MSW
2/10/23

Classical Galois Theory (§1.2)

(I) SETUP: Automorphisms, Normal, Seperable

- **Recall:** A splitting field of $p(x) \in F[x]$ is the smallest $E \supset F$ s.t. $p(x)$ splits into linear factors, i.e. $p(x) = \prod_{i=1}^{n}(x - a_i) \cdot c^{\in F}$

- **Def:** Let E be a field. An **automorphism** of E is an isomorphism from E to itself.
  - ↳ **Claim:** The set of all automorphisms form a group operation is fn. composition – check), called $\mathrm{Aut}\, E$.
- **Def:** An algebraic extension E/F is **normal** if (TFAE):
  (1) Any polynomial $p \in F[x]$ that is irreducible and has root in E, factors into linear factors in $F[x]$.
  (2) E is the splitting field over F of some set of polynomials
  (3) $F \leq E \leq \bar{F}$ (algebraic closure of F (smallest field s.t. every nonconst. $p(x) \in F[x]$ has a root in $\bar{F}$))
  Any automorphism of $\bar{F}$ (fixing elts of F) maps $E \to E$.

↳ **Examples:**

(a) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ normal extension: it is the splitting field of $p(x) = x^2 - 2 \in \mathbb{Q}[x]$

(b) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ not normal: consider $x^3 - 2 \in \mathbb{Q}(\sqrt{2})$. Roots are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ (where ω is the third root of unity, given by $e^{2\pi i/3}$), but ω (and hence 2 nonreal roots) $\notin \mathbb{Q}(\sqrt[3]{2})$. → $\mathbb{Q}[\sqrt[3]{2}, \omega]/\mathbb{Q}$ normal!

↳ **Pf that these defns are equivalent:**

① ⇒ ②: $\forall d \in F[x]$, take irreducible polynomial p_d. By ①, this factors into linear factors in $F[x]$. Then by defn. E is the splitting field of this family of polynomials. ✓

② ⇒ ③: Consider the extension $\bar{F}/F$, and take any $\sigma \in Aut(\bar{F}/F)$, i.e. aut. $\bar{F} \to \bar{F}$ that fixes F.
By assumption, E is the splitting field for $p_\alpha \in F[x]$, and σ maps p_α to itself (as σ fixes elts. of F).
⇒ As E is splitting field (i.e. set of all roots of p_α in $\bar{F}$), E is fixed by σ.

③ ⇒ ①: Let $\sigma \in Aut(\bar{F}/F)$. By assumption σ fixes F.
Let $p \in F[x]$ and α be a root of p in $E \subset \bar{E}$.
$\forall$ root β of p, $\exists$ aut. σ of $\bar{E}$ from $\alpha \mapsto \beta$.

$K \subseteq K(\beta) \subseteq \bar{K}$
$K \subseteq K(\alpha) \subseteq \bar{K}$
↳ both $\cong K[x]/(p(x))$

$\sigma(\alpha) = \beta$
$\sigma(E) = E$
$\alpha \in E \Rightarrow \beta = \sigma(\alpha) \in E$, so all roots in E.
∴ All three conditions are equivalent. □

- **Def**: A polynomial $f \in F[x]$ is called **seperable** if no multiple roots in $\bar{F}$.
⇔ $\gcd(f, f') = 1$ in $F[x]$.

↳ **Def**: $\alpha \in E$ called seperable (over F) if it is a root of a seperable polynomial in $F[x]$.

↳ **Def**: $F \subseteq E$ called seperable if all $\alpha \in E$ are seperable.

↳ **Examples** (and **non-examples**):

(a) **Non-ex**: $f(x) = (x-\alpha)^2 \ldots \Rightarrow f' = 2(x-\alpha)\cdots \gcd(f, f') \geq x - \alpha \neq 1$.

(b) **Ex**: $F \subseteq E$, $\operatorname{char} F = 0 \Rightarrow E \setminus F$ seperable (eg. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$)

↳ (does not always work for char = p > 0)

(c) Non-ex: $F = \mathbb{F}_p(t^p)$, $E = \mathbb{F}_p(t)$. Consider $p(x) = x^p - t^p \in F[x]$, factors into $(x-t)^p \in E$, where root has multiplicity p.

- Difference between seperable and normal?

$F \subseteq E$ f irreducible polynomial of $\alpha \in E$.

E normal $\Rightarrow$ all roots of f are in E.

