Intro to Algebra 2 W4-2

fat

March 15, 2024

Definition 1. If K/F is an algebraic extension such that K is the splitting field for a collection of polynomials in $F[x]$, then we say K is a **normal extension**. (Equivalently, given an irreducible $f(x) \in F[x]$, if $f(x)$ has a root α in K, then $f(x)$ splits completely in $K[x]$.)

We next show that any 2 splitting fields for $f(x) \in F[x]$ are isomorphic, so it makes sense to speak of ”the” splitting field for $f(x)$. We first prove a lemma.

Theorem 1 (Theorem 8)**.** Assume that $F \overset{\phi}{\simeq} F'$. Let $p(x)$ be a irreducible polynomial in $F[x]$ and $p'(x) = \phi(p(x))$. (Here $\phi(a_n x^n + \cdots + a_0) := \phi(a_n)x^n + \cdots + \phi(a_0))$ Let α be a root of $p(x)$ in some extension field of F, same for α' for $p'(x)$ in some F'. Then $\exists \tilde{\phi} : F(\alpha) \to F'(\alpha)$ an isomorphism such that $\tilde{\phi}|_F = \phi$ (i.e. $\tilde{\phi}(a) = \phi(a)\ \forall a \in F$). (That is, ϕ can be extended to an isomorphism $\tilde{\phi}$ from $F(\alpha)$ to $F'(\alpha)$ such that $\tilde{\phi}(\alpha) = \alpha'$.)

Proof.

It's clear that ϕ induces an isomorphism from $F[x]/(p(x))$ to $F'[x]/(p'(x))$. (Consider the ring homomorphism $F[x] \to F'[x]/(p'(x))$ defined by $f(x) \mapsto \phi(f(x)) + (p'(x))$. Check it's surjective with $\ker = (p(x))$.) On the other hand, theorem 4+6 says $F(\alpha) \simeq F[x]/(m_{\alpha,F}(x)) = F[x]/(p(x))$. Similarly $F'(\alpha') \simeq F'[x]/(p'(x))$. Combining every isomorphism, we see that $\exists$ an isomorphism $\tilde{\phi} : F(\alpha) \to F'(\alpha')$. Tracing the images of F and α under $\tilde{\phi}$, we see that $\tilde{\phi}|_F = \phi$ and $\tilde{\phi}(\alpha) = \alpha'$. e.g.

$$F(\alpha) \to F[x]/(p(x)) \to F'[x]/(p(x)) \to F'[x]/(p'(x)) \to F'(\alpha')$$

$$a \in F \to a + (p(x)) \mapsto \phi(a) + (p'(x)) \to \phi(a)$$

$$\alpha \to x + (p(x)) \mapsto \phi(x) + (p'(x)) = x + (p'(x))$$

□

Theorem 2 (Theorem 27)**.** Assume that $F \overset{\phi}{\simeq} F'$. Let $f(x) \in F[x]$ and $f'(x) = \phi(f(x))$. Let E be a splitting field for $f(x)$, E' be a splitting field for $f'(x)$. Then $\exists$ an isomorphism $\tilde{\phi} : E \to E'$ such that $\tilde{\phi}|_F = \phi$.

Proof.

We'll prove by induction on $n = \deg f(x)$. The case $n = 1$ is clear. Assume that the statement holds up to $\deg = n - 1$. Let $F(x)$ be a polynomial of $\deg n$ in $F[x]$. Let $g(x)$ be an irreducible factor of $f(x)$ in $F[x]$. Let

α be a root of $g(x)$ in E, α' be a root of $g'(x) = \phi(g(x))$ in E'. Let $E_1 = F(\alpha), E_1' = F'(\alpha')$. By theorem 8, ϕ can be extended to an isomorphism $\phi_1 : E_1 \to E_1'$ such that $\phi_1|_F = \phi, \phi_1(\alpha) = \alpha'$. Now we have

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

for some $h(x) \in E_1[x]$ ($\alpha \in E_1$).

$$f'(x) = (x - \alpha')h'(x) \cdots (1)$$

for some $h'(x) \in E_1'[x]$ ($\alpha' \in E_1'$). Now consider $\phi_1(f(x))$. We have $\phi_1(f(x)) = \phi(f(x)) = f'(x) \cdots (2)$ since $f(x) \in F[x]$ and $\phi_1|_F = \phi$. On the other hand

$$\phi_1(f(x)) = \phi_1(x - \alpha)\phi_1(h(x)) = (x - \alpha')\phi_1(h(x)) \cdots (3)$$

Comparing (1), (2), (3), we see that

$$h'(x) = \phi_1(h(x))$$

Now $\deg h(x) = n - 1 = \deg h'(x)$ and E is a splitting field for $h(x)$, E' is a splitting field for $h'(x)$. By the induction hypothesis, ϕ_1 can be extended to an isomorphism $\tilde{\phi} : E \to E'$ such that $\tilde{\phi}_{E_1} = \phi_1$. Then $\tilde{\phi}_F = \phi_1|_F = \phi$. $\square$

Corollary 1 (Corollary 28)**.** If E, E' are 2 splitting fields for $f(x) \in F[x]$, then $\exists$ an isomorphism $\phi : E \to E'$ such that $\phi(a) = a \; \forall a \in F$.