midterm 2 average $\underline{85/100}$.

Quiz 2 will be take-home: assign on Thursday, couple of days to solve, reminder to abide by CU code of conduct when solving.

Plan: finish Galois theory this week.

Then 3 more lectures: rings & modules over them.

roots of unity extensions

$E^* \supset \mu_n$ = all n-th roots of unity. cyclic group of order n

↑ best case

of order a div. of n

char 0

always find an extension of F (splitting field of x^n-1) that contains all nth roots of unity

n-th root of unity $\alpha^n=1$

primitive n-th root of unity ω $\omega^n=1$, $\omega^m \neq 1$ $1 \le m < n$

$$\Psi_n(x) = \prod_{\substack{\omega\text{-all prim}\\ n\text{-th roots of } 1 \text{ in } \mathbb{C}}} (x-\omega)$$

$\Psi_n(x) \in \mathbb{Z}[x]$

$\deg = \varphi(n)$ Euler phi f-n

irreducible

$$\begin{array}{ll} K & \text{split. field of } x^n-1 \\ \cup & \\ F & \end{array}$$

$\mathbb{Q}$

$\mathrm{Gal}(K/F)$ abelian

$\subset (\mathbb{Z}/n)^*$ inv. res mod n

ω - prim. root

$\sigma(\omega) = \omega^a \quad (a,n)=1 \quad Y = \{\omega^a \mid a \in (\mathbb{Z}/n)^*\}$

all prim n-R roots of unity

$K = F(\omega)$

$G = \mathrm{Gal}(K/F)$ acts on Y.

$$\begin{tikzcd} & \omega^{ab} & \\ & & \omega^{b} \arrow[ul, bend right] \\ \omega \arrow[rr] & & \omega^{a} & (\mathbb{Z}/n)^* \arrow[l] \end{tikzcd}$$

$G \subset (\mathbb{Z}/n)^*$

$\sigma \Longleftrightarrow a$ s.t. $\sigma(\omega) = \omega^a$

Solved cubic & quartic equations

$\mathrm{Gal} \rightarrow \begin{cases} x^3 + ax^2 + bx + c = 0 \\ x^4 + ax^3 + \dots + d = 0 \end{cases} \quad a,b,c,d \in \mathbb{Q}.$

$\cap$

S_3, S_4 solved by iterated radicals. $\sqrt{D}$

$x^n + a_{n-1}x^{n-1} \dots + a_0 = 0 \quad a_i \in \mathbb{Q}$

$n \geq 5 \quad S_n$ alternating $\underline{|A_5| = 60}$

$S_5 \supset A_5 \rightarrow$ simple

$S_2, S_3, S_4, S_5, \dots$

$\leftarrow$ built from abelian groups (solvable). $\rightarrow$ more complicated groups

only $\{1\}$ and A_5 as normal subgroups

$\underline{C_p}$ - simple, abelian $\quad A_5$ - simple ← first simple non-abelian group

$N \triangleleft G \quad N, \; G/N$

G is "glued" out of N & G/N.

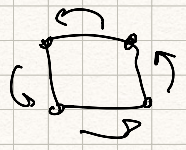
$C_2 \times C_2$ is "glued" from C_2, C_2

C_4 is glued from C_2, C_2

$\underset{\{1,g,g^2,g^3\}}{\underset{\shortparallel}{C_4}} \supset \underset{\{1,g^2\}}{\underset{\shortparallel}{C_2}}$ $C_2 \triangleleft C_4$ $C_4/C_2 \simeq C_2$

glued 2 C_2's in a natural way together into C_4.

D_4 - dihedral group



$\underset{4}{C_4} \subset \underset{8}{D_4}$ $[D_4 : C_4] = 2$

(rotations

$N \triangleleft G$

$gNg^{-1} = N$

Thm if $H \subset G$, index 2 $\Rightarrow H \triangleleft G$

normal: left cosets = right cosets.

