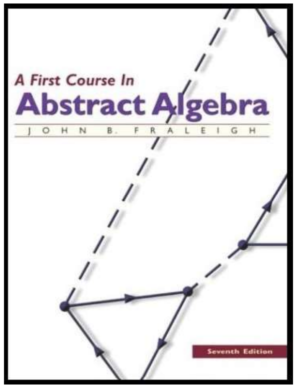
Introduction to Modern Algebra

Part X. Automorphisms and Galois Theory

X.49. The Isomorphism Extension Theorem



Theorem 49.3

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof. Consider all pairs (L, λ) where L is a field such that $F \leq L \leq E$ and λ is an isomorphism of L onto a subfield of $\bar{F}'$ such that $\lambda(a) = \sigma(a)$ for all $a \in F$. Let S be the set of all such pairs. S is nonempty since $(F, \sigma) \in S$. Define $\leq$ on S as $(L_1, \lambda_1) \leq (L_2, \lambda_2)$ if $L_1 \leq L_2$ and $\lambda_1(a)\lambda_2(a)$ for all $a \in L_1$ (in which case λ_2 extends λ_1 from L_1 to L_2).

Theorem 49.3 (continued 1)

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof (continued). Claim $\leq$ is a partial ordering of S.
For any $(L, \lambda) \in S$ we have $L \leq L$ and $\lambda(a) = \sigma(a)$ for all $a \in F \leq L$, so $(L, \lambda) \leq (L, \lambda)$ and $\leq$ is reflexive. If $(L_1, \lambda_1) \leq (L_2, \lambda_2)$ and $(L_2, \lambda_2) \leq (L_1, \lambda_1)$ then $L_1 \leq L_2$ and $L_2 \leq L_1$, so $L_1 = L_2$. Also, $\lambda_1(a) = \lambda_2(a)$ for all $a \in F$. So $(L_1, \lambda_1) = (L_2, \lambda_2)$ and $\leq$ is antisymmetric.
Suppose $(L_1, \lambda_1) \leq (L_2, \lambda_2)$ and $(L_2, \lambda_2) \leq (L_3, \lambda_3)$. Then $L_1 \leq L_2 \leq L_3$ and so $L_1 \leq L_3$. Also, $\lambda_1(a) = \lambda_2(a) = \lambda_3(a)$ for all $a \in F$. So $(L_1, \lambda_1) \leq (L_3, \lambda_3)$ and $\leq$ is transitive.

Theorem 49.3 (continued 2)

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof (continued). Let $T = \{(H_i, \lambda_i) \mid i \in I\}$ be a chain in S. Claim $H = \bigcup_{i \in I} H_i$ is a subfield of E.
Let $a, b \in H$ where $a \in H_i$ and $b \in H_j$. Then either $H_i \leq H_j$ or $H_j \leq H_i$ since T is a chain (definition of "chain"). WLOG, say $H_i \leq H_j$ then $a, b \in H_j$, so $a \pm b$, ab, and a/b for $b \neq 0$ are in H_j since H_j is a field. Since $H_j \subseteq H$, then $a \pm b$, ab, $a/b \in H$. Therefore, H is a field. Since for each $i \in I$ we have $F \subseteq H_i \subseteq E$ then $F \subseteq H \subseteq E$. So H is a subfield of E.

Theorem 49.3. (continued 3)

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof (continued). Define $\lambda : H \to \bar{F}'$ as $\lambda(c) = \lambda_i(c)$ for each $c \in H$ where $c \in H_i$. We need to show that λ is well defined (and hence independent of the choice of H_i). Notice that if $c \in H_i$ and $c \in H_j$ then either $(H_i, \lambda_i) \le (H_j, \lambda_j)$ or $(H_j, \lambda_j) \le (H_i, \lambda_i)$ since T is a chain. In either case $\lambda_i(c) = \lambda_j(c)$ and so $\lambda(c)$ is well defined.

