Lecture 16: Finite Galois Theory — The Fundamental Theorem

MAT205 Abstract Algebra II

Ma, Jia-Jun

Xiamen University Malaysia

Part I: Statement

Setup: the Galois Group and the Two Maps

Recall. E/F finite is *Galois* if normal and separable, equivalently $|\mathrm{Aut}(E/F)| = [E : F]$. Its *Galois group* is $G := \mathrm{Gal}(E/F) := \mathrm{Aut}(E/F)$, with $|G| = [E : F]$.

Two maps, between intermediate fields $F \subseteq K \subseteq E$ and subgroups $H \leq G$:

- field $\to$ group: $K \mapsto \mathrm{Gal}(E/K) = \{\sigma \in G : \sigma|_K = \mathrm{id}\}$;
- group $\to$ field: $H \mapsto E^H = \{x \in E : \sigma x = x \ \forall \sigma \in H\}$, the *fixed field*.

Both **reverse inclusions**: $K_1 \subseteq K_2 \Rightarrow \mathrm{Gal}(E/K_2) \leq \mathrm{Gal}(E/K_1)$, and $H_1 \leq H_2 \Rightarrow E^{H_2} \subseteq E^{H_1}$.

Fixed Field: Definition and Example

Definition. For $S \subseteq \mathrm{Aut}(E)$,

$$E^S = \{x \in E : \sigma(x) = x \text{ for all } \sigma \in S\}.$$

Example. $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $G = \{\mathrm{id}, a, b, c\} \cong V_4$ (the Klein four-group):

- $a : \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}$;
- $b : \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto \sqrt{3}$;
- $c = ab : \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}$.

Fixed fields here: $E^{\langle a \rangle} = \mathbb{Q}(\sqrt{2})$, $E^{\langle b \rangle} = \mathbb{Q}(\sqrt{3})$, $E^{\langle c \rangle} = \mathbb{Q}(\sqrt{6})$ (c fixes $\sqrt{2}\sqrt{3} = \sqrt{6}$), $E^G = \mathbb{Q}$.

Fixed Field: Basic Properties

Let $S \subseteq \mathrm{Aut}(E)$. Then:

- **Subfield.** E^S is a subfield of E ($0, 1 \in E^S$; closed under $+, -, \cdot, (\cdot)^{-1}$, since each σ is a field homomorphism).
- **Inclusion-reversing.** $S \subseteq T \Rightarrow E^T \subseteq E^S$ (more automorphisms to fix $\Rightarrow$ fewer fixed elements).
- **Generated subgroup suffices.** $E^{\langle S \rangle} = E^S$ — only the subgroup of $\mathrm{Aut}(E)$ generated by S matters.
- **Base-field containment.** Always $F \subseteq E^{\mathrm{Gal}(E/F)}$, by definition of $\mathrm{Gal}(E/F)$.
- **Galois characterization.** E/F finite Galois $\iff$ $E^{\mathrm{Gal}(E/F)} = F$ (recall from L15).

The Main Theorem of Galois Theory (Fraleigh 53.6)

Theorem. Let E/F be a finite Galois extension with $G = \mathrm{Gal}(E/F)$. For intermediate $F \subseteq K \subseteq E$, set $\lambda(K) = \mathrm{Gal}(E/K) \leq G$. Then λ is a **one-to-one map** of intermediate fields **onto** subgroups of G, with:

1. $\lambda(K) = \mathrm{Gal}(E/K)$.
2. $K = E^{\mathrm{Gal}(E/K)} = E^{\lambda(K)}$.
3. For $H \leq G$, $\lambda(E^H) = H$.
4. $[E : K] = |\lambda(K)|$ and $[K : F] = [G : \lambda(K)]$.
5. K/F is normal $\iff \lambda(K) \trianglelefteq G$; when so, $\mathrm{Gal}(K/F) \cong G/\lambda(K)$.
6. The lattice of subgroups of G is the *inverted* lattice of intermediate fields.

Anchors: $E \leftrightarrow \{1\}$, $F \leftrightarrow G$.

