Part X (§48-53)
Automorphisms and Galois Theory

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

January 22

48 The Conjugation Isomorphisms

Notation: For a field F, its algebraic closure will be denoted by $\overline{F}$.
Denote the inclusion by $j : F \hookrightarrow \overline{F}$.
Recall, it means

$$\mathrm{j} : \mathrm{F} \hookrightarrow \overline{\mathrm{F}} \quad \text{is algebraic,} \quad \text{and} \quad \overline{\mathrm{F}} \quad \text{is algebraically closed.}$$

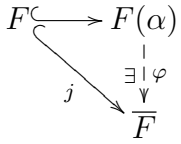
We also denote $x := j(x)$, when the inclusion j is understood. **Caution:** It is important to use a notation for the inclusion i. In general, there are many homomorphims $\epsilon : F \hookrightarrow \overline{F}$, and there may not be any canonical choice.

48.1 Foundation

Lemma 48.1. *Suppose $F \hookrightarrow F(\alpha)$ be an algebraic extension and $p(x) = irr(\alpha, F)$ be the its irreducible polynomial. Let $\overline{F}$ be the algebraic closure of F and $j : F \hookrightarrow \overline{F}$ be the inclusion. Suppose $\beta \in \overline{F}$ be a root of $p(x)$. Then, there is unique homomorphism $\varphi : F(\alpha) \longrightarrow \overline{F}$ such that*

$$\forall \;\; a \in F \quad \varphi(a) = a \quad \text{and} \quad \varphi(\alpha) = \beta.$$

Diagramatically,



$$\ni \quad \varphi(\alpha) = \beta.$$

Proof. Assume $\deg(p) = n$. Then, any $y \in F(\alpha)$ can written UNIQUELY, as

$$y = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \qquad where \quad a_i \in F.$$

In other words, each element

$$y = r(\alpha) \quad for\ some\ UNIQUE \quad r(x) \in F[x] \quad with \quad \deg(r) \leq n-1.$$

Define

$$\varphi(y) = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-1}\beta^{n-1}.$$

φ is well defined, because of uniqueness of the above expression. Clearly, $\varphi(\alpha) = \beta$ and $\varphi(x) = x$ for all $x \in F$. Remains to prove that φ is a ring/field homomorphism. Let

$$y = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}, \quad z = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$$

with $a_i, b_i \in F$. Write

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}, \quad g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}$$

Then, $y = f(\alpha), z = g(\alpha)$. We have

$$\varphi(y+z) = \varphi\left(\sum_{i=0}^{n-1}(a_i + b_i)\alpha^i\right) = \sum_{i=0}^{n-1}(a_i + b_i)\beta^i$$

$$= \sum_{i=0}^{n-1} a_i \beta^i + \sum_{i=0}^{n-1} b_i \beta^i = \varphi(y) + \varphi(z).$$

Now, write $f(x)g(x) = p(x)q(x) + r(x)$ where $r = 0$ or $\deg(r) < n$. Then

$$\varphi(yz) = \varphi(f(\alpha)g(\alpha)) = \varphi(p(\alpha)q(\alpha) + r(\alpha)) = \varphi(r(\alpha)) = r(\beta).$$

Also, since $p(\beta) = 0$, we have

$$\varphi(x)\varphi(y) = f(\beta)g(\beta) = p(\beta)q(\beta) + r(\beta) = r(\beta).$$

So,

$$\varphi(yz) = \varphi(x)\varphi(y).$$

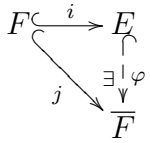
The proof is complete. ∎

Corollary 48.2. iLet F be a field, $\overline{F}$ be the algebraic closue, and $j : F \hookrightarrow \overline{F}$ be the inclusion. Let $p(x) \in F[x]$ be an irreducible polynomial and $\alpha, \beta \in \overline{F}$ and $p(\alpha) = p(\beta) = 0$. Then, then the is an isomorphism

$$\psi_{\alpha,\beta} : F(\alpha) \xrightarrow{\sim} F(\beta) \quad \ni \quad \forall a \in F \quad \varphi(a) = a \quad \text{and} \quad \varphi(\alpha) = \beta.$$

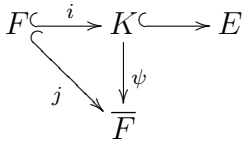
Proof. It follows from Lemma 48.1 that there is a homomorphism $\varphi : F(\alpha) \longrightarrow \overline{F}$ such that $\forall a \in F \quad \varphi(a) = a$ and $\varphi(\alpha) = \beta$. We claim $\varphi = \psi_{\alpha,\beta}$ satisfies the required. Since ant ring homomorphism from a field is injective, φ is injective.
From the definition (as vector space map) in Lemma 48.1,
it is clear $Image(\varphi) \subseteq F(\beta)$.
Since $F \subseteq Image(\varphi)$ and $\beta \in Image(\varphi)$, φ is onto. Therefore φ is an isomorphism. ∎

Theorem 48.3 (EmbeddingInClosure)**.** *Suppose $i : F \hookrightarrow E$ is an algebraic field extension* (and as usual $j : F \hookrightarrow \overline{F}$ denote the algebraic closure of F)*. Then, there is an (injective) homomorphism $\varphi : E \longrightarrow \overline{F}$ such that $\varphi_{|F} = Id_F$. Diagramatically,*



commutes.

Proof. We use Zorn's lemma. Let $\mathcal{E}$ be the set of all pairs (K, ψ) such that $F \hookrightarrow K \hookrightarrow E$ are extensions and $\psi : K \hookrightarrow \overline{F}$ is a homomorphism such that $\psi_{|F} = Id_F$. (*We say* ψ *extends* j.) Diargramatically:

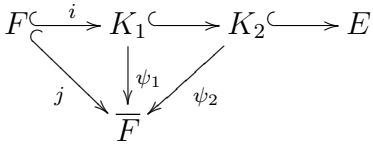


commutes.

First, $\mathcal{E}$ is a nonempty set, because (F, i) is in $\mathcal{E}$. We partially order $\mathcal{E}$ as follows:

$$For \quad (K_1, \psi_1), (K_2, \psi_2) \in \mathcal{E} \quad define \quad (K_1, \psi_1) \leq (K_2, \psi_2) \quad if$$
$$K_1 \subseteq K_2 \quad and \quad (\psi_2)_{|K_1} = \psi_1,$$

diargramatically:



commutes.

That means, if ψ_2 extends ψ_1 to K_2. Now, given a chain

$$(K_1, \psi_1) \leq (K_2, \psi_2) \leq (K_3, \psi_3) \leq (K_4, \psi_4) \leq \cdots$$

let $K_\infty = \cup_{i=1}^{\infty} K_i$. Then, K_∞ is a subfield on E. Define $\psi_\infty : K_\infty \longrightarrow \overline{F}$ by

$$\psi_\infty(x) = \psi_i(x) \qquad if \quad x \in K_i.$$

Then, ψ_∞ is a well defined homomorphism and $(K_i, \psi_i) \leq (K_\infty, \psi_\infty)$ for all i. So, (K_∞, ψ_∞) is an upper bound of the chain.

So, by Zorn's lemma $\mathcal{E}$ has maximal element (K, ψ). We claim, $K = E$. If not, there is an element $\alpha \in E$ such that $\alpha \notin K$. Note, α is algebraic over K.

Apply, lemma 48.1, to $\psi : K \hookrightarrow K(\alpha)$. It gives an extension $\varphi : K(\alpha) \hookrightarrow \overline{F}$ of ψ. This contradicts the maximality of (K, ψ). Hence, $K = E$ and ψ extends i to E.

The proof is complete. ∎

Remark. A Few points:

1. The theorem assures, that any algebraic extension $i : F \hookrightarrow E$, we can extend i to an embedding $\varphi : E \longrightarrow \overline{F}$.

2. But, there may be many such embeddings.

3. In fact, there are many such embeddings. Lemma 48.1 assures corresponding each root $\beta \in \overline{F}$, of $p(x) = irr(\alpha, F)$, there is one such embedding $F(\alpha) \hookrightarrow \overline{F}$.

4. **Counting number of such embedding is part of our goals**.

48.2 Conjugation

The following is an important concept in field theory.

Definition 48.4. *Suppose $F \hookrightarrow E$ is an algebraic field extension. Two elements $\alpha, \beta \in E$ are said to be* **conjugates over** *F, if $irr(\alpha, F) = irr(\beta, F)$.*

Example 48.5 (48.2)**.** *$\alpha, \beta \in \mathbb{C}$ are conjugates over $\mathbb{R}$ if and only if they are (good old) complex conjugates.*

Theorem 48.6 (48.3)**.** *(***Conjugate Isomorphism Theorem***) Let F be a field and $\alpha, \beta \in \overline{F}$. Assume irreducible degree* $\deg(\alpha, F) = n$*. Consider the (set theoretic) map*

$$\psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$$

defined by

$$\psi_{\alpha,\beta}(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-1}\beta^{n-1}$$

where $a_i \in F$. Then, $\psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$ is an isomorphism if and only if α, β are conjugates over F.

Remark. Note, $\psi_{\alpha,\beta}$ would not be a homomorphism, unless β, α are conjugates.

Proof. ((⇐) was seen before in 48.2) Let $p(x) = irr(\alpha, F)$. Then $p(\alpha) = 0$.

($\Longrightarrow$): Suppose $\psi_{\alpha,\beta}$ is an isomorphism. Then,

$$p(\beta) = \psi_{\alpha,\beta}(p(\alpha)) = \psi_{\alpha,\beta}(0) = 0.$$

So, $irr(\beta, F) = p(x) = irr(\alpha, F)$. So, α, β are conjugates. This implication is established.

