Field Theory (Before FTGT)

1°. Characteristic. prime field.

If we define $\underbrace{1+1+\cdots+1}_{n,\ 1\in F} = n\cdot 1_F$ and $0\cdot 1_F = 0$

then we have a natural ring homomorphism :

$$\varphi : \mathbb{Z} \longrightarrow F$$
$$n \longmapsto n\cdot 1_F$$

then we have $\mathbb{Z}/\ker\varphi \hookrightarrow F$

and we know that truth $\ker\varphi = ch(F)\mathbb{Z}$

so $\ker\mathbb{Z} = 0$ or $p\mathbb{Z}$, $chF = 0$ or p

$\Rightarrow$ take the fraction field of $im(\mathbb{Z}/\ker\varphi)$

is a subfield of F. which is the prime field of F.

2°. Extensio thm (extend of iso.)

<u>Thm</u>. Let $\varphi : F \xrightarrow{\sim} F'$ be an iso of fields.

$p(x)\in F[x]$ be irre. poly. $p'(x)\in F'[x]$ be the imaga

under the induced ring isomorphism

$$\tilde{\varphi}\quad F[x] \xrightarrow{\sim} F'[x]$$
$$p(x) \longmapsto p'(x)$$

Let α be a root of $p(x)$, β be a root of $p'(x)$ in some

extension of F and F' respectively

then we extend φ to isomorphism σ :

$$\begin{tikzcd} \sigma: & F(\alpha) \arrow[r, "\sim"] & F'(\beta) \\ \varphi: & F \arrow[u, dash] \arrow[r, "\sim"] & F' \arrow[u, dash] \end{tikzcd}$$

s.t. $\sigma: F(\alpha) \xrightarrow{\sim} F'(\beta)$, $\alpha \longmapsto \beta$

and $\sigma|_F = \varphi$

proof:

$$\begin{tikzcd} F(\alpha) \arrow[r, "\sim"] & \check{\varphi}: & F[x]/(p(x)) \arrow[r, "\sim"] & F'[x]/(p'(x)) \arrow[r, "\sim"] & F'(\beta) \\ \alpha & & x \arrow[ll, mapsto] & & x \mapsto \beta \\ & \tilde{\varphi}: & F[x] \arrow[uu, dash] \arrow[r, "\sim"] & F'[x] \arrow[uu, dash] & \\ & \varphi: & F \arrow[u, dash] \arrow[r, "\sim"] & F' \arrow[u, dash] & \end{tikzcd}$$

iso. by $\alpha \mapsto \beta$.

and $F \xrightarrow{\sim} F'$

3°. splitting field. Existence and Uniqueness.

Thm. (Existence) for any field F, $f(x) \in F[x]$. $\exists$ splitting field K.

Use induction on the degree n of $f(x)$.

If $n=1$ then take $E=F$

Spse $n>1$

1°. If the irreducible factors of f over F are all linear

then take $E=F$

2° Hence, set at least one of those irreducible factors

of $f(x)$ in $F[x]$ is of degree at least 2. denoted by $p(x)$

take $E_1 = F(\alpha) \cong F[x]/(p(x))$

over E_1, $f(x)$ has linear factor $x-\alpha$

then $f(x) = (x-\alpha) f_1(x)$ over E_1 where $\deg f_1(x) = n-1$

By induction $\exists$ splitting field E of $f(x)$ over E_1

Since $\alpha \in E_1 \subset E$, E is an extension of F containing all the roots of $f(x)$.

3°. Let K be intersection of all subfield of E containing F which also contain all the roots of $f(x)$. Then K is the splitting field of $f(x)$ over F

Thm (Uniqueness)

Let $\varphi : F \xrightarrow{\sim} F'$ be iso of fields.

$f(x) \in F[x]$, $f'(x) \in F'[x]$, $f'(x)$ is the image of $f(x)$ under

$$\tilde{\varphi} : F[x] \xrightarrow{\sim} F'[x]$$

Let E be a splitting field for $f(x)$ over F

E' be a splitting field for $f'(x)$ over F'

Then the iso φ extends to an iso σ $E \xrightarrow{\sim} E'$

also induction on the $\deg f = n$.

