HW due Apr 16

Tao Ju

April 16, 2014

Problem 31
Suppose that E is a splitting field over F and $p \in F[x]$ splits in E as $p(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where $\alpha_i \neq \alpha_j$ whenever $i \neq j$. Prove that the following are equivalent:
(1) p is irreducible.
(2) for any i, j there is $\sigma \in \text{aut}(E|F)$ such $\sigma(\alpha_i) = \alpha_j$.

Proof:
(1) $\Rightarrow$ (2):
Assume α_i, α_j are roots of $p(x)$ in E. Since $p(x) \in F[x]$ is irreducible, by Thm 34, $F(\alpha_i)$ and $F(\alpha_j)$ are isomorphic via an isomorphism ρ which fixes F. Since E is a splitting field over F and $F \subset F(\alpha_i) \subset E$, $F \subset F(\alpha_j) \subset E$, by Extension Lemma, ρ extends to $\sigma : E \to E$ an automorphism, so $\sigma \in \text{aut}(E|F)$.

(2) $\Rightarrow$ (1):
Suppose $p(x)$ can be decomposed into $f(x)g(x)$ where $f(x), g(x) \in F[x]$ and $\deg f, \deg g \geq 1$. Without loss of generality, we may assume $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k) = x^k + a_1x^{k-1} + \cdots + a_k$ where $a_i \in F$ for all i and $1 \leq k \leq n-1$. By our assumption, there is $\sigma \in \text{aut}(E|F)$ such $\sigma(\alpha_1) = \alpha_n$. So $\sigma(f(\alpha_1)) = \sigma(0) = 0$. On the other hand, $\sigma(f(\alpha_1)) = \sigma(\alpha_1^k + a_1\alpha_1^{k-1} + \cdots + a_k) = \sigma(\alpha_1)^k + a_1\sigma(\alpha_1)^{k-1} + \cdots + a_k = f(\alpha_n) \neq 0$, contradiction. Therefore p is irreducible.