($\Longleftarrow$): Now suppose α, β are conjugates. Then, $p(x) = irr(\alpha, F) = irr(\beta, F)$. Consider two homomorphism

$$\varphi_\alpha : F[x] \longrightarrow F(\alpha), \quad \varphi_\beta : F[x] \longrightarrow F(\beta)$$

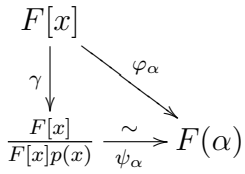
defined by

$$\varphi_\alpha(f(x)) = f(\alpha), \quad \varphi_\beta(f(x)) = f(\beta).$$

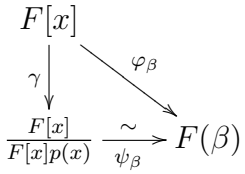
Both are well define homomorphism. Since α, β are algebraic, bothe are onto. Since $p(x) = irr(\alpha, F) = irr(\beta, F)$,

$$\ker(\varphi_\alpha) = F[x]p(x) = \ker(\varphi_\beta).$$

So, by fundamental theorem, $\varphi_\alpha, \varphi_\beta$ induce isomorphisms ψ_α, ψ_β, as follows



with $\varphi_\alpha = \psi_\alpha\gamma$;

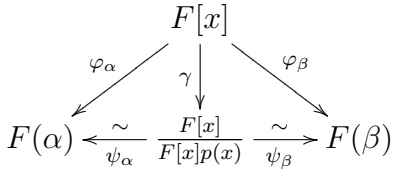


with $\varphi_\beta = \psi_\beta\gamma$.

Then,

$$\psi_{\alpha,\beta} = \psi_\beta\psi_\alpha^{-1} : F(\alpha) \xrightarrow{\sim} F(\beta).$$

Being composition of two isomorphisms, $\psi_{\alpha,\beta}$ is an isomorphism. Diagramatically,



commutes and $\psi_{\alpha,\beta} = \psi_\beta\psi_\alpha^{-1}$.

The proof is complete. ∎

Example 48.7 (48.7)**.** *(***Edited***) Consider* $\mathbb{Q}(\sqrt{5})$*. Then*

$$irr(\sqrt{5}, \mathbb{Q}) = x^2 - 5.$$

Another root of $x^2 - 5 = 0$ *is* $-\sqrt{5}$*. So,* $\sqrt{5}, -\sqrt{5}$ *are conjugates over* $\mathbb{Q}$*.*

By theorem 48.6,

$$\psi_{\sqrt{5},-\sqrt{5}} : \mathbb{Q}(\sqrt{5}) \xrightarrow{\sim} \mathbb{Q}(-\sqrt{5})$$

is defined by

$$\psi_{\sqrt{5},-\sqrt{5}}(a + b\sqrt{5}) = a - b\sqrt{5}.$$

48.3 Fixed Fields

Definition 48.8. *Suppose E is a field. An isomorphism $\varphi : E \xrightarrow{\sim} E$ is aslo called an* **automorphism** *of E.*

$Aut(E)$ will denote the set of all automorphisms of E.

Theorem 48.9 (48.14)**.** *$Aut(E)$ is a group under composition.*

Proof. Obvious/Exercise.

Definition 48.10. *Suppose E is a field.*

1. *Suppose $\sigma : E \xrightarrow{\sim} E$ is an automorohism of E. An element $a \in E$ is said to be* **left fixed by** *σ, if $\sigma(a) = a$.*
2. *Suppose $F \hookrightarrow E$ is a field extension. Let S be a set of automorphisms of E. We say F is* **left fixed by** *S, if*

$$\sigma(a) = a \qquad \forall \;\; a \in F \quad and \quad \forall \;\; \sigma \in S.$$

Theorem 48.11 (48.11)**.** *Suppose $S \subseteq Aut(E)$ is a set of authomorphisms of a field E. Define*

$$E_S = \{a \in E : \sigma(a) = a \quad \forall \;\; \sigma \in S\}.$$

Then, E_S is a subfield of E.

Proof. We need to show E_S is closed under addition, multiplication, additive inverse and multiplicative inverse. Let $a, b \in E_S$. Then,

$$for \quad \sigma \in S \quad \sigma(a + b) = \sigma(a) + \sigma(b) = a + b.$$

So, $a + b \in E_S$. Also,

$$\sigma(-a) = -\sigma(a) = -a \quad \forall \;\; \sigma \in S. \quad So, -a \in E_S.$$

Further,

$$for \quad \sigma \in S \quad \sigma(ab) = \sigma(a)\sigma(b) = ab.$$

So, $ab \in E_S$. Finally, for $a \in E_S$ and $a \neq 0$ we have

$$for \quad \sigma \in S \quad \sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}.$$

So, $a^{-1} \in E_S$.

Therefore, E_S is a subfield of E.

The proof is complete. ∎

Definition 48.12. *E_S defined above is called the* **fixed field of** *S. For any $\sigma \in Aut(E)$ the fixed field of σ is denoted by E_σ.*

Example 48.13 (49.13)**.** *Consider the automorphism $\psi_{\sqrt{5},-\sqrt{5}} : \mathbb{Q}(\sqrt{5}) \xrightarrow{\sim} \mathbb{Q}(\sqrt{5})$. Then the fixed field of $\psi_{\sqrt{5},-\sqrt{5}}$ is $\mathbb{Q}$.*

48.4 Groups of Extensions $F \hookrightarrow E$

Definition 48.14. *Suppose $F \hookrightarrow E$ is an extension of fields. Then, denote*

$$G(E/F) := \{\sigma \in Aut(E) : \sigma_{|F} = ID_F\}$$

This is the "set" of all $\sigma \in Aut(E)$ that leaves F fixed.

We prove below that $G(E/F)$ is a subgroup of $Aut(E)$. This group $G(E/F)$ is called **the group of E over F.** *It is also called the* **group of $F-$automorphisms of E.**

Theorem 48.15 (48.15)**.** *Suppose $F \hookrightarrow E$ is an extension of fields. Then $G(E/F)$ is a subgroup of $Aut(E)$.*

Further,

$$F \hookrightarrow E_{G(E/F)} \quad the\ fixed\ field\ of \quad G(E/F).$$

Proof. To see $G(E/F)$ we proceed as follows:

1. (**Closure of the multiplication**): Let $\sigma_1, \sigma_2 \in G(E/F)$. Then

$$for \quad s \in F \quad (\sigma_1\sigma_2)(x) = \sigma_1(\sigma_2(x)) = \sigma_1(x) = x.$$

So, $\sigma_1\sigma_2$ leaves F fixed. So, $G(E/F)$ is closed under the product (*the composition*).

2. (**Closure of inverses**): Let $\sigma \in G(E/F)$.

$$for \quad s \in F \quad \sigma(x) = x. \qquad so \quad x = \sigma^{-1}(x).$$

σ^{-1} leaves F fixed. So, $G(E/F)$ is closed under the inverses. Therefore $G(E/F)$ is subgroup of $Aut(E)$.

Now, to see the last assertion:

$$for \quad x \in F, \sigma \in G(E/F) \quad we\ have \quad \sigma(x) = x.$$

So, $F \hookrightarrow E_{G(E/F)}$. The proof is complete. ∎

Example 48.16 (48.17)**.** *Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then,*

1. $[E : \mathbb{Q}] = 4$.

2. $$G(E/\mathbb{Q}) = \{ID_E, \psi_{\sqrt{2},-\sqrt{2}}, \psi_{\sqrt{3},-\sqrt{3}}, \psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}}\}$$

Proof. Read from the textbook.

48.5 The Frobenius Automorphism

Theorem 48.17 (48.19)**.** *Let F be a field of characteristic p.*

1. *Then,*

$$\sigma_p : F \longrightarrow F \qquad defined\ by \quad \sigma_p(x) = x^p$$

is a homomorphism.

2. If F is finite then σ_p is an automorphism.

Proof. Since $px = 0$ for all $x \in F$, by binomial expansion

$$\sigma_p(x + y) = (x + y)^p = x^p + y^p = \sigma_p(x) + \sigma_p(y).$$

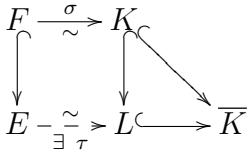
Also, $\sigma_p(xy)\sigma_p(x)\sigma_p(y)$. So, σ_p is a homomorphism.

Any homomorphism of fields is injective. So, by counting, when F is finite σ_p is surjective.

The proof is complete. ∎

49 The Isomorphism Extension Theorem

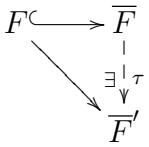
Theorem 49.1 (49.3)**. Isomorphism Extension Theorem**, *Simple Version): Let $F \hookrightarrow E$ be an algebraic extension of fields. Let $\sigma : F \xrightarrow{\sim} K$ be an isomorphism of fields and $\overline{K}$ be the algebraic closure of K. Then, σ can be extended to an automorphism $\tau : F \xrightarrow{\sim} L$ where L is a subfield of $\overline{K}$. Diagramatically,*



Proof. Follows immediately from theorem 48.3, by identifying K with F (or F with K). ∎

Corollary 49.2 (49.5)**.** *Suppose F is a field and $\overline{F}, \overline{F}'$ be two algebraic closure of F. Then there is an isomorphism $\tau : \overline{F} \xrightarrow{\sim} \overline{F}'$ such that $\tau_{|F} = Id_F$.*

Proof. Consider the diagram



Here τ exists by theorem 48.3.

