2. Fundamental Theorem of Galois Theory

Def: Let K be a field extension of F. An **F-automorphism** of K is an automorphism ϕ of K s.t. $\phi(b)=b$ $\forall b \in k$. The group $G := Gal(K/F)$ of all F-automorphisms of K is the **Galois group** of K/F.

Def: If $f(x) \in F[x]$ and K is the splitting field of $f(x)$, then the **Galois group of $f(x)$** over F is $G := Gal(K/F)$.

Example to motivate the Fundamental Theorem:

Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. **Note:** $f(x) = (x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-i\sqrt[4]{2})(x+i\sqrt[4]{2})$

Thus, the splitting field (over $\mathbb{Q}$) is $K = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.

$$[K:\mathbb{Q}] = [\underbrace{\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})}_{\text{min poly} = x^2+1}][\underbrace{\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}}_{\substack{\text{min poly} = x^4-2 \\ \text{(irred. by Eisenstein)}}}] = 4 \cdot 2 = 8$$

Now, let's find all $\mathbb{Q}$-automorphisms of $K = \mathbb{Q}(\sqrt[4]{2}, i)$.

Let $\sigma \in Gal(K/\mathbb{Q})$ be σ: $\begin{cases} \sqrt[4]{2} \longmapsto i\sqrt[4]{2} \\ i \longmapsto i \end{cases}$

Let $\tau \in Gal(K/\mathbb{Q})$ be τ: $\begin{cases} \sqrt[4]{2} \longmapsto \sqrt[4]{2} \\ i \longmapsto -i \end{cases}$

Note: $\sigma^4 = 1$, $\tau^2 = 1$, $\tau\sigma = \sigma^3\tau$.

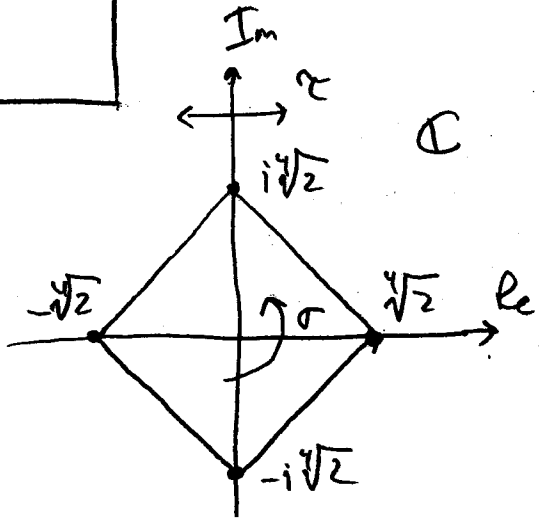
Also any $\mathbb{Q}$-automorphism of K sends:

$i \longmapsto$ root of x^2+1 (i.e., $i \longmapsto \pm i$).

$\sqrt[4]{2} \longmapsto \pm\sqrt[4]{2}$ or $\pm i\sqrt[4]{2}$.

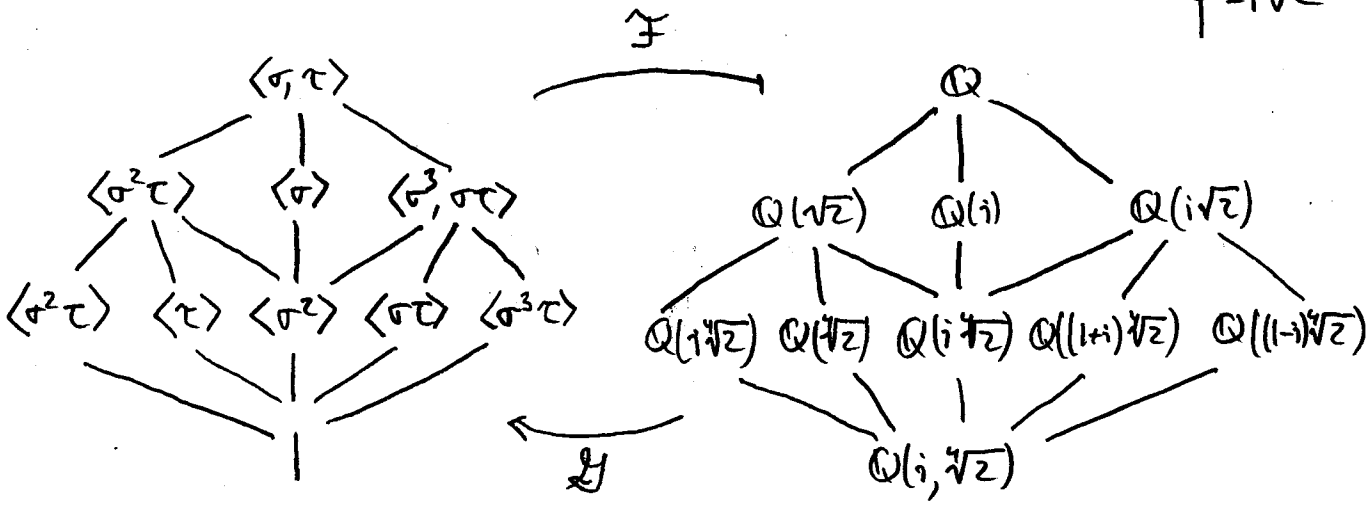
(2)

