5) Splitting field of $\Phi_n(x)$ over $\mathbb{Q}$.

$K = \mathbb{Q}(\zeta_n)$, $[K:\mathbb{Q}] = \varphi(n)$.

Every $\sigma \in Gal(K/\mathbb{Q})$ is determined by $\sigma(\zeta_n)$, and the possibilities are $\sigma(\zeta_n) = \zeta_n^a$, $1 \le a \le n$, $(a,n)=1$.

For each $1 \le a \le n$, $(a,n)=1$, write $\sigma_a \in Gal(K/\mathbb{Q})$ for the autom. deter. by $\sigma_a(\zeta_n) = \zeta_n^a$. Then

$$(\sigma_a \sigma_b)(\zeta_n) = \sigma_a(\zeta_n^b) = (\sigma_a(\zeta_n))^b = (\zeta_n^a)^b = \zeta_n^{ab}$$

$$\Rightarrow \sigma_a \sigma_b = \sigma_{ab}, \text{ so } Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

Lemma: If $f \in \mathbb{Q}[x]$, $\deg f = n$, and K is the spl. field of f over $\mathbb{Q}$, then $Gal(K/\mathbb{Q}) \le S_n$.

Pf: Let $\alpha_1, \dots, \alpha_n$ be roots of f in K.

Then $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Every element of $Gal(K/\mathbb{Q})$ can be identified with an element of S_n that permutes $\alpha_1, \dots, \alpha_n$, and the corresponding map $Gal(K/\mathbb{Q}) \to S_n$ is an injective homom. ☒

6) K the splitting field of $f(x)=x^5-4x+2$ over $\mathbb{Q}$.

Let $G=\mathrm{Gal}(K/\mathbb{Q})$. Then:

i) $G \leq S_5$

ii) G has an elem. of order 5:

f is irred. by E's @ $p=2$ $\Rightarrow 5 \mid [K:\mathbb{Q}] = |\mathrm{Gal}(K/\mathbb{Q})|$

$\Rightarrow \mathrm{Gal}(K/\mathbb{Q})$ has an elem. of order 5

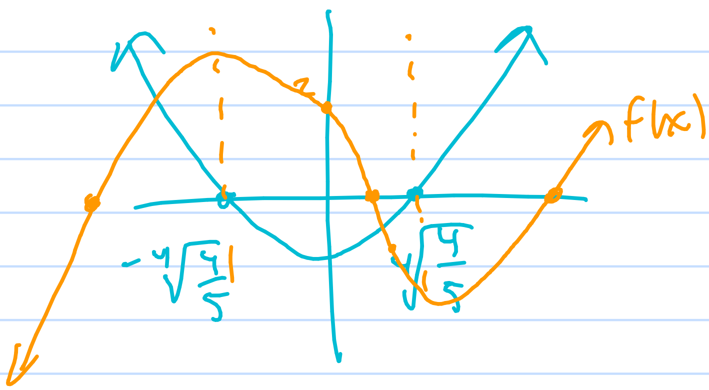
$\uparrow$
(5 is prime)

iii) G contains a transposition:

$f(x)=x^5-4x+2$, $\quad f'(x)=5x^4-4$

$f(0)=2$

$f\left(\frac{3}{4}\right)<0$



f has exactly 3 real zeros $\Rightarrow$ it has 2 non-real complex zeros

$\Rightarrow$ complex conjugation is a nontrivial element of G, which acts (under the identification with S_5) as a transposition.

Fact: Any subgroup of S_5 which contains a 5 cycle and a transposition, is all of S_5.

7) $K = \mathbb{F}_{p^n}$, $F = \mathbb{F}_p$.

K/F is Galois, because K is the splitting field of $f(x) = x^{p^n} - x$ over F.

$[K:F] = n \Rightarrow |Gal(K/F)| = n$.

Let $\sigma \in Gal(K/F)$ be defined by

$\sigma(\alpha) = \alpha^p$ (Frobenius automorphism — see hmwk 2).

From the homework, $\sigma^k = id \Leftrightarrow n \mid k$

$\Rightarrow Gal(K/F) = \langle \sigma \rangle \cong C_n$.

Straightedge and compass constructions

Start with the plane, identify it with $\mathbb{C}$, and start with $\{0,1\}$. Which points, angles, shapes, lengths, can we construct from these two points, using only a straightedge and compass. Allowed operations:

A1) Given any two distinct points which have been constructed, draw the line passing through them.

A2) Given z and w which have been constructed, draw a circle with center at z and radius $|z-w|$.

A3) We can throw in to our set of constructible numbers, any intersection point.

Def: Let $\mathcal{C}$ denote the subset of all constructible numbers in $\mathbb{C}$.

Greeks could figure out how to:

1) take square roots of lengths
2) bisect arbitrary angles
3) construct regular 3, 4, 5, 6, 8, 10, 17-gons.

However they couldn't figure out how to:

1) Construct regular 7 or 9-gons.
2) Trisect an arbitrary angle
3) Construct a square with same area as a circle of radius 1
4) "Double the cube" - i.e. construct $\sqrt[3]{2}$.