**Note**: The main thm work in char p if we insist on separable.

**Say**, $q = p^r$ Then $\mathbb{F}_q / \mathbb{F}_p$ is galois.

**Define**, $\varphi : \mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto x^p$ } this is a field automorphism.

↳ also in $\in Gal(\mathbb{F}_q / \mathbb{F}_p)$

We know, $x^q = x$ holds $\forall x \in \mathbb{F}_q$

$\Rightarrow \varphi^r = 1$ in $Gal(\mathbb{F}_q / \mathbb{F}_p)$ $\quad \varphi^k = \overbrace{\varphi \circ \cdots \circ \varphi}^{k} : x \to x^{p^k}$

we can't have $\varphi^k \equiv 1$ for $k < r$ b/c $x^{p^k} = x$ $\forall x \in \mathbb{F}_q$

↳ but this only has $\leq k$ roots

$\therefore \varphi$ has order $r$

On the other hand $[\mathbb{F}_q : \mathbb{F}_p] = r \Rightarrow \#Gal(\mathbb{F}_q / \mathbb{F}_p) \leq r$

$\Rightarrow$ $Gal(\mathbb{F}_q / \mathbb{F}_p)$ is cyclic, gen'd by $\varphi$.

Subgps of $\to$ corr to divisors of $r$.

if $d \mid r$ then assoc subgp is $\varphi^d$

$\overset{\text{main thm}}{\Longrightarrow}$ subfields of $\mathbb{F}_q$ corr to divisors of $r$

($d \leftrightarrow$ fixed field of $\varphi^d \cong \mathbb{F}_{p^d}$)

**Note**: $\langle \varphi \rangle$ is ab $\leftrightarrow$ all subgps are normal

So, all extn of finite fields are galois.

---

**F char 0**, $\zeta$ - $p^n$ root of unity ($p$ prime)

**Cl.1** $F(\zeta)$ is a Gal extn of $F$.

**Pf** $F(\zeta)$ is the splitting field of $x^p - 1$

$$x^p - 1 = \prod_{a \in \mathbb{F}_p} (x - \zeta^a), \quad \zeta^a \in F(\zeta)$$

→

We define $\chi : Gal(F(\zeta)/F) \longrightarrow \mathbb{F}_p^\times$

as follows, say $\sigma \in Gal(F(\zeta)/F)$

$\sigma(\zeta)$ is prim $p^{th}$ root of 1,

$\Rightarrow \sigma(\zeta) = \zeta^a$, $a \in \mathbb{F}_p$

def, $\chi(\sigma) = a$

**Claim** Defn of $\chi$ ind of choice of $\zeta$?

Say $\omega$ is a second prim $p^{th}$ root of 1

$\Rightarrow \omega = \zeta^b$ for some $b \in \mathbb{F}_p^\times$

$\Rightarrow \sigma(\omega) = \sigma(\zeta)^b = (\zeta^a)^b = (\zeta^b)^a = \omega^a$

**Claim** $\chi$ grp homo,

Say $\sigma, \tau \in Gal(F(\zeta)/F)$

$\zeta^{\chi(\sigma\tau)} = \sigma\tau(\zeta) = \sigma(\zeta^{\chi(\tau)}) = \sigma(\zeta)^{\chi(\tau)}$

$\Rightarrow \chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$. $= \zeta^{\chi(\sigma)\cdot\chi(\tau)}$

**Claim** $\chi$ is inj,

Say $\sigma, \tau \in Gal(F(\zeta)/F)$

if $\chi(\sigma) = \chi(\tau) \Rightarrow \sigma(\zeta) = \tau(\zeta)$

$\Rightarrow \sigma = \tau$ as $\zeta$ gens ext.