The Correspondence: Field Tower $\leftrightarrow$ Subgroup Tower

λ and $E^{(\cdot)}$ are mutually inverse and reverse inclusions, so the field tower and the subgroup tower are the same diagram flipped top to bottom.

$$\begin{tikzcd}
E \arrow[r, dotted, no head] \arrow[d, no head, "{[E:K]}"'] & \{1\} \arrow[d, no head, "|H|"] \\
K \arrow[r, bend left, "K \mapsto \mathrm{Gal}(E/K)"] \arrow[d, no head, "{[K:F]}"'] & H \arrow[l, bend left, "H \mapsto E^H"] \arrow[d, no head, "{[G:H]}"] \\
F \arrow[r, dotted, no head] & G
\end{tikzcd}$$

Going down the left tower the field shrinks $(E \to F)$; going down the right tower the group grows $(\{1\} \to G)$. Matched edges: $[E:K] = |H|$, $[K:F] = [G:H]$.

Part II: Proof of the Main Theorem

Recap: Conjugates, Embeddings, the Index

Fields $F \subseteq E \subseteq \overline{F}$.

- **Minimal polynomial.** For α algebraic over F, m_α^F denotes the unique monic irreducible polynomial in $F[x]$ with α as a root.
- **Conjugates.** α, β algebraic over F are *conjugate* if $m_\alpha^F = m_\beta^F$. Then there is an F-isomorphism $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$, $\alpha \mapsto \beta$.
- **Isomorphism Extension Theorem.** ψ extends to any normal $E \supseteq F(\alpha), F(\beta)$ inside $\overline{F}$.
- **The index.** $\{E : F\}$ = number of F-embeddings $E \to \overline{F}$.
- **Index chain.** $|\mathrm{Aut}(E/F)| \leq \{E : F\} \leq [E : F]$.
- **Separability + splitting.** Separable $\iff$ $\{E : F\} = [E : F]$; splitting field $\iff$ every F-embedding has image E $\iff$ $|\mathrm{Aut}(E/F)| = \{E : F\}$.
- **Galois.** Finite Galois = normal + separable $\iff$ $|\mathrm{Aut}(E/F)| = \{E : F\} = [E : F]$.

Restriction Theorem (Fraleigh 53.2) — Statement

When E/F is finite Galois, every intermediate field inherits the Galois structure, and the cosets of $\mathrm{Gal}(E/K)$ in G count the F-embeddings of K.

Theorem (Fraleigh 53.2). Let E/F be finite Galois with $G = \mathrm{Gal}(E/F)$, and $F \subseteq K \subseteq E$. Set $H := \mathrm{Gal}(E/K)$. Then:

1. E/K is finite Galois.
2. $H = \{\sigma \in G : \sigma|_K = \mathrm{id}\} \leq G$.
3. For $\sigma, \tau \in G$: $\sigma|_K = \tau|_K \iff \sigma, \tau$ lie in the same left coset of H in G.

Consequence. The F-embeddings of K in $\overline{F}$ correspond to the left cosets G/H. Since K/F is separable (a subextension of separable E/F), $\{K : F\} = [K : F]$; hence $[K : F] = [G : H]$.

Restriction Theorem — Proof

(1) E/K Galois. E is a separable splitting field over F; the splitting polynomials, viewed over $K \supseteq F$, still split in E. Separability of an element over F is preserved when the base field is enlarged to K (the irreducible polynomial over K divides the one over F, hence is still separable). So E/K is Galois.

(2) Subgroup. Every $\sigma \in \mathrm{Gal}(E/K)$ fixes F pointwise (since $F \subseteq K$), so $\sigma \in G$. Composition and inverses preserve "fixes K"; hence $H \leq G$.

(3) Cosets and restrictions. For $\sigma, \tau \in G$:

$$\sigma|_K = \tau|_K \iff \tau^{-1}\sigma|_K = \mathrm{id}_K \iff \tau^{-1}\sigma \in H \iff \sigma \in \tau H. \quad \square$$

Dedekind: Independence of Characters — Statement

A *character* of E into L is a multiplicative homomorphism $\chi : E^\times \to L^\times$. Each F-embedding $\sigma : E \to L$ restricts to a character $E^\times \to L^\times$; distinct embeddings give distinct characters.

Lemma (Dedekind). Distinct characters $\sigma_1, \ldots, \sigma_n : E^\times \to L^\times$ are *linearly independent over* L: if $a_1, \ldots, a_n \in L$ satisfy

$$a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0 \quad \forall x \in E^\times,$$

then $a_1 = \cdots = a_n = 0$.

Terminology. Call $(a_1, \ldots, a_n) \in L^n$, not all zero, with $\sum_i a_i\sigma_i(x) = 0$ for all $x \in E^\times$, a *relation* among the σ_i. Its *length* is the number of nonzero a_i. The lemma says: no relation exists.