$D_4 \underset{2}{\supset} C_4 \underset{2}{\supset} C_2 \underset{2}{\supset} \{1\}$

each subsequent quotient is abelian

Def G is solvable if $\exists$ a chain of subgroups

$G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_n = \{1\}$.

$G_{i+1} \triangleleft G_i$ G_i/G_{i+1} - abelian.

D_4-solvable, S_4-solvable

Ex Any group of order p^n is solvable (Rotman)

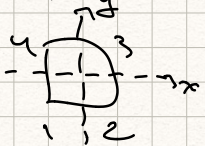
$\overset{24}{S_4} \underset{2}{\supset} \overset{12}{A_4} \supset \overset{4}{V_4}$
↑ normal

$S_4/A_4 = C_2$

normal in S_4? $\left\{ \begin{array}{l} \overset{4}{e=1} \\ (12)(34) \\ (13)(24) \\ (14),(23) \end{array} \right\}$

$V_4 \lhd S_4$ →

$\tau \sigma \tau^{-1}$ – same cycle type as σ

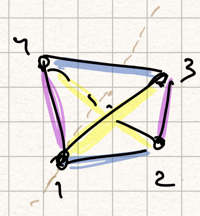


$V_4 \simeq C_2 \times C_2$
$\cap$
S_4

$V_4 \subset A_4$

$(1234)(567) \longrightarrow$

$(1537)(246)$



Rot(△) $= A_4$

Sym(△) $= S_4$

$A_4/V_4 \longrightarrow C_3$

$$\begin{tikzcd} \mathrm{Sym}(\triangle) = S_4 \arrow[r] \arrow[d, phantom, "\cup"] & S_3 \arrow[d, phantom, "\cup"] \\ A_4 \arrow[r] & C_3 \end{tikzcd}$$

permutations of pairs of opposite edges

$S_4 \overset{\lhd}{\underset{C_2}{\supset}} A_4 \overset{\lhd}{\underset{C_3}{\supset}} V_4 \overset{\lhd}{\supset} \{1\}$
↑ abelian

$A_4/V_4 \simeq C_3$

$S_4/A_4 = C_2$.

glued S_4 out of abelian groups C_2, C_3, V_4.

A_5 - simple

$G \longrightarrow [G,G]$ ← commutator subgroup.
generated by $[g,h] = ghg^{-1}h^{-1}$

$[g_1,h_1][g_2,h_2] . \quad [g_n,h_n]$.

$t[g,h] = t(ghg^{-1}h^{-1})t^{-1} =$

<u>Ex</u> $[G,G] \lhd G$.

$= \underbrace{tgt^{-1}}\,\underbrace{tht^{-1}}\,\underbrace{tg^{-1}t^{-1}}\,\underbrace{th^{-1}t^{-1}} =$

$G/[G,G]$ $\qquad = [tgt^{-1}, tht^{-1}]$.

abelian, maximal abelian quotient of G.

in quotient $G/[G,G]$.

$g, h \in G$ $\qquad \underline{ghg^{-1}h^{-1} = 1}$ $\qquad gh = hg$

G: gen, relations $\qquad$ to get $G/[G,G]$ add relations $gh = hg$

all pairs of generators commute

Ex $H \lhd G$

G/H - abelian $\Rightarrow$ $H \supset [G,G]$.

$\uparrow$ smallest subgroup $G/[G,G]$ - abelian

G_i/G_{i+1} - abelian

$G \supset G_1 \supset G_2 \supset G_3 \ldots \supset G_n = \{1\}$

$\cup$

$G \supset G^{(1)} = [G,G] \supset G^{(2)} = [G^{(1)}, G^{(1)}] \supset \ldots \; G^{(k)} = [G^{(k-1)}, G^{(k-1)}] = \{1\}$

iterated commutator subgroups of G.

Prop G is solvable iff $G^{(k)} = 1$ for some k.

for some non-triv. groups G, $[G,G] = G$.

If G is simple, non-abelian (not C_p) $\Rightarrow$ $[G,G] = G$

Such G is not solvable.

