Infinite Algebraic Extensions:

Examples: $\mathbb{Q} : \mathbb{Q}, \mathbb{F}_p : \mathbb{F}_p$

Today: review "normal", "separable" extensions, talk about Galois groups.

Prop: Let $N/K$ be an algebraic extension. Then $N$ is normal (over $K$) if every irreducible $f \in K[x]$ having a root in $N$ splits there.

Proof: Let $a \in K$. Then there exists $N/L$ algebraic s.t. $N/K$ normal, no subextension is normal, and $N$ is unique up to isom.

Pf: Observe: if $M/K$ is any extension, $M$ is a set of all subfield of $N$ normal over $K$, then $N$ is also normal.
(reason: if \( f \in k[x] \) irreducible, \( \alpha \in \overline{F} \), then \( \alpha \in F \) for any \( F \in \mathcal{F} \), so all roots of \( f \) are in \( F \), so all roots of \( f \) are in \( \bigcap \mathcal{F} \))

So if \( \overline{L} \) is an algebraic closure of \( L \) (also of \( K \))

Let \( N = \bigcap \{ L \mid F \in \mathcal{F}, \overline{F} \text{ normal over } K \} \).

Clear, (1) \( N \) normal over \( K \).

(2) \( N \) minimal \( \mathcal{F} \)-such (contained in every normal field containing \( L \))

Uniqueness: let \( \overline{N}_2 \) be another extension normal over \( K \), \( N_2 \) subfields contain \( L \) normal over \( K \)

Let \( \overline{R} \) be an algebraic closure of \( \overline{N} \).

Both \( \overline{R}, \overline{L} \) are algebraic closures of \( L \).

By uniqueness of the alg. closure,
have an L-isom $\varphi : \bar{L} \to R$.

$\bar{N}$ is the smallest subfield of $R$ containing $L$, normal over $L$. (if there was a smaller one, we could intersect it with $\bar{N}$)

So $\varphi(N) = \bar{N}$. (N is some thing for $\bar{L}$, and $\varphi$ preserves $L$=$K$ elementwise)

Similar idea: let $L/K$ be algebraic, $N/K$ normal. Then $\text{Aut}_K(N)$ acts transitively on $\text{Hom}_K(L,N)$.

Pf: let $\bar{N}$ be an algebraic closure

let $\varphi_1, \varphi_2 : L \to \bar{N}$ be $K$-hom.

$\varphi_1 \circ \sigma \varphi_2 : L \to \bar{N}$ where $\sigma$ is the $\sigma$-inclusion.

$\tau : N \to \bar{N}$ inclusion.
Then \( \overline{\sigma_1}, \overline{\sigma_2} \) are algebraic closures of \( \overline{\sigma} \).
By uniqueness have isom \( \sigma \in \text{Aut}(\overline{\sigma}) \) s.t. 
\[ \overline{\sigma_1} = \sigma \circ \overline{\sigma_2}. \]

(1) \( \overline{\sigma_1} \mathcal{F}_K = \overline{\sigma_2} \mathcal{F}_K \) (there are \( K \)-home) so 
\[ \sigma \in \text{Aut}_K(\overline{\sigma}). \]

(2) \( \overline{\sigma_1} = N \): if \( \alpha \in N \), let \( f = \min_{\alpha \in \mathcal{F}} \# \alpha \overline{\mathcal{F}} \) 
over \( K \). Then \( f(\overline{\sigma(\alpha)}) = 0 \) \( \overline{\sigma}(f(\alpha)) = 0 \)
(\( \sigma \) is a \( K \)-aut.), and \( f \) splits in \( \overline{\sigma} N \), so \( \overline{\sigma} \mathcal{F}(N) \).
So \( \overline{\sigma_1} \mathcal{F}_N \in \text{Aut}_K(\overline{\sigma}) \) s.t. 
\[ \overline{\sigma_1} = \overline{\sigma} \mathcal{F}_N \circ \mathcal{F}_2. \]

**Remark** Can calculate in \( K \), restrict 

to normal extensions, use uniqueness of \( K \) 
to set automorphisms.

**2)** separability:
If \( L/K \) is an algebraic extension then TFAE:
1) \( L/K \) is separable
2) \( L = K(SL) \), \( S \subset L \) is a set of separable elements.
**pf:** Illustrate the "locally finite" point of view.

1. \( L = K(L) \).
2. \( 1 \Rightarrow 2 ; \) let \( \alpha \in L \), then \( \alpha \in K(S) \), so \( \alpha \) is an arithmetic expression involving elements of \( K, S \), so there is a finite subset \( T \subseteq S \) s.t. \( \alpha \in K(T) \).

Then \( [K(T) : K] < \infty \), and we have seen this makes \( K(T) : K \) separable (count \( \text{Hom}_K(K(T), K) \)).

So \( \alpha \in K(T) \) \( \Rightarrow \) \( \alpha \) is separable \( \langle K \rangle \).

