check – Monster gps.

SL_n is normal subgp. of GL_n.

If G is infinite, the statement does not hold.

G H $\quad G = \bigcup_{g \in G} gHg^{-1}$

$G = GL_n(\mathbb{C})$ $\quad H =$ Upper triangular.

Every invertible matrix (over $\mathbb{C}$) can be diagonalized by an upper tar matrix.

Recall

Sylow's Thm → $|G| = p^r m \quad p \nmid m$

Existence (i) $\exists$ a subgp. of order p^r — Sylow p-subgp.

Relation (ii) Any 2 sylow-p-subgp. are conjugate.

$$P_1 = g P_2 g^{-1}$$

Number (iii) n_p – the no. of Sylow p-subgp.

$$n_p \equiv 1 \mod p. \qquad \text{Also } n_p \mid m.$$

Simple Groups:

A gp. G is called simple if it has no non trivial normal subgp.

Ex→ $\mathbb{Z}_p$ is simple.

$|G| = pq \quad p<q$ is not simple

$|G| = p^2 q$

$|G| = pqr$

The alternating group of degree n is simple. 12
$(n \neq 4)$

PAGE NO.:
DATE: / /

$\boxed{A_n \text{ is simple if } n \geq 5.}$

trivial
$\hookrightarrow A_2 \to$ simple
$\mathbb{Z}_3 \cong A_3 \to$ simple
$A_4 \to$ not simple.

$$A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

$\{1, (12)(34), (13)(24), (14)(23)\}$ is normal subgp.

not simple.

<u>Claim</u> A_n is generated by 3-cycles.

$$\sigma = (\ )(\ )(\ ) \ldots$$

$$(12)(34) = (123)(234)$$

$$(12)(23) = (123)$$

<u>Claim</u> Any two 3-cycles are conjugate in A_n. $A_n \subset S_n$

(We have proved this result for S_n.)

$$(123) = \pi \sigma \pi^{-1} \qquad \pi \in S_n$$

To show $g \in A_n$ (here $g = \pi$)

If $\pi \in A_n$ ✓

If not, let $\pi' = (45)\pi \in A_n$
(π is an odd permutation)

$$\pi' \sigma \pi'^{-1} = (45)\pi\sigma\pi^{-1}(45)$$
$$= (45)(123)(45)$$
$$= (123).$$

T. P. $\Rightarrow A_n$ is simple if $n \geq 5$

Suppose N be a non-trivial normal subgp.

$$\sigma \in N$$

Claim: N contains a 3-cycle

(If N contains a 3-cycle, then it contains all the 3-cycles.)

$$\sigma = \pi_1 \pi_2 \dots \pi_k$$

Case-1 Atleast one of them have length ≥ 4.

WLOG, assume that $\pi_1 = (1\,2\,3 \dots r)$ $r \geq 4$.

$$\sigma = (1\,2 \dots r)\, \pi_2 \pi_3 \dots \pi_k$$

Let $\phi = (1\,2\,3)$

$$\phi \sigma \phi^{-1} = \underbrace{(1\,2\,3)(1\,2 \dots r)(1\,3\,2)(1\,r\,r{-}1 \dots 2)}\sigma$$

$(1\,2\,3 \dots r)^{-1} = (1\,r\,r{-}1 \dots 2)$

$$= (1\,2\,4)\,\sigma$$

$$(1\,2\,4) = \phi \sigma \phi^{-1} \sigma^{-1} \in N$$

Case-2 All of them have length ≤ 3 and atleast 2 of them have length 3.

$$\sigma = (1\,2\,3)(4\,5\,6)\, \pi_3 \dots \pi_k$$

PAGE NO.:
DATE: / /

$\phi = (124)$

$$\phi\sigma\phi^{-1} = (124)(123)(456)(142)(465)(132)\sigma$$

$$= (12534)\sigma \longrightarrow \text{Apply Case-1}$$

Case-3 All of them have length ≤ 3 and exactly one of them have length 3.

$$\sigma = (123)\underbrace{\pi_2\pi_3\ldots\pi_k}_{\text{all transpositions}}$$

$$\sigma^2 = (132) \in N.$$

Case-4 All of them have length 2.

$$\sigma = (12)(34)\pi_3\ldots\pi_k.$$

$\phi = (123)$

$$\phi\sigma\phi^{-1} = (123)(12)(34)(132)(34)(12)\sigma$$

$$= (13)(24)\sigma$$

$$(13)(24) \in N \quad - (1)$$

$\psi = (135)$

$$N \ni (135)(13)(24)(153) = (24)(35) \in N \quad (2)$$

From (1) & (2) $(13)(24)(24)(35)$

$$= (135) \in N.$$

Scanned with OKEN Scanner

PAGE NO :
DATE : / /

Inversion

$$inv(\sigma) = \{(i,j) : i<j \text{ and } \sigma(i) > \sigma(j)\}$$

Recall,

pq is not simple
p^2q "
pqr "

- $|G| = pq$ $p<q$

$n_p \equiv 1 \mod p$ $n_p | q$
$n_q \equiv 1 \mod q$ $n_q | p$.

$n_q = 1$

C_q normal (not simple proved)

If $p \nmid q-1 \Rightarrow n_p = 1$ C_p.

Claim, $G = \underbrace{C_p}_{\langle x \rangle} \times \underbrace{C_q}_{\langle y \rangle}$ ($\mathbb{Z}_p \times \mathbb{Z}_q$)   normal

$C_p \cap C_q = \{1\}$
$G = C_p C_q$.

cyclic $\rightarrow$ $G = \langle xy \rangle$

x & y commute as "commutator"

$xyx^{-1}y^{-1} \in C_p \cap C_q$
$\Rightarrow xyx^{-1}y^{-1} = 1$
$xy = yx$.

If $p | q-1$ C_q - normal
C_p

$$G = C_p \rtimes C_q$$

If $|G| = 15 = 3 \times 5$

$3 \nmid 5-1$, "So any gp. of order 15 is cyclic."

- A group of order p^2q is not simple.

$|G| = p^2q$

$n_p \equiv 1 \bmod p$ $\quad n_p | q$

$n_q \equiv 1 \bmod q$ $\quad n_q | p^2$

Assume both n_p & $n_q > 1$. We should get a contradiction.