Automorphism	image of $\sqrt[4]{2}$	image of i
1	$\sqrt[4]{2}$	i
σ	$i\sqrt[4]{2}$	i
σ^2	$-\sqrt[4]{2}$	i
σ^3	$-i\sqrt[4]{2}$	i
τ	$\sqrt[4]{2}$	$-i$
$\sigma\tau$	$i\sqrt[4]{2}$	$-i$
$\sigma^2\tau$	$-\sqrt[4]{2}$	$-i$
$\sigma^3\tau$	$-i\sqrt[4]{2}$	$-i$



The Galois group is thus

$$G = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^3\tau \rangle \cong D_4$$



Subgroups of $Gal(K/F)$ — Intermediate subfields of $\mathbb{Q}(i, \sqrt[4]{2})$.

How to read this:

* Pick a subfield: $\mathbb{Q} \subseteq L \subseteq K = \mathbb{Q}(i, \sqrt[4]{2})$.

  The group $\mathcal{G}(L) = Gal(K/L)$ (L-automorphisms of K).

  i.e, $Gal(K/\mathbb{Q}) \geq \underbrace{Gal(K/L)}_{\mathcal{G}L} \geq Gal(\mathbb{Q}/\mathbb{Q})$.

* Pick a subgroup: $1 = Gal(\mathbb{Q}/\mathbb{Q}) \leq H \leq Gal(K/\mathbb{Q})$.

  The subfield $\mathcal{F}(H)$ is fixed element-wise by all automorphisms in H.

  i.e, $\mathbb{Q} \subseteq \mathcal{F}(H) \subseteq K = \mathbb{Q}(i, \sqrt[4]{2})$.

Note that the maps $\mathcal{F}$ & $\mathcal{G}$ are "inclusion-reversing"

Now, let's formalize this (There's actually even more structure!)

- IF L is an intermediate Field: $F \subseteq L \subseteq K$, define

  $\mathcal{G}L = Gal(K/L) = \{\phi \in G : \phi(a) = a \ \forall a \in L\}$.

  Note that $\mathcal{G}L \leq G = Gal(K/F)$.

- For any $H \leq G$, define

  $\mathcal{F}H = \{a \in K : \phi(a) = a \ \forall \phi \in H\}$.

  Note that $F \subseteq \mathcal{F}H \subseteq K$.

In summary:

$\mathcal{G}L =$ "all F-automorphisms that fix L elementwise"

$\mathcal{F}H =$ "all elements of K fixed by everything in H."

Exercise: (i) $\mathcal{G}F = G$
(ii) $\mathcal{G}K = 1$
(iii) $\mathcal{F}1 = K$
} follow immediately from def'ns.

But... (iv) $\mathcal{F}G \supseteq F$ (equality need not hold!)

Example: Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.

