1, HW 5 Ex 10.

Regard $\sigma \in Aut(G)$ as a bijective map from $G \to G$

Then we have $\sigma \in Sym(G) \simeq S_n$, $|G| = n$, $G = \{e = g_1, \dots, g_n\}$

$\sigma^2 = 1$ shows σ is a product of disjoint 2-cycle.

G_1 is those "fixed points" of σ

G_{-1} is those "support points + e" of σ

Remark. don't forget $\sigma \in Aut G$ so e is in both set.

Then $G = \langle G_1 \cup G_2 \rangle$ and $G_1 \cap G_2 = 1$ is obvious.

Now Let $h \in G$ $g \in G_1$

if $h \in G_1$ then $h^{-1}gh \in G_1$

if $h \in G_{-1}$

then 1° $h^{-1}gh = e$ $\Rightarrow$ only when $g = e$

If $h^{-1}gh \in G_{-1}$

2° $\sigma(h^{-1}gh) = h^{-1}g^{-1}h$

$$\sigma(h^{-1}gh) = hgh^{-1} = h^{-1}g^{-1}h$$

$\Rightarrow$ $h^2 g h^{-2} = g^{-1}$

$\sigma(h^2 g h^{-2}) = \sigma(g^{-1}) = g^{-1}$

$\sigma(h^2 g h^{-2}) = h^{-2} g^{-1} h^2$ $\Rightarrow$ $h^{-2} g^{-1} h^2 g = 1$ $\Rightarrow$ g commutes with h^2

Since $|G|$ odd, $\langle h^2\rangle = \langle h\rangle \Rightarrow g$ commutes with h

$\Rightarrow \sigma(h^{-1}gh) = \sigma(h^{-1}hg) = \sigma(g) = g \;\; \forall\, g \neq e$

$= g^{-1}$

$\Rightarrow$ Only possible condition: $\forall\, h \in G$, $h^{-1}gh \in G_1$

$\Rightarrow G_1 \trianglelefteq G \Rightarrow G = \langle G_1 \cup G_{-1}\rangle = G_1 G_{-1}$

$\boxed{\text{Nilpotent. Solvable. Series}}$

Def: A group G is said to be solvable if it has an abelian series. $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$, G_{i+1}/G_i is abelian.

Def. If G is a solvable group the length of a shortest abelian series in G is called the derived length of G

E.g. derived length $0 \Leftrightarrow G$ trivial

derived length $1 \Leftrightarrow$?

Def. A group G is called nilpotent if it has a central series that is $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ s.t. $G_{i+1}/G_i \subseteq Z(G/G_i)$

Def. If G nil. the length of a shortest central series of G is nilpotence class of G.

nil $\Rightarrow$ solvable. by def

Sol may not nil

E.g. $0 \Leftrightarrow$

$1 \Leftrightarrow$

S_3 is solvable but not nil.

$S_3 \trianglerighteq C_3 \trianglerighteq 1$ abelian series.

but $C_3/1 \not\subseteq Z(S_3/1)$ since $Z(S_3) = 1$

Def. derived series reach 1. $\Rightarrow$ G solvable.

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(n)} = 1. \quad \text{Since } G^{(i)}/G^{(i+1)} \text{ is abelian}$$

also G solvable $\Rightarrow$ derived series reach 1.

Let $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ is abelian series.

then $G^{(i)} \leq G_{n-i}$

proof it by induction.

when $i=0$, $G^{(0)} = G = G_n$

Suppose it's true for i

Then $G^{(i+1)} = (G^{(i)})' \leq (G_{n-i})'$, Since $G_{n-i}/G_{n-(i+1)}$ abelian.

it shows $(G_{n-i})' \leq G_{n-(i+1)}$

Thus $G^{(i+1)} \leq G_{n-(i+1)}$ done.

Remark: The intuition here is, derived series has the "fastest" speed "lower G to 1"

So the derived length of G = the length of derived series of G

Remark: Since $[x,y]^\theta = [x^\theta, y^\theta]$, $G^{(i)} \trianglelefteq G$ for all i

Thus we can say:

Every soluble group has a normal abelian series. i.e. an abelian series that all of those terms are normal in G

the derived series is an example.

Ref. $G^0 = G \trianglerighteq G^1 \trianglerighteq G^2 \trianglerighteq \cdots$ if it reach 1, i.e. $G^n = 1$, G is nilpotent.

where $G^1 = [G, G]$ $G^2 = [G, G^1]$

This is called lower central series.

$$G^i / G^{i+1} \subseteq Z(G/G^{i+1})$$

why? consider the commutator.

$\forall x \in G$ and $y \in G^i$

$[x, y] \in G^{i+1}$ shows in G/G^{i+1}

all elements of G^i/G^{i+1} lie in the center.

also we have upper central series:

$1 = Z_0(G) \trianglelefteq Z_1(G) \cdots$ if $Z_n(G) = G$ the G nil.

where $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$

$\boxed{\text{Thm}}$. Let $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ be a central series in a nil grp G. Then

(i). $G^i \leq G_{n-i}$ so $G^n \leq G_0 = 1$.

By induction, $i = 0$, $G^0 = G$ $G_n = G$ $G^0 \leq G_n$.