$n_p > 1$ & $n_q > 1$

$n_p = q$ $\quad n_q = p$ or p^2

$C_1 \quad C_2 \quad \cdots \quad C_{n_q}$ No. of elements having order q

$q \quad q \quad \cdots \quad q$ $= n_q(q-1)$

If $n_q = p^2 \Rightarrow p^2(q-1)$

Elements left $= p^2$

$\Downarrow$

$n_p = 1 \quad \Rightarrow\Leftarrow$

If $n_q = p$.

$p \equiv 1 \bmod q$ $\quad n_p = q \quad q \equiv 1 \bmod p$

$\Rightarrow q < p$ $\quad \Rightarrow p < q$

$\Rightarrow\Leftarrow$.

PAGE NO
DATE / /

- A gp. of order pqr is not simple. $\boxed{p<q<r}$

$$|G| = pqr.$$

$n_p \equiv 1 \bmod p$ $\quad$ $n_q \equiv 1 \bmod q$ $\quad$ $n_r \equiv 1 \bmod r$

$n_p \mid qr$ $\quad$ $n_q \mid pr$ $\quad$ $n_r \mid pq$

Assume $n_p > 1$, $n_q > 1$ & $n_r > 1$

$\Rightarrow n_r = pq$ $\quad$ (as $n_r \neq p$ and $n_r \neq q$)

$n_r = pq$ $\quad$ $n_q \geq p$, $\geq r$ both are true. $\quad$ $n_p \geq q$

$$pq(r-1) \qquad p(q-1) \qquad q(p-1)$$

$$pqr - \cancel{pq} + \cancel{pq} - p + qp - q + \underbrace{1}_{\text{identity}}$$

$$\Rightarrow pqr + (1-p)(1-q) > pqr$$

$\Rightarrow\!\!\!\!\times$

ore's conjecture

Q. finite simple gp. G

Claim: Every element of $g = xyx^{-1}y^{-1}$ for some $x, y \in G$.

OR equivalently

$G \times G \to G$ map is onto.

$(x, y) \to xyx^{-1}y^{-1}$

Classification of finite abelian gp →

⊛ Any finite abelian g.p. is a direct pdt. of cyclic gps.

Cauchy thm :– If $p \mid |G|$ $\exists$ an element of order 'p'.

lemma: Let G be a finite abelian p gp. s.t. G has a unique subgp. of order p. Then G is cyclic.

Pf :– induction used $|G| = p^r$

$\exists$ a subgp. of order p as $p \mid |G|$
→ $\exists$ an element of order 'p'

Make cyclic gp. of that element. → order p ✓

$H \subseteq K = \ker \phi = \{x : x^p = 1\}$

Claim: $K = H$. $\underbrace{x \in K}_{x \text{ has order } p}$ → $\underbrace{x \in H}_{\langle x\rangle \text{ has order } p \text{ unique}}$

$K \subseteq H$.

$\phi : G \to G$ gp. homo.
$x \to x^p$ as G is abelian.

$\underbrace{\frac{G}{H}}_{\text{order } p^{k-1}} \cong \phi(G) \subseteq \underbrace{G}_{\text{order } p^k}$

$\langle xH \rangle = \frac{G}{H}$ As cyclic by induction.

Claim: $G = \langle x \rangle$

PAGE NO.:
DATE: / /

Recall,

Let G be an abelian p-gp. s.t. G has exactly one subgp. of order p. Then G is cyclic.

Lemma, Let G be a finite abelian p-gp. Let C be a cyclic subgp. of G of max. order. Then $\exists H$ s.t. $G = C \times H$.

Pf If G is cyclic. Take $H = \{e\}$ ✓

By induction on order of G.

If G is not cyclic $\Rightarrow$ G has atleast 2 cyclic subgp. of order p. (contrapositive of above lemma)

$\Downarrow$

$\exists K$ s.t. $K \not\subseteq C$ $(|K| = p)$ as C is cyclic, it has exactly 1 subgp. of order p.

$\Downarrow$

$K \cap C = \{e\}$

2nd isomorphism thm $\rightarrow$ $\dfrac{CK}{K} \cong \dfrac{C}{C \cap K} \cong C$

cyclic subgp. $\leq \dfrac{G}{K}$

Let $\langle xK \rangle = \dfrac{CK}{K}$ ← We want to show $\dfrac{CK}{K}$ is cyclic of max. order.

$|C| = o(xK) \mid o(x) \leq |C|$ ✓

By induction, $\dfrac{G}{K} = \dfrac{CK}{K} \times \dfrac{H}{K}$

$\Rightarrow$

We can also get here directly by Sylow's thm.

PAGE NO.:
DATE: / /

also k/a structure thm.

$G = CK H = C \cdot H$

$$\underset{\{e\}}{\underset{\parallel}{C \cap H}} \subset \underset{\{K\}}{\underset{\parallel}{CK \cap H}} \Rightarrow G = C \times H.$$

Fundamental Thm. of Finite Abelian Gp:-

- Every finite abelian gp. can be uniquely written as a direct pdt. of cyclic subgps.

Pf → G

Let $p \mid |G|$

$G_p = \{g \in G : o(g) = p^k\}$ for some k. ← P-gp (Pf. by contradiction)

$G_p' = \{g \in G : p \nmid o(g)\}$

$G_p \cap G_p' = \{e\}$

We want to show $G = G_p \times G_p'$

$g \in G$ $\quad o(g) = p^r m \quad p \nmid m \quad g^{p^r m} = 1$

$g^m \in G_p$ $\qquad (p^r, m) = 1$

$g^{p^r} \in G_p'$ $\qquad sp^r + tm = 1$

$g = g^1 = g^{sp^r + tm}$

$= (g^{p^r})^s (g^m)^t$

We can also get here directly by Sylow's thm.

Similar argument →

$G = G_{p_1} \times G_{p_2} \times \dots \times G_{p_t}$

$\Longrightarrow$ Now proof that they are cyclic.