E seperable $\Rightarrow$ all roots of f are distinct.

(Normal + seperable $\Rightarrow$ f has n distinct roots in E, where $n = \deg f$; this is one defn. of Galois extension)

II GALOIS EXTENSIONS

- **Def**: Let E be a finite extension of a field F, i.e. $[E:F]=n$ for some $n\in\mathbb{Z}_{>0}$.

The **Automorphism Group** $\mathrm{Aut}(E/F)\leq\mathrm{Aut}(E)$ consists of all automorphisms that fix F, i.e. all $\sigma:E\to E\in\mathrm{Aut}(E)$ s.t. $\sigma(a)=a\ \forall a\in F$.

↳ **Claim**: $\mathrm{Aut}(E/F)$ is a subgroup of $\mathrm{Aut}(E)$, i.e.
① Closed under composition
② Contains identity
③ Contains inverses

↳ Can think of $\mathrm{Aut}(E/F)=\mathrm{Aut}(E)$ when $F\subseteq E$ prime subfield.
↳ When F is the prime subfield of E (smallest subfield, $\mathbb{Q}$ for char 0, $\mathbb{F}_p$ for char p), $\sigma(1)=1$ so $\forall a\in F$,
$\sigma(a)=\sigma(a\cdot 1)=a\cdot\sigma(1)=a\cdot 1=a\ \forall\sigma\in\mathrm{Aut}(E)$.

↳ Intuition: If E is the splitting field of a polynomial $p\in F[x]$, elts. $\sigma\in\mathrm{Aut}(E/F)$ permute the roots $\alpha_1,\dots,\alpha_n$ of p in E

↳ **Examples**:

(a) $\mathrm{Aut}(\mathbb{C}/\mathbb{R})=\{1,\sigma\}$ where,
1 is identity $(i\mapsto i)$, σ is complex conjugation $(i\mapsto -i)$, i.e. $\sigma(a+bi)=a-bi$.
(why? $\pm i$ root of $x^2+1\in\mathbb{R}[x]$, splits in $\mathbb{C}$)

(b) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})=\{1,\tau\}$ where,
1 is identity $(\sqrt{2}\mapsto\sqrt{2})$, τ permutes $(\sqrt{2}\mapsto-\sqrt{2})$, i.e. $\tau(a+b\sqrt{2})=a-b\sqrt{2}$
(why? $\pm\sqrt{2}$ root of $x^2-2\in\mathbb{Q}[x]$, splits in $\mathbb{Q}(\sqrt{2})$)

(c) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})=\{1,\sigma_1,\sigma_2,\sigma_3\}$ where,

1 is identity, $\sigma_1: \sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$; $\sigma_2: \sqrt{2} \mapsto \sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$; $\sigma_3: \sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$

(Why? $\pm\sqrt{2}, \pm\sqrt{3}$ roots of $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$, splits in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$).

↪ In fact, this is isomorphic to $S_2 \times S_2$ (Klein-4 group) – see Sect. III

(d) $\mathrm{Aut}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7\}$

(Why? $\pm i, \pm\sqrt[4]{2}$ roots of $x^4 - 2 = (x^2+\sqrt{2})(x^2-\sqrt{2}) \in \mathbb{Q}[x]$, splits in $\mathbb{Q}[\sqrt[4]{2}, i]$).

Aut. gp. is the Dihedral group D_4 (group of symmetries on a square), given by,

$\{r, s \mid r^4 = s^2 = 1, rsr^{-1} = 1\}$, where r = rotation, s = conjugation

$s: \sqrt[4]{2} \mapsto \sqrt[4]{2}$, $i \mapsto -i$; $r: \sqrt[4]{2} \mapsto \sqrt[4]{2}\, i$, $i \mapsto i$

Then $A \cong D_4 = \{1, r, s, sr, r^2, sr^2, r^3, sr^3\}$.

(e) $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$.

(Why? $\sqrt[3]{2}$ is one of three roots of $x^3 - 2 \in \mathbb{Q}[x]$, and is the <u>only</u> root contained in $\mathbb{Q}(\sqrt[3]{2})$, which does not contain the complex roots).

