Math 501: Problem Session 7

**Question:** what is a "radical"?

**Answer:** an element of the form \( \sqrt[m]{\beta} \).

\( \Rightarrow \) a root of a polynomial of the form \( t^m - \beta \).

---

A "radical extension" is one obtained by successively adjoining radicals:

\[ L = K(\alpha_1, \ldots, \alpha_k) \] where we have \( m_i \in \mathbb{Z}_{\geq 1} \) such that \( \alpha_i \in K(\alpha_1, \ldots, \alpha_{i-1}) \).

**Example:** \( K(\sqrt[3]{2}, \sqrt[3]{3 + 5}, \sqrt[8]{(5\sqrt[3]{2} + 2)^2 + \sqrt[3]{2}}) \)

(use the word "radical" rather than "root" because we want to talk about roots of polynomials)

If \( \Sigma \mid K \) is the splitting field of \( \overline{f} \in K[x] \), then \( \Sigma(\omega) = \sigma(\Sigma(\omega)) \downarrow \Sigma(\omega) \) / \( \Sigma(\omega) \)
reason, if \( f: \frac{1}{(x-\alpha_1)(x-\alpha_r)} \)

then \( \Sigma = K(\alpha_1, \ldots, \alpha_r) \)

so \( \Sigma(w): K(\alpha_1, \ldots, \alpha_r, w) = K(w)(\alpha_1, \ldots, \alpha_r) \)

---

**Proof (\( \sigma \)):** Let \( K \) finite, \( Gal(K) \), \( K < N_1, M_2 < L \)

\[ G = Gal(L/K), \ H_i = Gal(L/M_i). \]

Suppose \( \sigma \in G \) has \( \sigma(M_1) = M_2 \)

then \( \tau \in H_2 \) iff \( \forall \alpha \in M_2, \ \tau(\alpha) = \alpha \)

iff \( \forall \alpha \in M_1, \ \tau(\sigma(\alpha)) = \sigma(\alpha) \)

iff \( \forall \alpha \in M_1, \ (\sigma^{-1}\tau)(\alpha) = \alpha \)

iff \( \sigma^{-1}\tau \in H_1 \),

i.e. \( H_2 = \sigma^{-1}H_2\sigma, \ H_2 = \sigma H_1\sigma^{-1} \).

(That's why we use the same words for "conjugate subgroups" and "conjugate subfields".)

Conversely, if \( \sigma H_1\sigma^{-1} = H_2 \)

then if \( \alpha \in M_1 \), then \( \sigma(\alpha) \) stabilized by \( H_2 \):

iff \( \tau \in H_2 \), \( \sigma^{-1}\tau \sigma \in H_1 \), \( (\sigma^{-1}\tau)(\alpha) = \alpha \).
So $\sigma(\sigma(\alpha)) = \sigma(\alpha)$.

So $\sigma(M_1) \subseteq M_2$.

Symmetrically, $H_1 = \sigma^{-1} H_2 \sigma = \sigma(M_2) \subseteq M_1$.

So $f, \sigma^{-1}$ are an isom of $M_1, M_2$.

Difficult part: if $M_1/k, M_2/k$ isom as abstract extensions can extend isom to $L$.

Method 1: $L$ is the splitting field of some $f \in K[x]$. Then $L$ is the splitting field of $f$ over both $M_1$ and $M_2$. But $M_1, M_2$ isomorphic, so by uniqueness of splitting fields have isom $L \rightarrow L$ respecting isom $M_1 \rightarrow M_2$.

Method 2: Since $L/k$ is Galois, it's separable and so is $M_1/k$. By the primitive element theorem, have $g \in M_1$ s.t. $M_1 = k(\Theta)$.

Let $f: M_1 \rightarrow M_2$ be the $K$-isom. Then $M_2 = K(f(\Theta))$. 
Let $f$ be the min poly of $\theta$ over $K$. Then $\sigma(f(\theta)) = f(\sigma(\theta))$, i.e. $\theta, \sigma(\theta)$ are roots of $f$ in $L$.

By the transitivity of the $G$-action, have $\sigma \in G$ s.t. $\sigma(\theta) = \rho(\theta)$.

Then $\sigma(M_1) = \sigma(K(\theta)) = K(\sigma(\theta)) = K(\rho(\theta)) = K(f(\theta))

So $\sigma_{M_1}$ : $M_1 \to M_2$ is an isom.

(in fact $\sigma_{M_1} = \rho$)

$\sigma_{M_1}$

---

$\mathbb{V} = C_2 \times C_2 \cong (\mathbb{F}_2^2, +)$

(a) Suppose $\text{Gal}(L/K) \cong V$.

Subgrp lattice of $V$:

```
  \text{span } \{ (1,0) \}
  \text{span } \{ (1,0), (0,1) \}
  \text{span } \{ (1,0), (0,1), (1,1) \}
```

$\text{span } \{ (1,0), (0,1), (1,1) \}$
3) Have 3 intermediate fields \( K = \mathbb{Q}, \mathbb{Q}, \mathbb{Q, Q, Q} \cdot L \).

