Abstract Algebra

Root fields.

Definition Let K be a simple extension of a field F, then K is said to be a root field of an irreducible polynomial $f(x) \in F[x]$ if K Contains a root of $f(x)$.

For example The field $Q(\sqrt{2}) = \{a+\sqrt{2}b : a, b \in Q\}$ is a simple extension of Q and Contains a root $\sqrt{2}$ of an irreducible polynomial $f(x) = x^2 - 2$ over Q. Hence $Q(\sqrt{2})$ is the root field of the irreducible polynomial $x^2 - 2$ over the field Q.

For example: We Consider a polynomial

$$f(x) = x^2 - 2x + 2 \in Z_3[x].$$

Since $Z_3 = \{0, 1, 2\}$, so neither of the three elements $0, 1, 2$ is a root of $f(x) = 0$.

Thus $f(x)$ is an irreducible polynomial over the field Z_3.

If α be a root of $f(x)=0$, then

$$Z_3(\alpha) = \{a + b\alpha : a, b \in Z_3\}$$

is a simple extension of Z_3 and $Z_3(\alpha)$ is a finite field with 9 elements e.g.

$$0, 1, 2, \alpha, 2\alpha, 1+\alpha, 1+2\alpha, 2+\alpha, 2+2\alpha$$

Hence $Z_3(\alpha)$ is the root field of an irreducible polynomial $x^2 - 2x + 2$ over Z_3.

SPLITTING FIELD OR DECOMPOSITION FIELD

Definition Let K be an extension of a field F. Then K is said to be a splitting field of a polynomial $f x \in F[x]$ if it contains all its roots and there is no proper subfield of K which contains all the roots of $f(x)$.

OR

An extension K of a field F is said to be a splitting field of $f(x) \in F[x]$ if $f(x) \in K[x]$ is expressible as

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

where a is a non-zero element of F; $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$

$$K = F(\alpha_1, \alpha_2, \ldots \alpha_n).$$

Remark

(i) The splitting field of a polynomial is also sometimes referred to as its decomposition field.

(ii) There exists a decomposition field for every polynomial of positive degree over a field.

(iii) Decomposition fields are algebraic extensions.