(f) $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$

1 is identity, $\sigma_1: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega^2$, $\sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}$; $\sigma_2: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$, $\sqrt[3]{2}\omega \mapsto \sqrt[3]{2}$, $\sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}\omega$

$\sigma_3: \sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega^2$, $\sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}\omega$

$\sigma_4: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega \mapsto \sqrt[3]{2}$, $\sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}\omega^2$

$\sigma_5: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$, $\sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}$

In fact, this is isomorphic to S_3, gp. of permutations of a 3-element set. Taking $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\omega$, $\alpha_3 = \sqrt[3]{2}\omega^2$, we see ells: 1, $\sigma_1 = (1\ 2\ 3)$, $\sigma_2 = (1\ 3\ 2)$, $\sigma_3 = (2\ 3)$, $\sigma_4 = (1\ 2)$, $\sigma_5 = (1\ 3)$.

• **Def**: We say a finite extension E/F is **Galois** and set $G = Gal(E/F) := Aut(E/F)$ as its Galois group if (TFAE):

① E is normal and seperable over F.

② $[E:F] = |G|$ → useful specifically for the finite case
↳ In general, $[E:F] \geq |G|$; here sym. gp as large as possible.

③ $F = E^G$ } fixed pts. of E under elts. of G.

④ E is a splitting field of a seperable polynomial over F.

• We will prove these defns are equivalent!

↳ **Examples**:

Of the examples above, which are Galois extensions? which are not? (note $\sqrt{K}$)

↳ Galois: $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$

↳ Not Galois: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

• We WTS defns 1-4 are equivalent; first, a lemma.

• **Lemma**: $F \subseteq E$, $A = Aut(E/F)$. Then $|A| \leq [E:F]$ (E/F not necessarily Galois)

Pf:

Suppose $E = F(\alpha_1, \ldots, \alpha_n)$

$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \ldots \subseteq E$

extensions $F(\alpha_i)$ to $F(\alpha_1, \alpha_2)$ – $\deg [F(\alpha_1,\alpha_2) : F(\alpha_1)]$

α_1 root of p_1; irred. deg. $[F(\alpha_1):F]$

roots of $p_1 \leq \deg p_1$

E

⇒ (Continuing inductively) # of maps (Aut gp. elts) from $F \to E$ is $\leq [E:F]$. □

- Now we prove equivalence of defns:

④ ⇒ ①: trivial; splitting field of seperable poly. p_α ⇒ normal (as E is splitting field) and seperable (as p_α seperable). ✓

① ⇒ ②: Say E/F normal and seperable.

Embed $F \subset E \subset \bar{F}$.

E/F seperable ⇒ $\alpha_1, \ldots, \alpha_n$ distinct roots of poly. p_α ($n = [E:F]$).

$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \cdots$

$\downarrow$ $\swarrow$ $= [F(\alpha_1):F]$ (not <) because ① α_1 seperable ⇒ p_1 has $[F(\alpha_1):F]$ roots
$\bar{F}$ ② $\bar{F}$ alg. closed, so ctns. all roots.

Thus there are exactly (not <) $[E:F]$ extensions fixing elts. of $\bar{F}$.

Now, E/F normal ⇒ any homomorphism $E \to \bar{F}$ maps $E \to E$, as E is splitting field of polynomial $p \in F[x]$, and all roots of p contained in E

Thus, $[E:F] = n$ homomorphisms (fixing F) $E \to \bar{F}$, and they must all map E to itself (as E has all roots), so these are in fact exactly the automorphisms $E \to E$ fixing F (i.e. elts of G). Thus $|G| = [E:F] = n$. ✓

② ⇒ ③: Suppose $[E:F] = |G|$.

Now, elts. of G must fix $F \subseteq E$, so,

$F \subseteq E^G \subseteq E$.

Note that E/E^G by defn. has $|G|$ automorphisms, i.e. there are $|G|$ automorphisms (elts. of G) $E \to E$ that fix elts. of E^G.

Now:

$$\underbrace{[E:F] = |G| \leq [E:E^G]}_{\text{by Lemma}} \leq [E:F]$$

(the two circled $[E:F]$ are joined by an arrow marked $=$)

$F \leq E^G$
$[E:F] = [F:E^G][E:E^G]$

$\Rightarrow [E:F] = |G| = [E:E^G] = [E:F]$

$\Rightarrow$ (since $[E:F] = [F:E^G][E:E^G]$) $[F:E^G] = 1$.

$\Leftrightarrow E^G = F$. ✓

③ ⇒ ④: Suppose $E^G = F$.

Pick $\alpha \in E$.

Consider all conjugates of α under maps $\sigma_1, \dots, \sigma_n$ in G.