Dedekind — Proof

Suppose a relation exists. Among all relations, pick one of *shortest length* m, with nonzero terms relabelled $a_1, \dots, a_m$:

$$a_1\sigma_1(x) + \cdots + a_m\sigma_m(x) = 0 \quad \forall x \in E^\times.$$

Length 1. $a_1\sigma_1 = 0$ forces $a_1 = 0$ (take $x = 1$, $\sigma_1(1) = 1$). So $m \geq 2$.

Shorten the relation. Since $\sigma_1 \neq \sigma_m$, pick $y \in E^\times$ with $\sigma_1(y) \neq \sigma_m(y)$. Apply $(*)$ to yx:

$$\sum_{i=1}^{m} a_i\sigma_i(y)\sigma_i(x) = 0.$$

Multiply $(*)$ by $\sigma_m(y)$ and subtract from $(*')$:

$$\sum_{i=1}^{m-1} a_i\big(\sigma_i(y) - \sigma_m(y)\big)\sigma_i(x) = 0.$$

The σ_m term vanishes; the σ_1 term has nonzero coefficient $a_1(\sigma_1(y) - \sigma_m(y))$. This is a relation of length $\leq m - 1$ — contradicting minimality. $\square$

Artin's Theorem — Statement

Theorem (Artin). Let E be a field and $G = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n\}$ a finite subgroup of $\mathrm{Aut}(E)$. Let $K = E^G$ be its fixed field. Then:

$$[E : K] = |G| = n, \qquad E/K \text{ is Galois}, \qquad \mathrm{Gal}(E/K) = G.$$

Why it gives Property 3. For any subgroup $H \leq G$ of our Galois group, H is a finite subgroup of $\mathrm{Aut}(E)$, and Artin applied to H gives $\mathrm{Gal}(E/E^H) = H$ in one stroke.

Proof in two bounds. $[E : K] \leq n$ via a linear system with shortest-solution argument (also gives finiteness), then $[E : K] \geq n$ via a counting lemma from Dedekind.

Artin: $[E:K] \leq |G|$ (Upper Bound)

Show any $n+1$ elements $u_1, \ldots, u_{n+1} \in E$ are K-dependent. The $n \times (n+1)$ system

$$\sigma_i(u_1)\, c_1 + \cdots + \sigma_i(u_{n+1})\, c_{n+1} = 0 \quad (i = 1, \ldots, n)$$

has more unknowns than equations, hence a nonzero solution $(c_j) \in E^{n+1}$. Among such, pick one with the **fewest** nonzero entries; reorder so $c_1, \ldots, c_r \neq 0$, $c_{r+1} = \cdots = 0$; scale $c_1 = 1$.

Forcing $c_j \in K$. If some $c_j \notin K$, say $\sigma(c_2) \neq c_2$ for $\sigma \in G$: applying σ permutes the equations, so $(\sigma(c_j))$ is also a solution. Then $(c_j - \sigma(c_j))$ is a nonzero solution with $j = 1$ entry $= 0$ but $j = 2$ entry $\neq 0$ — strictly fewer nonzero entries. Contradiction. So all $c_j \in K$.

The $i = 1$ equation reads $\sum_j u_j c_j = 0$ with $c_j \in K$, $c_1 = 1$, a nontrivial K-dependence. Hence $[E:K] \leq n$; in particular $[E:K] < \infty$. $\square$

Artin: $[E : K] \geq |G|$ + Conclusion

Counting lemma (from Dedekind). A finite extension E/K has at most $[E : K]$ distinct K-automorphisms.

Proof. Suppose $\tau_1, \ldots, \tau_{m+1}$ are distinct K-automorphisms with $m = [E : K]$, and $w_1, \ldots, w_m$ a K-basis of E. The system $\sum_k \tau_k(w_j)x_k = 0$ $(j = 1, \ldots, m)$ has a nonzero $(x_k) \in E^{m+1}$. For $a = \sum_j c_j w_j$ $(c_j \in K)$:

$$\sum_k x_k \tau_k(a) = \sum_j c_j \sum_k x_k \tau_k(w_j) = 0,$$

so $\sum_k x_k \tau_k = 0$ as characters — contradicting Dedekind.

Lower bound + conclusion. G contains n distinct K-automorphisms $(K = E^G)$, so $n \leq [E : K]$. With the upper bound, $[E : K] = n$. $G \subseteq \mathrm{Gal}(E/K)$, and the counting lemma applied to $\mathrm{Gal}(E/K)$ gives $|\mathrm{Gal}(E/K)| \leq [E : K] = n = |G|$. So $G = \mathrm{Gal}(E/K)$ and $|\mathrm{Gal}(E/K)| = [E : K]$, i.e. E/K is Galois. $\square$

Property 2: $E^{\mathrm{Gal}(E/K)} = K$ (λ injective)

$K \subseteq E^{\mathrm{Gal}(E/K)}$. Every $\sigma \in \mathrm{Gal}(E/K)$ fixes K by definition.

