Math 501, Lecture 8.

So far: looked at field extensions \( L/K \):
- classified elements as transcendental: \( K(\alpha) \neq K(\bar{\alpha}) \)
- or algebraic: \( K(\alpha) = K[\bar{\alpha}] \)

The algebraic elements of \( L \) form a subfield.
\( \alpha \) is algebraic if \( \deg \) of min poly is \( \leq N \).
(\( = \) every element of \( K(\bar{\alpha}) \) is algebraic over \( K \) if \( \alpha \) is)

Thus: \( [M:K] = [N:L][L:K] \)

\( \left( \frac{M}{L} \right) \) degrees multiply in towers.

---

Part 3: Galois Theory

Next step: look more carefully at the connection between extensions? \( \alpha \) polynomials which have roots in the extensions?

So far: if \( f \) is irreducible, \( K[\bar{x}]/(f) \) is an extension where \( f \) has a root.

Today: Splitting fields.
Motivation: we want all roots of \( f \), not just one.

Def: Let \( L/K \) be an extension of fields. Say \( f \in K[x] \) splits in \( L \) if there exist \( \alpha_i \in L \) such that
\[
f = a_0 \cdot \prod_{i=1}^d (x - \alpha_i).
\]
("all roots of \( f \) lie in \( L \)"")

Midterm: set at home either 3rd or 4th week of October.

---

Point 1: inside some "universal domain" (= algebraically closed field)
\( L \) contains all roots of \( f \).

Point 2: "roots of \( f \)" doesn't have an independent meaning.

Def: Say \( E/K \) is a splitting field for \( f \) if \( f \) splits in \( E \) but not in any subextension.

Example: \[
\int \frac{dx}{1+x^2} = \frac{1}{1+x^2} = \frac{1}{(x+i)/(x-i)} = \frac{1}{x+i} - \frac{1}{x+i} \frac{1}{2i}.
\]
\( \mathbb{C} / \mathbb{R} \) is the splitting field.

Thms: (1) For any \( f \in K[x] \), there is a splitting field \( E \) for \( f \), in fact one where \( [E : K] \leq (\deg f)! \).

(2) Splitting fields are unique up to isomorphism. "\( \Sigma \in \mathbb{E} \) the splitting field of \( f \)" determines \( \Sigma \).
**Proof:**

1. Observe: if \( f \) splits in \( L \) (roots \( \{ \alpha_1, \ldots, \alpha_n \} \))
   then \( \Sigma = \mathbb{E}(\alpha_1, \ldots, \alpha_n) \) is a splitting field. \( f \) splits there, and \( \Sigma \) is necessarily contained in every subfield of \( L \) where \( f \) splits.

   So enough to construct an extension, where \( f \) splits.

Now let’s prove the claim by induction on \( \deg f \).

If \( \deg f = 1 \), \( f \) splits in \( K \) (Nothing to do).

Otherwise, let \( g \in K[x] \) be a irreducible factor of \( f \),

Let \( M = K[x]/(g) = K(\alpha) \) where \( \alpha \) is a root of \( g \), hence \( \deg M = \deg g \leq \deg f \), all roots of \( f \) other than \( \alpha \) are roots of \( \frac{f}{x-\alpha} \in M[x] \). By induction, \( \frac{f}{x-\alpha} \) has a splitting field \( \Sigma \) s.t. \( [\Sigma : M] \leq (\deg \frac{f}{x-\alpha})! = (\deg f - 1)! \)

Now \( f \) splits in \( \Sigma \) since \( \alpha \in M \subseteq \Sigma \), so we have a splitting field with \( [\Sigma : K] = [\Sigma : M][M : K] < (\deg f)! \).

(2) Similar induction.

