Lecture 14: Splitting Fields II.

$K/F$ is a splitting field for $f(x) \in F[x]$ if

(a) $f$ splits completely in $K[x]$.
(b) $f$ does not split completely in $L$ with $F \subseteq L \subseteq K$.

Ex: $Q(3\sqrt{2}, \rho = -\frac{1}{2} + \frac{\sqrt{3}}{2} i)$ is the splitting field of $x^3 - 2$.

Thm: Let $f(x) \in F[x]$. Then $\exists$ an extension $K/F$

which is a splitting field of $f(x)$.

Proof: Induction on $\deg f$. Let $f_1$ be an irreducible factor of $f(x)$ in $F[x]$. Let $L = F[x]/(f_1(x)) = F(\theta)$. Then $f(\theta) = 0$, so $f(x) = (x - \theta)f_2(x)$ in $L[x]$.

By induction, $\exists K/L$ in which $f$ splits completely as $(x - \theta_1) \cdots (x - \theta_n)$. Then $F(\theta_1, \ldots, \theta_n)$ is the splitting field for $f$.

(Can't be any smaller since $K[x]$ is a U.F.D.)
Cor: If \( K \) is a splitting field for \( f(x) \in F[x] \), then \( [K:F] = (\text{deg} f) \).

For a random polynomial in \( \mathbb{Z}[x] \), \( [K:\mathbb{Q}] = n! \) with prob \( \to 1 \).

Ex: \( x^n - 1 \) in \( \mathbb{Q}[x] \) has splitting field \( \mathbb{Q}(S_n) \subset \mathbb{C} \) where \( S_n = e^{2\pi i/n} \)

\( 1, S_n, S_n^2, \ldots, S_n^{n-1} \)

are distinct roots of \( x^n - 1 \), hence

\[ x^n - 1 = (x - 1)(x - S_n)(x - S_n^2) \cdots (x - S_n^{n-1}) \]

So \( \mathbb{Q}(S_n) \) is the splitting field of \( x^n - 1 \). An cyclotomic field.

Central example: In 19th century, F.L.T. was "proved" using the false fact that \( \mathbb{Z}[S_n] \) is a U.F.D. (Which fails for \( \mathbb{Z}[S_{23}] \))

Lead to introduction of ideals.
\( R = \mathbb{Z}[-5] \) \( \setminus \) all ineducibles

\[ 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \]

**Goal:** Enlarge \( R \) to \( S \) where UFD returns

\( (\text{Compare } \mathbb{Z}[-3] \leq \mathbb{Z}[\sqrt[3]{3} = p]) \)

not a UFD \( \xrightarrow{\text{as a UFD}} \)

Q: \( s \in S \), consider all mult. of 5 which are in \( R \)

(i.e. \( (5) \cap R \))

Closed under +, mult of elt to
by anything in \( R \), i.e. an ideal.

\[ 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \]

\[ (p_1 p_2)(p_3 p_4) \quad (p_1 p_3)(p_2 p_4) \]

Then \( (p_1) \cap R \equiv (2, 1 + \sqrt{-5}) \), so take

\[ p_1 = (2, 1 + \sqrt{-5}) \quad p_2 = (2, 1 - \sqrt{-5}) \]

\[ p_3 = (3, 1 + \sqrt{-5}) \quad p_4 = (3, 1 - \sqrt{-5}) \]

\( \{ \text{all prime ideals} \} \)

\( (6) = p_1 p_2 p_3 p_4 \) as ideals, and this factorization is unique.

Same true for e.g. ideals in \( \mathbb{Z}[\sqrt[3]{5}] \).
Back to fields: What is $[Q(\mathbb{S}_n) : Q] =$ ?

Case $n = p$ a prime. Then

$$x^{p-1} = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$$

$\Phi(x)$ cyclotomic polynomial

$\Phi$ is irreducible, by the following trick:

$$\overline{\Phi(x+1)} = \frac{(x+1)^{p-1} - 1}{x} = x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)x}{2} + p$$

irred. by Eisenstein.

Thm: Suppose $K, K'$ are splitting fields for

$f(x) \in F(x)$. Then $\exists$ a isom $\psi: K \rightarrow K'$

with $\psi|_F = id|_F$.

Pf: See text, think $K(x) \cong F[x]/m_{F, \alpha(x)}$.

Next, alg. closed fields
Problem 5 from the MT:

\[ K/F \text{ ext. of fields, } \alpha \in K. \{e_1, \ldots, e_n\} \text{ a } F\text{-basis of } K. \]

\[ T_\alpha : K \rightarrow K \text{ an } F\text{-linear trans.} \]

\[ \beta \rightarrow \alpha \cdot \beta \]

\[ A_\alpha \in M_n(F) \text{ matrix of } T_\alpha \text{ in } \{e_1, \ldots, e_n\}. \]

\[ \Phi : K \rightarrow M_n(F) \text{ a homomorphism of rings.} \]

\[ \alpha \mapsto A_\alpha \]

**Note:** If \( f \in F \) then \( \Phi(f) = (f f.0) \). As \( K \) is a field, this means \( \Phi \) is 1-1.

**But note:** If \( \alpha \in K \setminus F \) then \( \Phi(\alpha) \neq (\alpha \ 0 \ 0) \).

Let \( p(x) = \det(xI - A) \) be the char poly of \( A \).

By Cayley-Hamilton, \( p(A) = 0 \). Now

\[ \Phi(p(\alpha)) = \Phi(\alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0) \]

\[ = \Phi(\alpha)^n + \Phi(a_{n-1}) \Phi(\alpha)^{n-1} + \cdots + \Phi(a_1) \Phi(\alpha) + \Phi(a_0) \]

\[ \in \text{im } F \]

\[ = A^n + a_{n-1} A^{n-1} + \cdots + a_0 I = p(A) = 0 \]

As \( \Phi \) is 1-1, must have \( p(\alpha) = 0 \).