Group.

① **Def**:

Semigroup: satisfy Associate Law.

↓ if it contains a two-side id-element: e

Monoid: $ea = ae$, $\forall a \in$ Monoid.

↓ if $\forall a \in$ it, then exists a^{-1} (two-side)

Group: namely, $a^{-1}a = aa^{-1} = e$.

Remark: (1) We just talk the case that G is a multiple group.
If G is an Abelian group, then note G is a additive group. (namely, $a+b$ "replace" ab")

(2) e is unique, when $e_1e_2 = e_1 = e_2 = e$
a^{-1} is unique, when $a_1^{-1} = a_1^{-1}aa_2^{-1} = ea_2^{-1} = a_2^{-1}$

⇒ **First Group Def**:

G is a Semigroup, if and only if:

it contains left inverse and left id-element at the same time. ("right" the same)

pf: notice $(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = aa^{-1}$
$\therefore aa^{-1} = e = a^{-1}a$, then $ea = a = a(a^{-1}a) = ae$

Remark: have a left inverse and right id-element:
$A = \{a_i\}_1^n$, $*: a_k * a_j = a_j$, then $(A, *)$:
$\forall a_i$ is a left-id and right-inverse
(since a_i is id!) But A isn't a group!

Second Group Def:

G is a Semigroup, then G is a group.

$\Leftrightarrow$ $ax=b$, $ya=b$, $\forall a,b \in G$, then x,y has a solution (unique)

Pf: "$\Rightarrow$" $x=a^{-1}b$, $y=ba^{-1} \in G$. if $\exists$ (uniqueness)

$ax_1=b=ax_2$, By cancellation: $x_1=x_2$.

"$\Leftarrow$" $\forall c,a \in G$. $ax_0=c$, $x_1a=a$.

then $x_0, x_1 \in G$. ← 为了把 c 表示为 a 的形式!

$x_1c=x_1ax_0=ax_0=c$ $\therefore x_1$ is left-id (note e)

then $\forall b \in G$, $x_2b=e$, x_2 is left inverse of "b"

Third Group Def:

If G is a finite Semigroup which satisfies Left-Right-Cancellation

$\Rightarrow$ G is a group.

Pf: Assume $G=[a_i]_1^n$, then $a_ka_j=a_ka_{j'}$

$\Leftrightarrow$ $a_j=a_{j'}$, Since G is under closed operation

then $[a_ka_j]_{j=1}^n=[a_i]_1^n$, $\forall k$.

$\therefore$ $a_kx=a_j$ have a solution!

Remark: When G is infinite example:

$(\mathbb{N},0)$). It's wrong!

② Subgroup.

Def: G is a group. $H \subseteq G$. $H \neq \emptyset$. which is closed under the product in G. If H is a group (*), then H is the sub-G of G.

Note: $H < G$.

(*) If H is finite, it's necessary.

pf: Assume H is $\{a_k\}_{k=1}^{n}$. $\langle a_i \rangle \subseteq (\{a_k\}_{k=1}^{n}, *)$ then $\exists e \in \langle a_i \rangle$ (or $\langle a_i \rangle$ is infinite)

Then $\{a_k a_j\}_{j=1}^{n} = \{a_k\}_{k=1}^{n}$ (use 3rd-Group-Def)

$\Leftarrow$) $\forall a, b \in H$. $ab^{-1} \in H$. $\Leftarrow$) $\forall a, b \in H$. $ab, a^{-1}, b^{-1} \in H$

Corollary (1) $\{H_i\}_{i \in I}$ is the family of sub-G of G. Then $\bigcap_{i \in I} H_i$ is a sub-Group of G.

pf: $e \in H_i$. $\forall i$. $\therefore \bigcap H_i \neq \emptyset$. then $\forall ab^{-1} \in H_i$. $\forall i$.

$\Rightarrow ab^{-1} \in \bigcap_{i \in I} H_i$. where $a, b \in H_i$. $\forall i$.

