

Frank Moore
Algebra 901 Notes
Professor: Tom Marley

Theorem: Let F be a field and $f(x) \in F[x]$ be a non-constant polynomial. Then there exists a splitting field for $f(x)$ over F .

Proof: Induction on n , the degree of f . Let $g(x)$ be an irreducible factor of $f(x)$. So $g(t)$ is irreducible in $F[t]$. Therefore, $F[t]/(g(t))$ is a field, as $(g(t))$ is a maximal ideal in $F[t]$. Consider the field homomorphism $\phi : F \rightarrow F[t] \rightarrow F[t]/(g(t))$. Since $\phi(a) \neq \bar{0}$ in $F[t]/(g(t))$ for all $a \neq 0$, it is clear that ϕ is injective. Let $L = F[t]/(g(t)) = \{h(t) + (g(t)) \mid h \in F[t]\}$. Then $\phi : F \rightarrow L$ sends a to $a + (g(t)) = \bar{a}$. Since $F \cong \phi(F)$, we can identify F with its image in L , and assume that $F \subset L$. Let $\alpha = t + (g(t)) = \bar{t}$. Then

$$\begin{aligned} L &= \{a_0 + a_1t + \cdots + a_nt^n + (g(t)) \mid a_i \in F\} \\ &= \{(a_0 + (g)) + (a_1 + (g))(t + (g)) + \cdots + (a_n + (g))(t + (g))^n \mid a_i \in F\} \\ &= \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid a_i \in F\} \end{aligned}$$

Note that $g(\alpha) = g(\bar{t}) = g(\bar{t}) = \bar{0}$, since $g(t) \in (g(t))$. Therefore, α is a root of $g(x)$. So $g(x)$ has a root in L , so $f(x)$ has a root also. Therefore, $f(x) = (x - \alpha)h(x)$ for some $h(x) \in L[x]$. Note that $\deg h(x) = n - 1$. By induction, $h(x) \in L[x]$ has a splitting field E containing L . Therefore $f(x)$ splits completely in E . So, let $\alpha_1, \dots, \alpha_n$ be the roots of $f(x)$ in E . Then $F(\alpha_1, \dots, \alpha_n)$ is a splitting field for $f(x)$ over F .

Example: Find a splitting field and its degree of $f(x) = x^3 + x + 1$ in $\mathbb{Z}_2[x]$.

Solution: As $\deg f = 3$ and has no roots in \mathbb{Z}_2 , it is irreducible in $\mathbb{Z}_2[x]$. We let $L = \mathbb{Z}_2[t]/(t^3 + t + 1) = \mathbb{Z}_2(\alpha)$ where $\alpha = t + (t^3 + t + 1)$, i.e. $\alpha^3 + \alpha + 1 = 0$. In L , $x^3 + x + 1 = (x - \alpha)h(x)$ for some $h(x) \in L[x]$ with $\deg h = 2$. Does h factor in L or is it irreducible? Lets try and find h . Using long division and the relation $\alpha^3 + \alpha + 1 = 0$, you get that $h(x) = x^2 + \alpha x + (1 + \alpha^2)$. Also, note that $h(\alpha^2) = 0$ so that h splits in L . Therefore L is the splitting field for $x^3 + x + 1$ and $[L : \mathbb{Z}_2] = 3$.

Definition: Let E/F and E'/F' be field extensions. Suppose that $\sigma : F \rightarrow F'$ is an injective field hom. Then a field map $\tau : E \rightarrow E'$ is said **to extend** σ if $\tau|_F = \sigma$. For the following important special case, take $F = F'$ and $\sigma = \text{Id}_F$. Then τ extends Id_F if and only if τ fixes F (i.e. $\tau(a) = a$ for all $a \in F$).

Remark: Suppose $\sigma : F \rightarrow F'$ is a field isomorphism. Define

$$\begin{aligned} \tilde{\sigma} : F[x] &\rightarrow F'[x] \\ a_0 + a_1x + \cdots + a_nx^n &\mapsto \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \\ f(x) &\mapsto f^\sigma(x) \end{aligned}$$

Then $\tilde{\sigma}$ is a ring isomorphism, which is clear since σ is a field isomorphism.

