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 $F \subseteq L \subsetneq K$.

Ex: $\mathbb{Q}(\sqrt[3]{2}, \rho = -\frac{1}{2} + \frac{\sqrt{3}}{2}i)$ 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: Induct on $\deg f$. Let f_1 be an irred. 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.

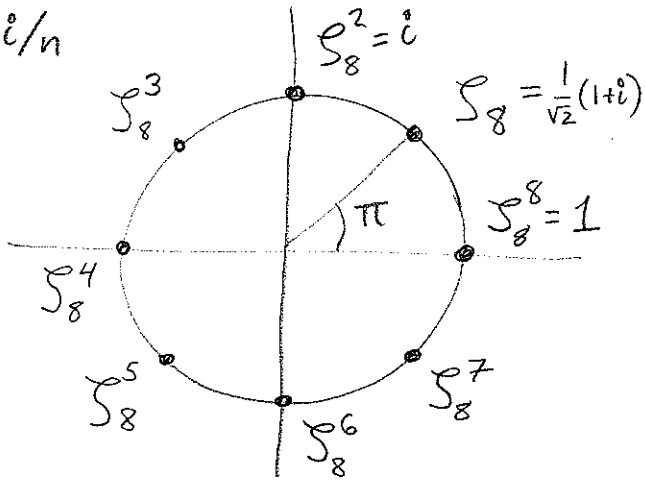
(Can't be any smaller since $K[x]$ is a U.F.D.)

Cor: If K is a splitting field for $f(x) \in F[x]$, then $[K:F] \leq (\deg f)!$

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

$\mathbb{Q}(\zeta_n) \subseteq \mathbb{C}$ where $\zeta_n = e^{2\pi i/n}$



$1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$

are distinct roots of $x^n - 1$,

hence

$$x^n - 1 = (x-1)(x-\zeta_n)(x-\zeta_n^2)\cdots(x-\zeta_n^{n-1})$$

So $\mathbb{Q}(\zeta_n)$ is the splitting fields.
↑ Cyclotomic field.

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

Lead to introduction of ideals

$R = \mathbb{Z}[\sqrt{-5}]$ ← all irreducibles ↓

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

Goal: Enlarge R to S where UFD returns

(Compare $\underbrace{\mathbb{Z}[\sqrt{-3}]}_{\text{not a UFD}} \subseteq \underbrace{\mathbb{Z}[\zeta_3 = \rho]}_{\text{is a UFD}}$)

Q: $s \in S$, consider all mult. of s which are in R (i.e. $(s) \cap R$)

closed under $+$, mult of elts by anything in R, i.e. an ideal.

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

$$(P_1P_2)(P_3P_4) \quad (P_1P_3)(P_2P_4)$$

Then $(P_1) \cap R \supseteq (2, 1+\sqrt{-5})$, so take

$P_1 = (2, 1+\sqrt{-5})$ $P_2 = (2, 1-\sqrt{-5})$

$P_3 = (3, 1+\sqrt{-5})$ $P_4 = (3, 1-\sqrt{-5})$

} all prime ideals.

$(6) = P_1P_2P_3P_4$ as ideals, and this factorization is unique.

Same true for e.g. ideals in $\mathbb{Z}[\zeta_n]$.

Back to fields: What is $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = ?$

Case $n = p$ a prime. Then

$$x^p - 1 = (x-1)\underbrace{(x^{p-1} + x^{p-2} + \cdots + x + 1)}_{\Phi(x)\text{ cyclotomic polynomial}}$$

Φ is ined. by the following trick:

$$\Phi(x+1) = \frac{(x+1)^p - 1}{x} = \underbrace{x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)}{2}x + p}_{\text{ined. by Eisenstein.}}$$

Thm: Suppose K, K' are splitting fields for $f(x) \in F(x)$. Then $\exists$ a isom $\psi: K \to K'$ with $\psi|_F = id|_F$.

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

Next, alg. closed fields

Problem 5 from the MT:

K/F ext. of fields, $\alpha \in K$. $\{e_1, \dots, e_n\}$ a F-basis of K.

$T_\alpha : K \to K$ an F-linear trans.
$\beta \longmapsto \alpha \cdot \beta$

$A_\alpha \in M_n(F)$ matrix of T_α in $\{e_1, \dots, e_n\}$.

$\underline{\Phi} : K \to M_n(F)$ a homomorphism of rings.
$\alpha \longmapsto A_\alpha$

Note: If $f \in F$ then $\underline{\Phi}(f) = \begin{pmatrix} f & & 0 \\ & f & \\ 0 & & f \end{pmatrix}$. As K is a field, this means $\underline{\Phi}$ is 1-1.

But not: If $\alpha \in K \setminus F$ then $\underline{\Phi}(\alpha) \neq \begin{pmatrix} \alpha & & 0 \\ & \alpha & \\ 0 & & \alpha \end{pmatrix}$.

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

By Caley-Hamilton, $p(A) = 0$. Now

$$\underline{\Phi}(p(\alpha)) = \underline{\Phi}(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \quad (a_i \text{ in } F)$$

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

($\underline{\Phi}(a_i)$ as in F)

$$= A^n + a_{n-1}A^{n-1} + \cdots + a_0 \cdot I = p(A) = 0.$$

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