$\alpha, \beta = \sigma_1(\alpha), \gamma = \sigma_2(\alpha), \dots$

Note $\alpha \neq \beta \neq \gamma \neq \dots$ (all distinct as $\sigma_1, \dots, \sigma_n$ dist. maps)

Consider $p(x) = (x-\alpha)(x-\beta)(x-\gamma)\cdots$

Notice: ① p seperable as all roots $(\alpha, \beta, \gamma, \dots)$ distinct.

② Fixed by G (as G permutes roots)

$\Rightarrow$ Coefficients in $E^G = F$ (by assump.)

$\Rightarrow p \in F[x]$

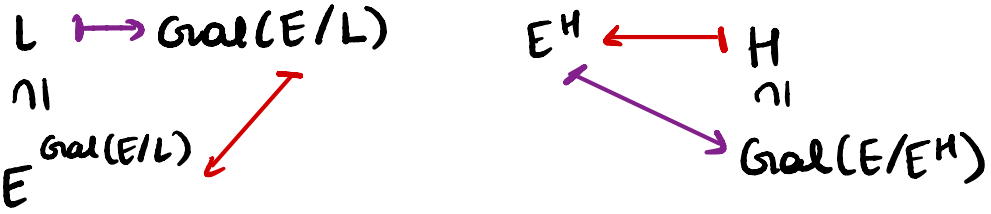
So any $\alpha \in E$ is root of sep. poly in $K[x]$, all roots in E. □

III FUNDAMENTAL THM OF GALOIS THEORY (finite case)

- **Thm**: Suppose E/F is a (finite) Galois extension with Galois gp. G. Then there is an order-reversing bijection from intermediate subfields $E \subseteq L \subseteq F$ and subgroups $1 \leq H \leq G$ s.t. $L \mapsto \mathrm{Gal}(E/L)$, $E^H \mapsfrom H$ } maps are inverses of each other.

  and E/L Galois $\Leftrightarrow H \triangleleft G$ normal subgroup, i.e. $\forall h \in H, g \in G$, $ghg^{-1} \in H$.

- **Intuition for pf**:



WTS $L = E^{\mathrm{Gal}(E/L)}$ and $H = \mathrm{Gal}(E/E^H)$

Since $L \subseteq E^{\mathrm{Gal}(E/L)}$ and $H \subseteq \mathrm{Gal}(E/E^H)$, suffices to show the sizes are the same, i.e.

Need to show:

① $(H \to E^H)$ $|H| = [E : E^H]$

↳ E/E^H Galois (defn. ③ in II), so ① true by defn. ②

② $(L \to \mathrm{Gal}(E/L))$ $[E : L] = |\mathrm{Gal}(E/L)|$

- We will look at a few examples of Galois correspondances before completing the pf!

• Examples:

(a) $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

Recall (from II): 4-elt. Galois gp. permutes roots $\pm\sqrt{2}, \pm\sqrt{3}$.

Say $f: \sqrt{2} \mapsto -\sqrt{2}$, and $g: \sqrt{3} \mapsto -\sqrt{3}$.

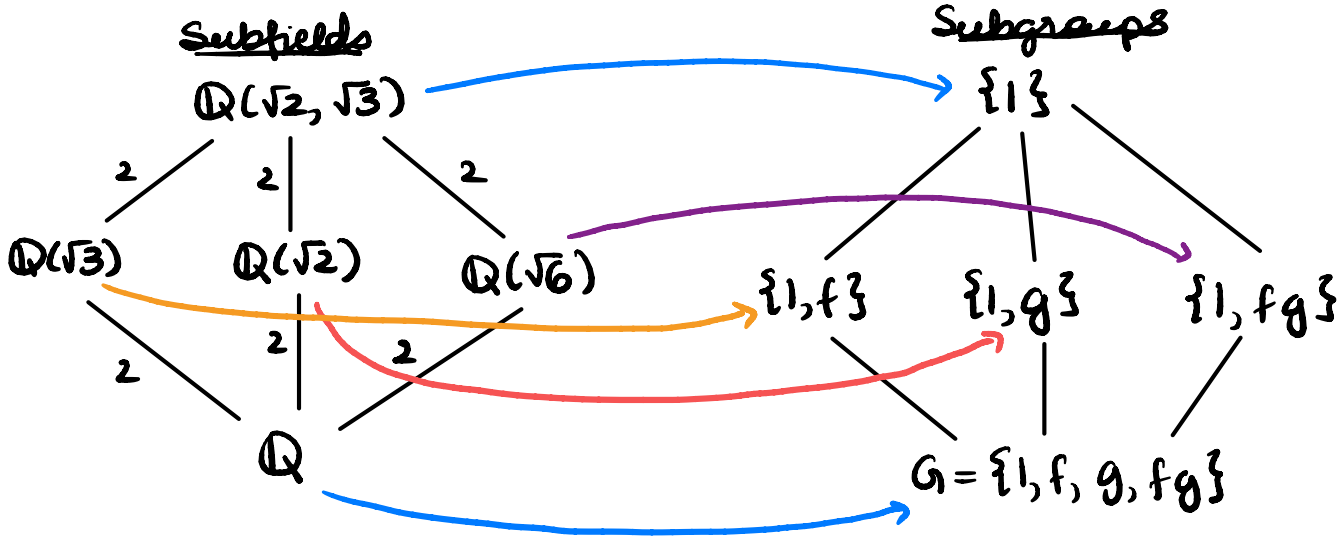
Then can say $G = \{1, f, g, fg\}$.