G_{p_1} $\longrightarrow$ C_1 be a cyclic subgp. of max. order in G_{p_1}

$$G_{p_1} = C_1 \times \underbrace{H_1}_{I}$$ (by last lemma)

break H, and so on finite steps

$$\Rightarrow G_{p_1} = C_1 \times C_2 \times \dots \times C_k$$

$$\underbrace{p_1^{k_1} \quad p_1^{k_2} \quad \dots \quad p_1^{k_k}}$$

I can rearrange such that $k_1 \geq k_2 \geq k_3 \dots \geq k_k$

$$G = \boxed{\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_1^{k_2}} \times \dots \times \mathbb{Z}_{p_1^{k_1}}} \times \boxed{\mathbb{Z}_{p_2^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \dots \times \mathbb{Z}_{p_2^{\cdot}}} \times \dots$$

~~Bringing all highest~~ factors in beginning

$$G = \boxed{\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{m_1}} \times \dots \times \mathbb{Z}_{p_k^{s_1}}} \times \boxed{\mathbb{Z}_{p_1^{k_2}} \times \mathbb{Z}_{p_2^{m_2}} \dots} \times \dots$$

$$= \mathbb{Z}_{p_1^{k_1} p_2^{m_1} \dots p_k^{s_1}} \times \mathbb{Z}_{\dots} \dots$$

$$G = \mathbb{Z}_{D_1} \times \mathbb{Z}_{D_2} \times \dots \times \mathbb{Z}_{D_k}$$ ✓

highest order

$$D_k \mid D_{k-1} \mid D_{k-2} \dots \mid D_2 \mid D_1$$

uniqueness

$D_1 = E_1$ then by induction $D_i = E_i$

$$G = \mathbb{Z}_{E_1} \times \mathbb{Z}_{E_2} \times \dots \times \mathbb{Z}_{E_k}$$

PAGE NO.
DATE:

$|G| = 24 = 2^3 \cdot 3^1$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
$3 = 1 + 1 + 1$
$3 = 2 + 1$ $\quad \mathbb{Z}_{2^2} \times \mathbb{Z}_2$
$3 = 3 + 0$ $\quad \mathbb{Z}_{2^3}$

$1 = 1 + 0$ $\quad \mathbb{Z}_3$

$|G| = p^k q^t$ Write partitions of k and t.

Q.1 $\mathbb{R}$ acts on $\mathbb{C}$ by $\quad a \in \mathbb{R} \quad z \in \mathbb{C}$

$a \cdot z = e^{ia} \cdot z$

Orbit $\rightarrow$ circle of radius $|z|$

$O_z = \{ e^{ia} z : a \in \mathbb{R} \} = \{ z' : |z'| = |z| \}$

$G_z = \{ a \in \mathbb{R} : e^{ia} z = z \} = \{ 2n\pi : n \in \mathbb{Z} \}$

Q.2 $H, K \rightarrow$ subgp. Order of HK? by orbit stabiliser Thm.

Grp $\rightarrow H \times K$ external direct pdt.
HK set

$(H \times K) \times HK \rightarrow HK$

$(h,k) \quad h_1 k_1 \mapsto h h_1 k_1 k^{-1}$

$O_{h'k'} = HK$.

$h'k' \rightarrow h_1 k_1$

as $(h_1 h'^{-1}, k_1^{-1} k')$

$G_1 = \{ (h,k) : h k^{-1} = 1 \}$
$= H \cap K$.

$|H||K| = |H \times K| = |HK| \, |H \cap K|$ ✓

1+1+1+1+1   1+1+1+1+2   1+1+1+3   1+1+4   0+5   1+4   2+3   2+2+1

Q.3   G: nontrivial finite gp.

$$G \times X \to X \qquad |X| \geq 2$$

no. of orbits $= 1$

T.S. $\exists g \in G$ s.t. g has no fixed pt.

$\therefore \exists g$ s.t. $g \cdot x \neq x$ $\forall x \in X$.

Burnside's Lemma →

$$\text{No. of orbits} = \frac{1}{|G|} \sum |X^g|$$

$$|X^g| = \{x \in X : gx = x\}$$

$$\to |G| = \sum |X^g|$$

Assume no fixed pt. $|X^g| \geq 1$ $\forall g$

for identity element $X^g \geq 2$ ✓

$\Rightarrow \Leftarrow$

Q.5 $5 = 5+0$
$= 4+1$
$= 3+2$
$= 3+1+1$
$= 2+1+1+1$
$= 2+2+1$
$= 1+1+1+1+1$

7 total.

$(12)(34)$
$(13)(45)$
$\vdots$

Any 2 permutation of same cycle type are conjugate to each other.

for $n \geq 3$ $|G| = |Z(G)| + \sum |C_x|$

$Z(G) = id.$ $\downarrow$ $\downarrow$ $\downarrow$

$n!$ 1 write all terms. ✓

(b) $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$

$Z(Q_8) = \{1, -1\}$

$C_i = \{gig^{-1} : g \in Q_8\}$

$\{i, -i\}$

$8 = 2 + 2 + 2 + 2$

$\{j, -j\}$

$\{k, -k\}$ 2, conjugacy class

(c) $A_4 = \{1, (123), (132), (234), (243), (134), (143), (124), (142), (12)(34), (13)(24), (14)(23)\}$

$Z(A_4) = \{1\}$ 1 conjugacy class

$(12)(34)\ (123)\ (34)(12) = (142)$

$(13)(24)\ (123)\ (24)(13) = (134)$

$(14)(23)\ (123)\ (23)(14) = (243)$

$\{(123), (243), (134), (142)\}$

$\{(132), (234), (143), (124)\}$

$12 = 1 + 4 + 4 + 3.$

$\Longrightarrow$

PAGE NO.:
DATE: / /

(a) $D_n = \{1, x, x^2, \ldots, x^{n-1}, \boxed{y, xy, x^2y, \ldots, x^{n-1}y}\}$

$x^n = y^2 = 1$

$yx = x^{-1}y$

$$Z(D_n) = \begin{cases} 1 & \text{, if } n \text{ is odd} \\ \{1, x^{n/2}\} & \text{, if } n \text{ is even} \end{cases}$$

n is odd

For some x^k:

$$x^i x^k x^{-i} = x^k$$

$$x^i y \, x^k y \, x^{-i} = x^{-k}$$

$\{x^k, x^{-k}\}$ $k = 1, 2, \ldots, \frac{n-1}{2}$

Others all have same $\{y, xy, x^2y, \ldots, x^{n-1}y\}$.