(2) $\bigcup_{i \in I} H_i = \langle \bigcup H_i \rangle$ (sub-group) $\Leftrightarrow$

$\forall i, j$. $H_i \subseteq H_j$ or $H_j \subseteq H_i$.

pf: $n=2$: ("$\Leftarrow$") is obviously

"$\Rightarrow$" $\forall a_i \in H_i \subseteq \langle H_1 \cup H_2 \rangle$ then $a_i^{-1} b_i \in \langle H_1 \cup H_2 \rangle$

$\forall b_i \in H_i \subseteq \langle H_1 \cup H_2 \rangle$

since $\langle H_1 \cup H_2 \rangle = H_1 \cup H_2$ $\therefore a_i^{-1} b_i \in H_1$ or H_2

Assume $a_i^{-1} b_i \in H_1$ then $a_i (a_i^{-1} b_i) = b_i \in H_1$

$\therefore H_2 \subseteq H_1$. $k=n$. by Induction

③ **Cosets** : "$H < G$. then $aRb \Leftrightarrow a^{-1}b \in H$"

R is a congruent Relation

Pf: $aRa \Leftrightarrow a^{-1}a = e \in H$. obviously!

$aRb \Leftrightarrow a^{-1}b \in H$. then $b^{-1}a \in H$. namely bRa

$aRb, bRc \Rightarrow a^{-1}c \in H$. $\therefore aRc$

Property: $|Ha| = |H|$
$= |aH|$

$\Rightarrow Ha = \{ha \mid h \in H\}$ is called Right coset

$aH = \{ah \mid h \in H\}$ is called Left coset

Then prove: $\bar{a} = aH$.

$\forall b \in \bar{a}$. $bRa \rightarrow a^{-1}b \in H$. $\therefore b \in aH \rightarrow \bar{a} \subseteq aH$

$\forall h \in H$. then $ah \in aH$. $ahRa \Leftrightarrow a^{-1}ah \in H$.

$\therefore ah \in \bar{a}$. $\therefore aH \subseteq \bar{a}$ $\therefore \bar{a} = aH$

$\Rightarrow aRb \Leftrightarrow aH = bH$ (resp. Left)

(2) The index of H in G which means the cardinal number of $\{aH \mid a \in G\}$.

Denote: $[G:H]$ ($[G:e] = |G|$, $[G:G] = 1$)

$\Rightarrow$ Lagrange Theroem: $H < G$. then:

$$|G| = [G:H]|H|$$

Pf: $[G:H]$ is the number of sets.

Since $aH \cap \dot{a}H = \emptyset$. then $|G| = [G:H]|H|$

Remark: If H is cyclic group. then order of H is $|H|$ which divide "$|G|$"!

corollary: If $k \subset H < G$. then $[G:H][H:k] = [G:k]$.

pf: $|G| = [G:k]|k|$, $|G| = [G:H]|H| = [G:H][H:k]|k|$.

⇒ Theorem 2. $H < G$. $k \subset G$. then $|Hk| = \frac{|H||k|}{|H \cap k|}$

pf: $H \cap k$ is subgroup of k or H.

Note that $Hk = \bigcup Hk_i$ $\therefore |Hk| = |H| \cdot n$.

n is the cardinal number of $\{Hk_i \mid k_i \in k\}$.

Denote $C = H \cap k$. then $[k : H \cap k] = \frac{|k|}{|H \cap k|}$

which is the cardinal number of Ck_i.

since $HC = H$. then $n = \frac{|k|}{|H \cap k|}$!

corollary: by $|G| \geq |kH|$. then we have: $[G:k] \geq [H : H \cap k]$.

→ "=" holds by $G = kH$

pf: $h(H \cap k) \longrightarrow hk$. homo. ($H/H\cap k$ → G/k)

Check it's homo-

It's epi- ⟺ $G = kH$.

To prove ⇒

$\forall x \in G$. $x \in xk$

$= hk \in Hk$.