---

**Recall**

**Def:** \( L/K \) is Galois if it's normal & separable.

**Examples:** \( \mathbb{Q} : \mathbb{Q} \), \( \mathbb{Q}(\sqrt{p}) : \mathbb{Q} \), \( \mathbb{Q}(\sqrt{m}) : \mathbb{Q} \), \( \mathbb{F}_p : \mathbb{F}_p \).

Why separable/normal: unions of such extensions + locally finite pov.

**Ex:** \( \mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{p}) \rightarrow \mathbb{Q}(\sqrt{p^2}) \rightarrow \mathbb{Q}(\sqrt{p^3}) \rightarrow ... \)

Let \( \alpha \in \mathbb{Q}(\sqrt{p^3}) \). Want to show \( \alpha \) is separable,
all roots of min poly of $f \in \mathcal{S}(x)$ are there. Well, have some $\alpha \in \mathcal{S}(f, x)$ then $\mathcal{S}(f, \alpha)$: it is separable \textit{if and only if}\[\text{char } \mathcal{S} = 0\]

$\Rightarrow$ all roots of $f$ are in $\mathcal{S}(f, \alpha) \Rightarrow$ in $\mathcal{S}(\mu_{p^n})$.

\underline{Non-example:} \[\overline{\mathbb{F}_p}(t) : \mathbb{F}_p(t)\]
not separable. (e.g. roots of $t^p - t$)
But: \[\{ \overline{\mathbb{F}_p}(t) \text{ sep } \} = \{ \text{ separable } / \mathbb{F}_p(t) \}\]
This is a subfield. (the subfield can, by this set is separable $\Rightarrow$ equal to the set)
Called separable closure of $\overline{\mathbb{F}_p}(t)$.

Must be normal: if $\alpha \in \overline{\mathbb{F}_p}(t)$ is separable, all roots of min poly of $\alpha$ are separable.
(separability is a property of the minimal poly)
(3) Galois theory

If $L/K$ is normal, separable, write $\text{Gal}(L/K) = \text{Aut}_K(L)$

Lemma: Let $\alpha \in L$. Then $L$ is a field $K \subset N \subset L$ s.t. $\alpha \in N$, $N/K$ finite, $N/K$ normal.

Pf: Take normal closure of $K(\alpha)$.

Lemma: Restriction hom $\text{Gal}(L/K) \rightarrow \text{Gal}(N/K)$ is surjective.

Pf: This was the claim before: different maps $N \cong N$ extend to $L$.

Cf. $\sigma \in \text{Aut}_K(N)$, have $\sigma \in \text{Aut}_K(L)$ st.

\[ \sigma = \mathcal{P} \circ \text{id}_N \]\n
(b. $\mathcal{P}$, $\text{id}_N$ are two embeddings $N \subset L$.)

Observe: Suppose that $\mathcal{P}(\alpha) \in \text{Gal}(L/K)$

Then have $\alpha$ s.t. $6(\alpha) \neq 7(\alpha)$,

then images of $\sigma; \mathcal{P}$ in finite quotient are different.
Question: Say \( N/k \) normal \& cN subfield, how can we have two embeddings \( L \) in \( N \)?

Example: \( N = \mathbb{Q} \), \( L = \mathbb{Q}(\sqrt{2}) \), \( \mathbb{Q}(i\sqrt{2}) \).

Have two embeddings of \( L \) in \( N \):

- \( \text{id}_L \) is an embedding.
- Let \( \sigma(a + b\sqrt{2}) = a - b\sqrt{2} \).
- Then \( \sigma : L \to L \) is also \( \sigma : L \to N \).

Similarly, 3 embeddings \( \mathbb{Q}(\sqrt{2}) \to N \):

Maps \( \sigma_j : \mathbb{Q}(\sqrt{2}) \to N \) s.t. \( \sigma_j(\sqrt{2}) = \sqrt{2}, w, w^3 = 1, j \text{ mod } 3 \).

Theorems: the partial maps \( \sigma_j : N \to N \) \( \sigma : L \to N \) extend to automorphisms.
$N/K$ normal $\theta(a, b, 1)$

We look at $\frac{1 + \sqrt{2}}{3 - \sqrt{3}} \in N$

want $G \cap \text{Aut}(N)$ s.t. $\theta(\sqrt{2}) = -\sqrt{2}$

but $\theta(\sqrt{3}) = \sqrt{3}$.

Result above: $\theta$ exists.

$\sqrt{\frac{1 + \sqrt{2}}{3 - \sqrt{3}}}$

Conjugate by $\sqrt{\frac{2 - \sqrt{2}}{2 + \sqrt{3}}}$

(take map $\sqrt{2} \to -\sqrt{2}$, extend arbitrarily)

might set $-\sqrt{\frac{2 - \sqrt{2}}{2 + \sqrt{3}}}$