Now, $\tau(\overline{F}) \hookrightarrow \overline{F}'$ is an algebraic extension. In fact, $\overline{F}'$ is algebraically closed and we check this. Let $\alpha \in \overline{F}'$. Then,

$$\sum_{k=1}^{n} j(a_k)\alpha^k = 0 \quad for\ some\ \ a_k \in F; \quad some\ \ a_k \neq 0.$$

Therefore,

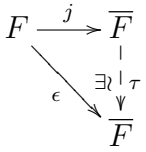
$$\sum_{k=1}^{n} \tau(i(a_k))\alpha^i = 0.$$

So, it is checked. Therefore, $\tau(\overline{F}) = \overline{F}'$. The proof is complete. ∎

A Key Tool:

A homomorphism $\epsilon : F \hookrightarrow E$ of fields is also called an **embedding**. We will use the following repeatedly:

Corollary 49.3 (twoEmbeddingInFbar)**.** *(Spring 15): Suppose F is a field and $j, \epsilon : F \longrightarrow \overline{F}$ are two embeddings. Then there is an isomorphism $\tau : \overline{F} \xrightarrow{\sim} \overline{F}$ such that $\epsilon = \tau j$. Diagrmatically,*



Proof. By theorem 48.3, there is a homomorphism $\tau : \overline{F} \longrightarrow \overline{F}$ such that the diagram commutes. Since $\tau(\overline{F}) \hookrightarrow \overline{F}$ algebraic, $\tau(\overline{F}) = \overline{F}$. Therefore, τ is surjective, hence an isomorphism. The proof is complete. ∎

49.1 How Many Embedding? Index

What is an Embedding?

1. Usually, an injective map is also called an embeddings. We can talk about embedding in any category (i.e. of any kind of objects).
2. For example, we may talk about embedding of the circle $\mathbb{S}^1$ in the sphere $\mathbb{S}^2$.
3. Also note that the circle $\mathbb{S}^1$ can be embedded in $\mathbb{S}^2$ in numerous ways. Any great circle of $\mathbb{S}^2$ is an embedding of $\mathbb{S}^1$.
4. In our context (category) of fields, any homomophism $\epsilon : F \longrightarrow E$ is injective. So, any such homomorphism ϵ is called **an embedding of F in E.**

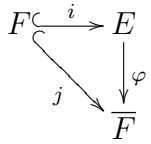
Given an algebraic field extension $F \hookrightarrow E$, we consider the question how many embeddings $E \hookrightarrow \overline{F}$ are possible?

Definition 49.4. Suppose $i : F \hookrightarrow E$ an algebraic extension.

1. Let $j : F \hookrightarrow \overline{F}$ be a fixed inclusion of F in its algebraic closure $\overline{F}$. (That means, j is a fixed embedding of F in $\overline{F}$.)
2. I will use $Emb_j(E)$ or $Emb_{F,j}$ to denote the set of all such embeddings.

$$\mathbf{Emb_j(E) = set\ of\ all\ embeddings} \quad \varphi : \mathbf{E} \longrightarrow \overline{\mathbf{F}} \quad \mathbf{that\ extends\ \ i}.$$

That means $Emb_j(E)$ is the set of φ so that the diagram



commutes.

When j is understood (or natural), we also write

$$\mathbf{Emb_F(E) = Emb_j(E)}.$$

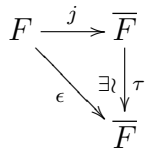
Lemma 49.5 (wellDCardinality)**.** (Spring 15): *Let $i : F \hookrightarrow E$ be a finite field extension and $j, \epsilon : F \hookrightarrow \overline{F}$ be two embeddings. Then, there is a bijection*

$$\iota : Emb_j(E) \xrightarrow{\sim} Emb_\epsilon(E).$$

In particular,

$$|Emb_j(E)| = |Emb_\epsilon(E)|.$$

Proof. By 49.3, there is an isomorphism τ such that the diagram

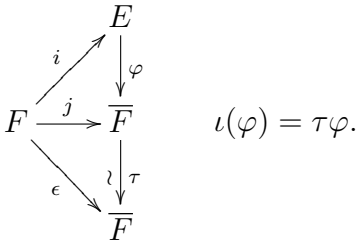


commutes.

Define

$$\iota : Emb_j(E) \xrightarrow{\sim} Emb_\epsilon(E) \quad by \quad \iota(\varphi) = \tau\varphi.$$

Diagramatically:



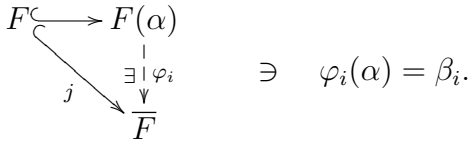
$\iota(\varphi) = \tau\varphi.$

It is easy to check, ι is bijective. The proof is complete. ∎

Theorem 49.6. (Spring 15): *Let $i : F \hookrightarrow E$ be a finite field extension and $j : F \hookrightarrow \overline{F}$ be an inclusion* (i.e. a fixed embedding).

1. *Then, the number of embedding $E \hookrightarrow \overline{F}$ is finite. That means, the cardinality*
$$|Emb_j(E)| < \infty.$$
2. *In fact,*
$$|Emb_j(E)|) \leq [E : F] \qquad \text{(the right side is called the degree of F} \hookrightarrow \text{E)}.$$

Proof. First, we assume $E = F(\alpha)$ is generated, over F, by one element $\alpha \in E$. Let $p(x) = irr(\alpha, F) \in F[x]$ be the irreducible polynomial of α. Let $deg(p(x)) = n$. Now, $p(x)$ has exactly n roots in $\overline{F}$, which may not be distinct. Let $\beta_1, \ldots, \beta_r \in \overline{F}$ be the distinct roots of $p(x)$.By lemma 48.1, there are embeddings φ_i as in the commutative diagram



$\ni \quad \varphi_i(\alpha) = \beta_i.$

So, we have exhibited, r distinct embeddings φ_i. Also, given such an embedding $\varphi : F(\alpha) \longrightarrow \overline{F}$, with $\beta = \varphi(\alpha)$, we have

$$p(\beta) = p(\varphi(\alpha)) = \varphi(p((\alpha)) = \varphi(0) = 0.$$

So, $\beta = \beta_i$ and $\varphi = \varphi_i$ for some $i = 1, 2, \ldots r$. So,

$$Emb_j(E) = \{\varphi_1, \ldots, \varphi_r\}.$$

Therefore, the number of such embedddings

$$|Emb_j(F(\alpha)| = r \leq n = [F(\alpha) : F] < \infty.$$

So, the theorem is established when $E = F(\alpha)$.

Now we deal with the general case. Since, E is finite over F, it is also finitely generated. Write $E = F(\alpha_1, \alpha_2, \ldots, \alpha_k)$. We will use induction on k, Write $L = F(\alpha_1, \alpha_2, \ldots, \alpha_{k-1})$. By induction,

$$|Emb_j(L)| \leq [L : F].$$

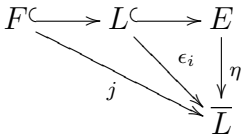
Write

$$Emb_j(L) = \{\epsilon_1, \epsilon_2, \ldots, \epsilon_r\} \qquad where \quad r = |Emb_j(L)| \leq [L : F].$$

Note that $L \hookrightarrow E = L(\alpha_r)$ is a finite extension. Also note $\overline{F} = \overline{L}$. For $i = 1, \ldots, r$ let

$$\mathcal{E}_i = \{\eta \in Emb_j(E) : \eta_{|L} = \epsilon_i\}$$

So, an element $\eta \in \mathcal{E}_i$ is characterized by the later triangle in the commutative diagram:



$So,\ by\ first\ part \quad |\mathcal{E}_i| \leq [E : L].$

Further,

$$Emb_j(E) = \bigcup_{i=1}^{r} \mathcal{E}_i \qquad is\ DISJOINT\ union\ of \quad \mathcal{E}_i.$$

So, we have

$$|Emb_j(E)| = \sum_{i=1}^{r} |\mathcal{E}_i| \leq r[E : L] \leq [L : F][E : L] = [E : F].$$

The proof is complete. ∎

The following is the version of theorem 49.6 given in the textbook. To the experts, there is little difference between these two versions. In any case, following version is unavoidable sometimes.

Theorem 49.7 (49.7)**.** *Let $F \hookrightarrow E$ be a finite extension of fields. Let $\sigma : F \xrightarrow{\sim} K$ be an isomorphism of fields. Then, σ extends to an isomorhism $\tau : E \xrightarrow{\sim} L$ where L is a subfield of $\overline{K}$. Diagramatically,*

$$\begin{array}{ccccc} F & \hookrightarrow & E & & \\ {\scriptstyle\sigma}\downarrow & \wr & \downarrow{\scriptstyle\exists\wr\,\tau} & & \text{commutes.} \\ K & \hookrightarrow & L & \hookrightarrow & \overline{K} \end{array}$$

Proof. It follows immediately from theorem 49.6, when you identify F and K via σ. The proof is complete. ∎

Definition 49.8. *Let $F \hookrightarrow E$ be a finite extension of fields. Define*

$$(\textbf{Index of E over F}) := |Emb_j(E)| \qquad \textit{where} \quad j : F \longrightarrow \overline{F} \quad \textit{is any embedding.}$$

By (49.5), Index is well daifined.

Notation: I will denote the Index by $|Emb_j(E)|$ or $|Emb_F(E)|$. The textbook uses the notation $\{E : F\}$. I will use $|Emb_j(E)|$. So,

$$(\textbf{Index of E over F}) := |Emb_j(E)| = |Emb_F(E)| = \{E : F\}.$$

Corollary 49.9 (49.9)**.** *Let $F \hookrightarrow L \hookrightarrow E$ be finite extensions of fields. Let $j : F \longrightarrow \overline{F}$ be a fixed embedding. Let $i : L \hookrightarrow E$ be the given inclusion. Then,*

$$|Emb_j(E)| = |Emb_L(E)||Emb_j(L)|.$$

(This is obviously similar to the degree formula $[E : F] = [E : L][L : F]$.)

