Previously

$\mathbb{F}$ a field, $\phi(x) \in \mathbb{F}[x]$ prime poly.

"$\mathbb{Z}/n\mathbb{Z}$"

$\mathbb{F} \subseteq \mathbb{k}$

$$\mathbb{k} = \mathbb{F}[x]/(\phi)$$

$$= \left\{ r(x) = a_k x^k + \dots + a_1 x + a_0 \;\middle|\; a_0, \dots, a_k \in \mathbb{F},\ k < n \right\}$$

$r_k X^k +$

$\mathbb{k}$ is a field w/ mod-ϕ arithmetic.

$\alpha = \pi(x)$

Denote $\pi : \mathbb{F}[x] \to \mathbb{k} = \mathbb{F}[x]/(\phi)$

$$\pi(f(x)) = f(x) \pmod{\phi(x)}$$

and $\alpha := \pi(x)$

for $\phi(X) \in \Bbbk[X]$,

$$\phi(\alpha) = \phi(\pi(x)) = \phi(x) \bmod \phi$$

$$= 0$$

$$\Rightarrow \quad \phi(X) = (X-\alpha)\cdot\psi(X)$$

Suppose $F(\alpha)$ is a min. field

s.th: $\begin{cases} 1) & F \subseteq F(\alpha) \\ 2) & \alpha \in F(\alpha) \end{cases}$

If $f(x) \in F[x]$, then

$$f(\alpha) \in F(\alpha).$$

Also, $\alpha^{-1} \in F(\alpha)$ so for

any $0 \neq g(x) \in F[x]$,

$$\frac{1}{g(\alpha)} \in \mathbb{F}(\alpha)$$

Thus, $\forall f, g \in \mathbb{F}[x]$, w/ $g(x) \neq 0$

$$\frac{f(\alpha)}{g(\alpha)} \in \mathbb{F}(\alpha)$$

$$=$$

ie

$$\mathbb{F}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; \begin{array}{l} f, g \in \mathbb{F}[x] \\ g \neq 0 \end{array} \right\}$$

$$\left(\frac{f(\alpha)}{g(\alpha)} \right)^{-1} = \frac{g(\alpha)}{f(\alpha)}$$

Write $f(x) = \phi(x)\, q_1(x) + r_1(x)$

$$g(x) = \phi(x)\, q_2(x) + r_2(x)$$

for q_1, q_2, r_1, r_2

(w/ $\deg r_1$, $\deg r_2 < \deg \phi$)

$$\Rightarrow \quad f(\alpha) = r_1(\alpha)$$

$$g(\alpha) = r_2(\alpha)$$

$$\Rightarrow \quad \frac{f(\alpha)}{g(\alpha)} = \frac{r_1(\alpha)}{r_2(\alpha)}$$

$$= r_1(\alpha) \cdot r_2(\alpha)^{-1} \in \mathbb{F}(\alpha)$$

Prop: $\mathbb{K} = \mathbb{F}[x]/(\phi) = \mathbb{F}(\alpha)$

Proof: $\mathbb{F}(\alpha)$ is the min. field containing $\mathbb{F}$ and α so $\mathbb{F}(\alpha) \subseteq \mathbb{K}$. Conversely,

$$\mathbb{K} \subseteq \mathbb{F}(\alpha)$$

$r(x)$ $\quad$ $r(\alpha)$ $\quad$ $\Rightarrow k = F(\alpha)$.

