Announcements:

Starting 4/13 – use $\boxed{\text{gather town}}$ for class meeting

weekend for how to access.

Flipped class – post videos 2 days before each class

starting for 4/15.

On 4/13 – "Practice" day to figure it out

we'll talk about homework problems for the current HW about Galois theory

Now due on Thursday 4/15.

4/15, 4/20, 4/22, 4/27 on rep theory

A single handout / homework for these.

due on 4/29

(Final on 5/3) in Zoom!

Grading for final 2 assignments:

each of these will count as 1 or 2 assignments (whatever is better for your grade)

Final format: Most likely like midterm but longer + one problem where you have to write out a proof (but there will be some options).

Theorem $\mathbb{C}$ is algebraically closed.

(We talked about a proof via complex analysis — below a proof due to Artin using calculus + Galois theory).

Lemma ① Any quadratic polynomial w/ coefficients in $\mathbb{C}$ has a root.

② Any odd degree polynomial over $\mathbb{R}$ has a root.

Proof ① x^2+ax+b ~ suffices to give $\sqrt{b^2-4ac}$

In polar coordinates $\sqrt{re^{i\theta}} = \pm\sqrt{r}\, e^{i\frac{\theta}{2}}$

② Intermediate value theorem

$f(x) = x^n + \dots$

n is odd then $x << 0$ $f(x) \sim x^n < 0$

then $x >> 0$ $f(x) \sim x^n > 0$

so $\exists$ x_0 s.t. $f(x_0) = 0$.

Proof: Let f be a monic polynomial over $\mathbb{C}$.

Let $K/\mathbb{C}$ be an extension such that

a) f has a root in K

b) $K/\mathbb{R}$ is Galois.

(Take any finite $L/\mathbb{C}$ where there is a root; $L = \mathbb{R}(\alpha)$ by primitive element; take K to be a splitting field of $M_\alpha(x) \in \mathbb{R}[x]$)

$G = \mathrm{Gal}(K/\mathbb{R})$

$H \leq G$ Sylow 2-subgroup.

$[K^H : \mathbb{R}] = [G:H] =$ odd #.

$K^H = \mathbb{R}(\beta)$ by primitive element theorem

$M_\beta(x) =$ minimal polynomial in $\mathbb{R}[x]$

has degree $[G:H]$ and its irreducible.

$[G:H]$ is odd so m_β has a root in $\mathbb{R}$

$\Rightarrow \deg m_\beta(x) = 1$ (since irred + has a root)

$\Rightarrow [G:H] = 1$

Conclusion: G is a 2-group i.e. $|G| = 2^n$ for some n.

$\mathrm{Gal}(K/\mathbb{C}) \leq \mathrm{Gal}(K/\mathbb{R}) = G$.

so $|\mathrm{Gal}(K/\mathbb{C})| = 2^m$

Suppose $m \geq 1$

Then $\mathrm{Gal}(K/\mathbb{C}) \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ (structure of 2-groups).

That gives a degree 2 extension $M/\mathbb{C}$

$M = \mathbb{C}(\gamma)$

$m_\gamma(x) \in \mathbb{C}[x]$ has degree 2

$\Rightarrow$ has a root (by Lemma)

contradicts $m_\gamma(x)$ irreducible degree 2.

↯

$m = 0$ so $|\mathrm{Gal}(K/\mathbb{C})| = 2^0 = 1$

i.e. $K = \mathbb{C}$

Thus f has a root in $\mathbb{C}$.

Solvability in radicals:

Obs: · We have a quadratic formula: roots of $x^2+bx+c = \frac{-b\pm\sqrt{b^2-4c}}{2}$

· There is a cubic formula ~ use $\sqrt[3]{\text{expressions in coefficients}}$ / $\sqrt{\ldots}$

sixth roots of unity.

· There is a quartic formula ...

· There is no quintic formula (or n-tic for $n \geq 5$): no general formula for the roots of degree 5 polynomial using nth roots and field operations on coefficients

We'll make this more precise then show something stronger using Galois theory.

Definition If K is a field $f(x) \in K[x]$ then f is solvable in radicals if there is an extension L/K where f splits s.t. there exists a chain of extensions

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_m = L$$

s.t. $L_i = L_{i-1}(\sqrt[k]{a})$ for some $a \in L_{i-1}$ and k

(we allow $a=1$, i.e. adding roots of unity)

Remark: If f is solvable in radicals then any root is gotten from the coefficients of f by iterating ring operations and radicals.

char $K = 0$

Theorem: If $f \in K[x]$ is separable then f is solvable in radicals $\iff$ $\mathrm{Gal}(f)$ is solvable.

(Recall G is solvable if $\exists$
$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_n = G$
s.t. H_i / H_{i-1} is cyclic.
(could ask to be abelian))

Example $x^5 - 6x + 3$ is not solvable in radicals
Because last time we saw Galois group is S_5
which is not solveable
(Derived series is $S_5 \trianglerighteq A_5 \trianglerighteq \{e\}$).
simple non-abelian).

Corollary: There is no quintic formula.

There is no n-tic formula $n \geq 5$ because last time we saw how to construct extensions of $\mathbb{Q}$ w/ Galois group S_n.
S_n not solvable for $n \geq 5$.

Proof of theorem: Easy direction:

If f solveable in radicals, then $\mathrm{Gal}(f)$ is solveable.

$$K = L_0 \leq L_1 \quad \dots \quad \leq L_m = L$$
$$L_{i+1} = L_i(a_i^{1/k_i}).$$

L contains a splitting field for f.

(Can make L bigger, Galois over K then

(since $\mathrm{Gal}(L/K)$ solvable $\Rightarrow$
$\mathrm{Gal}(f)$ is solvable because it's a quotient.)

Let's take $M = L(\mu_{\ell})$
← ℓth roots of unity where $\ell = \prod k_i$.

$$K \subseteq K(\mu_{\ell}) \subseteq L_1(\mu_\ell) \subseteq \cdots \subseteq L(\mu_\ell)$$
$$K = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$
$$M_{i+1} = M_i(\ell_i^{1/k_i}).$$
$$\mathrm{Gal}(M_{i+1}/M_i) \subseteq \mathbb{Z}/k_i\mathbb{Z} \quad \text{(exercise on your homework)}.$$

This is almost right but I haven't justified that M/K Galois, and in fact it might not be.

<u>But</u>: can modify this: at each step take roots also of all conjugates of ℓ_i by $\mathrm{Gal}(M_i/M_0)$.

Exercise to do this carefully.

<u>Hard direction</u>: If G solvable then f is solvable in radicals.

<u>Step (1)</u>: Add in all the roots of unity of order dividing $|G|$.

<u>Step (2)</u>: Kummer theory: ← On next HW

If K contains nth roots of unity and L/K has Galois group $\mathbb{Z}/n\mathbb{Z}$ ← n coprime then $L = K(a^{1/n})$ for some a. to characteristic of K

If $\mathbb{Z}/n\mathbb{Z}$ extension and char $K = p$
then need Artin-Schreier theory