Subfields: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2},\sqrt{3})$

$\sqrt{6} = \sqrt{2}\cdot\sqrt{3}$

Subgroups: $\{1\}$, $\{1,f\}$, $\{1,g\}$, $\{1,fg\}$, $\{1,f,g,fg\} = G$.

Correspondance:



$\mathbb{Q}(\sqrt{2},\sqrt{3}) \longmapsto \{1\}$ since only identity fixes all elts. of $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

$\mathbb{Q}(\sqrt{3}) \mapsto \{1,f\}$ since $\sqrt{3}$ is fixed under f.

$\mathbb{Q}(\sqrt{2}) \mapsto \{1,g\}$ since $\sqrt{2}$ is fixed under g.

$\mathbb{Q}(\sqrt{6}) \mapsto \{1,fg\}$ since $\sqrt{6} = \sqrt{2}\cdot\sqrt{3}$ is fixed under fg.

$\mathbb{Q} \mapsto G$ since all elts. of $\mathbb{Q}$ are fixed under all elts of G.

(Note "order-reversing": larger subgp fixes smaller subfield, & vice versa)

Here $G \cong S_2 \times S_2 = \langle a,b \mid a^2 = b^2 = (ab)^2 = 1 \rangle$, Klein Four Group.

(b) $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$

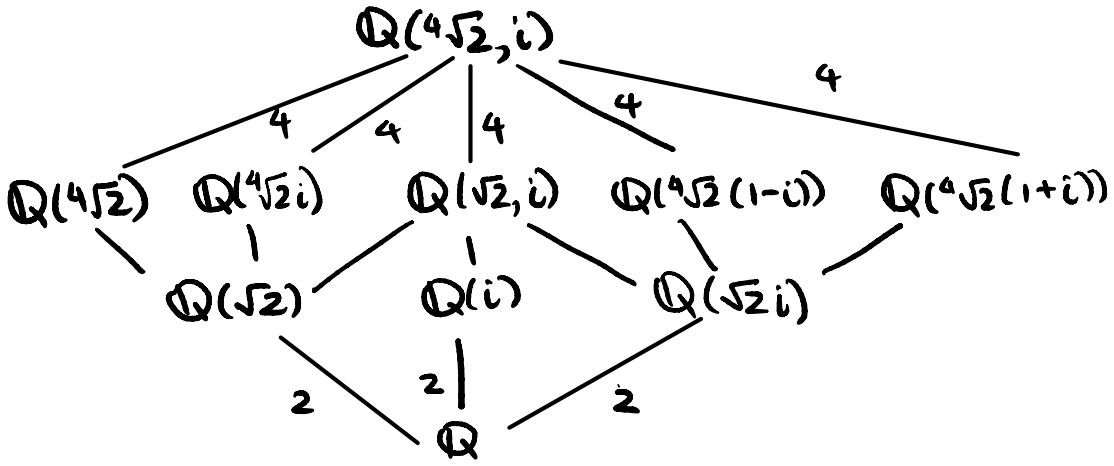
Recall (from (II)): 8-elt. Galois gp. permutes $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i$.