$\overline{1}$ //

Def: Let F be a field and $f(x) \in F[x]$. A splitting field for f over F is a field $F \subseteq E$ s.th:

1) f splits to linear factors over E ie

$$f(x) = \lambda (x-\alpha_1) \cdot \ldots \cdot (x-\alpha_n)$$

$\lambda, \alpha_1, \ldots, \alpha_n \in E$

2) E is minimal w/ this property, ie for any field $F \subseteq k \subseteq E$ s.th f splits over k

we must have $\mathbb{K} = \mathbb{F}$

Examples

1) $\mathbb{C}$ is a splitting field of $x^2+1 \in \mathbb{R}[x]$:

a) $x^2+1 = (x-i)(x+i)$
$\in \mathbb{C}[x]$

b) If $\mathbb{R} \subseteq \mathbb{K}$ and x^2+1 splits over $\mathbb{K}$ then $i \in \mathbb{K}$ and any field containing $\mathbb{R}$ and i must contain $\mathbb{C}$
$= \{ a+bi \mid a, b \in \mathbb{R} \}$

Note: $\mathbb{C} = \mathbb{R}(i)$

2) Take $\mathbb{k} = \{a+bi \mid a,b \in \mathbb{Q}\}$

Then $\mathbb{k}$ is a splitting field of $x^2+1 \in \mathbb{Q}[x]$

($\mathbb{F} = \mathbb{Q}$ $x^2+1 \in \mathbb{Q}[x]$)

and $\mathbb{k} = \mathbb{Q}(i)$

Thus

splitting field of $x^2+1 \in \mathbb{Q}[x]$ $= \mathbb{Q}(i) = \mathbb{Q}[x]/(x^2+1)$

Term: Field extension $\hookrightarrow$ subfield inclusion

$\mathbb{F} \subseteq \mathbb{k}$

Proposition: For any $f(x) \in \mathbb{F}[x]$ there exists a splitting field

of f over $\mathbb{F}$.

Proof: Wlog f is monic.

Write $f(x) = f_1(x) \cdot \ldots \cdot f_k(x)$

where $f_1, \ldots, f_k$ are prime over $\mathbb{F}[x]$.

Consider $\mathbb{K}_1 = \mathbb{F}[x]/(f_1)$.

Then f_1 has a root α_1 in $\mathbb{K}_1$ so

$$f_1(x) = (x - \alpha) f_1'(x)$$

in $\mathbb{K}_1[x]$.

$\Rightarrow \mathbb{K}_1 = \mathbb{F}(\alpha_1)$.

Now if $f_1'(x)$ doesn't split over $\mathbb{K}_1$

Say $f_1(x) = \varphi_1(x) \cdots \varphi_s(x)$

w/ $\varphi_1, \ldots, \varphi_s$ prime

poly's over k_1,

take $k_2 = k_1/(\varphi_1)$.

Then $k_2 = k_1(\alpha_1)$

where α_1 is a root

of φ_1.

Repeat this process.

Since f can have

only finitely many roots

we terminate at some

k_ℓ in which f

splits. We get a sequence of field inclusions

$$\mathbb{F} \subseteq \mathbb{k}_1 \subseteq \cdots \subseteq \mathbb{k}_2 = \mathbb{k}$$

and each $\mathbb{k}_{i+1}$ is the minimal field containing $\mathbb{k}_i$ and some root α_{i+1} of f. Thus $\mathbb{k}$ is the minimal field containing $\mathbb{F}$ and all roots of $f(x)$ ie $\mathbb{k}$ is a splitting field for f over $\mathbb{F}$. //

Theorem: Let $\rho: F \to F'$ is a field iso, and let

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

$$f'(x) = \rho(a_n) x^n + \cdots + \rho(a_1) x + \rho(a_0)$$

w/ $f \in F[x]$, $f' \in F'[x]$.

Let E be a splitting field of f over F and E' a splitting field of f' over F'.

Then there exist a field iso

$$\sigma: E \to E' \quad \text{s.t.h} \quad \sigma|_F = \rho.$$

Proof: By induction on $\deg f = n$.

Denote $\rho : F[x] \to F[x]$

$$\rho\left(\sum_i a_i x^i\right) = \sum_i \rho(a_i) x^i$$

ie $\rho(f) = f'$.

Observe

a) ρ is a ring iso

b) If $p(x)$ is a prime factor of $f(x)$ (in $F[x]$)

then $\rho(p(x))$ is a prime factor of $\rho(f(x)) = f'(x)$.

