

Lecture 26:

70

Previously on Math 418:

Thm K/F Galois, $G = \text{Gal}(K/F)$ Have a bijection

$$\left\{ \begin{array}{l} \text{subfields} \\ \text{of } F \subseteq E \subseteq K \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Subgrps} \\ H \leq G \end{array} \right\}$$

$$K_H \longleftarrow H$$

$$E \longrightarrow \text{Gal}(G/E)$$

Suppose K/\mathbb{Q} is Galois. Then $G = \text{Gal}(K/\mathbb{Q})$ is some finite group.

Q: Does every finite group arise this way?

Some ex's: $G = \mathbb{Z}_2, D_8, Q_8, \mathbb{Z}_8, S_3, \dots$

General Form:

$K = \mathbb{Q}(\alpha)$ where α is a root of a separable poly $f(x) \in \mathbb{Q}[x]$

|

which splits completely in $K[x]$

\mathbb{Q}

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

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

where $\rho(\sigma)$ sends $i \rightarrow j$ if $\sigma(\alpha_i) = \alpha_j$.

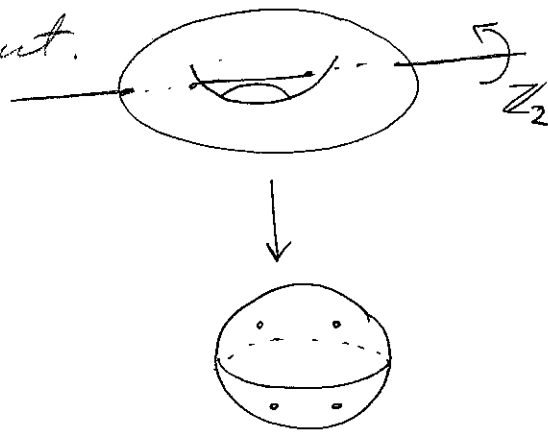
So $G \cong$ subgp of S_n . Q: is this a restriction?

A: No.

Conj (inverse Galois Problem) Every finite group
 $G = \text{Gal}(K/\mathbb{Q})$.

Known if we replace \mathbb{Q} with $\mathbb{C}(t)$, where
this is really a geometric statement.

False if we take \mathbb{F}_p instead of \mathbb{Q} .



Generic example when $G = S_n$

Fix F , and consider

$$K = F(x_1, \dots, x_n) = \text{field of fractions of } F[x_1, \dots, x_n]$$

Note $\text{Aut}(K) \cong S_n$ where S_n acts

on K via permuting the subscripts on the x_i .

Let $L = K_{S_n}$, the field of symmetric fns.

71

Example elts: So $\text{Gal}(K/L) = S_n$.

• anything in F

• $S_1 = x_1 + x_2 + \dots + x_n$

• $S_n = x_1 x_2 \dots x_n$

• $S_2 = \sum_{i < j} x_i x_j$

Eig. if $n=3$

• $S_k = \sum_{i_1 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k}$

$S_2 = x_1 x_2 + x_1 x_3 + x_2 x_3$

Elementary symmetric functions.

Thm: $L = F(s_1, s_2, \dots, s_n)$

Proof: Set $L' = F(s_1, \dots, s_n)$. Clearly $L' \subseteq L$.

Know $[K:L] = |S_n| = n!$. So, enough to show $[K:L'] \leq n!$. This follows since

$$\begin{aligned} m_{x_i, L}(x) &= \prod (x - x_i) = x^n - (x_1 + \dots + x_n)x^{n-1} + \dots + (-1)^n x_1 \dots x_n \\ &= x^n - S_1 x^{n-1} + S_2 x^{n-2} + \dots + (-1)^{n-1} S_{n-1} x + (-1)^n S_n \\ &\in L'[x] \end{aligned}$$

So K is the splitting field of a deg n poly in $L'[x] \Rightarrow [K:L'] \leq n!$ ▣

Consider any $f(x) \in F[x]$. Its discriminant is

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

Note: $D \in F$.

Cor of above: D can be expressed in terms of the coeffs of f in a uniform way.

Ex: deg $f = 2$. Notice.

$$\begin{aligned} (x_1 - x_2)^2 &= x_1^2 - 2x_1x_2 + x_2^2 \\ &= (x_1 + x_2)^2 - 4x_1x_2 = S_1^2 - 4S_2. \end{aligned}$$

So if $f(x) = x^2 + bx + c$, then

$$D = (-b)^2 - 4c = b^2 - 4c$$

Ex: $f(x) = x^3 + ax^2 + bx + c$

72

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

Notice that D is a square in K , with

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

So have

K	<u>Now:</u> $\text{cl}_f \text{Gal}(K/F) = S_n,$
$ $	
$F(\sqrt{D})$	then $\sqrt{D} \rightarrow -\sqrt{D}$ by e.g. (12)
$ $	
F	so $F(\sqrt{D}) \neq F$. (Assuming char $\neq 2$)

Ex: $n=2$. $\text{cl}_f D$ is a square, $K = F$

Otherwise $K = F(\sqrt{D})$, which is really just the quad. formula.

Ex: $n=3$, f irreducible.

$$\begin{aligned} D \text{ not a square in } F &\Rightarrow 2 \mid [K:F] \\ &\Rightarrow [K:F] = 6 \\ &\Rightarrow \text{Gal}(K/F) = S_3 \end{aligned}$$

D a square \Rightarrow every elt of $G \leq S_n$ is
even $\Rightarrow G = Z_3$.

In general, $\sigma \in S_n$ fixes $D \Leftrightarrow \sigma \in A_n$.