$G \cong D_4 = \{r, s \mid r^4 = s^2 = 1,\ rsr^{-1} = 1\}$

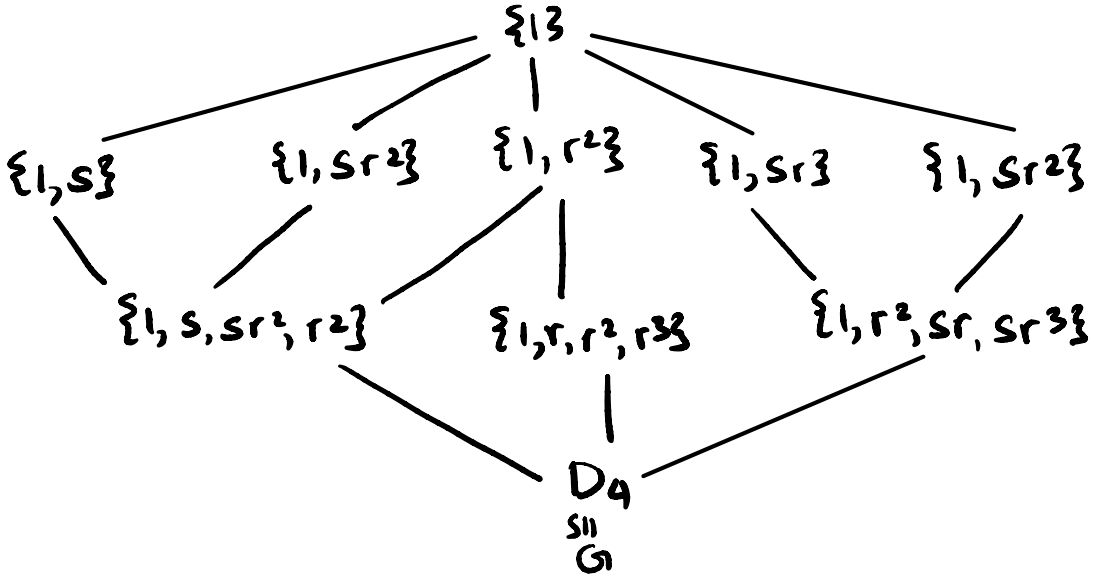
r (rotation) maps $\sqrt[4]{2} \mapsto \sqrt[4]{2}i,\ i \mapsto i$

s (conjugation) maps $\sqrt[4]{2} \mapsto \sqrt[4]{2},\ i \mapsto -i$.

<u>subfields</u>



<u>subgps</u>



$\{1\}$ corresponds to $\mathbb{Q}(\sqrt[4]{2}, i)$ as only identity fixes all 4 roots.

$\{1, s\}$ corresponds to $\mathbb{Q}(\sqrt[4]{2})$ since s fixes $\sqrt[4]{2}$.

$\vdots$ (so forth)

G corresponds to $\mathbb{Q}$ as all its elts. must fix $\mathbb{Q}$.