**Claim:** for any field \( K \), \( h \in K[x] \) of \( \deg n \), and any two splitting fields \( 2 : K \subseteq L \)

\( 2' : K \subseteq L' \)

there is an isomorphism of extensions \( \lambda: L \cong K \)

(i.e., \( \lambda \) is an isomorphism of fields and \( \lambda^n = 2' \))

the case \( n = 1 \) of the claim is clear (\( K \) is the only
splitting field, so $\beta, \beta'$ are isomorphic and so $L \cong K \cong L'$

Now let $f \in \mathbb{K}[x]$ have degree $n+1$. As before choose
irreducible factor $g \in \mathbb{K}[x]$ of $f$. Then $g$ has a root
in both $L, L'$, say $\alpha \in L, \alpha' \in L'$ are such roots:

Let $N = K(\alpha) \subset L, M' = K(\alpha') \subset L'$

\[
\begin{array}{c}
L' \\
\downarrow \quad \downarrow \\
L \\
\downarrow \\
M \\
\downarrow \\
K
\end{array}
\]

since both $M, M'$ are isomorphic to $K[\alpha]$ (or $K[\alpha']$), they
are isomorphic: have isomorphism $\mu : M \to M'$ respecting $K$, mapping
$\alpha \mapsto \alpha'$.

Also, $L/M$ is a splitting field for $f_{\alpha}$

(f splits in $L$; if $f \not\in \mathbb{K}$ split in a subextension containing
$M$, then $f$ would split there since $\alpha \in M$)

But $j_{\alpha}p : M \to L'$ is also a splitting field for $f_{\alpha}$

(apply same reasoning as $f_{\alpha'}$)

$\Rightarrow$ by induction (deg $\frac{f}{\alpha} = n$), have isomorphism $\lambda : L \to L'$

s.t.

\[
\begin{pmatrix}
L \\
\downarrow \quad \downarrow \\
L' \\
\downarrow \\
M \\
\downarrow \\
M' \\
\downarrow \\
K
\end{pmatrix}
\]

$\Rightarrow \lambda \circ j = j' \circ \mu$

$\Rightarrow \lambda \circ j = j' \circ \mu$

Example: Any quadratic extension (deg $L/K = 2$) is
a splitting field. Let $\alpha \in \mathbb{L}$, $K \subseteq \mathbb{L}$ so $[K(\alpha) : K] \leq 2$ so $[K(\alpha) : K] = 2$. $K(\alpha) = \mathbb{L}$, so min poly of $\alpha$ is quadratic, has one hence both roots in $\mathbb{L}$

But $\Omega(\sqrt{2})$ is not a splitting field of $x^2 - 2 \in \mathbb{Q}[x]$.

$$\sin \pi = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{2n+1}$$

Can't create a field of power series convergent in a disc even if $f$ has no poles in disc $\mathbb{D}$ can.

Can do: Look at field of meromorphic function on $\mathbb{C}$ for any $f \in \Omega$ have the "valuation ring" $R_f$ if $f$ doesn't have a pole.

Then $(1)$ for all $f \in \Omega$, at least one of $f$ is in $R_f$.

(2) have evaluation map $ev : R_f \to \mathbb{C}$

$$\cos \pi = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} \quad \text{invertible in } \mathbb{Q}(\pi+\pi)$$

because $\cos 0 \in \mathbb{Q}$

$$\Omega[\pi]/(\cos \pi) \cong \mathbb{R}(\pi)$$

$$\mathbb{Q}[\pi]/(\cos \pi) \cong \mathbb{R}(\pi)$$

$$\frac{f(x)}{(\cos \pi)} \in \mathbb{Q}[\pi]$$

$f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Z}$

Suppose $\frac{f}{x}$ not a root then $f(e^x) \in \frac{1}{e^2} \mathbb{Z}$

$|f(e^\frac{x}{2})| \geq \frac{1}{e^2}$
Suppose $f(x) : 0 \rightarrow \mathbb{R}$ and $rac{1}{2} \leq |f^{(n)}(x) - f^{(n)}(y)| = \frac{|x - y|}{n} \cdot f^{(n)}(y)$.

Thus it is fixed when $x, y$, $|x - y| > \frac{1}{2}$. 