Theorem 49.3 (continued 4)

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof (continued). Claim $\lambda : H \to \bar{F}'$ is an isomorphism of H onto a subfield $\lambda[H]$ of $\bar{F}'$. If $a, b \in H$ then there is (as above) an H_j such that $a, b \in H_j$ and

$$\begin{aligned} \lambda(a+b) = \lambda_j(a+b) &= \lambda_j(a) + \lambda(b) \text{ since } \lambda_j \text{ is an isomorphism} \\ &= \lambda(a) + \lambda(b) \\ \lambda(ab) = \lambda_j(ab) &= \lambda_j(a)\lambda(b) \text{ since} \lambda_j \text{ is an isomorphism} \\ &= \lambda(a)\lambda(b) \end{aligned} \quad (1)$$

So λ has the homomorphism property with respect to addition and multiplication.

Theorem 49.3 (continued 5)

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof (continued). Next, if $\lambda(a) = 0$ for $a \in H$, then $a \in H_i$ for some $i \in I$ and so $\lambda_i(a) = \lambda(a) = 0$ implies that $a = 0$ since λ_i is an isomorphism and hence one to one (by Corollary 13.18). Therefore (by Corollary 13.18) $Ker(\lambda) = 0$ and λ is onto $\lambda[H]$ and therefore λ is an isomorphism with $\lambda[H]$ a subfield of $\bar{F}'$.
Since each λ_i fixes F, then λ fixes F. So $(H, \lambda) \in S$. By construction (since $H_i \subseteq H$ for all $i \in I$), (H, λ) is an upper bound for chain T. Since T was an arbitrary chain, then every chain in S has an upper bound in S. So S satisfies the hypotheses of Zorn's Lemma.

Theorem 49.3 (continued 6)

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof. (Continued) Applying Zorn's Lemma, there is a maximal element of S, say (K, τ). Denote $\tau[K]$ as K' and so $K' \le \bar{F}'$. ASSUME $K \ne E$. Let $\alpha \in E/K$. Since E is an algebraic extension of F, α is algebraic over K. Let $p(x) = \text{irr}(\alpha, K)$. Consider the evaluation homomorphism $\varphi_\alpha : K[x] \to K(\alpha)$ (so the symbol x is simply replaced by α; see Theorem 22.4, "The Evaluation Homomorphisms for Field Theory").

Theorem 49.3 (continued 7)

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof (continued). Let ψ_α be the canonical isomorphism mapping $K[x]/\langle p(x)\rangle$ onto $K(\alpha)$ which corresponds to φ_α. The elements of $K[x]/\langle p(x)\rangle$ are cosets of $\langle p(x)\rangle$, say of the form $r(x) + \langle p(x)\rangle$. Since $p(\alpha) = 0$, then $\psi_\alpha(r(x) + \langle p(x)\rangle) = r(\alpha) \in K(\alpha)$. Notice that ψ_α is one to one since it maps cosets to elements of $K(\alpha)$ (whereas φ_α is not one to one; it maps elements from the same cosets of $\langle p(x)\rangle$ onto the same element of $K(\alpha)$).

Theorem 49.3 (continued 8)

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof (continued). If $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, consider $q(x) = \tau(a_0) + \tau(a_1)x + \tau(a_2)x^2 + \cdots + \tau(a_n)x^n \in K'[x] = \tau[K][x]$ where τ is from the maximal element (K, τ) of S. Since τ is an isomorphism, $q(x)$ is irreducible in $K'[x]$. Since $K' \leq \bar{F}'$, there is a zero α' of $q(x)$ in $\bar{F}'$. Similar to above, let $\psi_{\alpha'} : K'[x]/\langle q(x)\rangle \to K'(\alpha')$. Finally, let $\bar{\tau} : K[x]/\langle p(x)\rangle \to K'[x]/\langle q(x)\rangle$ be an isomorphism "extending" τ from K to $K[x]/\langle p(x)\rangle$ (since $K \cong K'$ and τ "maps" $p(x) \in K[x]$ to $q(x) \in K'[x]$, then such an isomorphic relation exists). We have $\bar{\tau}(x + \langle p(x)\rangle) = x + \langle q(x)\rangle$, for example.