Proof. The proof is embedded in the proof of the general case of theorem 49.6. Let me show the outline. We use the same notations as in (49.6). With $r = |Emb_j(L)|$ and

$$Emb_j(L) = \{\epsilon_1, \epsilon_2, \ldots, \epsilon_r\} \quad \textit{and} \quad \mathcal{E}_k = \{\eta \in Emb_j(E) : \eta i = \epsilon_k\}$$

Diagramatically:

$$\begin{array}{ccccc} F & \hookrightarrow & L & \overset{i}{\hookrightarrow} & E \\ & {\scriptstyle j}\searrow & \downarrow{\scriptstyle\epsilon_k} & & \downarrow{\scriptstyle\eta}\ . \\ & & \overline{L} & & \end{array}$$

We proved

$$Emb_j(E) = \bigcup_{k=1}^{r} \mathcal{E}_k \qquad is\ DISJOINT\ union\ of \quad \mathcal{E}_k.$$

Also note $|\mathcal{E}_k| = |Emb_{\epsilon_1}(E)| = |Emb_L(E)|$ for $i = k, \ldots, r$. So, we have

$$|Emb_F(E)| = \sum_{k=1}^{r} |\mathcal{E}_k| = r|Emb_L(E)| = |Emb_F(L)||Emb_L(E)|.$$

The proof is complete. ■

50 Splitting Fields

Definition 50.1 (DefOfSplittingField)**.** *Let F be a field and $j : F \hookrightarrow \overline{F}$ is a fixed embedding. Let $\Phi = \{f_i(x) : i \in I\}$ be a set of polynomials in $F[x]$. Let E be the subfield $\overline{F}$ generated by F and all the zeros of all the polynomials f_i, in $\overline{F}$. Then, E is called the* **splitting field of Φ over F.** *So,*

$$E = \cap\{L : L \hookrightarrow \overline{F} \ \ni \ is\ a\ subfield,\ F \hookrightarrow L, all\ zeros\ of\ f_i\ are\ in\ L\}.$$

1. The idea is, if E has zero of a polynomial $f \in F[x]$, then it contains all the zeros of F.
2. We will describe the splitting field of $\Phi = \{f_i(x) : i \in I\}$ below.

Before that let me introduce some noatation and this lemma.

Notation: Suppose $F \hookrightarrow E$ is an extension of fields and $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$. Let $F[x_1, x_2, \ldots, x_n]$ be the polynomial ring over F. We define the evaluation map

$$\varphi_{ev} : F[x_1, x_2, \ldots, x_n] \longrightarrow E \qquad by \quad \varphi_{ev}(f(x_1, x_2, \ldots, x_n)) = f(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Such an expression $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is called a **polynomial expression** or an **algebraic expression** in $\alpha_1, \alpha_2, \ldots, \alpha_n$.

1. φ_{ev} is a homomorphism of rings.
2. **Notation:** Then image of φ_{ev} is denoted by $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$. So,

   $$F[\alpha_1, \alpha_2, \ldots, \alpha_n] = \{f(\alpha_1, \alpha_2, \ldots, \alpha_n) : f \in F[x_1, x_2, \ldots, x_n]\}.$$

   Unless stated explicitly (or implicitly), this notation does not mean, that $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is the polynomial ring.

   (a) In the polynomial ring $f(x_1, x_2, \ldots, x_n) = 0$ if and only if all the coefficients are zero.

   (b) On the other hand, $f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$ for some $f \neq 0$, unless $\alpha_1, \alpha_2, \ldots, \alpha_n$ are "transcendental" over F.

3. Also recall the subfield of E generated by F and $\alpha_1, \alpha_2, \ldots, \alpha_n$ is denoted by $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Usually,

$$F[\alpha_1, \alpha_2, \ldots, \alpha_n] \neq F(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Lemma 50.2 (algGenbyAlpha)**.** *If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic over F, then $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is a field. In other words*

$$F[\alpha_1, \alpha_2, \ldots, \alpha_n] = F(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Proof. First, α_1 is algebraic over F. So, $F[\alpha_1]$ is a field. Note

$$F[\alpha_1, \alpha_2, \ldots, \alpha_n] = F[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}][\alpha_n]$$

and α_n is algebraic over $F[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}]$. By induction, $F[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}]$ is a field and hence so is $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$. The proof is complete. ∎

Now we are ready to give a description of the splitting fields.

Theorem 50.3 (theSplittingF)**.** Use the notations as in the definition 50.1. *Let*

$$\Psi = \{\alpha \in \overline{F} : f_i(\alpha) = 0 \ for \ some \ \ f_i \in \Phi\}.$$

So, Ψ is the collection of all zeros of the polynomials in Φ. Write

$$K = \{f(\alpha_1, \alpha_2, \ldots, \alpha_n) : n \geq 0, f \in F[x_1, \ldots, x_n], \alpha_i \in \Psi\}.$$

$$= \bigcup \{F[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}] : n \geq 0, \alpha_i \in \Psi\}$$

So, K is the set of all polynomial expressions in elements in Ψ. Then, K is a subfield of $\overline{F}$ and $K = E$ is the splitting field of Φ.

Proof. It is easy to see that K is closed under addition and multiplication. Suppose $\beta = f(\alpha_1, \alpha_2, \ldots, \alpha_n) \in K$ and $\beta \neq 0$. Since, α_i are algebraic over F, by lemma 50.2,

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F[\alpha_1, \alpha_2, \ldots, \alpha_n] \quad is \ a \ field.$$

Since $\beta \in F[\alpha_1, \alpha_2, \ldots, \alpha_n]$, $\beta^{-1} \in F[\alpha_1, \alpha_2, \ldots, \alpha_n] \subseteq K$. So, K is a subfield of $\overline{F}$.

It is also easy to see that $F \subseteq K$ and $\Psi \subseteq K$. Also, any field L containing F and Ψ must also contain each element $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of K. So,

$$E = \cap\{L : L \hookrightarrow \overline{F} \ \ni \ is\ a\ subfield,\ F \hookrightarrow L, all\ zeros\ of\ f_i\ are\ in\ L\} = K.$$

The proof is complete. ∎

Example 50.4. 1. **(50.2)** The field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ is the splitting field of $\{x^2 - 3, x^2 - 5\}$ over $\mathbb{Q}$.

2. $\mathbb{C}$ is the splitting field of $\{x^2 + 1\}$ over $\mathbb{R}$.

Theorem 50.5 (50.3)**.** *Let $F \hookrightarrow E \hookrightarrow \overline{F}$ be field extensions. Then, E is a splitting field over F if and only if, for every $\sigma \in Aut(\overline{F})$ with $\sigma_{|F} = Id_F$, $\sigma_{|E} \in Aut(E)$. Diagramatically:*

$$\begin{array}{ccccc} F & \hookrightarrow & E & \hookrightarrow & \overline{F} \\ \| & & \downarrow \sigma_{|E} & & \downarrow \sigma \\ F & \hookrightarrow & E & \hookrightarrow & \overline{F} \end{array} \quad \sigma \quad is\ given\ with \quad \sigma_{|F} = Id_F.$$

Proof. Suppose E is the splitting field of Φ over F. Description of E is given in theorem 50.3. (*We use the notations of (50.3)*) Now suppose $\sigma \in Aut(\overline{F})$ with $\sigma_{|F} = Id_F$. Let $\beta \in E$ then $\beta = f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_i \in \Psi$ and $f \in F[x_1, \ldots, x_n]$, as in (50.3). Then

$$\sigma(\beta) = \sigma(f(\alpha_1, \alpha_2, \ldots, \alpha_n)) = f(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n))$$

Note,$f_j(\alpha_i) = 0$ for some $f_j \in \Phi$. So, $f_j(\sigma(\alpha_i)) = \sigma(f_j(\alpha_i)) = 0$. So, $\sigma(\alpha_i) \in \Psi$. Therefore,

$$\sigma(\beta) = f(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)) \in E.$$

So, $\sigma(E) \subseteq E$. To see $\sigma(E) = E$, let $\beta = f(\alpha_1, \alpha_2, \ldots, \alpha_n) \in E$. Then,

$$\beta = \sigma(f(\sigma^{-1}(\alpha_1), \sigma^{-1}(\alpha_2), \ldots, \sigma^{-1}(\alpha_n))$$

by same argument, $\sigma^{-1}(\alpha_i) \in \Psi$. Hence $\beta \in \sigma(E)$. So, the restriction $\sigma_{|E}$ is an automorphism of E. So this implication is established.

