Project due noon Friday

H/w 6 rest of problems posted (due Tues. noon)

Recall: $\alpha \in \mathbb{C}$ is constructible over $\mathbb{Q}$ if $\mathrm{Re}\,\alpha$, $\mathrm{Im}\,\alpha$ are constructible over $\mathbb{Q}$. Equivalently, α is constructible if and only if it lies in some field K given by a sequence of deg 2 ext'ns.

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

Recall: 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.

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.

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

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 $\mathrm{Gal}(\text{splitting field of } f / F)$
sep.

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

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

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

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 <u>transitive</u> on the roots of f

Eventually: Galois groups for specific polys.

First: Galois gp. for "<u>general</u>" 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

$$\left.\begin{aligned}
s_1 &= x_1 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n = \sum_{i<j} x_i x_j \\
&\vdots \\
s_k &= \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} \cdots x_{i_k} \\
&\vdots \\
s_n &= x_1 x_2 \cdots x_k
\end{aligned}\right\}$$

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,

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

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

Prop 30: $G := \mathrm{Gal}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)) = S_n$

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

$\square$

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

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

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

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. fun. $\mathrm{Fix}\ S_n = F(s_1, \dots, s_n)$. $\square$

Examples:

1) $(x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2$

$= (x_1 + x_2)^2 - 4x_1x_2$

$= s_1^2 - 4s_2$

Note: s_i refers to $s_i(x_1, x_2)$ here

2) $x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3)$

$= s_1^2 - 2s_2$

Note: s_i refers to $s_i(x_1, x_2, x_3)$ here

Fun exercise: Let
(?)

$$E(t) := \sum_{r=0}^{n} e_r(x_1, \dots, x_n)t^r$$

Prove that

$$E(t) = \prod_{i=1}^{n} (1 + x_i t)$$

moved to homework

Thm 32: Let $s_1, \dots, s_n$ be indeterminates.

Then, $f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n \in F(s_1, \dots, s_n)[x]$

is sep. w/ Galois gp. S_n.

Pf: Let $x_1, \dots, x_n$ be the roots of f. Then $s_1, \dots, s_n$ are the elementary symm. polys in $x_1, \dots, x_n$.

Claim: no poly. relations over F btwn. $x_1, \dots, x_n$.

Pf: If so, let $p(t_1, \dots, t_n) \in F[t_1, \dots, t_n]$ s.t. $p(x_1, \dots, x_n) = 0$.

Let $\tilde{p}(t_1, \dots, t_n) = \prod_{\sigma \in S_n} p(t_{\sigma(1)}, \dots, t_{\sigma(n)})$.

Since $p \mid \tilde{p}$, $\tilde{p}(x_1, \dots, x_n) = 0$, but $\tilde{p}$ is sym. in the x's, and so gives a poly. rel'n btwn. $s_1, \dots, s_n$ by Fun. Thm. of Sym. Funs.

But by assumption, $s_1, \dots, s_n$ are indeterminates.

Thus, same setting as Prop 30 $\Rightarrow$ done. $\square$

Conclusion: if no alg. rel'ns btwn coeffs., Gal. gp. is S_n.

Over $\mathbb{Q}$, happens most of the time. Over $\mathbb{F}_p$, can't happen.