_0\alpha - 1 = 0$ which shows that α is algebraic over K. □

In the following we show that $K(c)$ is an infinite extension of K for every transcendental element c.

Corollary 0.11. *Let F/K be a field extension and $c \in F$. Then c is transcendental over K if and only if $K[c] \subsetneq K(c)$. In this case, $K[c] \simeq K[x]$ and $K(c) \simeq K(x)$.*

Proof. First part of this result follows from the above corollary, since $K[c] \subseteq K(c)$.

For the second part, consider the onto homomorphism $\psi : K[x] \longrightarrow K[c]$ by: for every $f(x) \in K[x]$,

$$\psi(f(x)) = f(c).$$

Since c is transcendental over K, there is no nonzero polynomial $f(x) \in K[x]$ such that $f(c) = 0$. Thus $\ker \psi = \{0\}$ showing that ψ is one-to-one. Thus $K[x] \simeq K[c]$.

Since $K(x)$ and $K(c)$ are the quotient fields of $K[x]$ and $K[c]$ respectively, $\psi : K[x] \longrightarrow K[c]$ induces an isomorphism $\psi^* : K(x) \longrightarrow K(c)$ defined by: for every $\frac{f(x)}{g(x)} \in K(x)$,

$$\psi^*(\frac{f(x)}{g(x)}) = \frac{f(c)}{g(c)}.$$

Therefore $K(c) \simeq K(x)$. □

If $m(x)$ is a polynomial of degree n, then the division algorithm for polynomials over a field implies that $K[x]/ < m(x) >$ is a vector space of dimension n over K with a basis $\{1+ < m(x) >, x+ < m(x) >, \cdots, x^{n-1}+ < m(x) >\}$. Also if $m(x)$ is irreducible over K, then $F = K[x]/ < m(x) >$ is a field and $c = x+ < m(x) > \in F$ is a root of $m(x)$. Thus, by the Corollary 1, we have:

Theorem 0.12. *Let F/K be a field extension, $c \in F$ be algebraic over K and $m(x)$ be the minimal polynomial of c over K. If $\deg m(x) = n$, then $\{1, c, c^2, \cdots, c^{n-1}\}$ is a basis of $K(c)$ over K. Thus*

$$[K(c) : K] = \deg m(x).$$

Proof. Let $\alpha \in K(c)$. Since c is algebraic over K, $K(c) = K[c]$. This implies that $\alpha = f(c)$ for some $f(x) \in K[x]$. Then, by the Division Algorithm, there are $q(x), r(x) \in K[x]$ such that

$$f(x) = m(x)q(x) + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg m(x)$. In either case we can assume that $r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1}$ where $r_i \in K$. Then $m(c) = 0$ implies that

$$\alpha = f(c) = r(c) = r_0 + r_1 c + \cdots + r_{n-1}c^{n-1}.$$

Hence $\{1, c, c^2, \cdots, c^{n-1}\}$ generates $K(c)$ over K. For the linear independence note that if there are $k_0, k_1, \cdots, k_{n-1} \in K$ some of which is nonzero such that

$$k_0 + k_1 c + \cdots + k_{n-1}c^{n-1} = 0$$

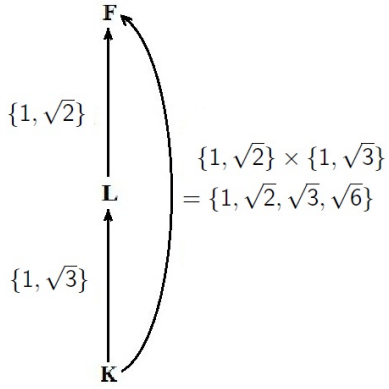
then $p(x) = k_0 + k_1 x + \cdots + k_{n-1}x^{n-1} \in K[x]$ becomes a nonzero polynomial of degree less than $\deg m(x)$ such that $p(c) = 0$ which contradicts that $m(x)$ is the minimal polynomial of c over K. Thus $\{1, c, c^2, \cdots, c^{n-1}\}$ is a basis of $K(c)$ over K. □

Now we give some examples to demonstrate applications of this theorem.

Example 0.13. *Consider the extension $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{Q}$. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is given by $m(x) = x^3 - 2$. So $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ is a basis of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. Thus*

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b2^{1/3} + c2^{2/3} | a, b, c \in \mathbb{Q}\}.$$

Example 0.14. *We can consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as $\mathbb{Q}(\sqrt{3})(\sqrt{2})$. Since $x^2 - 2$ is irreducible over $Q(\sqrt{3})$, the minimal polynomial of $\sqrt{2}$ over $Q(\sqrt{3})$ is $x^2 - 2$. Then $[\mathbb{Q}(\sqrt{3})(\sqrt{2}) : \mathbb{Q}(\sqrt{3})] = 2$ and $\{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{3})(\sqrt{2})$ over $\mathbb{Q}(\sqrt{3})$. Also $[\mathbb{Q}(\sqrt{3}), \mathbb{Q}] = 2$ and $\{1, \sqrt{3}\}$ is a basis of $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$. Thus, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$.*



Since $\{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{3})(\sqrt{2})$ over $\mathbb{Q}(\sqrt{3})$ and $\{1, \sqrt{3}\}$ is a basis of $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$, it follows that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. Thus $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$.

1 summary

- Let F/K be a field extension. Then $c \in F$ is called an algebraic element over K, if there is a nonconstant polynomial $f(x) \in K[x]$ such that $f(c) = 0$, i.e. if there exists $k_0, k_1, \cdots, k_n \in K$ not all zero such that

$$k_0 + k_1 c + \cdots + k_n c^n = 0.$$

  Otherwise c is called a transcendental element over K.

- A complex number α is called an algebraic number if α is an algebraic element over $\mathbb{Q}$ that is, if there is a nonconstant polynomial $f(x)$ with rational coefficients such that

$$f(\alpha) = 0.$$

  Otherwise $\alpha \in \mathbb{C}$ is called a transcendental number.

- Let F/K be a field extension of fields and $\alpha \in F$ be algebraic over K. Then there is a unique monic polynomial $m(x) \in K[x]$ of least degree such that $m(\alpha) = 0$.

- Let F/K be a field extension and $\alpha \in F$ algebraic over K. Then the unique monic polynomial $m(x) \in K[x]$ of least degree such that $m(\alpha) = 0$ is called the minimal polynomial of α over K.

  If $n = \deg m(x)$, then α is called algebraic of degree n over K.

- Let F/K be a field extension and $\alpha \in F$ algebraic over K. Then for every $f(x) \in K[x]$, $f(\alpha) = 0$ implies that $m(x) \mid f(x)$.

- Let F/K be a field extension and $\alpha \in F$ algebraic over K. Then $m(x) \in K[x]$ is the minimal polynomial of α over K if and only if it is a monic irreducible polynomial such that $m(\alpha) = 0$.

- Let F/K be a field extension and $\alpha \in F$. Then α is algebraic over K if and only if $K[\alpha] = K(\alpha)$. Moreover in this case, $K[\alpha] = K(\alpha) \simeq K[x]/ < m(x) >$.

- Let F/K be a field extension and $c \in F$. Then c is transcendental over K if and only if $K[c] \subsetneq K(c)$. In this case, $K[c] \simeq K[x]$ and $K(c) \simeq K(x)$.

- Let F/K be a field extension, $c \in F$ be algebraic over K and $m(x)$ be the minimal polynomial of c over K. If $\deg m(x) = n$, then $\{1, c, c^2, \cdots, c^{n-1}\}$ is a basis of $K(c)$ over K. Thus

$$[K(c) : K] = \deg m(x).$$