If $f(x) = p(x) \cdot q(x)$, then

$$f'(x) = \rho(f(x)) = \rho(p(x) \cdot q(x))$$

$$= \rho(p(x)) \cdot \rho(q(x))$$

$= p(p(x)) \cdot p(\quad)$

$\Rightarrow$ $p(p(x))$ is a factor of $f'(x) = p(f(x))$.

If $p(p(x)) = a(x) \cdot b(x)$

w/ $\deg a, \deg b \geq 1$,

$a, b \in F[x]$

and then $p(x) = \bar{p}^{-1}(p(p(x)))$

$= \bar{p}^{-1}(a(x)) \cdot \bar{p}^{-1}(b(x))$

and $\deg \bar{p}^{-1}(a)$, $\deg \bar{p}^{-1}(b) \geq 1$

Which cannot happen since $p(x)$ is prime in $F[x]$.

Suppose first that f splits

Suppose [illegible]
(to linear factors) over F.

Then $E = F$ is a splitting field of f, and $E' = F'$ is a splitting field of f'.

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E' \\ \| & & \| \\ F & \xrightarrow{\rho} & F' \end{array}$$

set $\sigma = \rho$.

otherwise, let $p(x)$ be a prime factor of $f(x)$ w/ $\deg p > 1$.

Let $F_1 = F[x]/(p)$.

Since $\rho(p(x))$ is prime in $F'[x]$, we also have a field

$$F_1' = F'[x]/$$

$\mathbb{F}_1 \quad = \qquad \nearrow \quad /(\rho(p))$

Note that we have a field iso

$$\rho_1 : \mathbb{F}_1 \longrightarrow \mathbb{F}' : \qquad (\rho_1' : \mathbb{F}' \to \mathbb{F}_1)$$

for $r, s \in \mathbb{F}_1 = \mathbb{F}[x]/_{(p)}$

$$\rho(r+s) = \rho(r) + \rho(s), \text{ etc.}$$

Since $p(x)$ has a root in $\mathbb{F}_1$,

$$\underline{\underline{p(x) = (x-a) \cdot p_1(x)}}$$

for $a \in \mathbb{F}_1$.

Then

$$\rho(p(x)) = \rho(x-a) \cdot \rho(p_1(x))$$
$$= (x - \rho(a)) \cdot \rho(p_1(x))$$

So $\rho(a)$ is a root of

$g(p(x))$. F_1

Thus $\underline{f(x) = (x-a)\cdot f_1(x)}$

$$f'(x) = (x - g(a)) \cdot f_1'(x)$$

where

$$f_1'(x) = g(f_1(x)).$$

with $\begin{pmatrix} \deg f_1 < \deg f \\ \deg f_1' < \deg f' \end{pmatrix}$

Let E_1, E_1' be splitting field of f_1, f_1' (resp.) over F_1, F_1' resp.

By induction $\exists$ iso

$$\begin{array}{ccc} E_1 & \xrightarrow{\sigma} & E_1' \\ \cup & & \cup \\ F_1 & \xrightarrow{} & F_1' \end{array}$$

$\cup_1$

$F \xrightarrow{f} F'$

We claim that E_1 is a splitting field for f over F:

- clearly f splits to linear factors over E_1
- $F \subseteq F_1 = F[x]/(p) = F(a) \subseteq E_1$

so E_1 is the minimal field in which f splits.

Similarly, E_1' is a

splitting field of f over F'.

So

$$\begin{array}{ccc} E_1 & \xrightarrow{\sigma}_{\cong} & E_1' \\ f & & f' \\ \cup & & \cup \\ F & \xrightarrow[\rho]{\cong} & F \end{array}$$

as desired. //

Corollary: A splitting field for f over F is unique up to iso.

Proof: Take $\rho = id : F \to F$.

$$\rho(f) = f$$

$$
\begin{array}{ccc}
E & \rightharpoonup & E \\
\cup & & \cup \\
F & \xrightarrow{\varphi} & F
\end{array}
$$