Conversely, suppose the diagram holds for all $\sigma \in Aut(\overline{F})$. We need to get prove E is a splitting field of some subset Φ of $F[x]$. Obvious candidate is

$$\Phi = \{f \in F[x] : f = irr(\alpha, F) \quad for\ some \quad \alpha \in E\}.$$

We will prove that E is, in deed, the splitting field of Φ. It is enough to prove that if $f(\beta) = 0$, for some $f \in \Phi$ and $\beta \in \overline{F}$, then $\beta \in E$. Suppose β and f are as stated. Then, there is an $\alpha \in E$ such that $irr(\alpha, F) = f(x)$. That means α, β are conjugates. By (48.6), there is an isomorphism

$$\psi_{\alpha,\beta} : F(\alpha) \xrightarrow{\sim} F(\beta) \quad \ni \quad \psi_{\alpha,\beta}(\alpha) = \beta, \ \ and \ \ \psi_{\alpha,\beta}(x) = x \ \ \forall \ \ x \in F.$$

Let $i : F(\alpha) \hookrightarrow \overline{F}$ denote the inclusion. Now, we apply the "key tool" (49.3) as follows

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\ i\ } & \overline{F} \\ & \searrow^{\psi_{\alpha,\beta}} & \Big\downarrow \exists \wr \sigma \\ & & \overline{F} \end{array} \qquad that\ means \ \ \exists \ \ \sigma \in Aut(\overline{F}) \ \ \ni \psi_{\alpha,\beta} = \sigma i.$$

Now apply the diagram in the hypothesis. So, the restrictin $\sigma_{|E} \in Aut(E)$. Therefore,

$$\beta = \psi_{\alpha,\beta}(\alpha) = \sigma(\alpha) \in E, \qquad since \ \ \sigma(E) = E.$$

So, E contains all the zeros of elements in Φ. So, E is the smallest field containing all the zeros of elements in Φ. So, E is the splitting field of Φ.

The proof is complete. ∎

Corollary 50.6 (50.6minus)**.** *Suppose E is as in 50.5 and satisfies one (or both) of the equivalent conditions. Then, E is splitting field of the set*

$$\Phi = \{g \in F[x] : g = irr(\alpha, F) \ \ \ni \ \ \alpha \in E\}$$

Proof. Follows from the proof of (50.5).

Corollary 50.7 (50.6)**.** *Suppose $F \hookrightarrow E \hookrightarrow \overline{F}$ are field extensions and E is a splitting field over F. Suppose $f(x) \in F[x]$ is an irreducible polynomial and f has a zero in E. Then,*

1. *All the zeros of f in E.*
2. *Equivalently, f product of linear factors in $E[x]$.*

Proof. By (50.6), E is the splitting field of

$$\Phi = \{g \in F[x] : g = irr(\alpha, F) \ \ni \ \alpha \in E\}.$$

Since $f \in \Phi$ all the zeros of f are in E. The proof is complete. ∎

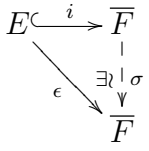
Corollary 50.8 (50.7)**.** *Suppose $F \hookrightarrow E \hookrightarrow \overline{F}$ are field extensions and E is a splitting field over F. Suppose $\epsilon : E \hookrightarrow \overline{F}$ is an embedding. Then $\epsilon \in G(E/F)$. So,*

$$So, \qquad G(E/F) = Emb_F(E).$$

In particular, if $|G(E/F)|$ is finite

$$\text{the Index} \quad |\mathrm{Emb_F(E)}| = |\mathrm{G(E/F)}|.$$

Proof. First, note $G(E/F) \subseteq Emb_F(E)$. Treat/denote the first extension $i : E \hookrightarrow \overline{F}$ as an inclusion. We need to prove $\epsilon \in G(E/F)$. Now, we apply (49.3) as follows



$$that\ means \ \ \exists \ \ \sigma \in Aut(\overline{F}) \ \ni \epsilon = \sigma i.$$

by (50.5), $\sigma_{|E} \in G(E/F)$. Clealrly, $\epsilon = \sigma_{|E} \in G(E/F)$. The proof is complete. ∎

Lemma 50.9 (extraOnSplitting)**.** *Suppose $F \hookrightarrow E \hookrightarrow K \hookrightarrow \overline{F}$ be field extensions and K is a splitting field over F. The K is a splitting field over E.*

Proof. Suppose K is the splitting field of $\Phi \subseteq F[x]$, over F. Then, K is also splitting field of $\Phi \subseteq F[x]$, over E. The proof is complete. ∎

Example 50.10 (50.8)**.** Note $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of

$$\{x^2 - 2, x^2 - 3\}.$$

One can check (see Example 48.17)

$$G\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\right) = \{\iota, \sigma_1, \sigma_2, \sigma_3\}$$

where ι is the identity homomorphism,

$$\sigma_1 = \psi_{\sqrt{2},-\sqrt{2}} \quad \textit{sending} \quad \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}.$$

and

$$\sigma_2 = \psi_{\sqrt{3},-\sqrt{3}} \quad \textit{sending} \quad \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}.$$

and

$$\sigma_3 = \sigma_1\sigma_2.$$

It is also clear

$$Emb_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})\right) = \{\iota, \sigma_1, \sigma_2, \sigma_3\} = G\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\right).$$

Example 50.11 (50.9)**.** The splliting field E of $x^3 - 2$ over $\mathbb{Q}$ is given by

$$E = \mathbb{Q}(2^{1/3}, 2^{1/3}e^{\frac{2\pi i}{3}}).$$

In this case

$$[E : \mathbb{Q}] = 6.$$

51 Seperable Extensions

Seperability of an extension $F \hookrightarrow E$ deals with the question of simplicity and/or multiplicity of the zeros of irreducible polynomials $p(x)$.

Definition 51.1. *Suppose F is a field and $\overline{F}$ the algebraic closure of F. Suppose $f(x) \in F[x]$ is a MONIC polynomial and*

$$f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r} \quad \textit{where} \quad \alpha_i \in \overline{F}, \quad \alpha_i \neq \alpha_j \quad \forall i \neq j$$

Then,

1. *We say α_i is a zero of $f(x)$,* **with multiplicity** *n_i.*
2. *If $n_1 = 1$, then we say α_1 is a* **simple zero of** *f.*
3. *If $n_1 \geq 2$, we say α_1 is a* **multiple zero of** *f.*

Theorem 51.2 (51.2)**.** *Let $p(x) \in F[x]$ be an irreducible polynomial. Then all the zeros of p have same multiplicity.*

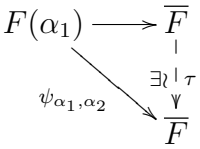
Proof. Write

$$p(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r} \quad \textit{where} \quad \alpha_i \in \overline{F}, \quad \alpha_i \neq \alpha_j \quad \forall i \neq j$$

We will prove that $n_1 = n_2 = \cdots = n_r$. By (48.1), for there is an isomorphism

$$\psi_{\alpha_1,\alpha_2} : F(\alpha_1) \xrightarrow{\sim} F(\alpha_2).$$

By (49.3), there is an isomorphism τ such that



Since $\tau(a) = a$ for all $a \in F$, p is invariant under τ.
Now, apply τ to the factorization of $p(x)$. We have

$$p(x) = (x-\alpha_2)^{n_1}(x-\alpha_1)^{n_2}(x-\tau(\alpha_3))^{n_3}\cdots(x-\tau(\alpha_r))^{n_r}.$$

Since $\overline{F}[x]$ is a UFD, $n_1 = n_2$. Similalry, $n_j = n_1$ for all $j = 1, \ldots r$.

Recall: $irr(\alpha, F)$ denotes the **MONIC** irreducible polynomial of α over F.

51.1 Derivatives

Simplicity of the zeros of a polynomial can be detected by its "derivatives" as define below.

Definition 51.3. *Let F be a field and*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x] \quad \textit{is a polynomial.}$$

Define **derivative** $f'(x) = \frac{df}{dx}$ *of $f(x)$ as follows:*

$$\frac{df}{dx} = f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + +2a_2 x + a_1.$$

(Note $f'(x)$ is defined formally; and there is no concept of limit here.)

Remark. Two points:

1. Suppose $char(F) = 0$ and $f(x) \in F[x]$. Then,

$$f'(x) = 0 \quad \Longleftrightarrow \quad f(x) = a_0 \in F \textit{ is a constant polynomial.}$$

2. Suppose $char(F) = p > 0$. Then, for $a \in F$,

$$\frac{d}{dx}(x^p - a) = px^{p-1} = 0.$$

In fact, for any $f(x) \in F[x]$ we have

$$f'(x) = 0 \quad \Longleftrightarrow \quad f(x) = g(x^p) \quad \textit{for some} \quad g(x) \in F[x].$$

Lemma 51.4. *Suppose $f(x), g(x) \in F[x]$. Then $f(x), g(x)$ have a common zero in $\overline{F}$ if and only if $f(x)$ and $g(x)$ have a nonconstant factor in $F[x]$* (equivalently, if $\gcd(f, g)$ in $F[x]$ is nonconstant).

Proof. ($\Leftarrow$): Suppose $f(x)$ *and* $g(x)$ have a nonconstant factor. Then $f(x) = p(x)f_1(x), g(x) = p(x)g_1(x)$, with $p, f_i, g_1 \in F[x]$ and $\deg(p) > 0$. So, $p(x)$ has a zero in $\overline{F}$, which would also be a common zero of $f(x)$ *and* $g(x)$. So, this implication is proved.

($\Rightarrow$): Suppose $f(x), g(x)$ have a common zero $\alpha \in \overline{F}$ in $\overline{F}$. So, $f(\alpha) = g(\alpha) = 0$.
Consider the ideal $I = F[x]f + F[x]g$. Since $F[x]$ is a PID, $I = F[x]f + F[x]g = [F[x]h$. If is enough to prove that h is a nonconstant polynomial. If h is constant then

$$I = F[x]f + F[x]g = F[x]h = F[x].$$

So,

$$1 = \lambda(x)f(x) + \eta(x)g(x) \quad for\ some \quad \lambda, \eta \in F[x].$$

Substituting $x = \alpha$ we have

$$1 = \lambda(\alpha)f(\alpha) + \eta(\alpha)g(\alpha) = 0, \quad which\ is\ a\ contradiction.$$

So, h is nonconstant. The proof is complete. ∎

Lemma 51.5 (H5.5.2)**.** *Let $f(x) \in F[x]$ be a polynomial. Then f has a multiple zero in $\overline{F}$ if and only if f, f' have a common nontrivial factor in $F[x]$.*

Proof. For the proof, we can assume f is MONIC.