Let $f(x) \in F[x]$. Then f is irreducible in $F[x] \Leftrightarrow f^\sigma$ is irreducible in $F'[x]$. Also, $\tilde{\sigma}((f(x))) = (f^\sigma(x))$. Therefore, we have that

$$\begin{aligned} \bar{\sigma} : F[x]/(f(x)) &\rightarrow F'[x]/(f^\sigma(x)) \\ g(x) + (f(x)) &\mapsto g^\sigma + (f^\sigma(x)) \end{aligned}$$

is a field isomorphism and furthermore, $\bar{\sigma}$ extends σ , as is clear by the definition of $\bar{\sigma}$.

Theorem: Let $\sigma : F \rightarrow F'$ be a field isomorphism, and let $f(x) \in F[x]$ be a nonconstant polynomial. Let E and E' be splitting fields for f and f^σ . Then there exists a $\tau : E \rightarrow E'$ which is an isomorphism of fields extending σ .

Proof: Let $n = \deg f$. If $n = 1$ then $E = F$ and $E' = F'$ so let $\tau = \sigma$. Suppose that $n > 1$. If $f(x)$ splits in F , then as above, $\tau = \sigma$. Let $p(x)$ be a monic nonlinear irreducible factor of $f(x)$. Then p^σ is a monic nonlinear irreducible factor of $f^\sigma(x)$. So, as f splits in E , p splits in E , so let α be a root of $p(x)$ in E and let $\beta \in E'$ be a root of $p^\sigma(x)$. Therefore, we have that $p(x) = \text{Irr}(\alpha, F)$ and $p^\sigma(x) = \text{Irr}(\beta, F')$. So, $F(\alpha) \cong F[x]/(p(x))$ and $F'(\beta) \cong F'[x]/(p^\sigma(x))$.

$$\phi : F[x]/(p(x)) \rightarrow F'[x]/(p^\sigma(x))$$

$$g + (p) \mapsto g^\sigma + (p^\sigma)$$

be the field isomorphism of the remark. Let π be the composition of the following maps (π is an isomorphism as each piece is):

$$F(\alpha) \rightarrow F[x]/(p(x)) \rightarrow F'[x]/(p^\sigma(x)) \rightarrow F'(\beta)$$

Then for $a \in F$, we have

$$a \mapsto a + (p) \mapsto \sigma(a) + (p^\sigma) \mapsto \sigma(a)$$

so that π extends σ . Now we have an isomorphism $\pi : F(\alpha) \rightarrow F'(\beta)$ which extends σ . Now we have the following diagram:

$$\begin{array}{ccc} E & \xrightarrow{\tau} & E' \\ \downarrow & & \downarrow \\ F(\alpha) & \xrightarrow{\pi} & F'(\beta) \\ \downarrow & & \downarrow \\ F & \xrightarrow{\sigma} & F' \end{array}$$

Write $f(x) = (x - \alpha)h(x)$, $h(x) \in F(\alpha)[x]$. Note that $\deg h = n - 1$. Notice that E is the splitting field for $h(x)$ over $F(\alpha)$ so by induction, we have that there exists a $\tau : E \rightarrow E'$ extending π , and hence extending σ also.

Corollary: Let E, E' be splitting fields for $f(x)$ in $F[x]$. Then there exists an isomorphism $\tau : E \rightarrow E'$ fixing F . For the proof, take $\sigma = \text{Id}_F$ and extend it to $\tau : E \rightarrow E'$.

Definition: Let S be a set. A relation \leq is called a partial order if for all $r, s, t \in S$ we have

1. $r \leq r$ (reflexive)
2. $r \leq s$ and $s \leq t$ implies that $r \leq t$ (transitive)
3. $r \leq s$ and $s \leq r$ implies that $r = s$ (antisymmetric)

We say that \leq is a total order on S if it is a partial order and for all $s, t \in S$ we have that $s \leq t$ or $t \leq s$. For example, \leq in the usual sense is a total ordering on R . As another example, let S be a nonempty set and $\mathcal{P}(S)$ be the powerset of S . Then inclusion is a partial order on $\mathcal{P}(S)$.

Definition: Let S be a poset and let $A \subset S$. Then an element $b \in S$ is said to be an upper bound for A if $a \leq b$ for all $a \in A$. An element $m \in S$ is called **maximal** if whenever $m \leq s$ for $s \in S$, we have that $m = s$.

Zorn's Lemma: Let $S \neq \emptyset$ be a poset and suppose every totally ordered subset of S has an upper bound in S . Then S has a maximal element. Note that this statement is equivalent to the axiom of choice. As an example of how to use this lemma, consider the following:

Proposition: Let V be a vector space over a field F and let S be a linearly independent subset of V . Then there exists a basis β of V containing S .

Proof: Let $\Lambda = \{T \mid S \subseteq$