Splitting field is $K = \mathbb{Q}(\omega, \sqrt[3]{2})$ $\omega = 3^{rd}$ root of unity.

$$[K:\mathbb{Q}] = [\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$$

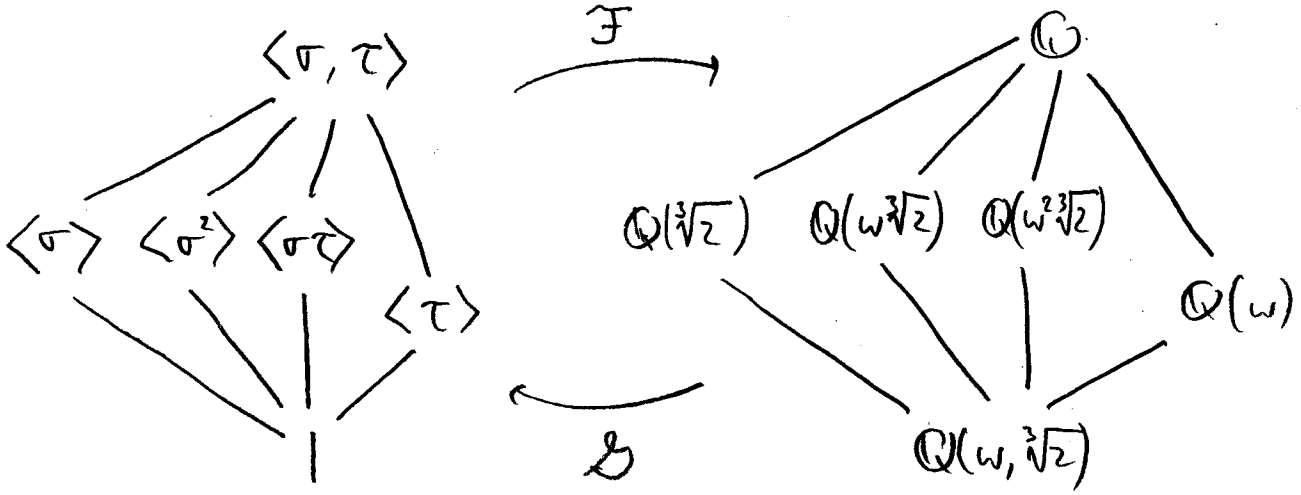
min poly $= x^2 + x + 1$ min poly $= x^3 - 2$

$\mathbb{Q}$-automorphisms:

σ: $\sqrt[3]{2} \longmapsto \sqrt[3]{2}$, $\omega \longmapsto \omega^2$

τ: $\sqrt[3]{2} \longmapsto \omega\sqrt[3]{2}$, $\omega \longmapsto \omega$

$$G = Gal(K/\mathbb{Q}) = \langle \sigma, \tau : \sigma^3 = 1,\ \tau^2 = 1,\ \sigma\tau = \tau\sigma^{-1} \rangle \cong S_3.$$



Note: Any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[3]{2})$ must fix $\sqrt[3]{2}$. (why?)

Thus, $\mathcal{F}G = \{a \in \mathbb{Q}(\omega, \sqrt[3]{2}) : \phi(a) = a\ \forall \phi \in G\} = \mathbb{Q}(\sqrt[3]{2}) \supsetneq \mathbb{Q}$

Def: If $\mathcal{F}G = F$, then K/F is a Galois extension.

* Equivalently, K/F is Galois iff every element $a \in K/F$ is moved by some $\phi \in Gal(K/F)$ (i.e., $\phi(a) \neq a$).

If $F \subseteq L \subseteq K$, then $\mathcal{F}\mathcal{G}L$ is the closure of L, and L is closed if $L = \mathcal{F}\mathcal{G}L$.

Dual: If $1 \leq H \leq G = Gal(K/F)$, then $\mathcal{G}\mathcal{F}H$ is the closure of H, and H is closed if $H = \mathcal{G}\mathcal{F}H$.

Prop 2.1: Suppose $F \subseteq E \subseteq L \subseteq K$ and $1 \leq J \leq H \leq Gal(K/F)$.

Then: (i) $\mathcal{G}L \leq \mathcal{G}E$ and $\mathcal{F}H \subseteq \mathcal{F}J$

(ii) $H \leq \mathcal{G}\mathcal{F}H$ and $L \subseteq \mathcal{F}\mathcal{G}L$

(iii) $\mathcal{G}L = \mathcal{G}\mathcal{F}\mathcal{G}L$ and $\mathcal{F}H = \mathcal{F}\mathcal{G}\mathcal{F}H$.

Pf: (i) & (ii): Exercise (easy!)

