# Lecture 15: Splitting Fields and Normal Extensions

## MAT205 Abstract Algebra II


Ma, Jia-Jun

Xiamen University Malaysia

# Part I: Splitting Fields

# Definition: Splitting Field

**Splits.** $f \in F[x]$ of degree $n \geq 1$ *splits* in an extension $E/F$ if it factors into linear factors in $E[x]$:

$$f(x) = c\,(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \qquad c \in F^\times,\ \alpha_i \in E.$$

**Definition.** $E/F$ is a *splitting field for $f$ over $F$* if

(i) $f$ splits in $E$, and

(ii) $E = F(\alpha_1, \ldots, \alpha_n)$ — generated over $F$ by the roots of $f$.

Condition (ii) forces minimality. So $\mathbb{C}$ is *not* a splitting field of $x^2-2$ over $\mathbb{Q}$: it splits there, but $\mathbb{C} \neq \mathbb{Q}(\sqrt{2})$.

**Examples.** $x^2-2$ over $\mathbb{Q}$: $\mathbb{Q}(\sqrt{2})$. $x^2+1$ over $\mathbb{R}$: $\mathbb{C}$. $x^2+x+1$ over $\mathbb{F}_2$: $\mathbb{F}_4$.

# Existence of Splitting Fields

**Convention.** Fix an algebraic closure $\overline{F}$ of $F$. By the isomorphism extension theorem (applied to $\mathrm{id}_F$), every algebraic extension of $F$ embeds into $\overline{F}$, so we view all of them as subfields of $\overline{F}$.

**Theorem.** Every $f \in F[x]$ of degree $n \geq 1$ has a splitting field $E$ over $F$ inside $\overline{F}$, with $[E : F] \leq n!$.

*Proof.*

- $\overline{F}$ is algebraically closed, so $f$ has roots $\alpha_1, \ldots, \alpha_n \in \overline{F}$. Put $E = F(\alpha_1, \ldots, \alpha_n)$ — a splitting field.
- Adjoin the roots one at a time: $[F(\alpha_1) : F] \leq n$, then $[F(\alpha_1, \alpha_2) : F(\alpha_1)] \leq n-1$ (the minimal polynomial of $\alpha_2$ divides $f/(x - \alpha_1)$), and so on.
- Multiplying, $[E : F] \leq n(n-1) \cdots 1 = n!$. □

Without a closure in hand, the roots can instead be built by the Kronecker step $F \rightsquigarrow F[x]/(p)$, iterated — exactly how $\overline{F}$ itself is constructed.

# Uniqueness of Splitting Fields

Inside the fixed $\overline{F}$, the splitting field of $f$ is the one subfield generated by its roots, $E = F(\alpha_1, \ldots, \alpha_n)$ — so "the" splitting field is well-defined. The only question is whether a different algebraic closure gives an isomorphic field.

**Theorem (Fraleigh, Exercise 50.25).** Any two splitting fields of $f$ over $F$ are isomorphic by an isomorphism fixing $F$.

*Proof.*

- Let $E \subseteq \overline{F}$ and $E' \subseteq \overline{F'}$ be splitting fields of $f$ in two algebraic closures of $F$.
- The two closures are $F$-isomorphic via some $\lambda : \overline{F} \to \overline{F'}$ (isomorphism extension theorem).
- $\lambda$ fixes $F$, so it permutes the roots of $f$; hence $\lambda(E) = F(\lambda\alpha_1, \ldots, \lambda\alpha_n) = E'$.
- So $\lambda$ restricts to an isomorphism $E \to E'$. $\square$

# Examples of Splitting Fields

- $x^3 - 2$ **over** $\mathbb{Q}$**.** Roots $\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2}$ with $\omega = e^{2\pi i/3}$. Splitting field $\mathbb{Q}(\sqrt[3]{2}, \omega)$:
$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = \underbrace{2}_{\omega} \cdot \underbrace{3}_{\sqrt[3]{2}} = 6 = 3!.$$
- $x^4 - 2$ **over** $\mathbb{Q}$**.** Roots $\pm\sqrt[4]{2},\ \pm i\sqrt[4]{2}$. Splitting field $\mathbb{Q}(\sqrt[4]{2}, i)$, degree $8$.
- $x^p - 1$ **over** $\mathbb{Q}$ **(**$p$ **prime).** With $\zeta = e^{2\pi i/p}$ a primitive $p$-th root of unity, the splitting field is $\mathbb{Q}(\zeta)$ (cyclotomic field), of degree $p - 1$.
- $x^{p^n} - x$ **over** $\mathbb{F}_p$**.** Its $p^n$ distinct roots form the field $\mathbb{F}_{p^n}$ — so $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$.

