Galois Theory

Idea Given a polynomial, how are its roots "sitting" in its splitting field? Is there a group acting on these roots?

Def K/F an extension $\mathrm{Aut}(K/F) = \{\text{automorphisms } \sigma \text{ of } K \mid \sigma(f)=f \ \forall f \in F\}$
$= \{\text{aut of } K \text{ fixing } F\}$

Remarks

1. $\mathrm{Aut}(K)$ is a group and $\mathrm{Aut}(K/F)$ is a subgroup
2. Everything in $\mathrm{Aut}(K)$ fixes prime subfield at least.

Key Prop Let $\alpha \in K$ be algebraic over F and $\sigma \in \mathrm{Aut}(K/F)$. Then α and $\sigma(\alpha)$ have the same minimal polynomial over F.

- i.e. σ permutes roots of irreducibles.

Proof Suppose $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$, $a_i \in F$. Apply σ:
$a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n = 0$. //

Ex $\mathbb{C}/\mathbb{R}$ $\sigma(z) = \bar{z}$ $(\sigma(a+bi) = a-bi)$

COR Irreducibles in $\mathbb{R}[x]$ are all linear or quadratic. Partial Fractions!

So Far: K/F field extension $\hookrightarrow$ subgroup $\mathrm{Aut}(K/F) \leq \mathrm{Aut}\, K$

Now in reverse...

Def/Prop Let $H \leq \mathrm{Aut}\, K$. Let $F = K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$. This is a subfield, called the fixed field of H, write $\mathrm{Fix}(H)$.

Ex Let $-$ be complex conj. $\mathrm{Fix}(\langle - \rangle) = \mathbb{R}$

Easy Prop

1. If $F_1 \subseteq F_2 \subseteq K$ then $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$
2. If $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ then $\mathrm{Fix}(H_2) \subseteq \mathrm{Fix}(H_1)$

- Have inclusion reversing maps from subfields of K to subgroups of $\mathrm{Aut}\, K$ and back

Ex
$$\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2}) & & \text{claim } \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{e\} \\ | & & \| \\ \mathbb{Q} & & \mathrm{Aut}(\mathbb{Q}/\mathbb{Q}) \end{array}$$
(compare to $\mathbb{Q}(\sqrt{2})$)

Thm Suppose $\varphi: F \xrightarrow{\cong} F'$, $f(x) \in F[x] \hookrightarrow f'(x) \in F'[x]$. Let E be a spl field of $f(x)/F$ and E' of $f'(x)/F'$. Then φ extends to an $\cong$

$$\begin{array}{ccc} E & \xrightarrow{\tilde{\varphi}} & E' \\ | & & | \\ F & \xrightarrow{\varphi} & F' \end{array}$$

Rmk Slightly stronger than uniqueness of spl fields, proof is by induction

Crucial Special Case Let E/F be spl field of $f(x) \in F[x]$

Thm The # of such extensions ψ in this case is $\leq [E:F]$ with equality iff $f(x)$ is separable.

Proof By induction on $[E:F]$, base case clear.
Choose $g(x) \mid f(x)$ irred, corr to $g'(x) \mid f'(x)$. Choose root α of $g(x)$, β of $g'(x)$.

$$\begin{array}{ccc} E & \text{---} & E' \\ | & & | \\ F(\alpha) & \xrightarrow{\exists} & F'(\beta) \\ | & & | \\ F & \xrightarrow{\psi} & F' \end{array}$$

{ # choices $\leq$ # roots $= [F(\alpha):F]$

Now induction

COR Let E/F be splitting field of $f(x) \in F[x]$. Then:

$$|Aut(E/F)| \leq [E:F] \quad w/= \iff f(x) \text{ separable}$$

Proof Apply above with $F \xrightarrow{id} F$.

Def Let K/F be finite. K is a Galois extension of F if $|Aut(K/F)| = [K:F]$. In this case $Aut(K/F)$ is the Galois group $Gal(K/F)$.

Example Splitting fields of separable polynomials are Galois. In this case the group is the Galois group of the polynomial.

Rmk $\deg f(x) = n$, the Galois group $\leq S_n$ order $\leq n!$

Examples

1. $\mathbb{C}/\mathbb{R}$ spl field of x^2+1, so $i \to \pm i$. ~~Both work~~
$Gal(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}_2$

2. $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is Galois, spl field of x^2-3 Also $\mathbb{Z}_2$

3. $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ SF of $(x^2-2)(x^2+3)$. Know Galois group of order 4.
Thus $\sqrt{2} \to \pm\sqrt{2}$ $\sqrt{3} \to \pm\sqrt{3}$ give all
$Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Compute lattice

4. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.