(iii): $L \subseteq \mathcal{F}\mathcal{G}L$ (by (ii)) $\Rightarrow \mathcal{G}L \geq \mathcal{G}\mathcal{F}\mathcal{G}L$ (by (i)). ✓

If $H = \mathcal{G}L$, then $\mathcal{G}L = H \leq \mathcal{G}\mathcal{F}H = \mathcal{G}\mathcal{F}\mathcal{G}L$. ✓
(by (ii))

Thus $\mathcal{G}L = \mathcal{G}\mathcal{F}\mathcal{G}L$.

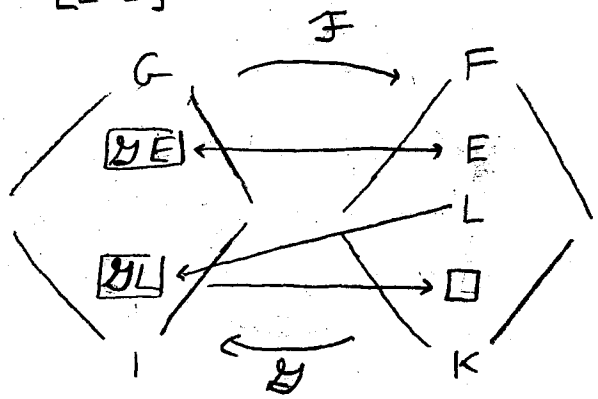
The proof that $\mathcal{F}H = \mathcal{F}\mathcal{G}\mathcal{F}H$ is analogous.

Prop 2.2: If $G = Gal(K/F)$, then all subgroups $\mathcal{G}L$ and all intermediate fields $\mathcal{F}H$ are closed. Moreover, $\mathcal{F}$ is a 1–1 inclusion-reversing correspondence:

$\{$closed subgroups of $G\} \xrightarrow{\mathcal{F}} \{$closed intermediate subfields $F \subseteq K\}$.

Pf: Direct corollary of Prop 2.1. $\mathcal{F}$ is a 1-1 correspondence because its inverse is $\mathcal{G}$.

Prop 2.3: Suppose $F \subseteq E \subseteq L \subseteq K$ and $[L:E] < \infty$.
Then $[\mathcal{G}E : \mathcal{G}L] \leq [L:E]$.



* In particular, E closed $\Rightarrow L$ closed.
i.e, the following can't happen:

Pf: Induction on $n = [L:E]$

Base case: $n = 1$. ✓

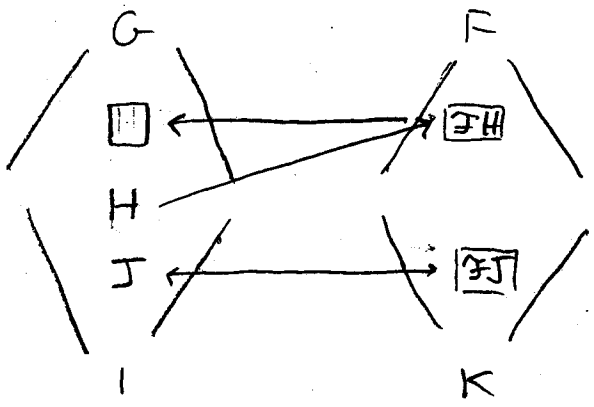
Case 1: $\exists\, M$ s.t. $E \subsetneq M \subsetneq L$.

Then, $[\mathcal{G}E : \mathcal{G}L] = [\mathcal{G}E : \mathcal{G}M][\mathcal{G}M : \mathcal{G}L]$ — Lagrange's thm
$\leq [M:E][L:M]$ — IltoP
$= [L:E]$ — Tower Law (Prop 1.1)

Case 2: $\nexists$ intermediate field M.
Pick any $a \in L \setminus E$. Then, $L = E(a)$.
Let $m(x)$ be the min'l poly of a over E (so $\deg m(x) = n$).
Goal: Show # cosets of $\mathcal{G}L$ in $\mathcal{G}E \leq$ # roots of $m(x)$ (why?).
Pick $\phi \in \mathcal{G}E$, and consider the left coset $\phi\mathcal{G}L$.
If $\theta \in \mathcal{G}L$, then $\theta(a) = a$.
Thus, for any $\phi\theta_1, \phi\theta_2 \in \phi\mathcal{G}L$: $\phi\theta_1(a) = \phi(a) = \phi\theta_2(a)$.
i.e, we have a map $\{\text{left cosets of } \mathcal{G}L\} \longrightarrow \{\text{roots of } m(x)\}$.
* Sufficies to show this is injective: Say $\phi_1\mathcal{G}L \neq \phi_2\mathcal{G}L$.
If $\phi_1(a) = \phi_2(a)$, then $\phi_1^{-1}\phi_2$ would fix $E(a) = L \Rightarrow \phi_1^{-1}\phi_2 \in \mathcal{G}L$ ↯
Thus the # of left cosets of $\mathcal{G}L \leq \deg m(x)$
i.e, $[\mathcal{G}E : \mathcal{G}L] \leq [L:E]$. □