# Part II: Normal Extensions

# Definition: Normal Extension

**Definition.** Let $E/F$ be algebraic, inside a fixed algebraic closure $\overline{F}$. Then $E/F$ is *normal* if every $F$-embedding $\sigma : E \to \overline{F}$ has image

$$\sigma(E) = E,$$

i.e. every such $\sigma$ is an $F$-automorphism of $E$ ($E$ is stable under every $F$-automorphism of $\overline{F}$).

**Why "normal."** With $G = \mathrm{Aut}(\overline{F}/F)$ and $H = \mathrm{Aut}(\overline{F}/E)$, the identity $\sigma H \sigma^{-1} = \mathrm{Aut}(\overline{F}/\sigma(E))$ shows $\sigma(E) = E$ for all $\sigma \Rightarrow H \trianglelefteq G$; in the Galois correspondence (separable case) the converse holds too, so normal subextensions match *normal subgroups* — the source of the name.

*Terminology.* Fraleigh's "finite normal extension" (Def 53.1) means a *separable* splitting field — our *Galois* extension. He calls the property above just "splitting field over $F$" (Cor 50.6). We keep the modern split (Hungerford, Dummit–Foote, Lang).

# Worked Example: $x^3 - 2$ over $\mathbb{Q}$ — not normal

In $\overline{\mathbb{Q}} \subset \mathbb{C}$, $x^3 - 2$ has roots $\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2}$ $(\omega = e^{2\pi i/3})$.

Take $E = \mathbb{Q}(\sqrt[3]{2})$, $[E : \mathbb{Q}] = 3$. An $F$-embedding $\sigma : E \to \overline{\mathbb{Q}}$ is fixed by $\sigma(\sqrt[3]{2})$, a root of $x^3 - 2$ — three in all:

- $\sigma_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \quad \sigma_1(E) = \mathbb{Q}(\sqrt[3]{2}) = E;$
- $\sigma_2 : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}, \quad \sigma_2(E) = \mathbb{Q}(\omega\sqrt[3]{2});$
- $\sigma_3 : \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}, \quad \sigma_3(E) = \mathbb{Q}(\omega^2\sqrt[3]{2}).$

But $\omega\sqrt[3]{2} \notin \mathbb{R}$ while $E \subset \mathbb{R}$, so $\sigma_2(E) \neq E$ and $\sigma_3(E) \neq E$: **two embeddings escape** $E$, hence $E/\mathbb{Q}$ is *not* normal. Only $\sigma_1$ is an automorphism, so $|\mathrm{Aut}(E/\mathbb{Q})| = 1 < 3$.

# Worked Example: $x^3 - 2$ — the splitting field is normal

Now $N = \mathbb{Q}(\sqrt[3]{2}, \omega)$, the splitting field of $x^3 - 2$, with $[N : \mathbb{Q}] = 6$; it contains all three roots.

Any $F$-embedding $\tau : N \to \overline{\mathbb{Q}}$ permutes the roots $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ and the pair $\{\omega, \omega^2\}$ (roots of $x^2 + x + 1$). Since $N$ is generated by these, $\tau(N) = N$ for **all six** embeddings — so $N/\mathbb{Q}$ is *normal*, and these six are exactly $\mathrm{Aut}(N/\mathbb{Q}) \cong S_3$, with $|\mathrm{Aut}(N/\mathbb{Q})| = 6 = [N : \mathbb{Q}]$.

$N$ is the *normal closure* of $E = \mathbb{Q}(\sqrt[3]{2})$: $N = \mathbb{Q}(\sigma_1(E), \sigma_2(E), \sigma_3(E))$, the compositum of the three images. "Not normal" = an embedding escapes; the splitting field adjoins the missing conjugates so none can.

# Characterizations of Normality

**Theorem.** For a finite extension $E/F$ inside $\overline{F}$, the following are equivalent. Since (3) is the definition, the content is that (1) and (2) characterize normality.

(1) Every irreducible $p \in F[x]$ with a root in $E$ splits in $E$ — i.e. $E$ contains all conjugates of each element.

(2) $E$ is the splitting field over $F$ of some $f \in F[x]$ (general algebraic case: of some *set* of polynomials).

(3) Every $F$-embedding $\tau : E \to \overline{F}$ has image $\tau(E) = E$ — the definition.