$C_y = \{y, xy, x^2y, \ldots x^{n-1}y\}$

n → odd $2n = 1 + \underbrace{2 + 2 + \ldots + 2}_{\frac{n-1}{2}} + n$ ✓

n → even

$C_y = \{y, x^2y, x^4y, \ldots\}$

and other $= \{xy, x^3y, \ldots\}$

$2n = 2 + \underbrace{2 + 2 + \ldots + 2}_{\frac{n-2}{2}} + \frac{n}{2} + \frac{n}{2}$ ✓

Q.9 $|G| = p^a$

T.S. G has a normal subgp. of order p^b, $\forall\, 0 \le b \le a$

Ans. G is a p-gp. Its center is non-trivial

$\Rightarrow$

Scanned with OKEN Scanner

$$H \leq Z(G) \neq \{e\}$$
$$|H| = p$$

Use Induction $\longrightarrow$ $\left|\frac{G}{H}\right| = p^{a-1}$

$$\left|\frac{K_1}{H}\right| \quad \left|\frac{K_2}{H}\right| \quad \cdots \quad \left|\frac{K_{a-1}}{H}\right|$$
$$p \qquad p^2 \qquad \cdots \qquad p^{a-1}$$

Recall,

Fundamental Thm. of finite abelian gps. –

– Every finite abelian gp. can be written as a direct (uniquely) pdt. of cyclic gps.

$$G = \mathbb{Z}_{D_1} \times \mathbb{Z}_{D_2} \times \cdots \times \mathbb{Z}_{D_k}.$$

$$D_{i+1} \mid D_i \quad \forall i.$$

(No such thm. for infite abelian gps.)

Finitely generated gps.

– We say G (gp.) is generated by S (set) if every element of G can be written as a pdt. (inverse also allowed.) of elements of 'S'.

$$g = s_1 s_2^{-1} s_3^{-1} \cdots$$

– If S is finite, then $G \rightarrow$ finitely generated gp.

$\longrightarrow$

Modules over PID.

$H \subset K \subset G$

normal in K — normal in G

H need not be normal in G.

PAGE NO.:
DATE: / /

(Exam)

Structure Thm for finitely generated abelian gp →

Every finitely generated abelian gp. G can be uniquely written as →

$$G \cong \mathbb{Z}^{(r)} \times \underbrace{(\mathbb{Z}_{D_1} \times \mathbb{Z}_{D_2} \times \cdots \times \mathbb{Z}_{D_k})}_{\text{torsion of the abelian gp.}}$$

$D_{i+1} \mid D_i$

r = rank of the abelian gp.

→ Let G be a gp. We say G has a subnormal series if we have a chain of subgps.

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{1\}$$

s.t. G_{i+1} is normal in G_i $\forall i$

⇒ $Q_8 \supseteq \{1, -1, i, -i\} \supseteq \{1, -1\} \supseteq \{1\}$ → Normal & Subnormal both

$D_4 \supseteq \{1, y, x^2, x^2y\} \supseteq \{1, y\} \supseteq \{1\}$ → Not normal, Subnormal ✓.

$S_n \supseteq A_n \supseteq \{1\}$

↳ simple (no non-trivial normal subgps)

$A_4 \supseteq \{1, (12)(34), (13)(24), (14)(23)\} \supseteq$

$\{1, (12)(34)\}$

$\supseteq \{1\}$

PAGE NO :
DATE : / /

$\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq \ldots \supseteq \{1\}$
as $\mathbb{Z}$ is abelian every subgp. is normal.

→ G be a gp. We say G has a composition series if ∃ a chain of subgps.

n → length of composition series.

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \{1\} \text{ s.t.}$$

G_{i+1} is normal in G_i ∀ i

and $\dfrac{G_i}{G_{i+1}}$ is simple ∀ i.

$G \supseteq N$ → max. normal subgp.

⇕

Claim : $\dfrac{G}{N}$ is ~~norma~~ simple.

Use correspondence thm.

$$\frac{H}{N} \subseteq \frac{G}{N} \Rightarrow \Leftarrow$$

Claim → Every finite gp. has a composition series.

Ex → $\underbrace{Q_8 \supseteq \{1,-1,j,-j\}}_{\mathbb{Z}_2} \supseteq \underbrace{\{1,-1\}}_{\mathbb{Z}_2} \supseteq \{1\}$ } simple

$S_4 \supseteq A_4 \supseteq \{1, (12)(34), (13)(24), (14)(23)\}$

$\underbrace{S_n \supseteq A_n}_{\mathbb{Z}_2} \supseteq \underbrace{\{1\}}_{A_n}$ $n \geq 5$ } simple

Proof by induction on order of G.

PAGE NO.:
DATE: / /

$\mathbb{Z}$ has no composition series.

$$\mathbb{Z} \geq 2\mathbb{Z} \geq 4\mathbb{Z} \geq \ldots \geq \{1\}$$

$$\mathbb{Z} \geq P_1\mathbb{Z} \geq P_1P_2\mathbb{Z} \geq \ldots \geq \{1\}$$ Never goes to 1.

Claim → Every finite gp. has a composition series.

Ex → Infinite gp. which have composition series

$f: \mathbb{N} \to \mathbb{N}$ $\quad S_\infty \geq A_\infty \geq \{1\}$.

$PSL_n(\mathbb{Q}) \longrightarrow \dfrac{SL_n}{\underbrace{Z(SL_n)}_{\text{center}}}$ } quotient gp.

Jordan-Hölder's Theorem:-

Let G be a gp. Suppose G has 2 composition series.

$$G = G_0 \geq G_1 \geq G_2 \geq \ldots \geq G_n = \{1\}$$

$$G = H_0 \geq H_1 \geq H_2 \geq \ldots \geq H_m = \{1\}$$

Then $m = n$ and $\forall i$ $\dfrac{G_i}{G_{i+1}} \cong \dfrac{H_k}{H_{k+1}}$ for some 'k'.

$$Q_8 \geq \{1, -1, i, -i\} \geq \{1, -1\} \geq \{1\}$$

$$Q_8 \geq \{1, -1, j, -j\} \geq \{1, -1\} \geq \{1\}.$$

$$\mathbb{Z}_6 \overset{\mathbb{Z}_2}{\geq} \{0, 2, 4\} \overset{\mathbb{Z}_3}{\geq} \{0\}$$

$$\mathbb{Z}_6 \overset{\mathbb{Z}_3}{\geq} \{0, 3\} \overset{\mathbb{Z}_2}{\geq} \{0\}$$

Q. Suppose G has a composition series.

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

N be a normal subgp. of G.
Does N also have a composition series?

Ans. We will use the fact — H & N be subgp. of G.
(Not exactly but motivation) N be normal in G.
$H \cap N$ is a normal subgp. of H.