As quadratic extensions of \( K, \text{char}(K) \neq 2 \), have \( \alpha_1, \alpha_2 \in K \) s.t.

\[ M_1 = K(\sqrt{\alpha_1}) \]

\( M_1 \) distinct, \( \alpha_1 \) distinct in \( K^2/(K^2)^2 \). \( \text{check!} \)

Consider \( K(\sqrt{\alpha_1}, \sqrt{\alpha_2}) \) this contains \( M_1 \) but isn't \( M_1 \). (\( \alpha_2 \) not a square in \( M_1 \) since \( \alpha_2 \) not a square in \( K \), not in \( \alpha_1(\sqrt{\alpha_1})^2 \))

So \( K(\sqrt{\alpha_1}, \sqrt{\alpha_2}) = L \).

(also \( M_2 = K(\sqrt{\alpha_1 \alpha_2}) \) - check!)

ep. \( \{\sqrt{3}, \sqrt{3}, \sqrt{5}\}, \{\sqrt{3}, \sqrt{5}\} \)

Converse: Suppose \( \alpha_1, \alpha_2 \) belong to different non-trivial classes in \( K^2/(K^2)^2 \).

Let \( L = K(\sqrt{\alpha_1}, \sqrt{\alpha_2}) \).

(1) \( L \) is normal (splitting field of \( (t^2 - \alpha_1)(t^2 - \alpha_2) \))

(2) \( L \) is separable (\( \text{char} K = \mathbb{Z} \leq \mathbb{Z} \)).

Know \( [L:K] = [L:K(\sqrt{\alpha_1})] [K(\sqrt{\alpha_1}):K] = 2 \cdot 2 = 4 \).
\( L \cong K(\sqrt{a_1}) \) since \( a_2 \) not square in \( K(\sqrt{a_1}) \).

Let \( G = \text{Gal}(L/K) \) act on \( \pm \sqrt{a_1}, \pm \sqrt{a_2} \).

If \( \sigma \in G \) then \( \sigma(\sqrt{a_1}) \in \{ \pm \sqrt{a_1} \} \)
\( \sigma(\sqrt{a_2}) \in \{ \pm \sqrt{a_2} \} \)

This is a map \( G \to \mathbb{Z}/2 \times \mathbb{Z}/2 \)
\( G' \times C_2 \)

Map is a 3d hom:

Map \( G \to \text{Gal}(M_1/K) \times \text{Gal}(M_2/K) \)

By restriction, \( M_i \) quadratic = normal

Map from \( G \) to \( V = C_2 \times C_2 \).

Injective: if \( \sigma \in G \) maps to \((id, id)\) it fixes both \( \sqrt{a_1}, \sqrt{a_2} \), i.e. \( L \) fixed.

\( |G| = [L : K] = 4 \times 2 \times 2 \) so map is an isom.

Idea: let \( G \) act on conjugates of generators \( a_1, a_2 \), embed \( G \) in a set of groups.
\(\mathbb{Q}(\sqrt{2}, \sqrt{3})\)

(a) \(\alpha^2 = (2 + \sqrt{2})(3 + \sqrt{3}) = 6 + 3\sqrt{2} + 2\sqrt{3} + \sqrt{6}\)

but this element is not in \(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})\), \(\mathbb{Q}(\sqrt{6})\).

So \(\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})\)

but \(6 + 3\sqrt{2} + 2\sqrt{3} + \sqrt{6}\) is not a square in this field, so
\[
[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2
\]
So \([\mathbb{Q}(\alpha) : \mathbb{Q}] = 8\).

Galois conjugates of \(\alpha\):
\[\pm\sqrt{(2 + \sqrt{2})(2 + \sqrt{3})}\]

total of 8 element (if all distinct)

if all contained in \(\mathbb{Q}(\alpha)\) then \(\mathbb{Q}(\alpha)\)
splitting field of the min poly of \(\alpha\)
Always have negatives. 
Start with \( \sqrt{(2-\sqrt{2})(3+\sqrt{2})} = \alpha \sqrt{\frac{2-\sqrt{2}}{2+\sqrt{2}}} \) 
how did we \( \text{change} \ \alpha \text{ to set here} \). 
\[ \alpha \sqrt{\frac{(2-\sqrt{2})(2+\sqrt{2})}{(2+\sqrt{2})^2}} \]

\[ = \alpha \cdot \frac{\sqrt{2}}{2+\sqrt{2}} \in \mathbb{Q}(\alpha) \]

\( \text{Numerator} \in \mathbb{Q} \)
\( \text{Denominator a square} \) \( \forall \beta \in \mathbb{Q}(\alpha) \)