Example A_5.
$\uparrow$ simple, not abelian

$[A_5, A_5] = A_5$

S_5 not solvable.

$$\left.\begin{array}{l}\underline{\underline{\text{Prop}}}\quad \underline{H \triangleleft G}.\ \text{Then } G \text{ is solvable iff}\\ \qquad H,\ G/H \text{ are solvable.}\end{array}\right]$$

$\Leftarrow$

$$G/H = \bar{G}_0 \supset \bar{G}_1 \supset \dots \supset \underline{\bar{G}_k = \{1\}}$$

$$\begin{tikzcd} H \arrow[r, phantom, "\subset"] \arrow[d] & G \arrow[d] \\ \{1\} \arrow[r, phantom, "\subset"] & G/H \end{tikzcd}$$

$$\underline{H = H_0 \supset H_1 \supset \dots} \supset H_n = \{1\}$$

$$\begin{tikzcd} G = q^{-1}(\bar{G}_0) \arrow[d, "q"'] \arrow[r, phantom, "\supset"] & q^{-1}(\bar{G}_1) \arrow[d] & \dots \supset q^{-1}(\bar{G}_k) = H \\ G/H \supset \bar{G}_0 \arrow[r, phantom, "\supset"] & \bar{G}_1 \dots & \supset \bar{G}_k = \{1\} \end{tikzcd}$$

$$q^{-1}(\bar{G}_i)/q^{-1}(\bar{G}_{i+1}) \cong \bar{G}_i/\bar{G}_{i+1}$$

$$G \supset q^{-1}(\bar{G}_1) \supset \dots \supset q^{-1}(\bar{G}_k) = H \supset H_1 \supset \dots \quad H_n = \{1\}$$

$\Rightarrow$ G is solvable.

Corollary: S_5 is $\underline{\text{not}}$ solvable $\qquad S_5 \overset{\triangle}{\supset} \underline{A_5}$

$\underline{\text{Prop}}$ if $G \supset A_5 \Rightarrow G$ is not solvable.

otherwise G is solvable

$$G = G_0 \supset G_1 \supset \dots \supset G_n = \{1\}$$

$$G_0 \cap A_5 \underset{=}{\supset} G_1 \cap A_5 \underset{=}{\supset} G_2 \cap A_5 \underset{=}{\dots} \underset{=}{\supset} G_n \cap A_5 = \{1\}.$$

$''$

$A_5 = [A_5, A_5]$

$$\underline{G_i \cap A_5 / G_{i+1} \cap A_5} \subset \underline{\underline{G_i/G_{i+1}}}$$

Prop If a subgroup H of a group G is not solvable $\Rightarrow$ G is not solvable either.

Corollary S_n is not solvable $n \geq 5$. $S_n \supset A_5$

A_n is simple if $n \geq 5$.

Some other simple finite groups. S_n, $\vdots$

$G = GL(n, \mathbb{F}_p)$ n invertible $n \times n$ matrices coeff. in $\mathbb{F}_p$.

$\uparrow$
finite

vect space $/\mathbb{F}_p$

not simple, nontrivial center

$V = \mathbb{F}_p^n$. symmetries

$\lambda \in \mathbb{F}_p^*$

$$\lambda \cdot I = \begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$$ in the center of G $Z = Z(G)$.

most of the time $GL(n, \mathbb{F}_p)/Z$ - this is simple

$A_n, n \geq 5$.

Gal. groups of iterated root extensions $\sqrt[n]{c}$ are solvable.

$f(x) = x^n - c$ E - splitting field

$\uparrow$
contains n-th roots of unity.

$F \supset \mathbb{Q}$

α, β roots

$$\left(\frac{\alpha}{\beta}\right)^n = \frac{\alpha^n}{\beta^n} = c/c = 1.$$

$\alpha \to \alpha\omega$ also a root.

