Last time:

Fun. Thm. of Galois theory

$$\left\{\begin{matrix}\text{int. fields}\\ F\subseteq E\subseteq K\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{subgps.}\\ H\leq G\end{matrix}\right\} \qquad \& \text{ properties}$$

$$E \longmapsto \mathrm{Aut}(K/E)$$

$$\mathrm{Fix}\, H \longleftarrow H$$

Rest of this unit: use this information to study field ext'ns

Today: When is the n-gon constructible by straightedge & compass?

Recall: $\mathcal{C}$ = field of constructible numbers $\subseteq \mathbb{C}$

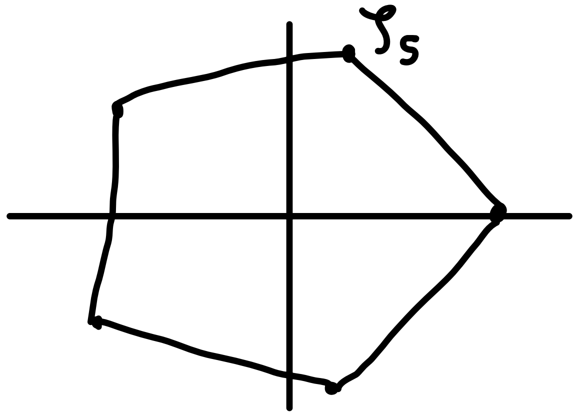
$a\in\mathcal{C} \Rightarrow \sqrt{a}\in\mathcal{C} \Rightarrow$ If $F\subseteq\mathcal{C}$, any deg 2 extn $F(\alpha)\subseteq\mathcal{C}$

$\alpha\in\mathcal{C} \Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}]$ is a power of 2

$\alpha\in\mathcal{C} \iff \exists\, \mathbb{Q}\subseteq E_1\subseteq \dots \subseteq E_k$ s.t. $\alpha\in E_k$ and

$$\left.\begin{matrix}[E_1:\mathbb{Q}]=2\\ [E_2:E_1]=2\\ \vdots\\ [E_n:E_{k-1}]=2\end{matrix}\right\} \text{use Galois theory to understand this}$$

n-gon constructible $\Leftrightarrow$ $\zeta_n = e^{2\pi i}$ constructible



$\zeta := \zeta_n$

Recall: $\mathbb{Q}(\zeta) = Sp_{\mathbb{Q}}(x^n - 1)$, so $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois

Prop: $\underbrace{Gal(\mathbb{Q}(\zeta)/\mathbb{Q})}_{G} \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Pf: $\sigma \in G$ determined by $\sigma(\zeta) = \zeta^a$, $\underbrace{\gcd(a,n) = 1}_{a \in (\mathbb{Z}/n\mathbb{Z})^\times}$

$\sigma_a(\zeta) = \zeta^a$

$\sigma_a \sigma_b(\zeta) = \sigma_a(\zeta^b) = (\zeta^b)^a = \zeta^{ab} = \sigma_{ab}(\zeta)$.

$\square$

Cor: G is abelian!

Ex: $n = 13$

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/13\mathbb{Z})^\times$$

cyclic w/ gen.

$\sigma = \sigma_2 : \zeta \mapsto \zeta^2$

Subgp. lattice:

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "3"'] \arrow[d, dash, "2"] & \\
\langle\sigma^4\rangle \arrow[d, dash, "2"'] & \langle\sigma^6\rangle \arrow[dl, dash, "3"] \arrow[dr, dash, "2"] & \\
\langle\sigma^2\rangle \arrow[dr, dash, "2"'] & & \langle\sigma^3\rangle \arrow[dl, dash, "3"] \\
 & \langle\sigma\rangle &
\end{tikzcd}$$

Int. field lattice

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "3"'] \arrow[d, dash, "2"] & \\
\mathbb{Q}(?) \arrow[d, dash, "2"'] & \mathbb{Q}(?) \arrow[dl, dash, "3"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(?) \arrow[dr, dash, "2"'] & & \mathbb{Q}(?) \arrow[dl, dash, "3"] \\
 & \langle\sigma\rangle &
\end{tikzcd}$$

Need elts. of $\mathbb{Q}(\zeta)$ fixed by subgps of G

Idea: sum over orbits

$\langle\sigma^6\rangle = \{1, \sigma^6\}$ $\quad$ $\langle\sigma^6\rangle\zeta = \{\zeta, \sigma^6\zeta\}$

Claim: $\zeta + \sigma^6\zeta$ is fixed by σ^6

Pf: $\sigma^{12} = 1$, so $\sigma^6(\zeta + \sigma^6\zeta) = \sigma^6\zeta + \zeta$ $\square$

$\sigma^6\zeta = \zeta^{2^6} = \zeta^{64} = \zeta^{-1}$

$\text{Fix}\langle\sigma^6\rangle = \mathbb{Q}(\zeta + \zeta^{-1})$ (correct degree since $\zeta^2 + (\zeta + \zeta^{-1})\zeta - 1 = 0$)

$\langle\sigma^4\rangle = \{1, \sigma^4, \sigma^8\}$

so

$$\text{Fix}\langle\sigma^4\rangle = \mathbb{Q}(\zeta + \sigma^4\zeta + \sigma^8\zeta)$$
$$= \mathbb{Q}(\zeta + \zeta^3 + \zeta^9)$$

$$
\begin{tikzcd}
 & & 1 \arrow[d, dash, "2"] \arrow[ddll, dash, "3"'] & \\
 & & \mathbb{Q}(\zeta+\zeta^{12}) \arrow[ddl, dash, "3"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\zeta+\zeta^3+\zeta^9) \arrow[dr, dash, "2"'] & & & \mathbb{Q}(\zeta+\zeta^5+\zeta^8+\zeta^{12}) \arrow[ddl, dash, "3"] \\
 & \mathbb{Q}(\zeta+\zeta^3+\zeta^4+\zeta^9+\zeta^{10}+\zeta^{12}) \arrow[dr, dash, "2"] & & \\
 & & \langle \sigma \rangle &
\end{tikzcd}
$$

Thm: The n-gon is constractible if and only if $\varphi(n)$ is a power of 2.

Pf: $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$, and we've already shown that this must be a power of 2.

Conversely, if $\varphi(n) = 2^k$, then since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois,

$G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is an abelian gp. of order 2^k

Abelian gps. have subgps. of every "possible" order (by Fun. Thm. of abelian gps.), so $\exists$

$$\mathrm{id} = G_0 \leq G_1 \leq \cdots \leq G_k = G \qquad |G_i| = 2^i$$

$\Updownarrow$ Galois corresp.

$$\mathbb{Q}(\zeta_n) = E_k \supseteq E_{k-1} \supseteq \cdots \supseteq E_0 = \mathbb{Q}$$

2 2 2

So $\zeta_n \in \mathcal{C}$.

Cor: The n-gon is constractible if and only if

$$n = 2^k p_1 \cdots p_r$$

Where the p_i are distinct primes of the form

$$p = 2^{2^s} + 1 \quad (\text{"Fermat prime"})$$

Pf: These are the numbers n s.t. $\varphi(n)$ is a power of 2.

$\square$