The p-th roots of 2 — p prime

$\zeta_p = e^{2\pi i/p}$. The roots of $x^p - 2$ are $\zeta_p^j \sqrt[p]{2}$ for $0 \le j \le p-1$.

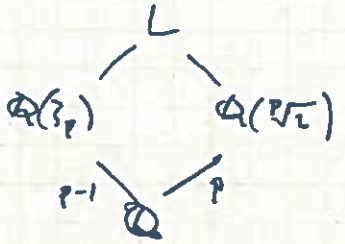
Thus $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p\sqrt[p]{2}, \zeta_p^2\sqrt[p]{2}, \dots, \zeta_p^{p-1}\sqrt[p]{2})$

$= \mathbb{Q}(\zeta_p, \sqrt[p]{2})$

is the splitting field of $x^p - 2$ over $\mathbb{Q}$.

Min poly of ζ_p is $x^{p-1} + x^{p-2} + \cdots + 1$ with roots ζ_p^i, $1 \le i \le p-1$.

Min poly of $\sqrt[p]{2}$ is $x^p - 2$ by Eisenstein criterion.



Tower thm + $\gcd(p, p-1) = 1$

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

Thus $|Gal(L/\mathbb{Q})| = p(p-1)$. Take $\sigma \in Gal(L/\mathbb{Q})$. Then σ is determined by $\sigma(\zeta_p) \in \{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$, $\sigma(\sqrt[p]{2}) \in \{\sqrt[p]{2}, \zeta_p\sqrt[p]{2}, \dots, \zeta_p^{p-1}\sqrt[p]{2}\}$.

Call $\sigma = \sigma_{i,j}$ if $\sigma(\zeta_p) = \zeta_p^i$, $\sigma(\sqrt[p]{2}) = \zeta_p^j \sqrt[p]{2}$

for some $1 \le i \le p-1$, $0 \le j \le p-1$. Every σ is of this form and there are only $(p-1)p$ choices for i, j, so all $\sigma_{i,j}$ are realized.

To determine group structure, we need to compute composition:

$$\sigma_{ij}\,\sigma_{rs}(\zeta) = \sigma_{ij}(\zeta^r) = (\sigma_{ij}\zeta)^r = \zeta^{ir}$$

$$\sigma_{ij}\,\sigma_{rs}(\sqrt[p]{2}) = \sigma_{ij}(\zeta^r\sqrt[p]{2}) = \sigma_{ij}(\zeta^r)\,\sigma_{ij}(\sqrt[p]{2}) = \zeta^{ir}\zeta^j\sqrt[p]{2}$$

$$= \zeta^{ir+j}\sqrt[p]{2}.$$

Thus $\sigma_{ij}\,\sigma_{rs} = \sigma_{ir,\,ir+j}$ where the subscripts are interpreted in $\mathbb{F}_p$.

Get a bijection $\mathbb{F}_p^\times \times \mathbb{F}_p \longrightarrow Gal(L/\mathbb{Q})$ but it's not a hom!

$$(i,j) \longmapsto \sigma_{ij}$$

Two perspectives on the group structure:

Geometry: Let $AGL_1(\mathbb{F}_p) = \{$ bij'ns $\mathbb{F}_p \to \mathbb{F}_p$ of the form $u \mapsto au+b$ for some $a, b \in \mathbb{F}_p \}$. Call this $\gamma_{a,b}$.

Easy to check $\gamma_{a,b}$ bij iff $a \in \mathbb{F}_p^\times$.

Gp op is comp'n, and

$$\gamma_{a,b} \circ \gamma_{c,d}(u) = \gamma_{a,b}(cu+d) = a(cu+d)+b = acu + (ad+b)$$

$$= \gamma_{ac, ad+b}$$

Thus $Gal(L/\mathbb{Q}) \xrightarrow{\cong} AGL_1(\mathbb{F}_p)$

$\sigma_{a,b} \longmapsto \gamma_{a,b}$

Semi-direct product

① Recall that if $G = NH$ for $N \trianglelefteq G$, $H \leq G$, $N \cap H = 1$, then $G = N \rtimes H$, the semi-direct product of N & H.

② For $\varphi: H \to Aut(N)$ hom, construct $N \rtimes_\varphi H$ with underlying set $N \times H$ and group op $(n_1, h_1)(n_2, h_2) = (n_1 \varphi(h_1)(n_2), h_1 h_2)$.

This recovers ① if $\varphi: h \mapsto (n \mapsto hnh^{-1})$ is the conjugation hom.

For $Gal(L/F)$, take $N = \{\sigma_{1,j} \mid j \in \mathbb{F}_p\} \cong \mathbb{F}_p \cong C_p$. Note that $N \trianglelefteq Gal(L/F)$. Take $H = \{\sigma_{i,0} \mid i \in \mathbb{F}_p^\times\} \cong \mathbb{F}_p^\times \cong C_{p-1}$.

Have $\sigma_{1,j}\sigma_{i,0} = \sigma_{1\cdot i, 1\cdot 0 + j} = \sigma_{i,j}$ so $NH = Gal(L/\mathbb{Q})$; clearly $N \cap H = 1$.

Finally compute $\sigma_{i0}\sigma_{1j}\sigma_{i0}^{-1} = (\sigma_{i\cdot 1, ij+0})\sigma_{i^{-1},0}$

$$= \sigma_{i,ij}\sigma_{i^{-1}0}$$

$$= \sigma_{1, i\cdot 0 + ij}$$

$$= \sigma_{1,ij}.$$

This corresponds to $\varphi: \mathbb{F}_p^\times \longrightarrow Aut(\mathbb{F}_p)$

$i \longmapsto (j \mapsto ij)$, the mult by i map.

Get $Gal(L/\mathbb{Q}) \cong \mathbb{F}_p \rtimes_{\text{mult}_i} \mathbb{F}_p^\times$.