Example from last time

\[ x = \frac{-1 + i\sqrt{3}}{2}, \quad x^2 = \frac{-1 - i\sqrt{3}}{2}, \quad x^3 = 1 \]

\[ 1 + x + x^2 = 0 \]

\[ x^2 = -1 - x \]

\[ w = \sqrt[3]{2} = 1.3 \ldots \]

Some fields

\[ k = \mathbb{Q}(x) \]

\[ \text{octan} \left( \frac{\sqrt{3}}{2} \right) = \frac{5}{3} \]

\[ = \left\{ a + b \frac{\sqrt{3}}{2} : a, b \in \mathbb{Q} \right\} \]

\[ \mathbb{Q} \left( \frac{\sqrt{3}}{2} \right) = \mathbb{Q} \left( \frac{\sqrt{3}}{2} \right) \]

\[ L = k(w) = \left\{ x + \frac{-1}{3} w + 2w^2 : x, y, z \in \mathbb{Q} \right\} \]

NEW

\[ F_i = \mathbb{Q}(\sqrt[5]{3}, w) = \left\{ c + d \sqrt[5]{3} w : c, d \in \mathbb{Q} \right\} \quad i = 0, 1, 2 \]

\[ \mathbb{Q} \left( \sqrt[5]{3}, w \right) \]

For \( F_0, F_1, F_2 \) are all subfields of \( L \)

\( L \) is a 3-dimensional vector space
over $K$ with basis \( \{ 1, w, w^2, \frac{1}{w}, \frac{1}{w^2} \} \)

$L$ is a $6$-dimensional vector space over $\mathbb{Q}$ with basis \( \{ 1, 3, w, w^3, w^2, w^5 \} \)

Note \( 3^2 = -1 \cdot 3 \) and \( w^3 = 2 \)

$L$ has some field automorphisms $\sigma$ and $\beta$ defined by

<table>
<thead>
<tr>
<th>$x$</th>
<th>$\sigma(x)$</th>
<th>$\beta(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>$3^2$</td>
<td>$3^2$</td>
</tr>
<tr>
<td>$\frac{1}{3}$</td>
<td>$\frac{1}{3}^2$</td>
<td>$\frac{1}{3}^2$</td>
</tr>
<tr>
<td>$w$</td>
<td>$w$</td>
<td>$w^5$</td>
</tr>
<tr>
<td>$w^3$</td>
<td>$w^3$</td>
<td></td>
</tr>
</tbody>
</table>

We find that $\beta^2 = $ identity

$\sigma^2 = 1$
\( \text{ocean} \cdot \text{bent} (w) = \text{ocean} (w \overline{3}) = w \overline{3} = -w \overline{1} \)

\( \text{bent} \cdot \text{ocean} (w) = \text{bent} (w) = w \overline{3} \)

The group generated by \( \text{ocean} \) and \( \text{bent} \) is isomorphic to \( S_3 \).

\( \overline{3}^w \)

The group \( G \) permutes the 3 cube roots of 2, namely \( w, \overline{3}w \) and \( \overline{3}^2 w \).
$L$ and its subfields $\bar{L}$

$K = K_{\text{bend}} \subseteq F_0 \subseteq F_1 \subseteq F_2 \subseteq \bar{L} = L$

$Q = K^G$

$G$ acts on $L$ by automorphisms

A subgroup $H \subseteq G$

Let $L^H = \{ x \in L : h(x) \text{ for all } h \in H \}$

= fixed pt set of $H$. 

$G_3 = S_3$ and its subgroups

$\langle e \rangle \triangleleft S_3 \triangleleft \langle \text{bend} \rangle \triangleleft \langle \text{ocean} \rangle \triangleleft \langle \text{bend}, \text{ocean} \rangle \triangleleft S_3$

$S_3/K_2 \cong C_2$

$\langle \text{bend} \rangle \trianglelefteq S_3$
$G$ is the Galois gp of $L$ over $\mathbb{Q}$

$\langle \text{bett} \rangle$

$\langle \text{soc} \rangle$

$K \supseteq \mathbb{F}_o$

etc.

There is a 1-1 correspondence between subfields of $L$ and subgps of $G$.

**Fundamental Theorem of Galois Theory**

Let $F \subseteq K \subseteq L$ be fields satisfying certain hypotheses (to be named later).

$L$ has a gp of automorphisms $G$ such that $L^n = F$
1) dim $L$ as a vector space over $F$ is $|G|$

2) each subgroup $H$ of $G$ fixes a different subfield $K$ of $L$ containing $F$ and vice versa. There is a 1-1 correspondence between subgroups of $G$ and subfields of $L$ containing $F$.

3) If $H$ is a normal subgroup of $G$ and $K = L^H$, then $G/H$ acts on $K$ fixing $F$.

Preview of coming attractions: Applications of Galois theory.
1) There is no general formula for the solution to a quintic (or higher degree) polynomial.

Remark: The example has to with solutions to \( x^3 - 2 = 0 \). \( L \) is the smallest field containing all its roots.

\( S_3 \) acts on \( L \). There are similar examples with quintic polynomials leading to \( S_5 \). \( S_5 \) is BAD, meaning not solvable.

2) Ruler + compass problems. The ancient Greeks could...
construct a regular \( n \)-gon
for \( n = 2^k, 3, 2^k, 5, 2^k \) and \( 15, 2^k \)
and NO OTHERS!

\sim 1796. Dames did it for \( n = 17 \).

Then (Dames) suppose \( n \) is prime.
One can construct a regular \( n \)-gon
with ruler + compass \( \iff n = 1 + 2^k \)
for some \( k \).

Remark Only 5 such primes are known.

Lemma \( 1 + 2^k \) can be a prime only
if \( k \) itself is a power of 2.
\[ 1 + 2^0 = 3 \quad 1 + 2^2 = 5 \quad 1 + 2^4 = 17 \]
\[ 1 + 2^6 = 65 \quad 1 + 2^8 = 65537 \]
\[ 1 + 2^{10} = 1 + 2^{10} \approx 4 \text{ billion} \]

is divisible by 641 (Euler).

No other Fermat primes are known.

3) Other R+C problems

a) Trisecting an angle: **IMPOSSIBLE**

b) “Doubling the cube” can be done with origami.
Impossibly with \( R+C \).

Possibly with origami.

D) "Ignoring the circle" impossible with either \( R+C \) or origami.

\[
\text{Lemma 1: } 1+2^k \text{ can be a prime only if } k \text{ itself is a power of } 2.
\]

**Proof:** Recall \( x^3+1 = (x+1)(x^2-x+1) \)

\( x=2^l \Rightarrow (2^{3l}+1) = (2^l+1)(4^l-2^l+1) = \text{not prime} \)

\( (x^5+1) = (x+1)(x^4-x^3+x^2-x+1) \)
\( (2^{5k+1}) \text{ is not prime} \)

\[
(x^{2m+1} + 1) = (x+1)(x^{2m} - x^{2m-1} \cdots - x + 1)
\]

\( x = 2^k \)

\[
2^{(2m+1)} + 1 \text{ is not prime}
\]

\( \rightarrow \) If \( k \) is divisible by any odd \( > 4 \), then \( 2^k + 1 \) is not prime.

(\( \exists k \))