Fixed Fields

Let K and L be two fields. $\sigma_1, \dots, \sigma_n$ be field homomorphisms $K \to L$.

$a \in K$ is fixed by $\sigma_1, \dots, \sigma_n$ if $\sigma_1(a) = \dots = \sigma_n(a)$. Set of all such elements be F. It turns out that F is a subfield of K. F is called the fixed field of K.

$\boxed{F = K^S}$ where $S = \{\sigma_1, \dots, \sigma_n\}$

$F = \{a \in K \mid \sigma_1(a) = \dots = \sigma_n(a)\} \subseteq K$.

Let K be any field and $\sigma_1, \dots, \sigma_n : K \to K$ be distinct field automorphisms (isomorphisms from K to K). Suppose $\{\sigma_1, \dots, \sigma_n\}$ forms a group under composition. If F is a fixed field of $\sigma_1, \dots, \sigma_n$, then $[K:F] = n$

Proof/ Remember, the first theorem of fixed fields: $[K:F] \geq n$.

Suppose $[K:F] > n$. We will choose $\alpha_1, \dots, \alpha_{n+1} \in K$ which are linearly independent over F. (so $\alpha_i \neq 0$)

Consider the following system of homogeneous linear equations

$$\begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_{n+1}) \\ \vdots & & \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_{n+1}) \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_{n+1} \end{bmatrix} = 0.$$

$$\text{or } A_{n\times(n+1)} \; X_{(n+1)\times 1} = 0.$$

Since the number of variables is greater than the number of equations, there exists atleast one nontrivial solution. We will choose a non trivial solution with the least number of non-zero coordinates

$(\beta_1, \dots, \beta_r, 0, \dots, 0)$ where $\beta_1, \dots, \beta_r \neq 0$

and $r \geq 1$.

If $r = 1$, then $\sigma_1(\alpha_1) \cdot \beta_1 = 0$

$\alpha_1 \neq 0 \Rightarrow \sigma_1(\alpha_1) \neq 0$

$\Rightarrow \beta_1 = 0$ which cant be.

Now lets assume $r \geq 2$.

$$\beta_1 \cdot \sigma_1(\alpha_1) + \cdots + \beta_r \sigma_1(\alpha_r) = 0.$$

$$\Rightarrow \beta_1 \beta_r^{-1} \sigma_1(\alpha_1) + \cdots + \sigma_1(\alpha_r) = 0$$

$$\Rightarrow \beta_1 \sigma_1(\alpha_1) + \cdots + \sigma_1(\alpha_r) = 0 \text{ by absorbing } \beta_r^{-1}. \quad (1)$$

Similarly we will get

$$\beta_1 \sigma_n(\alpha_1) + \cdots + \sigma_n(\alpha_r) = 0$$

In the group $\{\sigma_1, \ldots, \sigma_n\}$ under composition, let the identity element be σ_{id}.

When $\sigma_{id} = \sigma_1$, then (1) looks like

$$\beta_1 \alpha_1 + \cdots + \alpha_r = 0.$$

That looks like a non trivial linear relation between the α's, when all the β's are in F. So $\beta_i \notin F$ for all $i = \{1, \ldots, n\}$.

Let $\beta_1 \notin F$

$\Rightarrow \beta_1 \in K \setminus F$

$\Rightarrow \exists\, K$ such that $\sigma_K(\beta_1) \neq \beta_1$

Now, $\beta_1 \sigma_j(\alpha_1) + \cdots + \beta_{r-1}\sigma_j(\alpha_{r-1}) + \sigma_j(\alpha_r) = 0$
$\forall\, 1 \leq j \leq n$

$\Rightarrow \sigma_K\Big(\beta_1\sigma_j(\alpha_1) + \cdots + \sigma_j(\alpha_r)\Big) = 0$

$\Rightarrow \sigma_K(\beta_1)\cdot(\sigma_K\sigma_j)(\alpha_1) + \cdots + (\sigma_K\sigma_j)(\alpha_r) = 0$

Notice that $\{\sigma_K\sigma_1, \ldots, \sigma_K\sigma_n\}$ is a permutation of the group $\{\sigma_1, \ldots, \sigma_n\}$.

$\Rightarrow \sigma_K(\beta_1)\cdot\sigma_i(\alpha_1) + \cdots + \sigma_i(\alpha_r) = 0 \;\forall\, 1 \leq i \leq n.$

$\Rightarrow \{\beta_1 - \sigma_K(\beta_1)\}\cdot\sigma_i(\alpha_1) + \cdots + \{\beta_{r-1} - \sigma_K(\beta_{r-1})\}\sigma_i(\alpha_{r-1})$
$= 0$

We have found a new solution for the original system of equations original system of equations

$$\left(\beta_1 - \sigma_K(\beta_1), \ldots, \beta_{r-1} - \sigma_K(\beta_{r-1}), 0, \ldots, 0\right).$$

Here $\beta_1 - \sigma_K(\beta_1) \neq 0$. So the solution is non-trivial with atleast $(r-1)$ β's $\neq 0$. This is contradictory. Thus $[K:F] = n$.