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

Yes,

$$\underset{G\cap N}{\overset{\shortparallel}{N}} \supseteq \underset{\underset{\text{Normal}}{\underbrace{G_1 \cap N}}}{\overset{\shortparallel}{N_1}} \supseteq \underset{\underset{\text{Normal}}{\underbrace{G_2\cap N}}}{\overset{\shortparallel}{N_2}} \supseteq \dots \supseteq \underset{G_n \cap N}{\overset{\shortparallel}{N_n}} = \{1\} \quad \text{Subnormal series}$$

Proof:

Let $x \in N_2 = G_2 \cap N$ and $g \in N_1 = G_1 \cap N$

T.P. $gxg^{-1} \in N_2$
(N_2 is normal in N_1)

$gxg^{-1} \in G_2$ — $x \in G_2$ & $g \in G_1$, G_2 is normal in G_1

$gxg^{-1} \in N$ — $g, x \in N$, $gxg^{-1} \in N$

$$\Rightarrow gxg^{-1} \in G_2 \cap N = N_2$$

Now checking quotients — Use 2nd Isomorphism thm

To show simple $\rightarrow$

$$\frac{N_i}{N_{i+1}} = \frac{N\cap G_i}{N \cap G_{i+1}} = \frac{N\cap G_i}{(N\cap G_i)\cap G_{i+1}} = \frac{(N\cap G_i)G_{i+1}}{G_{i+1}}$$

If H is normal in G, Then $\frac{H}{N}$ is normal in $\frac{G}{N}$.

PAGE NO :
DATE : / /

$$\frac{N_i}{N_{i+1}} = \frac{(N \cap G_i)\, G_{i+1}}{G_{i+1}}$$

$(N \cap G_i)\, G_{i+1}$ is normal in G_i

$$\underbrace{\frac{N_i}{N_{i+1}}}_{\downarrow} \cong \frac{(N \cap G_i)\, G_{i+1}}{G_{i+1}} \text{ is normal in } \underbrace{\frac{G_i}{G_{i+1}}}_{\downarrow}$$

trivial or $\frac{G_i}{G_{i+1}}$ $\Longleftarrow$ simple.

$\downarrow$

simple

So N has a composition series.

PAGE NO.:
DATE: / /

Jordan Hölder's Theorem -

Let G be a gp. Suppose G has 2 composition series.

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

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \dots \supseteq H_m = \{1\}$$

Then $m = n$ and for $i \in \{1, 2, \dots, n\}$

$$\frac{G_i}{G_{i+1}} \cong \frac{H_k}{H_{k+1}} \text{ for some } 'k'.$$

Proof → $G = G_0 \supseteq G_1 \supseteq G_2 \dots \supseteq G_n = \{1\}$ — (1)

$\left\{ \frac{G_0}{G_{i+1}} , i = 0, 1, \dots, n-1 \right\}$

use induction on length of composition series.

$G = H_0 \supseteq H_1 \supseteq H_2 \dots \supseteq H_m = \{1\}$ — (2)

$\left\{ \frac{H_i}{H_{i+1}} , i = 0, 1, \dots, m-1 \right\}$

Base case: If $G = G_0 \supseteq \{1\}$ $n = 0$

$\Rightarrow G_0$ is simple $\Rightarrow H_0$ is simple.

$H_0 \supseteq \{1\}$ $m = 0$ ✓

Case-1: $G_1 = H_1$
↓
length$(n-1)$ by induction $n = m$ ✓.

Case-2: $G_1 \neq H_1$ $D = \overset{\text{normal}}{G_1} \cap \overset{\text{normal}}{H_1} \longrightarrow$ normal

As D is normal $\Rightarrow$ D has a composition series.

$$D = D_2 \supset D_3 \supset \dots \supseteq D_k = \{1\}$$

$\Longrightarrow$

Quotients of ③ & ④ $\left\{\frac{G}{G_1}, \frac{G_1}{D}, \frac{D}{D_3}, \ldots, \frac{D_{k-1}}{D_k}\right\}$ $\left\{\frac{G}{H_1}, \frac{H_1}{D}, \frac{D}{D_3}, \ldots, \frac{D_{k-1}}{D_k}\right\}$

Permute

PAGE NO.:
DATE: / /

$$G = G_0 \supseteq G_1 \supseteq \underset{}{\overset{D}{\overset{\|}{D_2}}} \supseteq D_3 \supseteq \ldots \supset D_k = \{1\} \quad — ③$$

simple ✓

Subnormal series.

$$G = H_0 \supseteq H_1 \supseteq \underset{\underset{D}{\|}}{D_2} \supseteq D_3 \supseteq \ldots \supseteq D_k = \{1\} \quad ④$$

Trying to prove $\frac{G_1}{D_2}$ & $\frac{H_1}{D_2}$ are simple →

$$H_1 \subseteq \underset{\text{normal}}{G_1H_1} \subseteq G$$

but H_1 is maximal normal in G

so $G_1H_1 = H_1$ or $G_1H_1 = G$ ✓

$G_1H_1 = H_1 \Rightarrow$

⇓

$G_1 \subset H_1 \subset G$

$\Rightarrow G_1 = H_1$

$\Rightarrow \Leftarrow$ (as $G_1 \neq H_1$ case)

$$\frac{G}{G_1} = \underbrace{\frac{G_1H_1}{G_1} \cong \frac{H_1}{G_1 \cap H_1}}_{2^{nd}\text{ iso. thm.}} \quad (G_1 \cap H_1 = D)$$

$$\Rightarrow \boxed{\frac{G}{H_1} \cong \frac{G_1}{D}}$$

simple

simple ✓ similarly $\frac{H_1}{D}$ simple ✓

③ & ④ are composition series of equal length

① & ③ ⇒ $n = k$

② & ④ ⇒ $m = k$

$\boxed{n = m}$ ✓

→ Proof of Fundamental Thm. of Algebra by Jordan Holder's thm –

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

$$\mathbb{Z}_n \supset \underset{\substack{\downarrow \\ \text{proper max. divisor of } n}}{\mathbb{Z}_{d_1}} \supset \mathbb{Z}_{d_2} \supset \cdots \supset \mathbb{Z}_{d_s} = \{1\}$$

$$\frac{\mathbb{Z}_n}{\mathbb{Z}_{d_1}} \cong \underset{\substack{\downarrow \\ \text{simple}}}{\mathbb{Z}_{p_1}}, \quad \frac{\mathbb{Z}_{d_1}}{\mathbb{Z}_{d_2}} \cong \underset{\substack{\downarrow \\ \text{simple}}}{\mathbb{Z}_{p_2}}, \text{ and so on} \ldots$$

$$o(G) = o\left(\frac{G}{H}\right) \cdot o(H)$$

$$n = \underbrace{p_1 p_2 \cdots p_s}_{\text{may be repeating}} \rightarrow \text{Existence} \checkmark$$

