Previously on Math 418:

**Theorem:** \( K/F \) is Galois, \( G = \text{Gal}(K/F) \) have a bijection

\[
\left\{ \text{subfields of } F \leq E \leq K \right\} \leftrightarrow \left\{ \text{subgroups } H \leq G \right\}
\]

\[
K_H \xleftarrow{\text{ }} H \xrightarrow{\text{ }} \text{Gal}(G/E)
\]

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

**Question:** Does every finite group arise this way?

Some exs: \( G = \mathbb{Z}_2, D_8, Q_8, \mathbb{Z}_8, S_3 \ldots \)

**General Form:**

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

which splits completely in \( K[x] \)

\[
f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)
\]
Get an embedding \( G \to \mathcal{G}_n \)
where \( p(\sigma) \) sends \( i \to j \) if \( \sigma(x_i) = x_j \).

Do \( G \cong \text{subgp of } \mathcal{G}_n \) ?
\( Q: \) Is this a restriction?
\( A: \) No.

\( \text{Conj} (\text{classifical Galois Problem}) \): Every finite group \( G = \text{Gal}(K/Q) \).

Known if we replace \( Q \) with \( \mathbb{C}(t) \), where this is really a geometric statement.
False if we take \( \mathbb{F}_p \) instead of \( Q \).

Generic example when \( G = \mathcal{G}_n \)
Fix \( F \), and consider
\[ K = F(x_1, \ldots, x_n) = \text{field of fractions of } F[x_1, \ldots, x_n] \]

Note \( \text{Aut}(K) \cong \mathcal{G}_n \) where \( \mathcal{G}_n \) acts
on \( K \) via permuting the subscripts on the \( x_i \).
Let \( L = K S_n \), the field of symmetric functions.

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

- anything in \( F \)
- \( S_1 = x_1 + x_2 + \cdots + x_n \)
- \( S_n = x_1 x_2 \cdots x_n \)
- \( S_2 = \sum_{i < j} x_i x_j \) \hspace{1cm} \text{E.g., if } n = 3 \hspace{1cm} S_2 = x_1 x_2 + x_1 x_3 + x_2 x_3 \)
- \( S_k = \sum_{i_1 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k} \)

**Thm:** \( L = F(s_1, s_2, \ldots, s_n) \)

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

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

\[
M_{x_{i_1}L}(x) = \prod (x - x_i) = x^n - (x_1 + \cdots + x_n) x^{n-1} + \cdots + (-1)^n x_1 \cdots x_n
\]

\[
= x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n
\]

\[
\in L'[x]
\]
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

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

where $\alpha_i$ are the roots of $f$ 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

$$(X_1 - X_2)^2 = X_1^2 - 2X_1X_2 + X_2^2 = (X_1 + X_2)^2 - 4X_1X_2 = S_1^2 - 4S_2.$$

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

$$D = (-b)^2 - 4c = b^2 - 4c$$
Ex: \( f(x) = x^3 + ax^2 + bx + c \)

\[
D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.
\]

Notice that \( D \) is a square in \( K \), with

\[
\sqrt{D} = \prod_{i<j} (x_i - x_j)
\]

So have

\[
\begin{array}{c}
K \\
F(\sqrt{D}) \\
F
\end{array}
\]

Now: if \( \text{Gal}(K/F) = S_n \),

then \( \sqrt{D} \rightarrow -\sqrt{D} \) by e.g. (12)

so \( F(\sqrt{D}) \neq F \) (Assuming that \( \neq 2 \))

Ex: \( n = 2 \). If \( D \) is a square, \( K = F \)

Otherwise \( K = F(\sqrt{D}) \), which is really just the quad. formula.
Ex: $n=3$, finitely.

D not a square in $F \Rightarrow 2 | [K:F]$ 

$\Rightarrow [K:F] = 6$

$\Rightarrow \text{Gal}(K/F) = S_3$

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

$\Rightarrow G = \mathbb{Z}_3$.

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