$E^{\mathrm{Gal}(E/K)} \subseteq K$. Take $\alpha \in E \setminus K$; we produce $\sigma \in \mathrm{Gal}(E/K)$ with $\sigma(\alpha) \neq \alpha$.

- E/K is Galois (Restriction Theorem 53.2), so m_α^K is separable and splits in E.
- $\alpha \notin K \Rightarrow \deg m_\alpha^K \geq 2$, so there is a root $\alpha' \in E$ with $\alpha' \neq \alpha$.
- The conjugation isomorphism $K(\alpha) \to K(\alpha')$, $\alpha \mapsto \alpha'$, fixing K, extends (Isomorphism Extension Theorem) to $\sigma \in \mathrm{Gal}(E/K)$ with $\sigma(\alpha) = \alpha' \neq \alpha$.

Injectivity. $\mathrm{Gal}(E/K_1) = \mathrm{Gal}(E/K_2) \Rightarrow K_1 = E^{\mathrm{Gal}(E/K_1)} = E^{\mathrm{Gal}(E/K_2)} = K_2$. $\square$

Property 3: $\mathrm{Gal}(E/E^H) = H$ (λ onto, via Artin)

Let $H \leq G$ be any subgroup. Then H is a **finite subgroup of** $\mathrm{Aut}(E)$ (finite because G is), and its fixed field is E^H by definition.

Apply **Artin's theorem** to H acting on E:

$$\mathrm{Gal}(E/E^H) = H, \quad [E : E^H] = |H|, \quad E/E^H \text{ is Galois.}$$

Equivalently, $\lambda(E^H) = H$: every subgroup of G is the image of the intermediate field E^H under λ. So λ is **onto**. $\square$

Combined with Property 2: λ is a **bijection** between intermediate fields and subgroups of G, with inverse $H \mapsto E^H$.

Property 4: Degree Dictionary

Let $K \leftrightarrow H = \mathrm{Gal}(E/K)$.

First identity: $[E:K] = |H|$**.** E/K is Galois (Restriction Theorem 53.2), so $|H| = |\mathrm{Gal}(E/K)| = [E:K]$.

Second identity: $[K:F] = [G:H]$**.** By multiplicativity of the degree (tower law):

$$[K:F] = \frac{[E:F]}{[E:K]} = \frac{|G|}{|H|} = [G:H].$$

Counting F-embeddings. By Restriction Theorem 53.2, the left cosets of H in G are in bijection with the F-embeddings $K \to \overline{F}$ (via $\sigma H \mapsto \sigma|_K$). Since K/F is separable, $\{K:F\} = [K:F]$. So $[K:F] = [G:H]$ counts the F-embeddings of K.

Property 6: Lattice Anti-Isomorphism and Finiteness

Inclusion-reversing. $K_1 \subseteq K_2 \Rightarrow \mathrm{Gal}(E/K_2) \subseteq \mathrm{Gal}(E/K_1)$. Combined with λ a bijection (Properties 2 + 3), this means the diagrams of intermediate fields and of subgroups of G are mirror images (Property 6 of Fraleigh 53.6).

The bijection also respects lattice operations. For intermediate K_1, K_2 with $H_i = \mathrm{Gal}(E/K_i)$:

$$\mathrm{Gal}(E/K_1K_2) = H_1 \cap H_2, \qquad \mathrm{Gal}(E/K_1 \cap K_2) = \langle H_1, H_2 \rangle.$$

- σ fixes the compositum $K_1K_2 \iff$ fixes K_1 and $K_2 \iff \sigma \in H_1 \cap H_2$.
- $E^{\langle H_1, H_2 \rangle} = E^{H_1} \cap E^{H_2} = K_1 \cap K_2$, so $K_1 \cap K_2 \leftrightarrow \langle H_1, H_2 \rangle$.

So compositum $\leftrightarrow$ intersection and intersection $\leftrightarrow$ join: a **lattice anti-isomorphism**.

Corollary. G has finitely many subgroups, so a finite Galois extension has only *finitely many intermediate fields*.