By J.H. thm → uniqueness ✓.

$$\Rightarrow G^{(1)} = \overset{\text{Commutator subgp.}}{[G\ G]} = \langle [x,y] : x,y \in G \rangle$$

where $\overset{\text{Commutator}}{[x,y]} = xyx^{-1}y^{-1}$

Is $G^{(1)}$ normal ? Yes

$$g[xy]g^{-1} = g\,x\,g^{-1}g\,y\,g^{-1}g\,x^{-1}g^{-1}g\,y^{-1}g^{-1}$$

$$= (gxg^{-1}).(gyg^{-1}).(gxg^{-1})^{-1}.(gyg^{-1})^{-1}$$

$$= [gxg^{-1}\ gyg^{-1}] \in G^{(1)} \checkmark$$

OR

$$\underset{z}{[xy]^{-1}}\ \underset{g}{g}\ \underset{z^{-1}}{[xy]}\ \underset{g^{-1}}{g^{-1}} = [z\ g] \in G^{(1)}$$

$$\Rightarrow g[xy]g^{-1} \in G^{(1)} \checkmark$$

PAGE NO:
DATE: / /

$G^{(1)} = [G\ G] = \langle [x,y] : x, y \in G \rangle$

$G^{(2)} = [G^{(1)}\ G^{(1)}] = \langle [z_1, z_2] : z_1, z_2 \in G^{(1)} \rangle$

$\vdots$

$G^{(n)} = [G^{(n-1)}\ G^{(n-1)}]$

Def^n G is <u>solvable</u> if $\exists n$ s.t. $G^{(n)} = \{1\}$

Ex → For abelian grps. $G^{(1)} = id.$

→ If $G = S_n$

We can say $[S_n\ S_n] \subseteq A_n$ (obvious) ✓

Now we show that $A_n \subseteq [S_n\ S_n]$

As A_n is generated by 3 cycles.

$$\overset{}{(123)} = \overset{x}{(13)}\overset{y}{(23)}\overset{x^{-1}}{(13)}\overset{y^{-1}}{(23)} \in [S_n\ S_n]$$

Every 3 cycle $\in [S_n\ S_n]$

$\Rightarrow A_n \subseteq [S_n\ S_n]$

$\therefore A_n = [S_n\ S_n]$

Recall

$G^{(1)} = [G\ G] = \langle [x,y] : x, y \in G \rangle$ ↳ normal subgp.

$\dfrac{G}{[G\ G]} \to$ abelian

$xG^{(1)}\, yG^{(1)}\, x^{-1}G^{(1)}\, y^{-1}G^{(1)}$

$= xyx^{-1}y^{-1}G^{(1)}$

$= G^{(1)}$

PAGE NO.:
DATE: / /

Claim → $[G\,G]$ is the smallest normal subgp. for which $\frac{G}{[G\,G]}$ is abelian.

Pf → Let N be normal s.t. $\frac{G}{N}$ is abelian.

$$\underline{T.S.} \rightarrow [G\,G] \subseteq N$$

$$xN\,yN = yN\,xN$$

$$\Rightarrow xyx^{-1}y^{-1}N = N \quad \Rightarrow xyx^{-1}y^{-1} \in N \;\; \forall x,y$$

$$\Rightarrow [G\,G] \subseteq N.$$

$$G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots \supseteq G^{(n)}$$

$G^{(1)} = [G\,G] = \langle [x,y] : x,y \in G \rangle$

$\cup$

$G^{(2)} = [G^{(1)}\,G^{(1)}] = \langle [z_1, z_2] : z_1, z_2 \in G^{(1)} \rangle$

$\cup$

$G^{(3)} = [G^{(2)}\,G^{(2)}]$

$\cup$

$\cup$

$G^{(n)} = [G^{(n-1)}\,G^{(n-1)}]$

$\Longrightarrow G^{(i)}$ is normal in G.

Pf Let $x \in G$. Proof by induction.

True for $i=1$. Let it be true for $i-1$.

$\underline{T.S.}$ $G^{(i)} \trianglelefteq G$

$z_1, z_2 \in G^{(i-1)}$ $\quad x \in G$

$$x[z_1, z_2]x^{-1} = [\underbrace{xz_1x^{-1}, xz_2x^{-1}}_{\in G^{(i-1)}}]$$

So $[xz_1x^{-1}, xz_2x^{-1}] \in G^{(i)}$

Inverse of Lagrange Thm is true for nilpotent groups.

PAGE NO. :
DATE : / /

$G^1 = [G, G]$
$\cup$
$G^2 = [G, G^1]$
$\cup$
$G^3 = [G, G^2]$
$\cup$
$\vdots$
$\cup$
$G^n = [G, G^{n-1}]$

We say G is nilpotent if $\exists n$ s.t. $G^n = \{1\}$.

$G^{(1)} = G^1$
$G^{(2)} \subseteq G^2$
$\vdots$
$G^{(r)} \subseteq G^r$

$\therefore$ Nilpotent $\Rightarrow$ Solvable

Ex- $G = Q_8$ $\quad [Q_8, Q_8] = \{1, -1\}$ $\quad$ $ij i^{-1} j^{-1} = ij(-i)(-j) = ijij = -1$.

$G^2 = \{1\}$

Nilpotent ✓ $\Rightarrow$ solvable ✓.

TFAE-

(1) G is solvable.

(2) $\exists$ a normal series
$$G = G_0 \supseteq G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$$
s.t. $\frac{G_i}{G_{i+1}}$ is abelian.

(3) $\exists$ a subnormal series
$$G = G_0 \supseteq G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$$
s.t. $\frac{G_i}{G_{i+1}}$ is abelian.