Suppose f has a multiple zero $\alpha \in \overline{F}$. Then

$$f(x) = (x - \alpha)^2 g(x) \quad for\ some\ g(x) \in \overline{F}[x].$$

So,

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x) = (x - \alpha)(2g(x) + (x - \alpha)g'(x))$$

So, α is a common zero of f, f'. By (51.4), f, f' have a common nontrivial factor in $F[x]$.

Conversely, suppose f, f' have a common nontrivial factor in $F[x]$. If f does not have a multiple zero, then

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n), \quad with \quad \alpha_i \in \overline{F}, \quad \alpha_i \neq \alpha_j \quad \forall i \neq j.$$

By product rule

$$f'(x) = \sum_{i=1}^{n} \frac{(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)}{(x - \alpha_i)}$$

It follows

$$f'(\alpha_1) = (\alpha_1 - \alpha_2) \cdots (\alpha_1 - \alpha_n) \neq 0.$$

Similarly,

$$f'(\alpha_i) \neq 0 \qquad \forall \;\; i = 1, \ldots, n.$$

So, f, f' have no common zero. So, they have no common factor, by (51.4). The proof is complete. ∎

Corollary 51.6. *Suppose $f(x) \in F[x]$ is an irreducle polynomial.*

1. *If $char(F) = 0$, then f has no multiple zero.*
2. *If $char(F) = p > 0$ then the following are equivalent:*
   - *(a) f has a multiple zero*
   - *(b) $f'(x) = 0$,*
   - *(c) $f(x) = g(x^p)$ for some $g \in F[x]$.*

Proof. Suppose f has a multiple zero. Then by (51.5), f *and* f' have a nontrivial common factor. Since, f is irreducible, its only notrivial factor is f. So, $f(x)$ divides f'. Since $\deg(f') < \deg(f)$, it follows $f' = 0$. If $char(F) = 0$ then this is impossible. If $char(F) = p > 0$ then $f' = 0$ means $f(x) = g(x^p)$ for some $g \in F[x]$.

Now suppose $char(F) = p > 0$. We just saw this implies $f'(x) = 0$. Then $f'(x) = 0 \Longrightarrow f(x) = g(x^p)$ for some $g \in F[x]$.

Now, if $f(x) = g(x^p) \Longrightarrow f'(x) = 0$ for some $g \in F[x]$. Then, $f'(x) = 0$. So, f, f' have a common factor. So, f has a multiple zero by (51.5). The proof is complete. ∎

Corollary 51.7. *Suppose $char(F) = p \neq 0$. Then, $f(x) = x^{p^n} - x$ has no multiple zero.*

Proof. $f'(x) = -1$ does not have any common factor with f. The proof is complete. ∎

51.2 Seperable Extansions

51.3 For simple extension $F \hookrightarrow F(\alpha)$

Definition 51.8. *Suppose $F \hookrightarrow E$ is a field extension and $\alpha \in E$ is algebraic over F. Assume $E \subseteq \overline{F}$. We say that α* **is seperable over** *F if all the zeros of $irr(\alpha, F)$ in $\overline{F}$ are simple zeros. That means*

$$irr(\alpha, F) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n), \quad with \quad \alpha_i \in \overline{F}, \quad \alpha, \alpha_2, \ldots, \alpha_n \text{ are distinct.}$$

By (51.6), this is equivalent to saying $\frac{d}{dx} irr(\alpha, F) \neq 0$.

Corollary 51.9. *Suppose $F \hookrightarrow E$ is an algebraic field extension.* (Assume $E \subseteq \overline{F}$). *If $char(F) = 0$, then for any $\alpha \in E$, α is seperable over F.*

Proof. Let $p(x) = irr(\alpha, F)$. Since $char(F) = 0$, then $p'(x) \neq 0$. So, p has no multiple zero. So, α is seperable over F. The proof is complete. ∎

Remark. This corollary 51.9, means seperability is NOT an issue when $char(F) = 0$.

Lemma 51.10. *Suppose $F \hookrightarrow E$ is a field extension and $\alpha \in E$. Assume $E \subseteq \overline{F}$. Then, α is seperable, over F, if and only if*

$$|Emb_j(F(\alpha))| = [F(\alpha) : F] \quad where \quad j : F \hookrightarrow \overline{F} \text{ is a } fixed \text{ inclusion.}$$

(That means if and only if index=degree.)

Proof. Suppose $p(x) = irr(\alpha, F)$ and $\deg(f) = n = [F(\alpha) : F]$. Suppose α is seperable over F. Then, f has n distinct zeros $\beta_1 = \alpha, \beta_2, \ldots, \beta_n \in \overline{F}$. Then, for $i = 1, \ldots, n$ there is an embedding (see 48.1)

$$\psi_{\alpha,\beta_i} : F(\alpha) \longrightarrow \overline{F} \qquad \psi_{\alpha,\beta_i}(\alpha) = \beta_i, \quad \psi_{\alpha,\beta_i}\psi_{\alpha,\beta_i}(x) = x \ \ \forall x \in F.$$

In fact,

$$Emb_{j,F}(F(\alpha)) = \{\psi_{\alpha,\beta_i} : i = 1, \ldots, n\}.$$

So, $|Emb_{j,F}(F(\alpha))| = n = [F(\alpha) : F]$.

Conversely, suppose $|Emb_{j,F}(F(\alpha))| = [F(\alpha) : F] = n$. Write

$$Emb_{j,F}(F(\alpha)) = \{\epsilon_i : i = 1, \ldots, n\}$$

Then, $\beta_i = \epsilon_i(\alpha)$ are n distinct zeros of p. So, p has no multiple zero. So, α is seperable over F. The proof is complete. ∎

51.4 For finite extensions $F \hookrightarrow E$

Definition 51.11. *Suppose $F \hookrightarrow E$ is a finite extension.*

1. *We say $F \hookrightarrow E$ is a* **seperable extension**, *if*

$$\textit{the index} = |Emb_j(E)| = [E : F] \quad \textit{the degree.}$$

2. *An irreducible polynomial $p(x)$ is said to be a* **seperable polynomial**, *if $p'(x) \neq 0$.* This is equivalent to saying p has no multiple zero.

Remark. For simple finite extensions $F \hookrightarrow F(\alpha)$ two definitions 51.8 and 51.11, of seperability coincides due to lemma 51.10.

Theorem 51.12 (51.7)**.** *Suppose $i : F \hookrightarrow E, \iota : E \hookrightarrow K$ are fintie field extensions. Then $F \hookrightarrow K$ is seperable if and only if both $i : F \hookrightarrow E$, and $\iota : E \hookrightarrow K$ are seperable.*

Proof. We have, by (49.9),

$$|Emb_F(K)| = |Emb_E(K)||Emb_F(E)|. \quad Further \quad [K : F] = [K : E][E : F].$$

Also, by (49.6)

$$|Emb_F(K)| \leq [K : F], \quad |Emb_E(K)| \leq [K : E], \quad |Emb_F(E)| \leq [E : F].$$

Now, $F \hookrightarrow K$ is seperable,

$$\implies |Emb_F(K)| = [K : F] \implies |Emb_E(K)| = [K : E], \ |Emb_F(E)| = [E : F]$$

So, $i : F \hookrightarrow E$, and $\iota : E \hookrightarrow K$ are seperable.

Conversely, if $i : F \hookrightarrow E$, and $\iota : E \hookrightarrow K$ are seperable. then Now, $F \hookrightarrow K$ is seperable. The proof is complete. ∎

Before we do the next important corollary, we have this lemma.

Lemma 51.13. *Suppose $F \hookrightarrow E \hookrightarrow K$ be extensions of fields. Let $\alpha \in K$ be algebraic over F and is seperable over K. Then, α is seperable over E.*

Proof. Suppose $p(x) = irr(\alpha, F)$ and $q(x) = irr(\alpha, E)$. Then, q divides p. So, $p(x) = q(x)g(x) \in E[x]$. Since p has no multiple zero, q does not have any multiple zero. So, α is seperable over E. The proof is complete. ∎

Corollary 51.14. *A finite extension $F \hookrightarrow E$ is seperable if and only if each $\alpha \in E$ are seperable* (see definition 51.8)

Proof. Suppose $F \hookrightarrow E$ is seperable and $\alpha \in E$. Then, $F \hookrightarrow F(\alpha) \hookrightarrow E$. So, by (51.12), $F \hookrightarrow F(\alpha)$ is seperable. So, by (51.10) $\alpha \in E$ is seperable (*as in defintions 51.8*).

Conversely, suppose $F \hookrightarrow F(\alpha)$ is seperable, for all $\alpha \in E$. Since $F \hookrightarrow E$ is finite, $E = F(\alpha_1, \ldots, \alpha_n)$. We have a chain of field extensions:

$$F \hookrightarrow F(\alpha_1) \hookrightarrow \cdots F(\alpha_1, \ldots, \alpha_{k-1}) \hookrightarrow F(\alpha_1, \ldots, \alpha_{k-1}, \alpha_k) \cdots \hookrightarrow E = F(\alpha_1, \ldots, \alpha_n).$$

By induction $F \hookrightarrow F(\alpha_1, \ldots, \alpha_{k-1})$ is seperable. Since, α_k is seperable over F, by (51.13), α_k is seperable over $F(\alpha_1, \ldots, \alpha_{k-1})$. By induction $F \hookrightarrow F(\alpha_1, \ldots, \alpha_{k-1})$ is seperable. So, by (51.12), $F \hookrightarrow F(\alpha_1, \ldots, \alpha_{k-1}, \alpha_k)$ is seperable. The proof is complete. ∎

51.5 When $char(F) = 0$

Corollary 51.15. *Suppose $F \hookrightarrow E$ is a finite extension and $char(F) = 0$. Then, $F \hookrightarrow E$ is a seperable extension.*

Proof. Follows immediately from (51.14) and (51.8). The proof is complete.∎

51.6 For algebraic extensions $F \hookrightarrow E$

We define seperable extensions $F \hookrightarrow E$ for algebraic extensions that are not necessarily finite.

