Lecture 26: Finding Galois Groups

Thm: K/F Galois, $G = Gal(K/F)$.

$$\left\{\begin{matrix}\text{subfields} \\ F \subseteq E \subseteq K\end{matrix}\right\} \xleftrightarrow{\text{bijection}} \left\{\begin{matrix}\text{subgroups} \\ H \leq G\end{matrix}\right\}$$

$$E \longmapsto G_E = Gal(K/E)$$

$$K_H \longleftarrow H$$

Q: Does every finite group arise as $Gal(K/\mathbb{Q})$, where $K/\mathbb{Q}$ is Galois?

could ask for other fields

Some groups that do occur: $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_8, Q_8, $\mathbb{Z}/8\mathbb{Z}$, S_3, ...

Any Galois $K/\mathbb{Q}$ is the splitting field of a separable $f(x) \in \mathbb{Q}[x]$ with roots $\alpha_1, \dots, \alpha_n \in K$.

Get an embedding $G \xrightarrow[\rho]{} S_n$

where $\rho(\sigma)$ sends i to j iff $\sigma(\alpha_i) = \sigma(\alpha_j)$

So $G \cong$ (subgp of S_n)

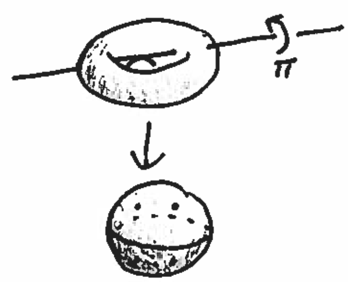
Q: Is this a restriction on G?

A: No.

Conj: (Inverse Galois Problem) Every finite group is $\mathrm{Gal}(K/\mathbb{Q})$ for some K.

Q: What about $\mathrm{Gal}(K/\mathbb{F}_p)$? A. Always cyclic!

Every finite gp does appear as $\mathrm{Gal}(K/\mathbb{C}(t))$. [Will discuss at length...]



This week's goal: extract $\mathrm{Gal}(K/F)$ from $f(x) \in F[x]$.

Start with the generic example where $G = S_n$.

Fix a field F. Consider $K = F(x_1, \dots, x_n)$
$=$ field of fractions of $F[x_1, \dots, x_n]$.

Note $\mathrm{Aut}(K) \geq S_n$ where
S_n acts on K by permuting the x_i according to their subscripts.

Set $L = K_{S_n}$ so that $Gal(K/L) = S_n$.

$\uparrow$ field of symmetric functions

Example elts:

- F
- $s_1 = x_1 + x_2 + \cdots + x_n$
- $s_n = x_1 x_2 \cdots x_n$
- $s_2 = \sum_{i<j} x_i x_j$ e.g. if $n = 3$, $s_2 = x_1x_2 + x_1x_3 + x_2x_3$
- $s_k = \sum_{i_1 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}$

Elementary Symmetric Functions

Thm: $L = F(s_1, \ldots, s_n)$

Pf: Set $L' = F(s_1, \ldots, s_n)$. Have $L' \subseteq L$ and $[K:L] = |S_n| = n!$ Hence is enough to show $[K:L'] \leq n!$ This follow since K is the splitting field of the following degree n poly in $L'[x]$:

$$\prod (x - x_i) = x^n - (x_1 + x_2 + \cdots + x_n)x^{n-1} + \cdots + (-1)^n x_1 \cdots x_n$$
$$= x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n$$

The <u>discriminant</u> of $f(x) \in F[x]$ is

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2$$ where α_i are the roots of F in some splitting field K.

Viewing D as a symmetric fn of the roots, a cor of the previous thm is that D can be expressed in terms of the coeff of f.

<u>Ex</u>: $\deg f = 2$.

$$D = (x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2 = (x_1 + x_2)^2 - 4x_1x_2$$
$$= (s_1)^2 - 4s_2$$

So if $f(x) = x^2 + \underbrace{b}_{-s_1} x + \underbrace{c}_{s_2}$, then $D = (-b)^2 - 4c = b^2 - 4c$

Where have we seen this before?

<u>Ex</u>: $f(x) = x^3 + ax^2 + bx + c$. It turns out

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$$

Note that D is a square in K, e.g.

$$\sqrt{D} = \prod_{i<j} (\alpha_i - \alpha_j)$$

$$\begin{array}{c} K \\ | \\ F(\sqrt{D}) \\ | \\ F \end{array}$$

Suppose $G = Gal(K/F) = S_n$.

Then $\exists\, \sigma \in G$ with $\sigma(\sqrt{D}) = -\sqrt{D}$),

e.g. $\sigma = (12)$. If $\underbrace{\text{char} \neq 2}_{\text{standing assumption}}$, this means $\sqrt{D} \notin F$.

$\underline{n=2}$: $f(x)$ irred in $F[x]$ of deg 2. Then $[K:F]=2$ and $Gal(K/F) \cong \mathbb{Z}/2\mathbb{Z} \cong S_2$. So $K = F(\sqrt{D})$

<u>Knew already</u>: Roots of x^2+bx+c are $\dfrac{-b \pm \sqrt{b^2-4c}}{2}$.

$\underline{n=3}$: $f(x)$ irred of deg 3. Have $G \leq S_3$.

<u>Q</u>: Could $G = \langle (12) \rangle$? <u>A</u>. No as must be able to take any root of f to any other.

So poss are: $G = \langle (123) \rangle \cong \mathbb{Z}/3\mathbb{Z} \iff [K:F]=3$
$\iff D$ is a square in F

$G \cong S_3 \iff [K:F]=6 \iff D$ is <u>not</u> a square in F.