Pf $\quad 1 \Rightarrow 2$ (done)

$2 \Rightarrow 3$ (trivial)

$[3 \Rightarrow 1] \Rightarrow$

PAGE NO.:
DATE: / /

$(3 \Rightarrow 1)$

Claim: $G^{(i)} \subseteq G_i \quad \forall i$.

$$G^{(1)} \subseteq G_1 \quad \left(\because \frac{G}{G_1} \text{ is abelian}\right)$$

Use induction → T.S. $G^{(i+1)} \subseteq G_{i+1}$

$$\frac{G_i}{G_{i+1}} \text{ abelian} \Rightarrow \frac{G^{(i)}}{G_{i+1}} \text{ abelian.}$$

$$\Rightarrow G^{(i+1)} \subseteq G_{i+1} \checkmark.$$

- D_n is solvable

$$D_n = \{1, x, x^2, \dots, x^{n-1}, y, xy, \dots, x^{n-1}y\}$$

$$D_n \supseteq \{1, x, x^2, \dots, x^{n-1}\} \supseteq \{1\} \checkmark$$ → subnormal series satisfying (3).

same for nilpotent

- A subgp. of a solvable gp. is solvable.

$$H \subseteq G$$

$$H^{(i)} \subseteq G^{(i)} \quad \forall i \quad \checkmark$$

same for nilpotent

- H – normal in G. Quotient is solvable. (for solvable gp.)

$$\left[\frac{G}{H}, \frac{G}{H}\right] = \frac{G^{(1)}H}{H}$$

$$xHyHx^{-1}Hy^{-1}H = xyx^{-1}y^{-1}H$$

$$\left(\frac{G}{H}\right)^{(i)} = \frac{G^{(i)}H}{H}$$

PAGE NO.:
DATE: / /

$H \trianglelefteq G$ (normal)

- G is solvable iff H and $\frac{G}{H}$ are solvable.

Pf → ($\Rightarrow$) done

($\Leftarrow$) $\left(\frac{G}{H}\right)^{i} = \frac{G^{(i)}H}{H}$

$\exists n$ s.t. $\left(\frac{G}{H}\right)^{(n)} = H$ ← identity element.

$\Rightarrow \frac{G^{(n)}H}{H} = H \Rightarrow G^{(n)} \subseteq H$

also $H^{(m)} = \{1\}$.

$\Rightarrow G^{(m+n)} \subseteq H^{(m)} = \{1\}$

$\Rightarrow G$ is solvable.

- Let G be nilpotent. Then $Z(G) \neq \{1\}$ ← non trivial center.

Pf → $\exists n$ s.t. $G^{n} = \{1\}$

Let n be smallest s.t. $G^{n} = \{1\} \rightarrow G^{n-1} \neq \{1\}$

$[G, \underbrace{G^{n-1}}_{\text{belongs to } Z(G) \neq \{1\}}] = \{1\}$ ✓.

- $\frac{G}{Z(G)}$ is nilpotent $\Leftrightarrow$ G is nilpotent.

Pf ($\Rightarrow$) $\left(\frac{G}{Z(G)}\right)^{n} = \{1\}$ $\quad \frac{G^{n}Z(G)}{Z(G)} = Z(G)$

$\Rightarrow G^{n} \subseteq Z(G)$

$\Rightarrow G^{n+1} = \{1\}$

($\Leftarrow$) done earlier.

Date: 5

- Every gp. of odd order is solvable. (Feit - Thomson)
- Any gp. of order $p^a q^b$ is solvable. (Burnside)

- Any p-gp is nilpotent.

$|G| = p^n$

- $n \geq 5$ S_n is not solvable.

$S_n \supseteq A_n \supseteq A_n \supseteq A_n \ldots$

(as A_n is simple)

- $S_4 \supseteq A_4 \supseteq \{1, (12)(34), (13)(24), (14)(23)\} \supseteq \{1\}$

solvable.

- S_3 is solvable but not nilpotent.

as center is ~~non~~ trivial.

- D_n is nilpotent iff $n = 2^k$.

- Upper triangular matrices — Solvable over GL_n.

Recall,

G

$G' = [G, G]$

$G^2 = [G, G']$

$\vdots$

$G^n = [G, G^{n-1}]$

- We say G is nilpotent iff $\exists n$ s.t. $G^n = \{1\}$
- Any p-gp. is nilpotent.
- S_n is not nilpotent $n \geq 3$

S_n is not solvable $n \geq 5$.

PAGE NO.:
DATE:

- G is nilpotent then $Z(G) \neq \{1\}$
- G is nilpotent iff $\frac{G}{Z(G)}$ is nilpotent.

PS-7 Q.8 G is nilpotent $\quad H \subsetneq G$

$$H \neq N_G(H) = \{g \in G : gHg^{-1} = H\}$$

OR

$$H \subsetneq N_G(H)$$

$$G = G^0 \supseteq G^1 \supseteq G^2 \supseteq \dots \supseteq G^n = \{1\}$$

Choose k s.t.

$$G^{k+1} \subset H \text{ but } G^k \not\subseteq H$$

Let $x \in G^k \setminus H$. Claim:- $x \in N_G(H)$

Let $y \in H$

$$[x\,y] = \underline{xy}x^{-1}\underline{y^{-1}} \in G^{k+1} \subset H$$

$$xyx^{-1} \in H$$

$$\Rightarrow \boxed{x \in N_G(H)}$$

$$\boxed{\& \; x \notin H}$$

$$\Rightarrow \boxed{H \subsetneq N_G(H)}$$

\# G is nilpotent, $p \mid |G|$, Let P be a Sylow p-subgp.

Claim:- $N_G(N_G(P)) = N_G(P)$

Sylow p-subgp

$$P \subsetneq N_G(P) \subseteq G$$

from nilpotency.

Sylow p subgp.

P is normal Sylow of $N_G(P)$

$\Rightarrow P$ is unique Sylow subgp of $N_G(P)$

PAGE NO.:
DATE: / /

$x \in N_G(N_G(P))$

$xPx^{-1} \subseteq xN_G(P)x^{-1} = N_G(P)$

$P = xPx^{-1}$ $\quad x \in N_G(P)$ ✓

$\Rightarrow N_G(N_G(P)) \subseteq N_G(P)$ ✓

$N_G(P) \subseteq N_G(N_G(P)) \to$ By defn.

$\Rightarrow N_G(P) = N_G(N_G(P))$.

Claim – Any Sylow p-subgp. of a nilpotent gp is normal.
$\Updownarrow$
unique

Pf $\Rightarrow$ P – Sylow p-subgp. of G

If $N_G(P) = G$ ✓ P is normal.

