Abstract Algebra

Theorem on Decomposition field

Theorem:- Decomposition fields are algebraic extensions.

Proof:- Let k be the decomposition field of a polynomial $f(x)$ over a field, and let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of $f(x)$, then we shall prove that k is algebraic extension of F.

Since $\alpha_1, \alpha_2, \dots, \alpha_n$ are the roots of $f(x) = 0$, then

$$k = F(\alpha_1, \alpha_2, \dots, \alpha_n)$$

we write

$$k_1 = F(\alpha_1)$$
$$k_2 = k_1(\alpha_2) = F(\alpha_1, \alpha_2)$$
$$k_3 = k_1(\alpha_3) = F(\alpha_1, \alpha_2, \alpha_3)$$
$$\dots\dots\dots$$
$$k = k_n = k_{n-1}(\alpha_n) = F(\alpha_1, \alpha_2, \dots \alpha_3)$$

But each of the elements $\alpha_1, \alpha_2, \dots, \alpha_n$ is the root of a non-zero polynomial over F, they $\alpha_1, \alpha_2, \dots, \alpha_n$ are all algebraic elements over F.

Since each of fields $F, k_1, k_2 \dots k_n = k$, is obtained on adjoining an algebraic element to its predecessor field extensions, so that each of the degrees

$$[k_1 : F], [k_2 : k_1], \dots, [k : k_{n-1}]$$

is finite, then by transivity of extension fields,

$$[K : F] = [k : k_{n-1}][k_{n-1} : k_{n-2}] \dots [k_2 - k_1] : [k_1 : F]$$

is finite. Thus k is finite extension of F.

But every finite extension is an algebraic extension. Hence K is an algebraic extension

UNIQUENESS OF DECOMPOSITION FIELD

It will now be shown that the decomposition field of any polynomial of positive degree is unique apart from isomorphism i.e. any two decomposition fields of a polynomial are the same.

In order to prove this result, we need to introduce the notion of continuation of isomorphic mappings.

F - ISOMORPHISM AND F- AUTOMORPHISM

Definition 1 :- Let K_1 and K_2 be any be any two extensions of a field F. Then an isomorphism $\sigma : K_1 \rightarrow K_2$ is said to be F-isomorphism, if $\sigma(a) = a \; \forall \; a \in F$.

Definition 2 :- Let K be an extension of a field F. Then an F-isomorphism $\sigma : K \rightarrow K$ is said to be F-automorphism.

Theorem :- If E is a splitting field of a polynomial $f(x) \in F[x]$ any isomorphism between subfields of E over F can be extended to an F-automorphism.

Proof :- Let K_1 and K_2 be any two subfield of E and suppose that $F \subset K_1 \subset E$ and $F \subset K_2 \subset E$. Also $K_1 \equiv K_2$.

The polynomial $f(x)$ may be considered to have coefficients in either K_1 or K_2 and let $f^*(x)$ be the polynomial whose coefficients in K_2 correspond by the isomorphism to those of $f(x)$ in K_1. Then E is a splitting field of $f(x)$ over K_1 as well as a splitting field of $f^*(x)$ over K_2. Hence the isomorphism between K_1 and K_2 can be extended to an F- automorphism of E.