1° If $f(x)$ has all its roots in F the $f(x)$ splits in $F[x]$

also $f'(x)$ splits in $F'[x]$

Hence, $E = F$ and $E' = F'$, take $\sigma = \varphi$

this is also the case for $n=1$.

2°. Assume for all field F. iso φ. poly. $f \in F[x]$ with $\deg < n$, proved.

Now let $p(x)$ be an irr. factor of f in $F[x]$ of degree at least 2 and $p'(x)$ be the image $\tilde{\varphi}(p(x))$ so its the corresponding irr. factor of $f'(x)$ in $F'[x]$

If α is a root of $p(x)$ and β is .... $p'(x)$.

then we have extending iso:

$$\begin{tikzcd} \sigma' : F(\alpha) \arrow[r, "\sim"] & F'(\beta) \\ \varphi : F \arrow[u, dash] \arrow[r, "\sim"] & F' \arrow[u, dash] \end{tikzcd}$$

Let $F_1 = F(\alpha)$, $F_1' = F'(\beta)$, $\sigma' : F_1 \xrightarrow{\sim} F_1'$

and $f(x) = (x-\alpha) f_1(x)$ over F_1

$f'(x) = (x-\beta) f_1'(x)$ over F_1'

$\deg f_1 = \deg f_1' = n-1$

Let E. E' be splitting field of $f_1(x)$ over F_1
$f_1'(x)$ over F_1'

by induction.

$$\begin{tikzcd} \sigma : E \arrow[r, "\sim"] & E' \\ \sigma' : F_1 \arrow[u, dash] \arrow[r, "\sim"] & F_1' \arrow[u, dash] \end{tikzcd}$$

, done.

$\sigma \quad E_1 \xrightarrow{\sim} E_1' \quad , \sigma|_F = \varphi$

$\boxed{\text{E.g.}}$ $x^n - 1$ cyclotomic fields. (over $\mathbb{Q}$)

roots of this poly is called n^{th} roots of unity.

over $\mathbb{C}$ we have n distinct root.

$$e^{\frac{2\pi i k}{n}} = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}.$$

this n roots form a $\underline{\text{cyclic group}}$

the generator of this is called a primitive n^{th} root of unity

if ζ_n is primitive, $(a, n) = 1$

i.e. ζ_n^a $1 \le a < n$ is also a primitive root.

there are precisely $\varphi(n)$ primitive n^{th} roots

The field $\mathbb{Q}(\zeta_n)$ is called the cyclotomic field of n^{th} roots of unity

E.g. if p prime.

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

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = \downarrow \quad \text{is irr.}$$

so $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

generalize it.

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ 1 \le d < n}} \Phi_d(x)}$$

$\zeta_i \in \Theta_n$

all n^{th} primitive root.

or equivalently. $x^n - 1 = \prod_{\substack{d \mid n \\ 1 \le d \le n}} \Phi_d(x)$

or $\Phi_n(x) = \prod_{\substack{1 \le a \le n \\ (a,n)=1}} (x - \zeta_n^a)$, $\zeta_n = e^{\frac{2\pi i}{n}}$.

or $\Phi_n(x) = \prod_{\zeta_i \text{ is a primitive } n\text{th root}} (x - \zeta_i)$.

$\Phi_1 = x - 1$

$\Phi_2 = x + 1$

$\Phi_3 = x^2 + x + 1$ $\quad \Phi_3 \Phi_1 = x^3 - 1$

$x^4 - 1 = \Phi_1 \Phi_2 \Phi_4$

$\Phi_4 = x^2 + 1$.

$\vdots$

property:

1°. $\Phi_n(x)$ is monic. integer coefficient.

By induction. $n=1$ $\Phi_1(x) = x - 1$ ✓

sps. $k < n$. $\Phi_k(x)$ monic. integer coefficient.

then for n. $\prod_{d \mid n, 1 \le d < n} \Phi_d(x)$ is monic. integer coefficient.