Definition 51.16. *Suppose $F \hookrightarrow E$ is an algebraic extension. We say $F \hookrightarrow E$ is a seperable extension, if each $\alpha \in E$ is algebraic over F.*

51.7 The Premitive Element Theorem

Definition 51.17. *Recall an extension $F \hookrightarrow F(\alpha)$ of fields is called a* **simple extension**.

Theorem 51.18 (51.15)**.** *Suppose $F \hookrightarrow E$ is a finite seperable extension. Then, $E = F(\alpha)$, for some $\alpha \in E$.* (In other words, finite seperable extensions are simple)

Proof. If F is finite, so is E. Then E^* is generated by one element α, as a group.(*We skipped the proof*) So, $E = F(\alpha)$.

Now assume F is an infinete field. We have $E = F(\alpha_1, \ldots, \alpha_n)$. We will use induction. By induction $F(\alpha_1, \ldots, \alpha_{n-1}) = F(\beta)$ for some β. With $\gamma = \alpha_n$, we have $E = F(\alpha_1, \ldots, \alpha_n) = F(\beta, \gamma)$. Let

$$p(x) = irr(\beta, F), \qquad q(x) = irr(\gamma, F).$$

Let

$$\beta_1 := \beta, \beta_2, \ldots, \beta_n \in \overline{F} \quad \textit{be distinct zeros of} \quad p$$

and

$$\gamma_1 := \gamma, \gamma_2, \ldots, \gamma_m \in \overline{F} \quad \textit{be distinct zeros of} \quad q.$$

So,

$$p(x) = (x - \beta)(x - \beta_2) \cdots (x - \beta_n), \qquad q(x) = (x - \gamma)(x - \gamma_2) \cdots (x - \gamma_m).$$

Since F is infinite, there is an $a \in F$ such that

$$a \neq \frac{\beta_i - \beta}{\gamma - \gamma_j} \quad \forall \;\; i, j \;\; \textit{with} \;\; j \neq 1.$$

So,

$$a(\gamma - \gamma_j) \neq \beta_i - \beta. \qquad So, \qquad \beta + a\gamma \neq \beta_i + a\gamma_j \qquad \forall \;\; i, j \;\; \textit{with} \;\; j \neq 1.$$

$$Let \quad \alpha = \beta + a\gamma. \qquad So, \qquad \alpha - a\gamma_j \neq \beta_i \qquad \forall \;\; i, j \;\; \textit{with} \;\; j \neq 1.$$

$$Write \qquad h(x) = p(\alpha - ax) \in F(\alpha)[x].$$

Then,

$$h(\gamma) = p(\alpha - a\gamma) = p(\beta) = 0, \quad \textit{and} \quad h(\gamma_j) = p(\alpha - a\gamma_j) \neq 0 \ \forall\, j = 2, 3, \ldots, m.$$

So h, q has a common factor in $F(\alpha)[x]$. In $\overline{F}$ only common zero of g and h is γ. So, only common factor of q and h in $\overline{F}[x]$ is $x - \gamma$. So, $x - \gamma$ is also the common factor of q and h in $F(\alpha)[x]$. So, $\gamma \in F(\alpha)$. Also, $\beta = \alpha - a\gamma \in F(\alpha)$. So, $E \subseteq F(\alpha) \subseteq E$. The proof is complete. ∎

Corollary 51.19. *Suppose $F \hookrightarrow E$ is a finite field extension and $char(F) = 0$. Then, $E = F(\alpha)$ for some $\alpha \in E$.*

Proof. In this case, $F \hookrightarrow E$ is seperable. So, (51.18) applies. The proof is complete. ∎

52 Totally Inseperable Fields

Skip.

53 Galois Theory

This section may be considered as the "climax" of all of what we did on Fields. The author considers it as the climax of the entire textbook. As was done in the textbook, lest me also recall all the major results we developed in Part X.

1. (Theorem 48.6): Suppose $F \hookrightarrow E \hookrightarrow \overline{F}$ and $\alpha \in E$. Suppose $\beta \in \overline{F}$ is a conjugate of α. Then, there is an isomorphism:
$$\psi_{\alpha,\beta} : F(\alpha) \xrightarrow{\sim} F(\beta) \quad \alpha \mapsto \beta, \quad and \quad \psi_{\alpha,\beta}(x) = x \ \ \forall\ x \in F.$$

2. Suppose $F \hookrightarrow E \hookrightarrow \overline{F}$ and $\sigma \in G(\overline{F}/F)$. Then, $\sigma(\alpha)$ is a conjugate of α, for any $\alpha \in E$.

3. Suppose $F \hookrightarrow E$ is an extension of fields and $S \subseteq G(E/F)$. Then,
$$E_S = \{\alpha \in E : \sigma(\alpha) = \alpha \ \ \forall \ \ \sigma \in S\} \quad is\ a\ field.$$
E_S is called the **fixed field of** S.
$$We\ also\ have \qquad F \hookrightarrow E_S \hookrightarrow E.$$
$$In\ particular \qquad F \hookrightarrow E_{G(E/F)} \hookrightarrow E.$$

4. (Theorem 50.5, 50.8): Suppose $F \hookrightarrow E \hookrightarrow \overline{F}$ and E is a splitting field over F. Then,
$G(E/F) = Emb_F(E)$. $\qquad In\ particular, \quad |G(E/F)| = |Emb_F(E)| = Index.$

5. Suppose $F \hookrightarrow E$ is a finite field extension. Then
the index $\ |Emb_F(E)|\ $ *divides* degree $\ [E : F]$ $\qquad$ (I skiped)
If $F \hookrightarrow E$ is a finite seperable field extension, then
$$Then,\ the\ index \quad |Emb_F(E)| = [E : F].$$
Also, $F \hookrightarrow E$ is seperable if and only if $irr(\alpha, F)$ has all zeros with multiplicity 1.

6. Finally, suppose $F \hookrightarrow E$ is a finite seperable splitting field extension. Then,
$$|G(E/F)| = Emb_F(E)| = [E : F].$$

7. Suppose $char(F) = 0$. Then any algebraic extension $F \hookrightarrow E$ of fields is seperable.

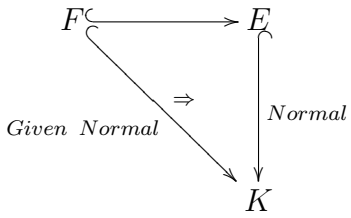
53.1 Normal Extension

Definition 53.1. *Suppose $F \hookrightarrow E$ is a finite extension. We say $F \hookrightarrow E$ is a* **normal extension**, *if it is a seperable splitting field over F.* In particular, if $char(F) = 0$ then a spilitting field extension is called a **normal extension**.

Definition 53.2. *Suppose $F \hookrightarrow E$ is a finite normal extension. Then $G(E/F)$ is called the* **Galois Group of E over F.**

Theorem 53.3 (53.2)**.** *Suppose $F \hookrightarrow E \hookrightarrow K \hookrightarrow \overline{F}$ are field extensions. Suppse K s a finite normal extension of F. Then,*

1. *$E \hookrightarrow K$ is a finite normal extension of E. Diagramatically stated as:*



2. *We have*
$$G(K/E) = \{\sigma \in G(K/F) : \sigma_{|E} = Id_E\}.$$

3. *For $\sigma, \tau \in G(K/F)$ we have*
$$\sigma_{|E} = \tau_{|E} \qquad \Longleftrightarrow \qquad the\ left\ cosets \quad \sigma G(K/E) = \tau G(K/E).$$

Proof. Since $F \hookrightarrow K$ is seperable, by (51.12), so is $E \hookrightarrow K$. Now, suppose $\sigma \in Emb_E(K)$. Since $Emb_E(K) \subseteq Emb_F(K)$, we have $\sigma \in Emb_F(K)$. Since $F \hookrightarrow K$ is a splitting field, by (50.5) $\sigma_{|K} \in G(K/F)$. So, $\sigma_{|K}$ is a automorphism. So, by (50.5), $E \hookrightarrow K$ is a splitting field over E and hence norma over E. So, (1) is established.

Note (2), only gives a description of $G(K/E)$ and there is nothing to prove. However, $G(K/E)$ is a subgroup of $G(K/F)$. Now, suppose $\sigma, \tau \in G(K/F)$ and $\sigma_{|E} = \tau_{|E}$. So, $(\tau^{-1}\sigma)_{|E} = Id_E$. Therefore, $(\tau^{-1}\sigma) \in G(K/E)$.

So, $\tau G(K/E) = \sigma G(K/E)$. Conversely, suppose $\tau G(K/E) = \sigma G(K/E)$. Then $(\tau^{-1}\sigma) \in G(K/E)$. So, $(\tau^{-1}\sigma)_{|E} = Id_E$. Therefore, $\sigma_{|E} = \tau_{|E}$. So, (3) is established. The proof is complete. ∎

Question: With notations as in (53.3) and in the light of it, the question reamins, when is $F \hookrightarrow E$ is normal?