Prop 2.4: Suppose $1 \leq J \leq H \leq G := \mathrm{Gal}(K/F)$ and $[H:J] < \infty$.

Then $[\mathcal{F}J : \mathcal{F}H] \leq [H:J]$.



* In particular, J closed $\Rightarrow$ H closed.
i.e., the following can't happen:

** Useful special case: Finite subgroups of G are closed (because 1 is closed).

PF: Let $\{\phi_1 = 1, \phi_2, \ldots, \phi_n\}$ be a complete set of left coset representatives for J in H.

For sake of contradiction, suppose that $[\mathcal{F}J : \mathcal{F}H] > n = [H:J]$.
Then $\exists\ a_1, \ldots, a_n, a_{n+1} \in \mathcal{F}J$, all linearly independent over $\mathcal{F}H$.
Let A be the $n \times (n+1)$ matrix $A = (a_{ij}) := (\phi_i(a_j))$, which is a linear transformation $K^{n+1} \longrightarrow K^n$.

Thus, the system $A\vec{x} = \vec{0}$ has a non-trivial solution:

$$\begin{bmatrix} \phi_1(a_1) & \phi_1(a_2) & \cdots & \phi_1(a_{n+1}) \\ \phi_2(a_1) & \phi_2(a_2) & \cdots & \phi_2(a_{n+1}) \\ \vdots & \vdots & \ddots & \\ \phi_n(a_1) & \phi_n(a_2) & \cdots & \phi_n(a_{n+1}) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ x_{n+1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Choose a non-zero solution with the fewest nonzero entries, say WLOG (by relabeling) that it is $\vec{b} = (1, b_2, \ldots, b_k, 0, \ldots, 0)^T$ $b_i \neq 0$ $i \leq k$.

Note: Any size-k subset of $\{a_1, \ldots, a_{n+1}\}$ is linearly independent over $\mathcal{F}H$, thus not all of $1, b_2, \ldots, b_k$ can be in $\mathcal{F}J$.
WLOG, assume $b_2 \notin \mathcal{F}J$.

Choose $\phi \in H$ s.t. $\phi(b_2) \neq b_2$.

Consider the system of equations $\Phi(A)\vec{x} = \vec{0}$, where

$$\Phi(A) := \left(\phi\Phi_i(a_j)\right)_{n\times(n+1)}$$

Note: For any 2 elts $\phi\Theta_1, \phi\Theta_2 \in \phi J$ (the left coset),

$\phi\Theta_1(a) = \phi(a) = \phi\Theta_2(a)$.

Thus, $\{\phi\Phi_1, \ldots, \phi\Phi_n\}$ is a complete set of left-coset representatives, and so the equations (rows) in the systems $\Phi(A)\vec{x} = \vec{0}$ and $A\vec{x} = \vec{0}$ are rearrangements of each other.

Therefore, $\{\phi(1), \phi(b_2), \ldots, \phi(b_k), 0, \ldots, 0\}$ is also a solution to $A\vec{x} = \vec{0}$.

But $\phi(1) = 1$, so $(1, \phi(b_2), \ldots, \phi(b_k), 0, \ldots, 0) - (1, b_2, \ldots, b_k, 0, \ldots, 0)$ is a solution with fewer than k nonzero entries. $\lightning$ □

Thm 2.5: (1) Suppose $F \subseteq E \subsetneq L \subseteq K$, E is closed & $[L:E] < \infty$.
Then L is closed, and $[\mathcal{G}E : \mathcal{G}L] = [L:E]$.

(2) Suppose $1 \leq J \leq H \leq G = Gal(K/F)$, J closed & $[H:J] < \infty$.
Then H is closed, and $[\mathcal{F}J : \mathcal{F}H] = [H:J]$.

