

Splitting field or Decomposition field

If $f(x) \in F[x]$, a finite extension E of F is said to be a splitting field over F if over E , but not in over any proper subfield of E , $f(x)$ can be factorised as a product of linear factors.

The field F is called base field or initial field.

Thm: There exists a splitting field for every $f(x) \in F[x]$

Proof: Let $f(x) \in F[x]$ be of degree n . First we will prove that there exists a finite extension E of F of degree at most $n!$ in which $f(x)$ has n roots.

We shall prove this by method of induction on n , the degree of $f(x)$.

Let $f(x) \in F[x]$ be of degree 1.

i.e. let $f(x) = a_0x + a_1$, where $a_0, a_1 \in F$, $a_0 \neq 0$

Now F is itself an extension of F and $[F:F] = 1$.

also $-\frac{a_1}{a_0} \in F$ is a root of $a_0x + a_1$.

Thus if $\deg f(x) = 1$, then there is a finite extension F of F of degree at most $1! = 1$ in which $f(x)$ has 1 root.

Let us assume that theorem is true for any field for all polynomials of degree less than n . Let $f(x)$ be a polynomial of

degree n over a field F . We know that there exists an extension E_0 of F with $[E_0:F] \leq n$ in which $f(x)$ has a root, say α . By factor theorem in $E_0[x]$, $f(x)$ factors as

$$f(x) = (x - \alpha)q(x)$$

where degree of $q(x) = \deg f(x) - 1 = n - 1$

Now $q(x)$ is polynomial over E_0 of degree $n - 1$

So by induction hypothesis there is an extension E of E_0 of degree at most $(n - 1)!$ in which $q(x)$ has $n - 1$ roots. Since any root of $f(x)$ is either α or roots of $q(x)$, therefore we obtain in E , all n roots of $f(x)$.

Now E is extension of E_0 and E_0 is an extension of F , so E is an extension of F . We have

$$[E:F] = [E:E_0][E_0:F]$$

$$\leq (n - 1) \cdot n = n!$$

Thus E is finite extension of F of degree at most $n!$ in which $f(x)$ has n roots.

Now the main proof

Let $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$, $a_0 \neq 0$

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be n roots in E of $f(x)$. Then by factor theorem.

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

So $f(x)$ splits up completely over E as a product of first degree factors. Thus we see that there exists a finite extension E of F which decomposes $f(x)$ as a product of linear factors. Consequently a finite extension of F of minimum degree which also possesses this property.

This minimal extension will be a splitting field for $f(x)$ because no proper subfield of this minimal extension can split $f(x)$ as a product of linear factors.

Another defⁿ of splitting field

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

$$f(x) = a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$

where $a_0 \in F$ & $\alpha_1, \alpha_2, \dots, \alpha_n \in E$

$$\& E = F(\alpha_1, \alpha_2, \dots, \alpha_n).$$