Abstract Algebra

Irreducible Polynomial and Simple Extensions

ThinkBS: Basic Sciences in Engineering Education

Kadir Has University, Turkey

Irreducible Polynomial

Let E be a field extension of F, and let $\alpha \in E$ be algebraic over F. Then $\{f(x) \in F[x] \mid f(\alpha) = 0\} =< p(x) >$ for some polynomial $p(x) \in F[x]$. Furthermore, $p(x)$ is irreducible over F.

As a corollary let E be an extension field of F, and let $\alpha \in E$ be algebraic over F. Then there is a unique irreducible polynomial $p(x) \in F[x]$ such that $p(x)$ is monic, $p(\alpha) = 0$, and for any polynomial $f(x) \in F[x]$ with $f(\alpha) = 0$, $p(x)$ divides $f(x)$.

Irreducible Polynomial

Let E be a field extension of a field F, and let $\alpha \in E$ be algebraic over F. The unique monic polynomial $p(x)$ discussed above is called the irreducible polynomial for α over F or the minimal polynomial for α over F, and it is denoted $irr(\alpha, F)$. The degree of the polynomial $irr(\alpha, F)$ is called the degree of α over F and this number is denote by $deg(\alpha, F)$.

Example 1: $irr(\sqrt{2}, \mathbb{Q}) = x^2|2$. (why?) $\sqrt{2}$ is algebraic over $\mathbb{Q}$ of degree 2.

Example 2: $irr(\sqrt{1+\sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2$. (why?) $\sqrt{1+\sqrt{3}}$ is algebraic over $\mathbb{Q}$ of degree 4.

Simple Extensions

Let E be an extension field of a field F, and let $\alpha \in E$. Let ϕ_α be the evaluation homomorphism of $F[x]$ into E with $\phi_\alpha(a) = a$ for $a \in F$ and $\phi_\alpha(x) = \alpha$. We consider two cases:

- Suppose α is algebraic over F. Then the kernel of ϕ_α is $< irr(\alpha, F) >$. Since $< irr(\alpha, F) >$ is a maximal ideal of $F[x]$, therefore, $F[x]/ < irr(\alpha, F) >$ is a field and is isomorphic to the image $\phi_\alpha(F[x])$ in E. This subfield is the smallest subfield of E containing F and α. We denote this field by $F(\alpha)$.
- Suppose α is transcendental over F. Then ϕ_α gives an isomorphism of $F[x]$ with a subdomain of E. Thus in this case $\phi_\alpha(F[x])$ is not a field but an integral domain that we denote by $F[a]$. Now, E contains a field of quotients of $F[a]$, which is thus the smallest subfield ofE containing F and α. As before, we also denote this field by $F(\alpha)$.

Example: Since π is transcendental over $\mathbb{Q}$, the field $\mathbb{Q}(\pi)$ is isomorphic to the field $\mathbb{Q}(x)$ of rational functions over $\mathbb{Q}$ in the indeterminate x. Thus from a structural viewpoint, an element that is transcendental over a field F behaves as though it were an indeterminate over F.

An extension field E of a field F will be called a simple extension of F if $E = F(\alpha)$ for some $\alpha \in E$.

Theorem: Let $E = F(\alpha)$ be a simple extension of a field F with α algebraic over F. Let $n = deg(\alpha, F)$. Then every $\beta \in F(\alpha)$ can be uniquely expressed in the form

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$$

with $b_i \in F$.

Let E be an extension field of F and let $\alpha \in E$ be algebraic over F. If $deg(\alpha, F) = n$, then $F(\alpha)$ is a vector space over F with dimension n and basis $\{a, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Furthermore, every element $\beta \in F(a)$ is algebraic over F and $deg(\beta, F) \leq deg(\alpha, F)$

Example: The polynomial $p(x) = x^2 + x + 1$ in $\mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$. (why?) We know that there is an extension field E of $\mathbb{Z}_2$ containing a zero α of $x^2 + x + 1$. This extension $\mathbb{Z}_2(\alpha)$ has as elements $0 + 0\alpha = 0$, $1 + 0\alpha = 1$, $0 + 1\alpha = \alpha$, and $1 + 1\alpha = 1 + \alpha$. This is a field with 4 elements, and for the multiplication one need to see that $\alpha^2 = -\alpha - 1 = \alpha + 1$. (why?)

$\mathbb{C}$ as an Extension of $\mathbb{R}$

We have seen before that $\mathbb{R}[x]/ < x^2 + 1 >$ is an extension field of $\mathbb{R}$. Consider

$$\alpha = x + < x^2 + 1 >$$

Then $\mathbb{R}(\alpha) = \mathbb{R}[x]/ < x^2 + 1 >$ and it consists of all elements of the form $a + b\alpha$ for $a, b \in \mathbb{R}$. But since $\alpha^2 + 1 = 0$, we see that α plays the role of $i \in \mathbb{C}$, and $a + b\alpha$ plays the role of $a + bi \in \mathbb{C}$. Hence, we can consider $\mathbb{C}$ as the extension field of $\mathbb{R}$:

$$\mathbb{C} \simeq \mathbb{R}(\alpha)$$

The number $i \in \mathbb{C}$ has minimal polynomial $x^2 + 1$ over $\mathbb{R}$ and $\mathbb{C} = \mathbb{R}(i)$. Thus for every complex number β, $deg(\beta, \mathbb{R}) \leq 2$. This implies that every complex number that is not a real number is a zero of some irreducible polynomial of degree two in $R[x]$.