Example: $G := \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$, $\zeta := \zeta_5$

$$G = \{\sigma_1 : \zeta \mapsto \zeta,$$
$$\sigma_2 : \zeta_5 \mapsto \zeta^2,$$
$$\sigma_4 : \zeta_5 \mapsto \zeta^4, \quad = \zeta^{-1}$$
$$\sigma_3 : \zeta_5 \mapsto \zeta^3\}$$

Let $H = \{\sigma_1, \sigma_4\}$

Let $\alpha = \zeta + \sigma_4 \zeta = \zeta + \zeta^{-1}$

Then, $\sigma_4 \alpha = \zeta^{-1} + \zeta = \alpha$, so $\mathrm{Fix}\, H = \mathbb{Q}(\alpha)$

What is this field?

$$\alpha^2 + \alpha - 1 = \zeta^2 + 2 + \zeta^3 + \zeta + \zeta^4 - 1 = 0$$

Quad. formula $\Rightarrow \alpha = -\frac{1}{2} \pm \frac{\sqrt{5}}{2}$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$.

In general, if p is an odd prime,

$$\begin{cases} \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p), & \text{if } p \equiv 1 \bmod 4 \\ \mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\zeta_p), & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

Constractability of the n-gon

Def: $\alpha \in \mathbb{C}$ is constructible over $\mathbb{Q}$ if $\mathrm{Re}\,\alpha$, $\mathrm{Im}\,\alpha$ are constructible over $\mathbb{Q}$.

Prop: α is constractible if and only if it lies in some field K given by a sequence of deg 2 ext'ns.

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = K, \quad [K_i : K_{i-1}] = 2.$$

Pf sketch: If $\alpha \in \mathbb{R}$, we know this true in case $K_i = K_{i-1}(\sqrt{D_i})\ \forall i$. By the quadratic formula (p. 522), all degree 2 ext'ns E/F are of this form, so the prop holds.

Need to show $\alpha \in \mathbb{C}$ satisfies this criterion iff $\mathrm{Re}\,\alpha$, $\mathrm{Im}\,\alpha$ do.

$$m_{\alpha,\mathbb{Q}}(\bar{\alpha}) = \overline{m_{\alpha,\mathbb{Q}}(\alpha)} = 0, \text{ so } \bar{\alpha} \in \mathbb{Q}(\alpha)$$

This means that $\frac{1}{2}(\alpha + \bar{\alpha}) = \mathrm{Re}\,\alpha$, $\frac{1}{2}(\alpha - \bar{\alpha}) = \mathrm{Im}\,\alpha \in \mathbb{Q}(\alpha)$

Conversely, $\alpha \in \mathbb{Q}(i, \mathrm{Re}\,\alpha, \mathrm{Im}\,\alpha)$, and $[\mathbb{Q}(i, \mathrm{Re}\,\alpha, \mathrm{Im}\,\alpha) : \mathbb{Q}(\mathrm{Re}\,\alpha, \mathrm{Im}\,\alpha)] = 2$. $\square$

Construction of reg. n-gon $\Leftrightarrow$ construction of ζ_n

Lemma: ζ_n constructable $\Leftrightarrow$ $\varphi(n)$ is a power of 2.

Pf: $\Rightarrow$: Tower Law

$\Leftarrow$: $G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is an abelian gp. with order 2^m, $m \in \mathbb{Z}_{\geq 0}$. Then, G has subgps.

$$G = G_0 > G_1 > \cdots > G_m = 1$$

with

$$[G_{i+1} : G_i] = 2 \quad \forall i$$

If $K_i = \mathrm{Fix}\, G_i$, then $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = \mathbb{Q}(\zeta_n)$ is the desired sequence. $\square$

Fermat prime: prime of the form $p = 2^{2^s} - 1$: $3, 5, 17, 257, \ldots$

Prop 29: The regular n-gon is constructible if and only if $n = 2^k p_1 \cdots p_r$, $k \in \mathbb{Z}_{\geq 0}$, p_i distinct Fermat primes.

Pf sketch: these are the numbers for which $\varphi(n)$ is a power of 2 $\square$

Can actually use this to construct ζ_n.