Property 5: Normal Subgroups $\leftrightarrow$ Normal Subextensions

Theorem. For finite Galois E/F, $G = \mathrm{Gal}(E/F)$, $K \leftrightarrow H = \mathrm{Gal}(E/K)$:

$$K/F \text{ normal (equivalently Galois)} \iff H \trianglelefteq G,$$

and then restriction $\sigma \mapsto \sigma|_K$ gives an isomorphism

$$\mathrm{Gal}(K/F) \cong G/H.$$

(Separability of K/F is automatic — a subextension of separable E/F — so "normal" and "Galois" coincide here.)

Property 5 — Proof

By Restriction Theorem 53.2, every F-embedding $K \to \overline{F}$ is the restriction $\sigma|_K$ of some $\sigma \in G$, with image $\sigma(K)$.

Step 1: K/F **normal** $\iff \sigma(K) = K$ **for all** $\sigma \in G$**.** Normality means every F-embedding $K \to \overline{F}$ has image K. Combined with the line above, this is $\sigma(K) = K$ for all $\sigma \in G$.

Step 2: $\sigma(K) = K \iff \sigma H \sigma^{-1} = H$**.** By the conjugation identity (L15) $\mathrm{Gal}(E/\sigma K) = \sigma H \sigma^{-1}$, and λ injective (Property 2), $\sigma(K) = K \iff \mathrm{Gal}(E/\sigma K) = \mathrm{Gal}(E/K) \iff \sigma H \sigma^{-1} = H$.

Combined. K/F normal $\iff \sigma H \sigma^{-1} = H$ for all $\sigma \in G \iff H \trianglelefteq G$.

Quotient. When $H \trianglelefteq G$: restriction $\Phi : G \to \mathrm{Gal}(K/F)$, $\sigma \mapsto \sigma|_K$, is a homomorphism. Onto by Restriction Theorem 53.2 + normality (every F-embedding of K is now an F-automorphism). Kernel $= \{\sigma : \sigma|_K = \mathrm{id}\} = H$. First Isomorphism Theorem: $\mathrm{Gal}(K/F) \cong G/H$. $\square$

Part III: Examples

Abelian: $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ (V_4)

$G = \mathrm{Gal}(E/\mathbb{Q}) \cong V_4$ (the Klein four-group) $= \{\mathrm{id}, a, b, c\}$ ($a : \sqrt{3} \mapsto -\sqrt{3}$; $b : \sqrt{2} \mapsto -\sqrt{2}$; $c = ab$). Each node shows a field over its corresponding subgroup (in blue); the bijection reverses inclusions, so $E \leftrightarrow \{1\}$ and $\mathbb{Q} \leftrightarrow G$:

$$\begin{tikzcd}
 & \begin{array}{c} E \\ \{1\} \end{array} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\begin{array}{c} \mathbb{Q}(\sqrt{2}) \\ \langle a \rangle \end{array} \arrow[dr, dash] & \begin{array}{c} \mathbb{Q}(\sqrt{3}) \\ \langle b \rangle \end{array} \arrow[d, dash] & \begin{array}{c} \mathbb{Q}(\sqrt{6}) \\ \langle c \rangle \end{array} \arrow[dl, dash] \\
 & \begin{array}{c} \mathbb{Q} \\ G \end{array} &
\end{tikzcd}$$

Every edge has degree 2, so every subgroup has index 2. G abelian $\Rightarrow$ every subgroup normal $\Rightarrow$ every intermediate field is Galois over $\mathbb{Q}$ (each degree 2, $\mathrm{Gal} \cong \mathbb{Z}/2$).

Cyclic: $\mathbb{F}_{p^n}/\mathbb{F}_p$ — Subfields $\leftrightarrow$ Divisors

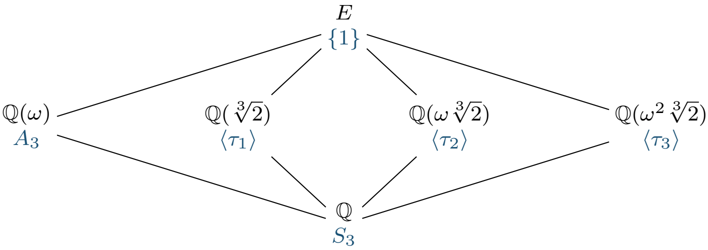
$\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois of degree n (the splitting field of $x^{p^n} - x$), with $G = \langle\varphi\rangle \cong \mathbb{Z}/n$ generated by the Frobenius $\varphi(x) = x^p$ (order n). For $d \mid n$, the subgroup $\langle\varphi^d\rangle$ (order n/d, index d) has fixed field $\{x : x^{p^d} = x\} = \mathbb{F}_{p^d}$ (degree d). So **subfields $\leftrightarrow$ divisors of** n, and for divisors d, e of n, $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e} \iff d \mid e$.