Suppose. $G^i \leq G_{n-i}$

$$G_{n-i}/G_{n-(i+1)} \subseteq Z(G/G_{n-(i+1)})$$

$\Rightarrow [G, G_{n-i}] \leq G_{n-(i+1)}$

$\Rightarrow G^{i+1} = [G, G^i] \leq [G, G_{n-i}] \leq G_{n-(i+1)}$ done.

(ii). $G_i \le Z_i(G) \Rightarrow Z_n(G) \geq G_n = G \Rightarrow Z_n(G) = n$.

By induction. $G_0 = 1 \le Z_0(G) = 1$.

suppose. $G_i \le Z_i(G)$.

$G_{i+1}/G_i \subseteq Z(G/G_i)$

$Z_{i+1}/Z_i = Z(G/Z_i)$

$[G, G_{i+1}] \subseteq G_i \le Z_i(G) = [G, Z_{i+1}]$

$\Rightarrow G_{i+1} \le Z_{i+1}(G)$. done.

(iii). nilpotence class of G = the length of upper series = the length of lower series.

Suppose. nil class of G is m.

by (i). lower series length $\le m$

by (ii) upper series length $\le m$

they are also central series

$\Rightarrow$ _____ = _____ = _____ ,

$\boxed{\text{Review}}$

class 1. Basic concepts of grp. ring. field.

class 2. Extension of $\mathbb{Q}$. α is algebraic. means $\exists f \in \mathbb{Q}[x]$, $f(\alpha)=0$

$[\mathbb{Q}(\alpha):\mathbb{Q}]$ = dimension of $\mathbb{Q}(\alpha)$ veiwed as a vector space over $\mathbb{Q}$.

$= \deg f$ s.t f irre poly over $\mathbb{Q}$ and $f(\alpha)=0$.

e.g. $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. $\{1, \sqrt{2}\}$

$\underline{x^2-2=0}$ $\quad \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2-2)$ basis $\{1, x\}$.

coset. lagrange thm. ($\underbrace{\text{Fermat. Euler}}_{\text{cyclic group}}$)

class 3.
class 4

3 isomorphic thm of grp

1°. $\varphi: G \to H$ homo. $G/\ker\varphi \cong \operatorname{im}\varphi$.

2°. $H, K \trianglelefteq G$, $H < K$ $\quad (G/H)/(K/H) \cong G/K$.

In other words. normal subgrp of G containing H and G/H has $1 \longleftrightarrow 1$ correspondence.

3°. $H. K \trianglelefteq G$ $\quad HK/K \cong H/H\cap K$

$$\begin{tikzcd} & HK \arrow[dl, dash] \arrow[dr, dash] & \\ H \arrow[dr, dash] & & K \arrow[dl, dash] \\ & H\cap K & \end{tikzcd}$$

diamond iso.

direct product. Cyclic group. Dihedral group. Symmetric group

D_{2n} s

class 5. $|G| = p^2$ then $G = \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$

G must be abelian

class 6. ring. field. — I write before.

subring. ideal. iso thm of ring

class 7. field extension. fin field.

class 8. FT FAG derived series. solvable.

class 9. Simplicity of A_n $n \geq 5$, Cayley Thm.

class 10. GA. Orbit - Stabilizer Thm. Sylow 1st Thm.

class 11. Sylow 2. 3 thm.

$\boxed{\text{Midterm}}$ 6 part. 120 full marks.

30%. so your point/4 ⇝ final grade

1°. field. field extension, * how to show f is irred?

⇒ show not ~~root~~ root exist in your base field F

is not enough.

e.g : $f \in \mathbb{Q}[x]$ $f = x^6+2x^2+1$ is not irre

although it has no rational roots.

take $\mathbb{Q}$ as e.g.

if f is reduc. f is product of deg 1 or 2 poly.

i.e. $\begin{cases} f \text{ has root} \\ f \text{ has no root but product of deg 2 poly.} \end{cases}$ ✓.

So. $\deg f = 1$ irr

$\deg f = 2$. show no root

$\deg f = 3$. show no root * ($f = gh$, $\deg g = 1$ $\deg h = 2$

f reduc $\iff$ f has root)

$\deg f = 4$. show 1° no root

2° $f \neq gh$. $\deg g = \deg h = 2$.

⋮

2° Ring. recall. ideal. * prime ideal.

if $a, b \in R$ s.t $ab \in I$ then $a \in I$ or $b \in I$.

e.g. $\mathbb{Z}$, (3), if $ab \in (3)$, $3|a$ or $3|b$.

unit (has multi. inverse) zero divisor : if $a \neq 0$ and $b \neq 0$

$R \setminus 0$ all unit called division ring but $ab = 0$, a, b called zero divisor.

Ring without zero divisor called domain.

Comm domain with identity called integral domain.

R comm. with iden.

*. maximal ideal.

$I \lhd R$ have $\nexists J$ $I \lhd J \lhd R$, $R/I \to$ field. Since it has no non-trivial ideal.

Can a unit $i \in I \lhd_{max} R$?

no $(i) = R \lhd I$ ↯.

3°. GA. Orbit - stab class equation.

very useful.

recall transitive. semiregular. regular.

4. Sylow. how to prove it (understand the approach but not recite it!)

application : some certain ordered group is not simple.

5. FTFAG.

1°. Give you a order. identify all type.

2°. Count element in a certain group.

subgroup in a certain group

6. New Def.

Have the ability to prove new things use what you have learned.