$\alpha, \alpha\omega, \alpha\omega^2, \ldots \alpha\omega^{n-1}$

$$x^n - c = (x-\alpha)(x-\alpha\omega)\dots(x-\alpha\omega^{n-1})$$

$\mathrm{Gal}(E/F)$ - solvable

E add a root α of $x^n - c$. $\alpha\omega^i$

$\cup$

K - add all n-th roots of unity

$\cup$

F $\sigma(K)=K$

$$\begin{tikzcd}
E \arrow[r, "\sigma"] & E \\
K \arrow[u, phantom, "\cup"] \arrow[r, "\sigma|_K"] & K \arrow[u, phantom, "\cup"] \\
F \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}$$

$\sigma \in G = \mathrm{Gal}(E/F)$ $\sigma(K)=K$

$\downarrow$

induces an aut of K

$$G \xrightarrow{\beta} \mathrm{Gal}(K/F) = H.$$

$$\ker\beta = \mathrm{Gal}(E/K)$$

G E

$\cup$ $\ker\beta$

K

$\cup$ $H = \mathrm{Gal}(K/F)$

F

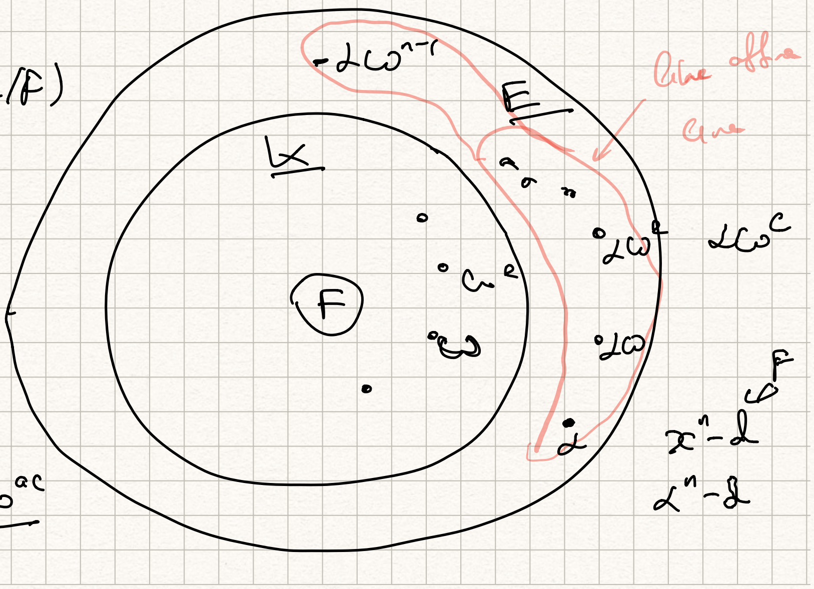
$G \supset \ker\beta \supset \{1\}$

$\sigma \in G$

$\underline{\sigma(\omega)} = \underline{\omega^a}$

describes action of σ on K

$\sigma(\underline{\omega^c}) = \sigma(\omega)^c = \underline{\omega^{ac}}$



$\sigma(\alpha) = \alpha\omega^{b}$ $\boxed{a\in(\mathbb{Z}/n)^*}$

$\sigma(\underline{\alpha\omega^c}) = \sigma(\alpha)\sigma(\omega^c) = \sigma(\alpha)\sigma(\omega)^c =$

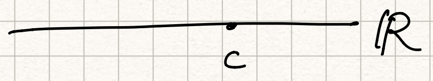
$= \alpha\omega^b\omega^{ac} = \alpha\omega^{\underline{ac+b}}.$ $\boxed{b\in\mathbb{Z}/n}$

$\sigma(\omega) = \omega^a$

$\sigma(\alpha) = \alpha\omega^b.$ $\sigma(\underline{\alpha}\omega^{\boxed{c}}) = \underline{\alpha}\,\omega^{\boxed{ac+b}}$

σ described by $(\underset{(\mathbb{Z}/n)^*}{\overset{\cap}{a}},\underset{\mathbb{Z}/n}{\overset{\cap}{b}})$ c a number