Def: choose $H \leq G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, ζ: prim. nth root of 1

The quantity $\sum_{\sigma \in H} \sigma(\zeta)$ is called a <u>period</u> of $\mathbb{Q}(\zeta_n)$.

Note: when $H=1$, the periods are just the prim. roots.

When n is prime, can show that $\text{Fix } H = \mathbb{Q}(\text{periods of } H)$

If $H_1 < H_2$, $[H_2 : H_1] = 2$, then each period η of H_1 satisfies a quad. eqn. over $\mathbb{Q}(\text{periods of } H_2)$, so can use quad. formula to express η in terms of sqrts. of periods of H_2, which themselves are expressible in the same way using periods of larger subgps.

e.g.

$$16 \operatorname{Re} \zeta_{17} = -1 + \sqrt{17} + \sqrt{2(17-\sqrt{17})}$$
$$+ 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17-\sqrt{17})} - \sqrt{2(17+\sqrt{17})}}$$

---

§14.6: Galois gps. of polys.

Recall: Galois gp of $f \in F[x]$ is $\text{Gal}(\text{splitting field of } f / F)$
sep.

$\text{Gal}(f) := \text{Gal}_F(f)$

$\alpha_1, \ldots, \alpha_n$ roots of f: $\sigma \in \text{Gal}_F(f)$ permutes $\alpha_1, \ldots, \alpha_n$

$$\text{Gal}(f) \underset{\substack{\text{inj.}\\ \text{homom.}}}{\hookrightarrow} S_n$$

If $f(x) = f_1(x) \cdots f_k(x) \in F[x]$,

$\mathrm{Gal}(f) \leq S_{n_1} \times \cdots \times S_{n_k}$

By Thm. 13.27, if f irred $/F$, $\exists\, \sigma \in \mathrm{Gal}(f)$ s.t.

$\sigma(\alpha_1) = \alpha_i \ \forall i$.

i.e. $\mathrm{Gal}(f)$ is transitive on the roots of f

Eventually: Galois groups for specific polys.

First: Galois gp. for "general" deg n polys.

Def: Let $x_1, \ldots, x_n$ be indeterminates. The general deg n poly is

$f_{gen} := (x - x_1)(x - x_2) \cdots (x - x_n)$.

Let

$$\left.\begin{aligned}
s_1 &= x_1 + \cdots + x_n \\
s_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_2 x_3 + x_2 x_4 + \cdots + x_{n-1} x_n = \sum_{i<j} x_i x_j \\
&\vdots \\
s_k &= \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} \cdots x_{i_k} \\
&\vdots \\
s_n &= x_1 x_2 \cdots x_k
\end{aligned}\right\}$$

elementary symm. polys. usually written e_k

We have $f_{gen} = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n$.

For any field F,

$$F(x_1, \ldots, x_n) / F(s_1, \ldots, s_n) \text{ is a Galois ext'n !}$$

(in particular, finite, alg., sep.)

Prop 30: $G := Gal(F(x_1, \ldots, x_n)/F(s_1, \ldots, s_n)) = S_n$

Pf: We know that $G \leq S_n$ since $\deg f_{gen} = n$.
Every $\sigma \in S_n$ gives an autom. of $F(x_1, \ldots, x_n)$, and the s_n are fixed under permutations of $x_1, \ldots, x_n$, so $S_n \leq G$ also.

$\square$

Def: A rat'l fun. $f(x_1, \ldots, x_n)$ is <u>symmetric</u> if for all $\sigma \in S_n$

$$f(\sigma(x_1), \ldots, \sigma(x_n)) = f(x_1, \ldots, x_n)$$

Fundamental Thm of Sym. Funs (Cor 31): Any sym. fun in $x_1, \ldots, x_n$ is a rat'l fun in $s_1, \ldots, s_n$.

Pf: Since $S_n = \mathrm{Gal}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n))$, $F(s_1, \dots, s_n) = \mathrm{Fix}\, S_n$. By def'n, a symm. is in $\mathrm{Fix}\, S_n = F(s_1, \dots, s_n)$. $\square$