Pf: For intuition, see the "pictures" in Props. 2.3 & 2.4.

(1) $[L:E] = [L:\mathcal{F}\mathcal{G}E] \leq [\mathcal{F}\mathcal{G}L : \mathcal{F}\mathcal{G}E] \leq [\mathcal{G}E : \mathcal{G}L] \leq [L:E]$.

($[L:E] = [L:\mathcal{F}\mathcal{G}E]$: E is closed; $[\mathcal{F}\mathcal{G}L : \mathcal{F}\mathcal{G}E] \leq [\mathcal{G}E : \mathcal{G}L]$: Prop. 2.1; $[\mathcal{G}E : \mathcal{G}L] \leq [L:E]$: Prop 2.3)

(2) $[H:J] = [H:\mathcal{G}\mathcal{F}J] \leq [\mathcal{G}\mathcal{F}H : \mathcal{G}\mathcal{F}J] \leq [\mathcal{F}H : \mathcal{F}J] \leq [H:J]$.

($[H:J] = [H:\mathcal{G}\mathcal{F}J]$: J is closed; $[\mathcal{G}\mathcal{F}H : \mathcal{G}\mathcal{F}J] \leq [\mathcal{F}H : \mathcal{F}J]$: Prop. 2.1; $[\mathcal{F}H : \mathcal{F}J] \leq [H:J]$: Prop 2.4)

□

Cor: (1) All finite subgroups of $Gal(K/F)$ are closed.

(2) If K/F is Galois, $F \subseteq E \subseteq K$ and $[E:K] < \infty$, then E is closed, and thus K/E is Galois.

Pf: (1) The subgroup 1 is closed.

(2) Since K/F is Galois, F is closed.

By Thm 2.5, E is closed $\Rightarrow E$ is the fixed field of $\mathcal{G}E = Gal(K/E)$

$\Rightarrow K/E$ is Galois. □

Def: If $F \subseteq E \subseteq K$, say E is <u>stable</u> if $\phi(E) \subseteq E$ for all $\phi \in G := Gal(K/F)$.

Note: If E is stable, then $\phi^{-1}(E) \subseteq E \Rightarrow E = \phi\phi^{-1}(E) \subseteq \phi(E) \subseteq E$

$\Rightarrow \phi(E) = E \quad \forall \phi \in G$.

Prop 2.6: (1) If $F \subseteq E \subseteq K$ and E is stable, then $\mathcal{G}E \triangleleft G$.

(2) If $H \triangleleft G$, then $\mathcal{F}H$ is stable.

Pf: Exercise (HW).

Cor: (1) If $F \subseteq E \subseteq K$ and E is stable, then the closure $\mathcal{F}\mathcal{G}E$ is stable.

(2) If $H \triangleleft G$, then $\mathcal{G}\mathcal{F}H \triangleleft G$.

Pf: (1) E stable $\Rightarrow \mathcal{G}E \triangleleft G \Rightarrow \mathcal{F}\mathcal{G}E$ stable. ✓

(2) $H \triangleleft G \Rightarrow \mathcal{F}H$ stable $\Rightarrow \mathcal{G}\mathcal{F}H \triangleleft G$. ✓

□

Prop 2.7: If K/F is Galois and $F \subseteq L \subseteq K$, and L is stable, then L/F is Galois.

Pf: If $a \in L \setminus F$, then $\phi(a) \neq a$ for some $\phi \in Gal(K/F)$.

Let $\theta := \phi|_L$. Since L is stable, θ is an F-autom. of L.

Thus $\theta \in Gal(L/F)$, and $\theta(a) \neq a \Rightarrow L/F$ is Galois. □

Thm 2.8: Suppose K/F is Galois, $f(x) \in F[x]$ is irreducible, and $f(x)$ has a root $a \in K$. Then $f(x)$ splits over K and all roots are distinct.

Pf: WLOG, assume $f(x)$ is monic, i.e., $f(x) = m_{a,F}(x)$.

Note: For each $\phi \in G$, $\phi(f(x)) = f(x)$, and $\phi(a)$ is a root of $f(x)$.

Let $a_1, \ldots, a_k$ be all the distinct roots of the form $\phi(a)$, $\phi \in G$.

