Math 501: lecture 15

Galois theory

Definition: A normal, separable algebraic extension is called a Galois extension.

We have shown:
1. If $L/K$ is Galois, $\#\Aut_K(L) = n$.
2. If $G \leq \Aut(L)$ finite, then $[L: \text{Fix}(G)] = |G|$. 

Example: $F$ field, $L = F(x_1, \ldots, x_n)$ (function field in $n$ variables). Then $S_n \leq \text{GL}(L)$ by permuting the variables. $c(x_1, x_2) = x_2^3 x_1$.

Definition: $K = L^{S_n} = \text{Fix}(S_n)$ is called the field of symmetric rational functions, fraction field of the ring of symmetric polynomials $F[x_1, x_2, \ldots, x_n]^{S_n}$. (More on this in PS6)

Observation: $\prod (x - x_i) = \sum \prod_{i \neq j} x_{i+j} \sum_{\text{sym} \subseteq [n]} \prod_{i \in \text{sym}} x_i \sum_{\text{sym} \subseteq [n]} \prod_{i \in \text{sym}} H_{\text{sym}}(L)$

Symmetric polynomial $\rightarrow S_{n-k}(x_1, \ldots, x_n)$
By previous results, $[K : F] = n!$, $\text{Aut}_K(L) = S_n$.

Corollary: Let $G$ be any finite group. Embed $G$ in some $S_n$ (Cayley's theorem), take $F(x_1, x_2, \ldots, x_n)$ to get an extension with $\text{Aut}_K(L) = G$.

Conj.: Every finite group is $\text{Aut}_K(L)$ for some finite normal extension $L/K$.

("inverse Galois problem")

(Conjectures due to G. Malle lamenting such extensions)

---

Technology: $L \xrightarrow{\theta} L' \xrightarrow{\phi} L''$ $\phi \in \text{Hom}_{k}(L, M)$

If $f \in K[x]$, $\alpha \in L$, then $\theta(f(\alpha)) = (\phi(f))(\theta(\alpha)) = f(\theta(\alpha))$

So $f(\alpha) = 0$ iff $\theta(f) = 0$

Corollary: $\text{Aut}_K(L)$-orbit of $\alpha \in L$ satisfies $f(\alpha) = 0$ is contained in $\{ \text{roots of } f \}$, is finite.

(If $L/K$ algebraic, $\text{Aut}_K(L)$ acts with finite orbits)
Add normality: \( L \to N \to M \)

\( L, N \) extensions of \( K \)
\( N/K \) normal, \( M \) extension of \( N \).

Claim: \( \tau(L) \subseteq N \).

Proof: Let \( \alpha \in L \), let \( f \in K[x] \) be the min poly.

Then \( \tau(\alpha) \) is a root of \( f \) in \( N \). By normality, \( f \) splits in \( N \), so all roots of \( f \), including \( \tau(\alpha) \), are in \( N \), so \( \tau(\alpha) \in N \).

Lemma: \( f \in K[x] \) irreducible, \( N/K \) normal. If \( f \) splits in \( N \) then \( \text{Aut}_K(N) \) acts transitively on the roots.

(start with \( \alpha \in N \). Can make two different sets:
\( \text{Aut}_K(N) \cdot \alpha \subseteq \{ \text{roots of min} \} \)

Lemmal: sets are equal)

(explicit symmetry easy to check. "natural" set from pov of \( K \))

("nothing to say about roots of f except that")
(weak version: all extensions gotta be roots of f are isomorphic (to K[x]/f))
(strong: isom extends to map N \to N)

(cf. see them about triangles)

Pf: let \( g \in K[x] \) st. \( N \) is the splitting field of \( g \) over \( K \). Let \( \alpha, \beta \) be roots of \( f \). Then \( N \) is a splitting field of \( g \) over \( K(\alpha), K(\beta) \).

\[
\begin{array}{c}
N \quad N \\
\downarrow \quad \downarrow \\
K(\alpha) \stackrel{?}{\rightarrow} K(\beta)
\end{array}
\]

By thm on uniqueness of splitting field, have a compatible isom. \( N \to N \).

[Ex: same holds if \( NK \) infinite]

Prop: let \( L \subseteq K \) be finite, \( NK \) finite, normal \( \sigma, \tau \in \text{Hom}_K(L, N) \) (saw for each \( \sigma \), have \( \text{aut} \sigma \in \text{Aut}_K(N) \) st. \( \sigma((\sigma(\alpha)) = \sigma(\alpha) \))

Pf: let \( L = K(\alpha) \) this is the lemma
In general, do same: let $g_k$ be st. $N$ is a splitting field of $g$ over $K$, then $N$ is a splitting field of $g$ over $F(L), E(L)$.

$N \rightarrow \mathbb{P} \rightarrow N$

$\sigma(L) \rightarrow \tau(L)$ compatible with $K$.

Notes: By induction, extends to all extensions.