53.2 The Main Theorem of Galois Theory

Definition 53.4. *Suppose K is a finite normal extension of a field F. Then that group $G(K/F)$ is called the* **Galois group of K over F.**

Theorem 53.5 (53.6)**.** *Let K be a finite normal extension of a field F. We assume $F \hookrightarrow K \hookrightarrow \overline{F}$. Denote*

$$\mathcal{F} = \{E : F \hookrightarrow E \hookrightarrow K \text{ are field extensions}\}$$

and

$$\mathcal{G} = \{H : H \subseteq G(K/F) \text{ is a subgroup}\}.$$

Define a map

$$\lambda : \mathcal{F} \longrightarrow \mathcal{G} \quad by \quad \lambda(E) = G(K/E).$$

Conversely, define

$$\Phi : \mathcal{G} \longrightarrow \mathcal{F} \quad by \quad \Phi(H) = K_H.$$

Then,

1. $\Phi\lambda = Id_{\mathcal{F}}$. *That means, for $E \in \mathcal{G}$ we have*

$$E = \Phi\lambda(E) = \Phi(G(K/E)) = K_{G(K/E)}.$$

2. *Also, $\lambda\Phi = Id_{\mathcal{G}}$. That means, for subgroups $H \subseteq G(K/E)$, we have*

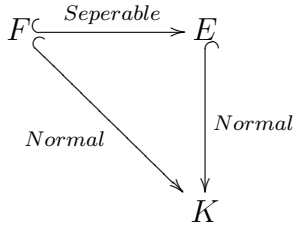
$$H = \lambda\Phi(H) = \lambda(K_H) = G(K/K_H).$$

3. *λ, Φ are bijections and inverses of each other.*

4. *For $E_1, E_2 \in \mathcal{F}$ we have*

$$E_1 \subseteq E_2 \iff \quad G(K/E_1) \supseteq G(K/E_2), \quad \text{that mean} \quad \iff \lambda(E_1) \supseteq \lambda(E_2).$$

Proof. The hypthesis of the theorem is $F \hookrightarrow K$ is a finite normal extension. Along with the immediate consequences (50.9, 51.12), diagramatically, hypothesis is stated as:



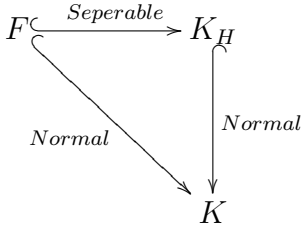
$$\textit{Recall} \quad \textbf{Normal} = \textbf{Seperable} + \textbf{Splitting}$$

To prove (1), it is easy to see

$$E \subseteq K_{G(K/E)}.$$

Now, suppose $\alpha \in K$ and $\alpha \notin E$. We will prove $\alpha \notin K_{G(K/E)}$. Since $E \hookrightarrow K$ is a normal extension, all the zeros of $irr(\alpha, E)$ have multiplicty 1. Since $\alpha \not\in E$, we have $\deg(irr(\alpha, E)) \geq 2$. Let $\beta \in \overline{F}$ be a zero of $irr(\alpha, E)$, such that $\alpha \neq \beta$. Since K is a splitting field over F, $\beta \in K$. Let $\psi_{\alpha,\beta} : E(\alpha) \xrightarrow{\sim} E(\beta$ be as in (48.6). By our "Key Tool" (49.1), $\psi_{\alpha,\beta}$ extends to an automorphism $\tau : \overline{F} \xrightarrow{\sim} \overline{F}$. Again since K is a splitting field, by (50.5) $\sigma = \tau_{|K} \in G(K/e)$. So, $\sigma(\alpha) = \beta \neq \alpha$. So, $\alpha \notin K_{G(K/E)}$. So, $E = K_{G(K/E)}$ and (1) is established.

Now we prove (2). For $H \in \mathcal{G}$, it is clear $H \subseteq G(K/K_H)$. Now we have the diagram



$$\textit{Recall} \quad \textbf{Normal} = \textbf{Seperable} + \textbf{Splitting}$$

Since $K_H \hookrightarrow K$ is seperable, by premitive element theorem (51.18), $K = K_H(\alpha)$ for some $\alpha \in K$. Since $K_H \longrightarrow K$ is a normal extension, by (50.8), and definition of seperability, we have

$$n := \deg(irr(\alpha, K_H) = [K : K_H] = |Emb_{K_H}(K)| = |G(K/K_H)|.$$

$$\textit{Let} \quad |H| = r \quad \textit{and} \quad H = \{\sigma_1 = Id, \sigma_2, \ldots, \sigma_r\}$$

$$and \qquad f(x) = \prod_{i=1}^{r}(x - \sigma_i(\alpha))$$

Coefficients of $f(x)$ are left fixed by H. So, $f(x) \in K_H[x]$. Since $\sigma_1 = Id$, we have α is a zero of f. So, $irr(\alpha, K_H)$ divides f. So, $\deg(f) = r \geq n$.

$$r = |H| \geq |G(K/K_H)|. \quad Since \;\; H \subseteq G(K/K_H) \quad H = G(K/K_H).$$

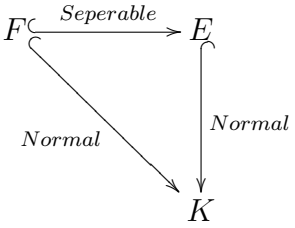
So, (2) is established. Also, (3) follows from (1, 2). Proof of (4) is easy, follows from the defintions.

The proof is complete. ∎

Theorem 53.6 (53p6Part2)**.** *As in (53.5), let $F \hookrightarrow K$ be a finite normal extension. Use the notations as above (53.5). For $E \in \mathcal{F}$, we have the degree*

$$[K : E] = |\lambda(E)| = |G(K/E)| \quad and \quad [E : F] = (G(K/F) : G(K/E)).$$

Proof. As in (53.5), the hypothesis is given by the diagram



Recall **Normal = Seperable + Splitting**

The proof is just number cranchng. First, note $E \hookrightarrow K$ is also a normal extension over E. Since both $F \hookrightarrow K$, $E \hookrightarrow K$ are seperabble and a splitting fields, by defintion and by (50.8),

$$[K : E] = |Emb_E(K)| = |G(K/E)|, \;\; and \;\; [K : F] = |Emb_F(K)| = |G(K/F)|.$$

It also follows

$$[E : F] = \frac{[K : F]}{[K : E]} = \frac{|G(K/F)|}{|G(K/E)|} = (G(K/F) : G(K/E)).$$

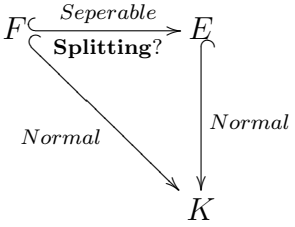
The proof is complete. ∎

Now we state and prove the last part of the Galois theorem:

Theorem 53.7 (53p6Part3)**.** *As in (53.5), let $F \hookrightarrow K$ be a finite normal extension and $F \hookrightarrow E \hookrightarrow K$ be an intermediate field. Use the notations as above (53.5).Then, E is a normal extension of F if and only if $\lambda(E) := G(K/E)$ is a normal subgroup of $G(K/F)$. Further, if $\lambda(E)$ is a normal subgroup of $G(K/F)$, we have*

$$G(E/F) \simeq \frac{G(K/F)}{G(K/E)}.$$

Proof. Again, recall the diagram



Recall **Normal = Seperable + Splitting**

First, suppose $F \hookrightarrow E$ is normal, we prove $G(K/E)$ is normal in $G(K/F)$. Let $\sigma \in G(K/F), \tau \in G(K/E)$. We prove $\sigma^{-1}\tau\sigma \in G(K/E)$. Let $\alpha \in E$. Since E is a splitting field, by (50.5) $\sigma_{|E} \in G(E/F)$. So,

$$\sigma(\alpha) \in E, \quad so \quad \tau(\sigma(\alpha)) = \sigma(\alpha). \qquad Hence, \quad \sigma^{-1}(\tau(\sigma(\alpha))) = \sigma^{-1}\sigma(\alpha) = \alpha.$$

So $(\sigma^{-1}\tau\sigma)_{|E} = Id_E$. So, $\sigma^{-1}\tau\sigma \in G(K/E)$. Therefore, $G(K/E)$ is a normal subgroup of $G(K/F)$.

Conversely, assume $G(K/E)$ is a normal subgroup of $G(K/F)$. We will prove $F \hookrightarrow K$ is normal. We only need to prove E is a splitting field over F. We will use (50.5). So let $\eta \in G(\overline{F}/F)$. Since, $F \hookrightarrow K$ is a splitting field, $\sigma = \eta_{|K} \in G(K/F)$. For $\tau \in G(K/E)$, $\sigma^{-1}\tau\sigma \in G(K/E)$. So, $\alpha \in E$,

$$\sigma^{-1}\tau\sigma(\alpha) = \alpha, \qquad hence \quad \tau(\sigma(\alpha)) = \sigma(\alpha).$$

So,

$$\sigma(\alpha) \in K_{G(K/E)} = E. \quad So, \quad \sigma(E) = \eta(E) \subseteq E.$$

Considering vector space dimension over F, we have $\eta(E) = E$. So, $F \hookrightarrow E$ is normal.

We need to show,

$$G(E/F) \simeq \frac{G(K/F)}{G(K/E)}.$$

Define, by restriction, the homomorphism,

$$\varphi : G(K/F) \longrightarrow G(E/F) \quad by \quad \varphi(\sigma) = \sigma_{|E}.$$

The map φ is well defined, because by (50.5) $\sigma_{|E} \in G(E/F)$. To prove φ is onto, let $\gamma \in G(E/F)$. Then, γ extends to an element in $G(K/F)$. So, $\varphi(\gamma) = \sigma$. Hence φ is onto. Clearly, also $\ker(\varphi) = G(K/F)$. So, by Fundamental theorem, φ induces an isomorphsm, as required. The proof is complete. ∎