Set $g(x) = \prod_{i=1}^{k} (x - a_i)$. Goal: show $g(x) = f(x)$.

Clearly, $\phi(g(x)) = g(x)$ $\forall \phi \in G$.

Thus, $g(x) \in F[x]$ (F is the fixed field for G).

Now, $g(x)$ is monic and $g(a) = 0 \Rightarrow m_{a,F}(x) \mid g(x)$.

But $\deg g(x) \leq \deg f(x) = m_{a,F}(x) \Rightarrow g(x) = f(x)$. □

Cor 1: Suppose $F \subseteq L \subseteq K$ and L/F is Galois & algebraic.

Then L is stable.

Pf: If $\phi \in Gal(K/F)$ and $a \in L$, then $\phi(a)$ is a root of $m(x) = m_{a,F}(x)$, since $\phi(m(x)) = m(x)$.

Thm 2.8 $\Rightarrow m(x)$ splits over $L \Rightarrow \phi(a) \in L \Rightarrow L$ is stable. □

Cor 2: If K/F is Galois and algebraic, and $F \subseteq L \subseteq K$, then L is stable iff L/F is Galois.

Pf: ($\Leftarrow$) Cor 1.

($\Rightarrow$) Prop 2.7

Prop 2.9: Suppose $F \subseteq L \subseteq K$, and L is stable. Then there is an isomorphism $G/\mathcal{G}L \longrightarrow \{\theta \in Gal(L/F) : \theta \text{ extends to an automorph. of } K\}$.

Pf: If $\phi \in G$, then $\theta := \phi|_L \in Gal(L/F)$, since L is stable.

Define: $f : Gal(K/F) \longrightarrow Gal(L/F)$

$$\phi \longmapsto \phi|_L$$

$\ker f = \{\phi \in G : \phi|_L = 1\} = \mathcal{G}L$.

Apply FHT for rngs. $\square$

The results in this section can be summarized as follows:

Thm 2.10 (Fundamental Theorem of Galois Theory):

Suppose K/F is a finite Galois extension, and $G = Gal(K/F)$. Then

(1) The map $\mathcal{F}$ is a 1-1 inclusion-reversing correspondence between the subgroups of G and intermediate fields $F \subseteq L \subseteq K$.

(2) If $J \leq H \leq G$, then $[H:J] = [\mathcal{F}J : \mathcal{F}H]$ (in particular, $|G| = [K:F]$).

(3) $H \lhd G$ iff $\mathcal{F}H = L$ is Galois over F, in which case $Gal(L/F) \cong G/H$.

Pf: (1) Since K/F is finite & Galois, all intermediate fields are closed (Thm 2.5), so $\mathcal{F}\mathcal{G}L = L$ and $\mathcal{G}\mathcal{F}H = H$. ✓

(2) Also by Thm 2.5, $[H:J] = [\mathcal{F}J : \mathcal{F}H]$ for $J \subseteq H \subseteq G$. ✓

(3) "$H \lhd G \Leftrightarrow \mathcal{F}H$ Galois" is immediate from Prop 2.6 & Thm 2.8, Cor 2.

If $H \lhd G$ and $L = \mathcal{F}H$, then by Prop 2.9,

$$G/H = G/\mathcal{G}\mathcal{F}H = G/\mathcal{G}L \longrightarrow \mathrm{Gal}(L/F).$$

Also, $|G/H| = |G|/|H| = |G|/|\mathcal{G}L| = |G|/[\mathcal{G}L : \mathcal{G}K]$

$$= [K:F]/[K:L] = [L:F] = |\mathrm{Gal}(L/F)| \quad ✓$$

□

Cor: If K/F is finite and $|\mathrm{Gal}(K/F)| = [K:F]$, then K is Galois over F.

Pf: Let $G = \mathrm{Gal}(K/F) = \mathrm{Gal}(K/\mathcal{F}G)$.

Then $\mathcal{F}G = \mathcal{F}\,\mathrm{Gal}(K/\mathcal{F}G) \Rightarrow K/\mathcal{F}G$ is Galois

$\Rightarrow |G| = [K : \mathcal{F}G]$ (Thm 2.10)

$\Rightarrow [K:F] = [K : \mathcal{F}G]$

$\Rightarrow \mathcal{F}G = F$ and K/F is Galois. □