5. $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is Galois, spl field of x^3-2.
This extension has degree 6 so we know it is $\cong S_3$
compute lattice

6. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, so we know Galois group has order n.
Exercise The Frobenius map fixes $\mathbb{F}_p$ and has order n. Thus

$$Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}_n = \langle Frob \rangle$$

Fundamental Thm of Galois Theory

Let K/F be a Galois Extension, $G = Gal(K/F)$. Then $\exists$ a bijection

$$\{\text{subfields } E \text{ with } F \subseteq E \subseteq K\} \longleftrightarrow \text{subgroups } H \text{ of } G$$

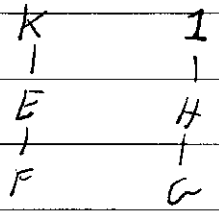
as before such that

1. These maps are mutual inverse, i.e. $H \leq G \to Fix\,H \to Gal(K/Fix\,H) = H$

   $E \to Gal(K/E) \to Fix(Gal\,K/G) = E$

   and inclusion reversing

2. Suppose $E \longleftrightarrow H$. Then $[K:E] = |H|$ $[E:F] = [G:H]$



3. K/E is Galois and $Gal(K/E) = H$.

4. E/F is Galois $\longleftrightarrow H \trianglelefteq G$. If so then $Gal(E/F) \cong G/H$

5. The lattices of subgroups and subfields are "dual," i.e.

   - Subfields $E_1, E_2 \longleftrightarrow$ subgroups H_1, H_2 then

     $E_1 E_2 \longleftrightarrow H_1 \cap H_2$

     $E_1 \cap E_2 \longleftrightarrow \langle H_1, H_2 \rangle$

Proof: Next time

Example Splitting field of x^8-2

$\zeta_8 = e^{2\pi i/8}$ and $\sqrt[8]{2}$ generate spl field.

Now $e^{2\pi i/8} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$ and $\sqrt{2} = (\sqrt[8]{2})^4$. Thus

Fact Splitting field is $\mathbb{Q}(\sqrt[8]{2}, i)$ has degree 16. The Galois group G has 16 elements

Rmk Any $\sigma \in G$ maps $i \to \pm i$ and $\sqrt[8]{2} \to \sqrt[8]{2}\,\zeta_8^a$ $0 \le a < 7$.

Corollary All 16 of these extend to field automorphisms, no checking!

Def $\sigma: \sqrt[8]{2} \to \zeta_8 \sqrt[8]{2}$ $\quad i \to i$ $\qquad \tau: \sqrt[8]{2} \to \sqrt[8]{2}$ $\quad i \to -i$

Notation $\theta = \sqrt[8]{2}$ $\quad \zeta = \zeta_8$

$$\sigma: \begin{cases} \theta \to \zeta\theta \\ i \to i \\ \zeta \to \zeta^5 = -\zeta \end{cases} \qquad \text{since } \zeta = \tfrac{1}{2}\theta^4 + \tfrac{1}{2}\theta^4 i$$

$$\tau \begin{cases} \theta \to \theta \\ i \to -i \\ \zeta \to \zeta^7 \end{cases}$$

Exercise $\mathrm{Gal}(\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^8 = \tau^2,\ \sigma\tau = \tau\sigma^3 \rangle$

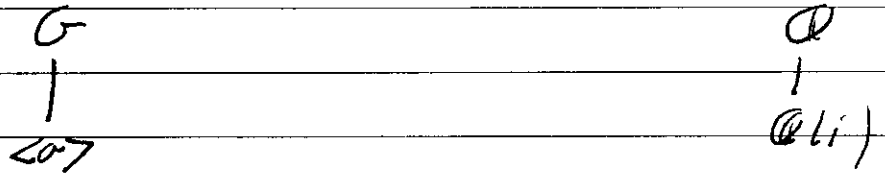
called quasi dihedral.

Warning $\sqrt[8]{2}$ has x^8-2 m.p

ζ_8 has x^4+1 minpoly but not $\mathbb{Q}$ chains.

$\theta^4 = \zeta_8 + \zeta_8^7$

Examples $\langle\sigma\rangle \trianglelefteq G$ of index 2 s.t. $Fix(\sigma)$: $\mathbb{Q}$ index 2. obviously $= \mathbb{Q}(i)$.



etc...

Ex $\langle\sigma^4\rangle \trianglelefteq G$ and $G/\langle\sigma^4\rangle \cong D_8$

$\|$

$\mathbb{Z}/4\mathbb{Z}$

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

$\forall$ σ^4: $\mathbb{Q} \to \mathbb{Q}$ s.t. $Fix(\sigma^4) = \mathbb{Q}(i, \sqrt{2})$ deg 8

$i \to i$

$\sqrt{2} \to \sqrt{2}$ and is a S.F.

$Gal(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) \cong D_8$

S.F. of $x^4 - 2$