Theorem 49.3 (continued 9)

Theorem 49.3. Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Let $\bar{F}'$ be an algebraic closure of F'. Then σ can be extended to an isomorphism τ of E onto a subfield $\bar{F}'$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.

Proof (continued). Then $\psi_{\alpha'}\bar{\tau}\psi_\alpha^{-1} : K(\alpha) \to K'(\alpha')$ is an isomorphism of $K(\alpha)$ onto a subfield $K'(\alpha')$ of $\bar{F}'$, since $K \leq K(\alpha)$ and $\psi_{\alpha'}\bar{\tau}\psi_\alpha^{-1}$ "extends" τ from K (and so $\psi_{\alpha'}\bar{\tau}\psi_\alpha^{-1}(a) = \tau(a) = \sigma(a)$ for all $a \in F$). So $(K, \tau) < (K(\alpha), \psi_{\alpha'}\tau\psi_\alpha^{-1})$, which is a contradiction to the maximality of (K, τ). Therefore the assumption that $K \neq E$ is false and $K = E$. So τ is an isomorphism of $E = K$ onto a subfield $\tau(E) = \tau(K)$ of $\bar{F}'$ such that $\tau(a) = \sigma(a)$ on F, and the result follows. □

Theorem 49.7

Theorem 49.7. Let E be a finite extension of field F. Let σ be an isomorphism of F onto a field F', and let $\bar{F}'$ be an algebraic closure of F'. Then the number of extensions of σ to an isomorphism τ of E onto a subfield of $\bar{F}'$ is finite, and independent of F', $\bar{F}'$, and σ. That is, the number of extensions is completely determined by the two fields E and F.

Proof. Consider two isomorphisms $\sigma_1 : F \to F_1'$ and $\sigma_2 : F \to F_2'$ and let $\bar{F_1}'$ and $\bar{F_2}'$ be the algebraic closures of F_1' and F_2' respectively. Then $\sigma_2\sigma_1^{-1} : F_1' \to F_2'$ is an isomorphism. By Corollary 49.5, since $F_1' \cong F_2'$, then $\bar{F}_1' \cong \bar{F}_2'$ and by the Isomorphism Extension Theorem (Theorem 49.3) there is an isomorphism $\lambda : \bar{F}_1' \to \bar{F}_2'$ which extends the isomorphism $\sigma_2\sigma_1^{-1} : F_1' \to F_2'$. Also by the Isomorphism Extension Theorem (Since E is an extension field of F) there are isomorphisms τ_1 extending σ_1 such that $\tau_1 : E \to \tau_1[E] \subset \bar{F_1}'$.

Theorem 49.7 (continued 1)

Theorem 49.7. Let E be a finite extension of field F. Let σ be an isomorphism of F onto a field F', and let $\bar{F}'$ be an algebraic closure of F'. Then the number of extensions of σ to an isomorphism τ of E onto a subfield of $\bar{F}'$ is finite, and independent of F', $\bar{F}'$, and σ. That is, the number of extensions is completely determined by the two fields E and F.

Proof (continued). Now for each such τ_1 we can define $\tau_2 = \lambda\tau_1$ where $\tau_2 : E \to \tau_2[E] \subset \bar{F_2}'$.
Since λ extends $\sigma_2\sigma_1^{-1}$ and τ_1 extends σ_1, then $\tau_2 = \lambda\tau_1$ extends σ_2. Similarly, we could have defined τ_1 in terms of τ_2 as $\tau_1 = \lambda^{-1}\tau_2$. So for each $\tau_1 : E \to \tau_1[E] \subseteq \bar{F_1}'$ there is a $\tau_2 : E \to \tau_2[E] \subseteq \bar{F_2}'$, and conversely. So there is a one to one correspondence between such τ_1 and τ_2, independent of F' and $\bar{F}'$. So the number of extensions of σ to an isomorphism τ of E onto a subfield of $\bar{F}'$ is independent of F', $\bar{F}'$, and σ.