**Prop** For any $F$ of char 0

$\exists$ canonical inj grp homo $\chi : Gal(F(\zeta)/F) \to \mathbb{F}_p^\times$

In particular, $Gal(F(\zeta)/F)$ is cyclic of ord $\mid p-1$

(if we don't insist prime then still works $(\mathbb{Z}/n\mathbb{Z})^\times$ so we get cyclic)

**Warn** $\chi$ is not bijective in general. eg $F \supset \Sigma \supset F(\Sigma)$ is bij

**Rep** $\chi$ is a bijection if $F = \mathbb{Q}$

**Pf** $\Sigma$ is root of $\frac{x^p-1}{x-1} = \underbrace{x^{p-1} + x^{p-2} + \cdots + 1}_{\text{irred } / \mathbb{Q}}$

splitting.

$\Rightarrow [\mathbb{Q}(\Sigma) : \mathbb{Q}] = p-1$

$\Rightarrow \# \mathrm{Gal}(\mathbb{Q}(\Sigma)/\mathbb{Q}) = p-1$

↳ so inj of earlier map $\Rightarrow$ surj.

So, $\mathrm{Gal}(\mathbb{Q}(\Sigma)/\mathbb{Q}) \cong \mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)$

**Q** What is the subfield $E$ of $\mathbb{Q}(\Sigma)$ corr to subgp $\langle -1 \rangle \subset \mathbb{F}_p^\times$? (p odd)

$\mathbb{Q}(\Sigma)$ — 2 — $E$ — $\mathbb{Q}$

$\langle -1 \rangle$ has order 2 $\Rightarrow [\mathbb{Q}(\Sigma) : E] = 2$

Let $\gamma \in \mathrm{Gal}(\mathbb{Q}(\Sigma)/\mathbb{Q})$ be cx conj

Then $\gamma \neq 1$ but $\gamma^2 = 1$

So $\gamma$ is unique elt of order 2

$\Rightarrow \chi(\gamma) = -1$

$\mathbb{Q}(\Sigma + \bar{\Sigma}) \subset E = \mathbb{Q}(\Sigma)^\gamma$ ($\Sigma + \bar{\Sigma} = 2\cos(\frac{2\pi}{n})$)

$\Rightarrow \Sigma + \bar{\Sigma}$ fixed by $\gamma$

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

have $\Sigma$ as a root

$\Rightarrow [\mathbb{Q}(\Sigma), \mathbb{Q}(\Sigma + \bar{\Sigma})] \leq 2$

as degree not 1, it is 2. So $E = \mathbb{Q}(\Sigma + \bar{\Sigma})$

→

P 000

Q1 $(\mathbb{F}_p^\times)^2 \subset \mathbb{F}_p^\times$ has index 2.

Let $F$ = Fixed field of $(\mathbb{F}_p^\times)^2$

What is $F$?

$\mathbb{Q}(\zeta)$ / $F$ / $\mathbb{Q}$ | 2

Consider $g' = \sum_{a \in \mathbb{F}_p^\times} \zeta^{a^2}$ ] sum of $\zeta$ over $(\mathbb{F}_p^\times)^2$.

Automatically $g' \in F$

Let $g = 1 + g' = \sum_{a \in \mathbb{F}_p} \zeta^{a^2}$

This is analogous to $\int_{-\infty}^{\infty} e^{-x^2}\,dx = I$

$$I^2 = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-(x+y)^2}\,dx\,dy = \int_0^{2\pi}\int_0^{\infty} e^{-r^2} r\,d\theta\,dr$$

$$= \pi,$$

$\Rightarrow I = \sqrt{\pi}$

$p \equiv 1 \mod 4$

$$g^2 = \sum_{a,b \in \mathbb{F}_p} \zeta^{a^2+b^2}$$

$p \equiv 1 \ (4) \Rightarrow \exists\, i^2 = -1$ in $\mathbb{F}_p$

$a^2 + b^2 = a^2 - (ib)^2 = (a+ib)(a-ib)$, $u$, $v$

$$= \sum_{u,v \in \mathbb{F}_p} \zeta^{u,v}$$

$$= \sum_{u \neq 0} \underbrace{\sum_{v \in \mathbb{F}_p} \zeta^{uv}}_{0} + \sum_{u=0} \underbrace{\sum_{v \in \mathbb{F}_p} \zeta^{v}}_{p}$$

$g^2 = p \Rightarrow g = \sqrt{p}$

So, $F = \mathbb{Q}(\sqrt{p})$.