Operational form of (3): every automorphism of $\overline{F}$ fixing $F$ maps $E$ onto itself — a normal extension has no "outward" embeddings, only self-maps. (Fraleigh 50.3 + Cor 50.6; Hungerford Thm V.3.14.)

# Characterization: Proof

$(1) \Rightarrow (2)$. Write $E = F(\alpha_1, \ldots, \alpha_r)$ and set $f = \prod_i m_{\alpha_i,F}$. Each $m_{\alpha_i,F}$ has a root in $E$, so by (1) splits in $E$; thus $E$ is the splitting field of $f$.

$(2) \Rightarrow (3)$. An $F$-embedding $\tau$ sends each root of $f$ to a root of $f$ (it fixes the coefficients), so it permutes the finite root set. Since $E$ is generated by those roots, $\tau(E) = E$.

$(3) \Rightarrow (1)$. Let $p \in F[x]$ be irreducible with a root $\alpha \in E$, and $\beta \in \overline{F}$ any root of $p$. The conjugation isomorphism $F(\alpha) \to F(\beta)$ extends to an embedding $\tau : E \to \overline{F}$ with $\tau(\alpha) = \beta$. By (3), $\beta = \tau(\alpha) \in E$. So $p$ splits in $E$. $\square$

# Examples via the Characterization

**Normal** (each is a splitting field, hence normal):

- $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ — splitting field of $(x^2-2)(x^2-3)$.
- $\mathbb{C}/\mathbb{R}$ — splitting field of $x^2+1$; likewise $\overline{F}/F$.
- $\mathbb{F}_{p^n}/\mathbb{F}_p$ — splitting field of $x^{p^n}-x$; $\quad \mathbb{Q}(\zeta_n)/\mathbb{Q}$ — of $x^n-1$.

**Lemma (degree $2 \Rightarrow$ normal).** If $[E:F]=2$ and $\alpha \in E \setminus F$ has (monic) $m_\alpha = x^2+bx+c$, the second root $\beta = -b-\alpha \in E$ (sum of roots $-b \in F$); so every $F$-embedding sends $\alpha$ into $E$, giving $\sigma(E)=E$.

**Not normal.** $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ — $x^4-2$ has $\sqrt[4]{2}$ but not $\pm i\sqrt[4]{2}$ (the embedding $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$ escapes). [$\mathbb{Q}(\sqrt[3]{2})$: the worked example above.]

# Normal Closure

**Theorem.** Every finite $E = F(\alpha_1, \ldots, \alpha_r)$ sits inside a smallest normal extension of $F$: the splitting field $N$ of $f = m_{\alpha_1,F} \cdots m_{\alpha_r,F}$, the *normal closure* of $E/F$.

- $N$ is normal (a splitting field) and contains $E$; any normal extension containing $E$ contains every conjugate of each $\alpha_i$, hence contains $N$ — so $N$ is minimal.
- Equivalently, $N$ is the compositum of all images $\tau(E)$, $\tau$ ranging over the $F$-embeddings $E \to \overline{F}$.

**Example.** $E = \mathbb{Q}(\sqrt[3]{2})$ has three $\mathbb{Q}$-embeddings into $\overline{\mathbb{Q}}$, sending $\sqrt[3]{2}$ to $\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2}$. The compositum of their images is $N = \mathbb{Q}(\sqrt[3]{2}, \omega)$, the splitting field of $x^3 - 2$ — degree $6$.

# Normality under Composites and Intersections

**Theorem.** If $E_1, E_2$ are finite normal extensions of $F$ inside $\overline{F}$, then the compositum $E_1E_2$ and the intersection $E_1 \cap E_2$ are normal over $F$.

*Proof.* Use the automorphism form: $K/F$ is normal iff every $F$-automorphism $\sigma$ of $\overline{F}$ fixes $K$ setwise. For such $\sigma$, normality of $E_1, E_2$ gives $\sigma(E_1) = E_1$ and $\sigma(E_2) = E_2$, so

$$\sigma(E_1E_2) = E_1E_2, \qquad \sigma(E_1 \cap E_2) = E_1 \cap E_2.$$

Both are stable under every such $\sigma$, hence normal. □

By contrast, stacking two normal steps need not give a normal extension — normality is not transitive.

**Example.** $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are normal; their compositum $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is normal, their intersection is $\mathbb{Q}$.