$$
\begin{tikzcd}
& \begin{array}{c}\mathbb{F}_{p^6}\\ \{1\}\end{array} \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
\begin{array}{c}\mathbb{F}_{p^2}\\ \langle\varphi^2\rangle\end{array} \arrow[dr, dash, "2"'] & & \begin{array}{c}\mathbb{F}_{p^3}\\ \langle\varphi^3\rangle\end{array} \arrow[dl, dash, "3"] \\
& \begin{array}{c}\mathbb{F}_{p}\\ \langle\varphi\rangle = G\end{array} &
\end{tikzcd}
$$

Take $n = 6$: the subfield lattice is the divisor lattice of 6. (G cyclic, so every subextension is normal.)

Non-abelian: $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ (S_3)

$E = \mathbb{Q}(\sqrt[3]{2}, \omega)$, $[E : \mathbb{Q}] = 6$, $G \cong S_3$ permuting the roots $r_1 = \sqrt[3]{2},\ r_2 = \omega\sqrt[3]{2},\ r_3 = \omega^2\sqrt[3]{2}$ ($\omega = e^{2\pi i/3}$); write $\rho = (r_1\, r_2\, r_3)$ (so $A_3 = \langle\rho\rangle$) and τ_i for the transposition fixing r_i. Each node shows a field over its corresponding subgroup (in blue):



Inclusion reversed: $E \leftrightarrow \{1\}$, $\mathbb{Q} \leftrightarrow S_3$. Degrees: $\mathbb{Q}(\omega)$ has degree 2 ($\leftrightarrow A_3$, index 2); the three cubic fields have degree 3 ($\leftrightarrow$ the order-2 subgroups $\langle\tau_i\rangle$, index 3).

S_3: Normal vs Non-normal

$A_3 \trianglelefteq S_3$ (index 2) $\Rightarrow \mathbb{Q}(\omega)/\mathbb{Q}$ is normal/Galois, degree 2, with $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong S_3/A_3 \cong \mathbb{Z}/2$ ($\mathbb{Q}(\omega)$ splits x^2+x+1).

The three order-2 subgroups are not normal $\Rightarrow \mathbb{Q}(\sqrt[3]{2}),\ \mathbb{Q}(\omega\sqrt[3]{2}),\ \mathbb{Q}(\omega^2\sqrt[3]{2})$ are *not* normal over $\mathbb{Q}$ — the failure seen directly via x^3-2 (a root, but not all roots). G permutes the three, matching the three conjugate subgroups.

Reading via Property 5. The group's internal structure (which subgroups are normal, the conjugacy of the transpositions) *is* the field structure (which subfields are normal, the conjugacy of $\mathbb{Q}(\sqrt[3]{2})$ with its siblings).

Part IV: Infinite Galois Theory (Krull)

Infinite Galois Theory — Krull's Theorem (Statement)

When E/F is an arbitrary (possibly infinite) Galois extension — algebraic, normal, separable — the Main Theorem generalizes, but the Galois group needs a topology.

Krull topology on $G = \mathrm{Gal}(E/F)$. Basis of open neighborhoods of $\sigma \in G$: cosets $\sigma \cdot \mathrm{Gal}(E/L)$ for L ranging over finite Galois subextensions $F \subseteq L \subseteq E$. Then G is a **profinite topological group**:

$$G \;\cong\; \varprojlim_{L} \mathrm{Gal}(L/F).$$

Theorem (Krull, 1928). The maps $K \mapsto \mathrm{Gal}(E/K)$ and $H \mapsto E^H$ are inclusion-reversing inverse bijections between intermediate fields $F \subseteq K \subseteq E$ and **closed** subgroups $H \leq G$. Moreover:

- $\mathrm{Gal}(E/K)$ open in $G \iff [K : F]$ finite (and then index $= [K : F]$).
- K/F Galois $\iff \mathrm{Gal}(E/K)$ closed normal in G; then $\mathrm{Gal}(K/F) \cong G/\mathrm{Gal}(E/K)$ as topological groups.

Without the "closed" qualifier, λ fails to be onto: an infinite Galois group has too many subgroups. In the finite case every subgroup is closed (discrete topology), recovering Fraleigh 53.6.