# May 26 : Discussion

## Problem 9.1

$p$ prime

$\rho = e^{2\pi i/p}$ prim. $p^{th}$ root of unity

$\mathbb{Q} \subset \mathbb{Q}(\rho)$ field ext

(a) $\mathbb{Q} \subset \mathbb{Q}(\rho)$ Galois with

$$\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) = (\mathbb{Z}/p)^\times = \mathbb{Z}/(p-1)$$

Need to show $\mathbb{Q} \subset \mathbb{Q}(\rho)$ is finite, normal & separable

What is min poly of $\rho$?

know $\rho$ is a root of

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

min poly of $\rho = x^{p-1} + \cdots + 1$

$\Rightarrow \mathbb{Q} \subset \mathbb{Q}(\rho)$ finite ✓

Even know $|\mathbb{Q}(\rho) : \mathbb{Q}| = p-1$

Since $\mathrm{char}(\mathbb{Q}) = 0$, separable ✓

Is $\mathbb{Q} \subset \mathbb{Q}(\rho)$ the splitting field of $x^{p-1} + \cdots + 1$?

Yes! Because

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

Know $|\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})| = p-1$

Any element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ permutes roots of min poly of $\rho$

$\Rightarrow \sigma(\rho) = \rho^i$ for some $i = 1, \ldots, p-1$

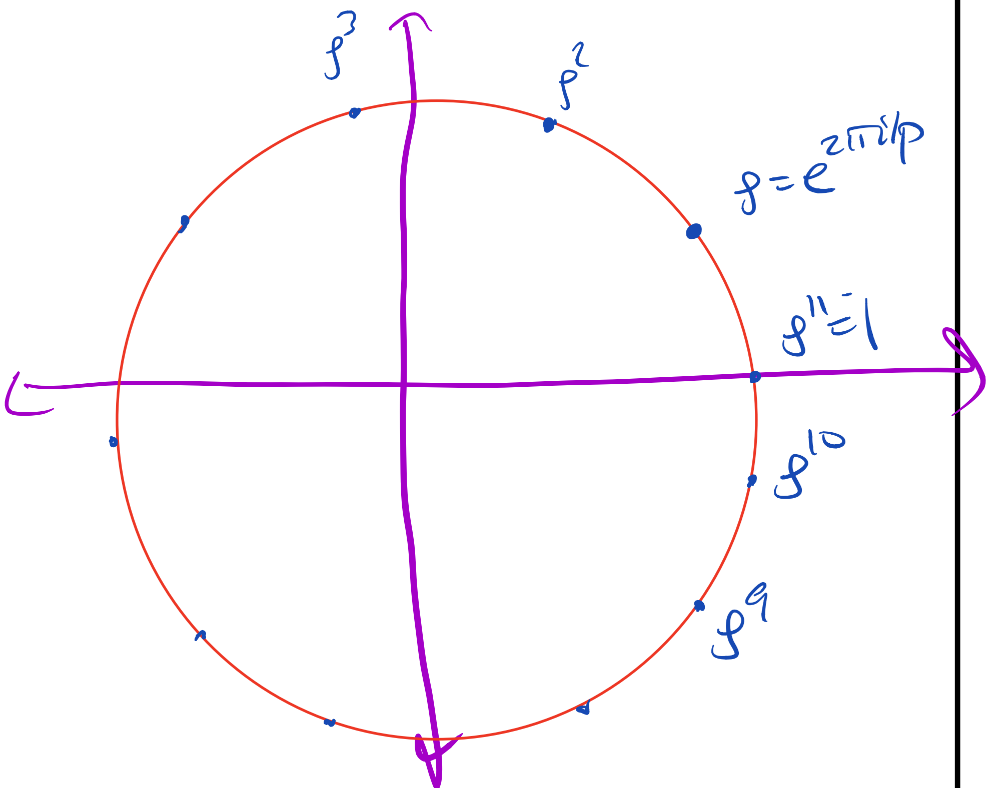
And $\sigma(\rho)$ uniquely determines $\sigma$

$$\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) \cong (\mathbb{Z}/p)^\times$$

$\sigma \longmapsto i$ where $\sigma(\rho) = \rho^i$

Check: group isom.

Roots of unity are points on the unit circle $|z|=1$ in $\mathbb{C}$




On Friday, we will consider a more general situation:

$K$ field of char $= 0$

$\rho$ prim $n^{th}$ root of unity

Consider $K \subset K(\rho)$

Don't know degree b/c we don't know $K$. For instance, $K$ could contain $\rho$.

We'll show $K \subset K(\rho)$ Galois

$\mathrm{Gal}(K(\rho)/K)$ is abelian!

What are the subgroups of $\mathbb{Z}/n$?

$\mathbb{Z}/n = \langle a \rangle \quad a^n = e$ identity

$$\left\{ \begin{matrix} \text{subgroups} \\ H \subset \mathbb{Z}/n \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{pos. integers } d \\ d \mid n \end{matrix} \right\}$$

$$H \longmapsto |H|$$

$$\langle a^{n/d} \rangle \longleftarrow d$$

For $\mathbb{Q} \subset \mathbb{Q}(\rho)$ and $d \mid p-1$, what is the corresponding inter. field ext

$$\mathbb{Q} \subset E \subset \mathbb{Q}(\rho)$$

---

In $\mathbb{Z}/5$

$2 \quad 2^2 = 4 \quad 2^3 = 3 \quad 2^4 = 1$

$3$

__Example__ $p = 5 \quad \rho = e^{2\pi i/5}$

$\mathbb{Q} \subset \mathbb{Q}(\rho)$ deg 4 ext

$$\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) = (\mathbb{Z}/5)^\times = \mathbb{Z}/4 = \langle \sigma \rangle$$

$$\sigma : \mathbb{Q}(\rho) \to \mathbb{Q}(\rho)$$
$$\rho \longmapsto \rho^2$$

Know $\langle \sigma \rangle = \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) = \mathbb{Z}/4$

Consider $H = \langle \sigma^2 \rangle \subset \mathbb{Z}/4$

Know $\sigma^2(\rho) = \rho^{-1} = \rho^4$

Want to examine $\mathbb{Q}(\rho)^H$

Look at $\rho$: not fixed

$\sigma^2(\rho) = \rho^{-1}$

$\Longrightarrow \rho + \sigma^2(\rho) = \rho + \rho^{-1} \in \mathbb{Q}(\rho)^H$

$\rightsquigarrow \mathbb{Q} \subset \mathbb{Q}(\rho + \rho^{-1}) \subset \mathbb{Q}(\rho)$

## Observations

In general, can't get an explicit handle on generator of $(\mathbb{Z}/p)^\times$. Just know that there exist generators

$$(\mathbb{Z}/p)^\times = \langle a \rangle$$

$\Rightarrow$ Define $\sigma$ by $\sigma(\rho) = \rho^a$

$\Rightarrow$ $\langle \sigma \rangle = \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$

Given $\underbrace{H = \langle a^{\frac{p-1}{d}} \rangle}_{\text{order } d} < \mathbb{Z}/(p-1)$

"

$$\mathbb{Q}(\rho)^H = \sum_{\tau \in H} \tau(\rho)$$

$$= \sum_{i=0}^{d-1} \sigma^i(\rho)$$

$$= \sum_{i=0}^{d-1} \rho^{a^i}$$ "

Check!