# Normality Is Not Transitive

Consider the tower

$$\mathbb{Q} \;\subset\; \mathbb{Q}(\sqrt{2}) \;\subset\; \mathbb{Q}(\sqrt[4]{2}).$$

- Each step has degree $2$, hence is normal.
- But $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is *not* normal: $x^4 - 2$ has the root $\sqrt[4]{2}$ but its roots $\pm i\sqrt[4]{2}$ are non-real, so not in $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$.

So two stacked normal steps need not give a normal extension. (By contrast, algebraicity is transitive.) What is always true: if $E/F$ is normal, then $E/K$ is normal for every intermediate $K$.

# The Index $\{E : F\}$ and the Bound $\{E : F\} \leq [E : F]$

**Definition.** $\{E : F\}$ is the number of $F$-embeddings $E \to \overline{F}$.

**The chain.**

$$|\mathrm{Aut}(E/F)| \;\leq\; \{E : F\} \;\leq\; [E : F].$$

- $|\mathrm{Aut}(E/F)| \leq \{E : F\}$: every $F$-automorphism of $E$ is in particular an $F$-embedding $E \to \overline{F}$ (its image is $E$).
- $\{E : F\} \leq [E : F]$: for $E = F(\alpha)$, an $F$-embedding sends $\alpha$ to a root of $m_\alpha$, and $m_\alpha$ has at most $\deg m_\alpha = [F(\alpha) : F]$ roots, so $\{F(\alpha) : F\} \leq [F(\alpha) : F]$. Index and degree are both multiplicative over a tower, so the bound multiplies up to $\{E : F\} \leq [E : F]$.

# Index and Normality

Two equalities in the chain $|\mathrm{Aut}(E/F)| \leq \{E : F\} \leq [E : F]$, two properties:

- $|\mathrm{Aut}(E/F)| = \{E : F\} \iff E/F$ normal (Fraleigh Cor 50.7): the embeddings with image $E$ are exactly the automorphisms, so the counts agree iff *every* embedding has image $E$ — which is normality.
- $\{E : F\} = [E : F] \iff E/F$ separable: the bound $\{F(\alpha) : F\} \leq [F(\alpha) : F]$ is an equality iff $m_\alpha$ has $\deg m_\alpha$ *distinct* roots, i.e. no repeated roots — the definition of $\alpha$ separable; multiplicativity lifts this to $E/F$.

*Separable regime.* Over a perfect field (char $0$ or finite — most of this course), $\{E : F\} = [E : F]$ automatically, so $|\mathrm{Aut}(E/F)| = [E : F] \iff E/F$ normal.

# Galois Extensions = Normal + Separable

**Theorem.** For a finite extension $E/F$,

$$|\mathrm{Aut}(E/F)| = [E:F] \quad \iff \quad E/F \text{ normal and separable.}$$

Both inequalities $|\mathrm{Aut}(E/F)| \leq \{E:F\} \leq [E:F]$ become equalities: normal closes the left, separable the right.

**Definition.** Such an $E/F$ is a *Galois extension*; one writes $\mathrm{Gal}(E/F) := \mathrm{Aut}(E/F)$. (This is Fraleigh's "finite normal extension", Def 53.1.)

- $\mathbb{F}_{p^n}/\mathbb{F}_p$: Galois, $\mathrm{Gal} \cong \mathbb{Z}/n\mathbb{Z}$.
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$: Galois, $|\mathrm{Gal}| = 4$.
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$: not Galois — $|\mathrm{Aut}| = 1 < 3$, the deficit is non-normality.

# Worked Example: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ Is Galois

$E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $[E : \mathbb{Q}] = 4$, basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. A $\mathbb{Q}$-automorphism sends $\sqrt{2} \mapsto \pm\sqrt{2}$ and $\sqrt{3} \mapsto \pm\sqrt{3}$ — four of them:

| | id | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $\sqrt{2}$ | $\sqrt{2}$ | $\sqrt{2}$ | $-\sqrt{2}$ | $-\sqrt{2}$ |
| $\sqrt{3}$ | $\sqrt{3}$ | $-\sqrt{3}$ | $\sqrt{3}$ | $-\sqrt{3}$ |

- $\mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}, a, b, c\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, with $|\mathrm{Gal}| = 4 = [E : \mathbb{Q}]$.
- $E$ is the splitting field of $(x^2 - 2)(x^2 - 3)$ (normal) and separable — hence Galois.
- Fixed fields: $\langle a \rangle \to \mathbb{Q}(\sqrt{2})$, $\langle b \rangle \to \mathbb{Q}(\sqrt{3})$, $\langle c \rangle \to \mathbb{Q}(\sqrt{6})$ — three subgroups matching three intermediate fields, the Galois correspondence.