$\therefore G \subseteq Hk \subseteq G$

④ Normality and quotient groups

Def: $N < G$. the following conditions equal:

i) $\forall a \in G$. $aNa^{-1} \subset N$. 其中 $aNa^{-1} = \{ana^{-1} \mid n \in N\}$.

ii) $aN = Na$. for all $a \in G$.

iii) $\forall a_1, a_2 \in G$. $a_1N \cdot a_2N = a_1a_2N$

其中 $a_1N \cdot a_2N = \{a_1n_1a_2n_2 \mid n_1, n_2 \in N\}$.

pf: i) → ii) $\forall a_1 \in G$. $a_1Na_1^{-1} \subset N$ $\therefore a_1na_1^{-1} = n_2$. $\forall n_1$. $\exists n_2 \in N$.

~~其中 $n_1, n_2 \in N$. then $a_1n_1 = n_2a_1$ $\therefore a_1N \subseteq Na_1$. converse by~~

$\therefore \forall\ aN = Na$.

$a_1^{-1}Na_1 \subset N$.

ii) → iii) $\forall a_1n_1a_2n_2 \in aN\cdot aN$

$a_1n_1a_2n_2 = a_1a_2n_1n_2 \in a_1a_2N$

$\forall a_1a_2n \in a_1a_2N.\ a_1a_2n = a_1ea_2n$

$\in a_1N\cdot a_2N \ \therefore a_1N\cdot a_2N = a_1a_2N$

iii) → i) $ana^{-1} = an\cdot a^{-1}e \in aN\cdot a^{-1}N$

$= aa^{-1}N = N \ \therefore ana^{-1} \in N.$

Then. if N satisfies the conditions above. we say it's normal in G. denote it "$N \triangleleft G$"

Obviously. Abelian group is normal about every subset.

Theorem. $K < G.\ N \triangleleft G.$

then (1) $N \cap K$ is normal in K. → 相当 $N/K \triangleleft G/K$

(2) N is normal in NVK. → 对 $K \triangleleft G$.

and $NK = NVK = KN$. $NK < G$

(3) if K is normal in G, too.

and $K \cap N = \{e\}$. the $nk = kn.\ \forall k \in K.\ n \in N$.

Pf: (1) $\forall a \in K.\ a(N\cap K)a^{-1} \subset N.$

since $N \triangleleft G.\ N \cap K \subseteq N.$

Moreover. Since $N \cap K < K$. then.

$a(N\cap K)a^{-1} \subset N \cap K$. which is closed!

(2) trivial. Since $NVK \subseteq G$. by the former.

Then. we can denote the element

i.e. NVK. by $n_1k_1n_2k_2\cdots n_rk_r$.

Since $k \in K$. $k \in G$. $Nk = kN$.

then can be writed as $\prod_1^r n_i \prod_1^r k_i = NK$.

(3) $Nk = kn \iff n^{-1}k^{-1}nk = e$

$\Leftarrow$ $N \cap K = \{e\}$. $\Rightarrow$ Prove $n^{-1}k^{-1}nk \in N$ and $\in K$.

Since $n^{-1}k^{-1}n \in K$. $k^{-1}nk \in N$. then ✓.

Then. we define operation on the quotient

Set $= G/N$. If $N \trianglelefteq G$. by $=(aN)(bN)=abN$

Pf: 1) well-defined? under the equvillant relation R:

$aRb \iff a^{-1}b \in N$.

then a_1Rb_1. $a_2Rb_2 \Rightarrow a_1a_2Rb_1b_2$. 需:

$a_2^{-1}a_1^{-1}b_1b_2 \in N$. 即 $a_1^{-1}b_1$. $a_2^{-1}b_2 \in N$.

then $a_1^{-1}b_2(b_2^{-1}a_1^{-1}b_1b_2) \in N$. $\Leftarrow$ $b_2^{-1}Nb_2 \in N$. ✓

2) Associate law is obvious. And:

Id-element $= eN$. Inverse $= a^{-1}N$ of aN.

(5) **Homomorphisms**

Def: $f: G \to H$ is homo. If:

$f(a *_G b) = f(a) *_H f(b)$

Property: (1) $f(e_G)=e_H$, $f(a^{-1})=f(a)^{-1}$

Pf: $f(e_G\cdot e_G)=f(e_G)\cdot f(e_G)=f(e_G)$

$f(a\cdot a^{-1})=f(e_G)=e_H=f(a)f(a^{-1})$

(2) $\ker f \lhd G$.