(c) $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$

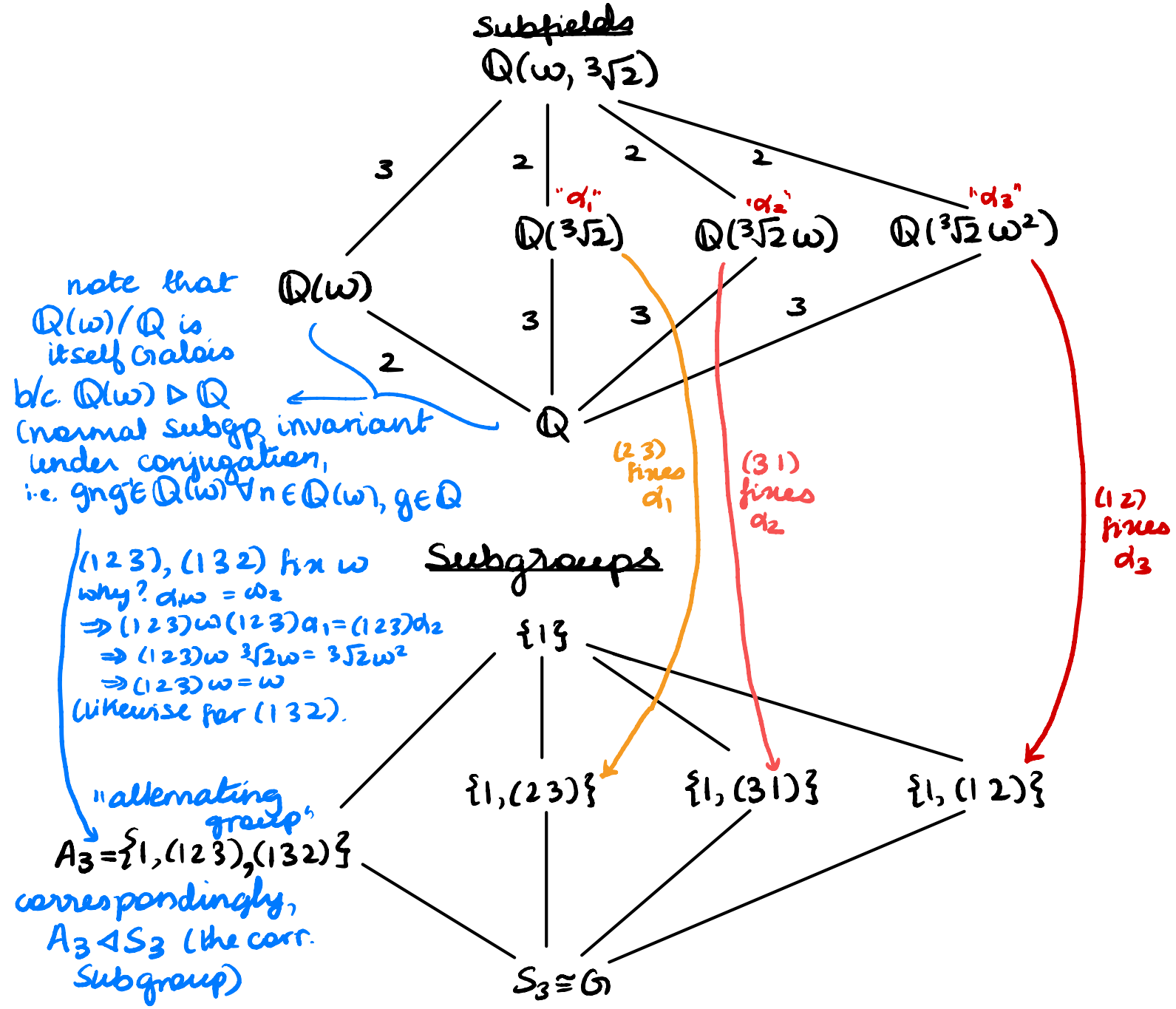
Recall (from (II)): G-elt. Galois gp. permutes $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$, where $\omega = e^{2\pi i/3}$ (3^{rd} root of unity).

Here $G \cong S_3$, the gp. of permutations of 3 elts.

We can describe the elts. of G as permutation cycles:

taking $1 = \sqrt[3]{2}, 2 = \sqrt[3]{2}\omega, 3 = \sqrt[3]{2}\omega^2$, we have,

Identity $= 1$, $\sigma_1 = (1\,2\,3)$, $\sigma_2 = (1\,3\,2)$, $\sigma_3 = (2\,3)$, $\sigma_4 = (1\,2)$, $\sigma_5 = (1\,3)$.



- **Pf of Fundamental Thm.:**

Recall, suffices to show that, given $F \subseteq L \subseteq E$ and $1 \leq H \leq G$,

① $|H| = [E : E^H]$

② $[E : L] = |\mathrm{Gal}(E/L)|$

Pf:

First, we claim ① follows directly from the fact that (by Ⅱ) E/E^H is a Galois extension with Galois gp. H, so we must have $|H| = [E : E^H]$. ✓

Now, consider ②:

$F \subseteq L \subseteq E$

$$|\mathrm{Gal}(E/F)| = \sum_{\substack{\text{maps} \\ F \to L}} (\#\text{ extensions from } L \to E)$$

$|\mathrm{Gal}(E/F)| = [E:F]$ (because E/F Galois)

$\sum_{\text{maps } F \to L} \leq [L:F]$

$(\#\text{ extensions from } L \to E) \leq [E:L]$

(both are equalities)

$$\Rightarrow [E:F] \leq [L:F] \cdot [E:L] = [E:F] \quad (\star)$$

$$=$$

i.e. $(\#\text{ of extensions from } L \to E) = [E:L]$ (since $\leq$ becomes $=$ by $(\star)$)

$\Rightarrow |\mathrm{Gal}(E/L)| = [E:L]$ as desired. □