$x^n - 1 = \Phi_n(x) \cdot g(x)$ so $\Phi_n(x)$ monic. ✓

prop2. $\Phi_n(x)$ is irr. in $\mathbb{Q}[x]$.

Sps $\Phi_n(x) = gh$. $g, h \in \mathbb{Z}[x]$, monic $\deg g \geq 1$

g irr.

claim. if $g(\zeta)=0$, p prime $p \nmid n$ then ζ^p is a root of g.

if not. $\Phi_n(\zeta^p)=0$ (since $\Phi_n(\zeta)=0$ and $(n,p)=1$)

So $h(\zeta^p)=0$.

$\Rightarrow$ $x=\zeta$ is common root of $g(x)$ and $h(x^p)$

Consider. $\bar{\ }: \mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$

$f(x) \longmapsto \bar{f}(x)$

then $\bar{g}$ and $\bar{h}(x^p)$ has common root in $\bar{\mathbb{F}}_p$

But $\bar{h}(x^p) = (\overline{h(x)})^p$

$\Rightarrow$ $\bar{g}$, $\bar{h}$ has common root in $\bar{\mathbb{F}}_p$.

But $\bar{\Phi}_n \mid x^n-1$

and $(x^n-1, nx^{n-1})=1$ $\Rightarrow$ x^n-1 no repeat root. $\lightning$.

By our claim. if $\zeta^i \in \mathcal{O}_n$ then $(i,n)=1$.

let $i=p_1 \cdots p_t$, then $p_j \nmid n$ $\forall j$.

then ζ^i is $g(x)$ root $\Rightarrow$ $g(x) = \Phi_n(x)$.

Cor. $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$

$\boxed{\text{E.g}}$ Splitting field of x^p-2. p prime.

take $x^p-2=0$ one root is $\zeta_p \cdot \sqrt[p]{2}$ Let E denotes the field

1°. $E \subset \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$

$\Rightarrow [E:\mathbb{Q}] \le p(p-1)$

2°. $[E:\mathbb{Q}] = [E:\mathbb{Q}(\sqrt[p]{2})]\underbrace{[\mathbb{Q}(\sqrt[p]{2}):\mathbb{Q}]}_{p}$

$[E:\mathbb{Q}] = [E:\mathbb{Q}(\zeta_p)]\underbrace{[\mathbb{Q}(\zeta_p):\mathbb{Q}]}_{p-1}$

$(p, p-1) = 1$.

$\Rightarrow [E:\mathbb{Q}] = p(p-1) \Rightarrow E = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[p]{2}, \zeta_p) & \\
\mathbb{Q}(\zeta_p) \arrow[ur, dash, "\mathbb{Z}_p \quad p"] & & \mathbb{Q}(\sqrt[p]{2}) \arrow[ul, dash, "p-1"'] \\
 & \mathbb{Q} \arrow[ul, dash, "\mathbb{Z}_{p-1} \quad p-1"] \arrow[ur, dash, "p"'] &
\end{tikzcd}$$

4. Separable. inseparable.

Important Thm: A polynomial $f(x)$ has a multiple root α if and only if α is also a root of $f'(x)$.

($\Rightarrow$) sps α is multiple root of $f(x)$.

Then over a splitting field.

$$f(x) = (x-\alpha)^n g(x)$$

$$f'(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n g'(x)$$

($\Leftarrow$). sps α is common root.

$$f(x) = (x-\alpha) h(x)$$

$$f'(x) = h(x) + (x-\alpha) h'(x) \quad \text{since } f'(\alpha)=0 \text{ by}$$

it shows $h(\alpha)=0 \Rightarrow f'(\alpha)=0$

Cor. Every irred. poly. over a field of char 0 is separable

Prop. Every irred. poly over a fin field F is separable.

Def. The field K is said to be separable over F if every element of K is the root of a separable poly over F.

Cor. fin extension of fin field or char 0 field is separable.