---

**Add separability.** If $L/K$ is normal + separable call it Galois, call $\text{Gal}(L/K) = \text{Aut}_K(L)$ the Galois group of the extension.

**Thm:** Let $[L:K] = n$. TFAE:

1. $L/K$ Galois
2. $\text{Aut}_K(L)$ has order $n$
3. Fixed field of $\text{Aut}_K(L)$ is $K$

**Pf:** So w.r.t. if $L/K$ Galois then have $n$ $K$-maps $L \rightarrow L$. (Target is normal, source separable, home
at least one map). Maps are surjective as injective
\[ C(1) \Rightarrow (2) \]
also \( (2) \Rightarrow (3) : \text{let } F = \text{Fix}(\text{Aut}_K(L)) \)
Then \( [L : F] = \# \text{Aut}_K(L) \)
\[ = \sum [F : K] = \frac{[L : K]}{\sum [E : L]} = \frac{\#}{\# \text{Aut}_K(L)} \]
so LHS = 1 \iff RHS = 1.
that \( (2) \implies (1) \) is \( H.W. \)

Next time: let \( L/K \) be finite Galois, \( G = \text{Gal}(L/K) \)
there have bijections
\[
\left\{ \text{subfields of } L \right\} \leftrightarrow \left\{ \text{subgrp of } G \right\}
\]
\[
M \mapsto \text{Gal}(L/M)
\]
\[
\text{Fix}(C_H) \leftrightarrow H
\]
\[ + \left[ L : \text{Fix}(C_H) \right] = \# H \]
\[ \left[ \text{Fix}(C_H) : K \right] = \left[ G : H \right] \]
(inclusion, reversing)
Fix \( (H)/K \) normal if \( H \subseteq G \)
then \( \text{Gal}(Frac(H)/K) \cong G/H \).

---

**Ex:** Let \( A, B \subseteq \text{subsets of Hilbert space} (\mathbb{R}^n, \text{Euclidean metric}) \)
suppose \( f: A \to B \) isometry:
\[
    ||f(a) - f(b)|| = ||a - b||
\]
for all \( a, b \in A \).

Then \( f \) extends to an isometry of the whole space.

\[ \text{End.} \quad A \quad B \]

**False** if \( \| (\mathbf{x}) - (\mathbf{w}) \| = \max \{ \|x - x\|, \|y - w\| \} \)

\( N \text{ dig field, normal } K \)
\( L_1, L_2 \text{ subfields isomorphic as } K \text{ extensions.} \)
Let $\omega$ be a root of poly $p \in \mathbb{Q}_1[x]$.

$\sigma : \mathbb{Q}_1 \to \mathbb{Q}_2$ isom. Why does $\sigma(p)$ have a root? (in $\mathbb{Q}_2$)

$p = x^3 + \sqrt{2} x^2 + \left(\frac{5}{2} + \frac{\sqrt{2}}{2}\right)x + \sqrt{2} \cdot 7 = 0$

$\in \mathbb{Q}(\sqrt[4]{2})[x]$.

Suppose $\sqrt[4]{2}$ normal $\mathbb{Q} x^n$, $\sqrt[3]{2} \in \mathbb{Q}$.

does $p' = x^3 + (3\sqrt[3]{2} \omega) x^2 + \left(\frac{5}{2} + \frac{\sqrt[3]{2} \omega^2}{2}\right)x - \sqrt[3]{2} \omega \cdot 7$ have a root? $\in \mathbb{Q}(\sqrt[3]{2} \omega)[x]$.
(roots of $x^3 - 2$ are $\sqrt[3]{2}, \sqrt[3]{2} w, \sqrt[3]{2} w^2$)

Let $p: \mathbb{N} \to \mathbb{N}$ be such $p(\sqrt[3]{2}) = \sqrt[3]{2} w$.

Then $p(p(x)) = p'$, if $p(x) > 0$

then $p(p(x)) = (f(x))(p(x)) = p'(f(x)) = 0$

As long as $\theta(\sqrt[3]{2}) \to \omega(\sqrt[3]{2} w)$

$$\omega = \frac{-1 + \sqrt{3} i}{2} \quad \text{(fact: } \sqrt[3]{2} w \text{ root of } 4)\quad x^3 - 2$$

$$x^2 - 2x - 2$$

$$|\frac{a}{b}| = \frac{1}{b}$$

$$|a| = \frac{1}{p}, \quad 1 < |a| = \frac{1}{p^2}, \quad \text{when } p \neq a, b$$

$$\text{Also, check } 1|x+y| \leq |x| + |y| \quad |xy| \leq 1$$

$$d(x, y) = |x - y| \text{ metric on } \mathbb{Q}$$

Problem: What is the completion.
ODE \quad y' = y \\

Does it have a solution?

L = K(\alpha_1, \ldots, \alpha_r), \quad f_i = \text{min poly of } \alpha_i \\
normal closure of L/K = \text{splitting field of } f_i.