$c\in\mathbb{Z}/n \longleftrightarrow \mathbb{R}.$



affine transformation.

shifts by b. $c\mapsto c+b.$ scaling $c\mapsto ac$

$\underline{c}\mapsto\underline{ac+b}.$ $0\mapsto b.$

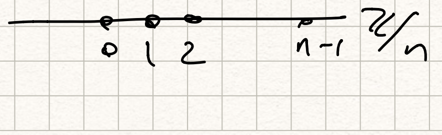
$$\begin{pmatrix} a & b\\ \underline{0} & \underline{1}\end{pmatrix}\begin{pmatrix} c\\ \underline{1}\end{pmatrix} = \begin{pmatrix} ac+b\\ 1\end{pmatrix}$$

group of matrices $H = \left\{\begin{bmatrix} a & b\\ 0 & 1\end{bmatrix} \middle| a\in\mathbb{R}^*, b\in\mathbb{R}\right\}$

Claim this is a group. (exercise)

$$\begin{pmatrix} a_1 & b_1\\ 0 & 1\end{pmatrix}\begin{pmatrix} a_2 & b_2\\ 0 & 1\end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2+b_1\\ 0 & 1\end{pmatrix} \leftarrow \text{mult. rules}$$

H - affine symmetries of $\mathbb{R}$
$\uparrow$
$\mathbb{Z}/n.$



H_n - affine symmetries of $\mathbb{Z}/n$

$$H_n = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, \underline{a} \in \underline{(\mathbb{Z}/n)^*},\ \underline{b} \in \mathbb{Z}/n \right\}.$$

$$\uparrow$$

$$\begin{pmatrix} a^{-1} & x \\ 0 & 1 \end{pmatrix}$$

<u>Claim</u> 1) This is a <u>finite</u> group

$$|H_n| = \varphi(n) \cdot n$$

$$\phi(n)$$

2) <u>H_n is solvable</u>

$$H_n \supset \widetilde{H}_n = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \,\middle|\, b \in \mathbb{Z}/n \right\} \supset \{1\}$$

check that normal in H_n

$\uparrow$ abelian

$$H_n / \widetilde{H}_n \simeq (\mathbb{Z}/n)^* \leftarrow \text{ab group inv. residues}$$

$\alpha, \alpha\omega, \alpha\omega^2, \ldots \quad \alpha\omega^{n-1}$ like a copy of $\mathbb{Z}/n$

$$\sigma(\underline{\alpha\omega}^{c}) = \underline{\alpha\omega}^{ac+b}$$

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c \\ 1 \end{pmatrix} = \begin{pmatrix} ac+b \\ 1 \end{pmatrix}$$

$G \subset H_n$ - aff symm of $\mathbb{Z}/n$.

$\uparrow$ $\quad$ ↑ solvable

G is solvable

$E \to$ splitting field $x^n - d$, (change c to d)

earlier

$\cup$

$F \qquad G = \mathrm{Gal}(E/F) \qquad G \subset H_n.$

solvable

$\underline{x}^{n_1} - \underline{d_1} \quad x^{n_2} - d_2 \quad x^{n_3} - d_3$

roots of 1 of order n_1

n_2

$\vdots$

n_k

$$F \subset E_1 \subset E_2 \subset E_3 \quad \subset E_k$$

$$\underbrace{d_2 \qquad d_3 \qquad \cdots}$$

<u>Prop</u> $G = \mathrm{Gal}(E_k/F)$ is solvable

First add all roots of unity of order

$n_1, n_2 .. n_k$ $n = \mathrm{lcm}(n_1, \dots, n_k)$

$x^n - 1$ roots of unity (add first)

C

$F \subset E_0 \subset E_1 \subset E_2 \quad .. \subset E_k$

$\leftarrow$ a single root of d_2 $x^{n_2} - d_2$.

$x^{\boxed{n_1}} - d_1$ add a single root α_1

$\alpha_1 \omega_1^c$

__Thm__ $G = Gal(E_k / F)$ is solvable.