Theorem 49.7 (continued 2)

Theorem 49.7. Let E be a finite extension of field F. Let σ be an isomorphism of F onto a field F', and let $\bar{F}'$ be an algebraic closure of F'. Then the number of extensions of σ to an isomorphism τ of E onto a subfield of $\bar{F}'$ is finite, and independent of F', $\bar{F}'$, and σ. That is, the number of extensions is completely determined by the two fields E and F.

Proof (continued). We now show that the number of extensions of σ is finite. Since E is a finite extension of F, then $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$ for some $\alpha_1, \alpha_2, ..., \alpha_n$ in E, by Theorem 31.11.
For $\alpha_i \in \{\alpha_1, \alpha_2, ..., \alpha_n\}$, let $irr(\alpha_i, F) = a_{i0} + a_{i1}x + a_{i2}x^2 + ... + a_{im_i}x^{m_i}$ where $a_{ik} \in F$. Then
$a_{i0} + a_{i1}(\alpha_i) + a_{i2}(\alpha_i)^2 + ... + a_{im_i}(\alpha_i)^{m_i} = 0$ and so
$\tau(a_{i0} + a_{i1}(\alpha_i) + a_{i2}(\alpha_i)^2 + ... + a_{im_i}(\alpha_i)^{m_i}) = \tau(0)$ or
$\tau(a_{i0}) + \tau(a_{i1})\tau((\alpha_i)) + +... + \tau(a_{im_i})(\tau(\alpha_i))^{m_i} = 0$ or
$\sigma(a_{i0}) + \sigma(a_{i1})\tau((\alpha_i)) + ... + \sigma(a_{im_i})(\tau(\alpha_i))^{m_i} = 0$ since τ extends σ and $a_{ik} \in F$.

Theorem 49.7 (continued 3)

Theorem 49.7. Let E be a finite extension of field F. Let σ be an isomorphism of F onto a field F', and let $\bar{F}'$ be an algebraic closure of F'. Then the number of extensions of σ to an isomorphism τ of E onto a subfield of $\bar{F}'$ is finite, and independent of F', $\bar{F}'$, and σ. That is, the number of extensions is completely determined by the two fields E and F.

Proof (continued). So the only possible value for $\tau(\alpha_i)$ is as a zero of $\sigma(a_{i0}) + \sigma(a_{i1})x + \sigma(a_{i2})x^2 + ... + \sigma(a_{im_i})x^{m_i} \in F[x]$ and hence there are only m_i possible values for $\tau(\alpha_i)$. Therefore the number of values of τ on $\alpha_1, \alpha_2, \ldots, \alpha_n$ are finite and since a basis for $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is $1, \alpha_1, \alpha_2, \ldots, \alpha_n$, then there are only a finite number of extensions of σ to E. □

Corollary 49.10

Corollary 49.10. If $F \leq E \leq K$ where K is a finite extension field of the field F, then $\{K : F\} = \{K : E\}\{E : F\}$.

Proof. Let $\sigma : F \to \bar{F}$ (into) be an isomorphism of E with $\sigma[E] \leq \bar{F}$ which fixes F. By definition, there are $\{E : F\}$ such σ. Let $\tau : K \to \bar{F}$ be an isomorphism of K with $\tau[K] \leq \bar{F}$ which fixes E. By definition, there are $\{K : E\}$ such τ. Next, the mapping

$$u(x) = \begin{cases} \sigma\tau(x) & \text{if} x \in E \\ \tau(x) & \text{if } x \in K \backslash E \end{cases} \quad (2)$$

is an isomorphism of K with $u[K]$ which fixes F.
So the number of such u is $\{K : F\} = \{K : E\}\{E : F\}$ by the Multiplication Rule. □