Similarly \( \sqrt{3-\sqrt{2}} \):
\[ \sqrt{\frac{3-\sqrt{2}}{3+\sqrt{2}}} = \sqrt{\frac{(3-\sqrt{2})(3+\sqrt{2})}{(3+\sqrt{2})^2}} = \sqrt{\frac{9-2}{(3+\sqrt{2})^2}} \]
\[ = \frac{\sqrt{6}}{3+\sqrt{2}} \in \mathbb{Q}(\alpha^2) \]

\( \mathbb{Q}(\alpha) \) contains \( \pm \alpha, \pm \alpha \cdot 2+\sqrt{2}, \pm \alpha \cdot 3+\sqrt{2} \),
\[ \pm \alpha \cdot \frac{2+\sqrt{2}}{(2+\sqrt{2})(3+\sqrt{2})} \]

\( \text{i.e. the conjugates of } \alpha \)
\( \text{(can see all distinct; multiply by elements } \pm 1 \text{.)} \)

(b) Compute Galois gp, have three obvious subfields \( \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6}) \)
\( M_2, M_3, M_6 \)
so three obvious subgps \( H_i = \text{Gal}(\Omega(3)/M_i) \)

order 4. Show: 

\[
\begin{align*}
H_1 : & <i> \\
H_2 : & <j> \quad \text{s.t. } ij = k \\
H_3 : & <k>
\end{align*}
\]

one \( \Omega(3) \) conjugate an \( \pm \alpha, \pm \frac{\sqrt{6}}{3 + \sqrt{3}} \)

Can \( \sigma \in H_2 \) map \( \alpha \to -\alpha \), fix \( \alpha \frac{\sqrt{6}}{3 + \sqrt{3}} \)?

This would mean \( \sigma \left( \frac{\sqrt{6}}{3 + \sqrt{3}} \right) = -\frac{\sqrt{6}}{3 + \sqrt{3}} \)

but Galois orbit of \( \frac{\sqrt{6}}{3 + \sqrt{3}} \) is \( \frac{\pm \sqrt{6}}{3 + \sqrt{3}} \)

To get to \( -\frac{\sqrt{6}}{3 + \sqrt{3}} \) need to fix \( \sqrt{6} \)

But this can't happen if \( \sigma \) fixes \( \Omega(3) \)

So \( H_2 : \Omega(3) = \Omega(12, 3) \) 

\[
\begin{align*}
\sigma(\sqrt{2}) & \mapsto \sqrt{2} \\
\sigma(\sqrt{6}) & \mapsto \sqrt{6}
\end{align*}
\]

\( \sigma \)

(ie. \( H_2 \) has unique element of order 2, so \( H_2 \cong \text{C}_4 \))

Generator has \( \sigma(\alpha) = \pm \frac{\sqrt{6}}{3 + \sqrt{3}} \).
cycle 1's

To find a group study subgys to get subgys find sub fields \( \mathbb{A} \),
give access to subgys \( H = \text{Gal}(L/K) \)
& to home \( G \to \mathbb{A}/H = \text{Gal}(L/K) \)
if \( N \) is normal \( (K) \)

Fund thm of Algebra

\( \text{Calc b): if } f \in \mathbb{R}[x], \text{ has odd degree, then } f \text{ has a root.} \)

\( \Rightarrow \mathbb{R} \text{ has no extensions of odd degrees } > 1. \)

(If \( K/\mathbb{R} \) has odd degree \( n, \alpha \in K \), min poly \( f \) of \( \alpha \) has degree dividing \( n \), \( b \) is irreducible, so \( f \) has deg \( b, \alpha \in \mathbb{R} \).)
Let $K$ be a finite extension of $\mathbb{R}$
Let $N/\mathbb{R}$ be a normal closure, a
finite Galois extension, say $G = \text{Gal}(N/K)$
Let $P_2 \subseteq G$ be a 2-Sylow subgroup.
Let $L = \text{Fix}(P_2)$. Then $[L:R] = [G:P_2]$ is odd, so $L = \mathbb{R}$, by Galois Correspondence $P_2 = G$, so $[N:R]$ is a power of 2.

Claim: If $|G| = 2^m$ then $[N:R]$ is m successive quadratic extensions of $\mathbb{R}$.
For $p$-ary have subgroups of any order dividing their order.

But $C_2$ is unique quadratic extension of $\mathbb{R}$

([\mathbb{R}^x/(\mathbb{R}^x)^2] = C_2)$

and $C_2$ has no quadratic extensions

([C^x/(C^x)^2] = 2^2)$

So $N = \mathbb{R}$ or $N = C$. 
So only alg. extensions of $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}$.

If we allow non-commutative fields (division algebras),

then (Hurwitz) only real division algebras

over $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}, H = \text{Span}_\mathbb{R} \{1, i, j, k\}$

$$= \mathbb{R}[\mathbb{O}_8]/(i^2 = j^2 = k^2 = -1, ij, \text{etc.})$$