If $N_G(P) \subsetneq G$ $\Rightarrow N_G(P) \subsetneq N_G(N_G(P))$
$\Rightarrow \Leftarrow$ (Last claim)

Q9 PS-7

Thm – G is nilpotent iff G is a direct pdt. of its Sylow-subgps.

Pf ($\Leftarrow$) Pdt. of 2 nilpotent gps. is nilpotent.
Sylow-subgps are P-gps. $\Rightarrow$ nilpotent
$\Downarrow$
G is nilpotent ✓

($\Rightarrow$) $P_1, P_2, \dots, P_r$ be the distinct primes divides $|G|$.

By order constitution.

$|G| = H_1 H_2 \dots H_r$ $\quad |G| = p_1^{k_1} . p_2^{k_2} \dots p_r^{k_r}$

$\quad H_1 \quad H_2 \quad H_r$ } intersection = identity.

$\Rightarrow G = H_1 \times H_2 \times \dots \times H_r$

PAGE NO.:
DATE: / /

Converse of Lagrange Thm.

PS-7 Q.10 $|G| = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$

$m \mid |G|$ then $\exists$ a subgp. of order m in G.

$m = p_1^{s_1} p_2^{s_2} \ldots p_r^{s_r}$ $G \cong H_1 \times H_2 \times \ldots \times H_r$

$p_1^{k_1} \; p_2^{k_2} \ldots p_r^{k_r}$

$K_1 \times K_2 \times \ldots \times K_r$

(Q.9 of PS-6)

\# G is nilpotent iff for every $x, y \in G$ s.t. $(o(x), o(y)) = 1$.

then we have $xy = yx$.

$$G = \underset{p_1^{r_1}}{H_1} \times \underset{p_2^{r_2}}{H_2} \times \ldots \times \underset{p_k^{r_k}}{H_k}$$

As $(o(x), o(y)) = 1$

$x = (x_1, x_2, \ldots, x_k)$ Either $x_i = 1$ or $y_i = 1$ $\forall i$.

$y = (y_1, y_2, \ldots, y_k)$

PAGE NO.:
DATE: / /

Q.11 $D_n \supseteq \{1, x, \ldots, x^{n-1}\} \supseteq \{1\}$ D_n is solvable ✓.

2nd part → If $n = 2^k$
$|D_n| = 2^{k+1} \Leftarrow P\,gp \Rightarrow$ nilpotent ✓

If D_n is nilpotent.
Let $n \neq 2^k \Rightarrow P \to$ odd prime s.t. $P \mid 2n$
$\Rightarrow P \mid n$.

$o(x^{n/p}) = p$

$\Rightarrow x^{n/p} \neq x^{-n/p}$

$x^{n/p}$ y coprime order $\Rightarrow$ commute $x^{n/p} y = y x^{n/p} = x^{-n/p} y$

$\Rightarrow x^{n/p} = x^{-n/p}$
$\Rightarrow \Leftarrow$.

Q.1 $GL_n(\mathbb{Z}_p)$

$|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$

$= p^{\frac{n(n-1)}{2}} (\ldots)$

$$\begin{array}{c} p \quad p \\ \begin{pmatrix} 1 & * & * & * & \cdots \\ & 1 & * & * & \cdots \\ & & 1 & * & \cdots \\ & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}_{n^2} \end{array}$$

Total $\frac{n(n-1)}{2}$

$P^{\frac{n(n-1)}{2}}$

↑ Sylow p. subgp.

PAGE NO.:
DATE: / /

PS-7 Q.2 $72 = 2^3 \cdot 3^2$

$n_3 \equiv 1 \mod 3$

$n_3 \mid 8 \Rightarrow n_3 = 1, 4, \cancel{8}$

Let $n_3 = 4$

H_1, H_2, H_3, H_4

$G \longrightarrow S_4$

$o(G) = 72 \quad o(S_4) = 24$

↳ Non trivial kernel.

PS-7 Q.3 $255 = 3 \times 5 \times 17$

$n_{17} \equiv 1 \mod 17$

$n_{17} \mid 15 \quad n_{17} = 1$ ✓

$|H| = 17$

$H = \langle a \rangle$.

$\left|\frac{G}{H}\right| = 15, \quad \frac{G}{H} = \langle bH \rangle$

$o(bH) \mid o(b)$

$o(b) = 15$, or 255 → done ✓ proved cyclic.

$o(b) = 15$

$bab^{-1} \in H = \langle a \rangle$

$bab^{-1} = a^i$

$b^2ab^{-2} = ba^ib^{-1} = (bab^{-1})^i = a^{i^2}$

PAGE NO.:
DATE: / /

$b^k a b^{-k} = a^{i^k}$

$b^{15} a b^{-15} = a^{i^{15}} \Rightarrow i^{15} \equiv 1 \mod 17$

$i^{16} \equiv 1 \mod 17 \leftarrow$ Fermat's Little Theorem.

$(15, 16) = 1 \Rightarrow 15r + 16s = 1$

$i = 15r + 16s$ $\quad i = 1$

$ab = ba$

$o(a) = 17$ $\quad ab = ba$ (as $i = 1$)
$o(b) = 15$

$o(ab) = 255$ ✓ $\rightarrow$ cyclic.

Q4 $|G| = 30$ has a normal subgp. of order 5.
$= 2 \times 3 \times 5$.

$n_5 \equiv 1 \mod 5$ $\quad n_5 | 6$ $\quad n_5 = 1$ or $n_5 = 6$

$n_3 \equiv 1 \mod 3$ $\quad n_3 | 10$ $\quad n_3 = 1$ or $n_3 = 10$

If $n_5 = 6$ and $n_3 = 10$
24 elements $\quad$ 20 elements > 30 ✗✗

So $n_5 = 1$ or $n_3 = 1$
$\quad H \quad K$ $\quad$ normal $|HK| = 15$ Index $= 2$ normal

If $n_5 = 1$
we are done.

$H \subseteq HK \subseteq G$

$g \in G$

$gHg^{-1} \subseteq gHKg^{-1} \subseteq G$ $\quad gHg^{-1} = H$
$\quad \| \qquad\qquad \|$
$\quad H \qquad\quad HK$ $\qquad \forall g \in G$.

$3^2 =$

$GL_n(\mathbb{Z}_p)$ $(p^n - 1)(p^n - p)$. $3 \quad 23 \quad 10$ $2+1$ $1+1+1$.