Pf: 1) $\ker f<G$. $\forall a,b\in\ker f$.

then $f(a^{-1}b)=f(a^{-1})f(b)=f(a)^{-1}f(b)=e_H$

$\therefore a^{-1}b\in\ker f$.

2) $\forall a\in G$. $f(a\ker f a^{-1})=f(a)e_H f(a^{-1})=e_H$

$\therefore a\ker f a^{-1}\in\ker f$.

(3) 保号群性:

设 $f:G\to H$, hom.

$A<G$, $B<H$.

then $f(A)<H$

$f^{-1}(B)<G$!

Them. (1) Canonical projection:

$N\lhd G$. $\pi: G\to G/N$ by $\pi(a)=aN$ → $H<G$. then $HN=\pi^{-1}(\pi(H))$ ↓ then $H=\pi^{-1}(\pi(H))\Leftrightarrow H=N$!

then π is epi-, with $\ker\pi=N$.

Pf: π is homo, obviously. $\forall aN$, $\exists a\mapsto aN$.

epi- is trivial. then, $\ker\pi=\{a\mid \pi(a)=eN\}$

$=\{a\mid aN=N\}=N$.

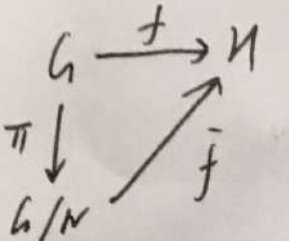
(2) Lemma. $f: G\to H$. homo. $N\lhd G$.

and $N\subseteq\ker f$. then $\exists$ unique $\bar f$

$: G/N\to H$. $\bar f(aN)=f(a)$. s.t.

$\mathrm{Im}f=\mathrm{Im}\bar f$. $\ker\bar f=\ker f/N$.

Pf: graph:



"$\bar{f}\pi = f$"

1°) If $b \in aN$, then $b = an$.

$f(b) = f(an) = f(a)f(n) = f(a)$

$\therefore \bar{f}(aN) = f(a)$ is well-defined.

2°) $\bar{f}(aN \cdot bN) = \bar{f}(abN) = f(ab)$

$= f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$. $\therefore \bar{f}$ is homo

3°) Since $\bar{f}(aN) = f(a)$. $\therefore \mathrm{Im}\bar{f} = \mathrm{Im}f$

And $aN \in \ker\bar{f} \Leftrightarrow f(a) = e \Leftrightarrow a \in \ker f$

$\therefore \ker\bar{f} = \ker f / N$.

4°) Uniqueness. by graph. $\bar{f}$ is determined by f

corolary: ① First. Iso Theorem:

$f: G \to \mathrm{Im}f$, homo. then $\mathrm{Im}f \cong G/\ker f$.

pf: $\ker f \lhd G$. Let $N = \ker f$. then $\ker f / N = N$.

which means $\bar{f}$ is mono-, And f is epi-, then $\bar{f}$ is iso- $\therefore \mathrm{Im}f \cong G/\ker f$.

Remark: iso- conditions construct $\begin{cases} N = \ker f \\ f \text{ is epi-} \end{cases}$

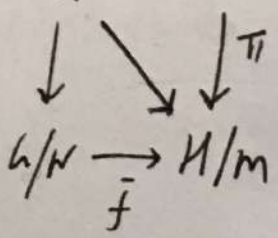
corollary ②: $f: G \to H$, homo, $N \lhd G$, $M \lhd H$.

$f(N) < M$, then f induce $\bar{f}: G/N \to H/M$ by $\bar{f}(aN) = f(a)M$.

and when $f(N) = M$. $\mathrm{Im}f \vee M = H$.

then. $G/N \cong H/M$.

graph:



1) $\pi f(G) = f(G)M$. is homo

2) $\ker\pi = M$. then.

$\pi f(G) = f(G)M = M$ (=)

$f(a) \in M$. Sim $f(N) < M$.

$\therefore N < f^{-1}(M)$, $\therefore N \subseteq \ker\pi f$

by the Lemma, it's done.

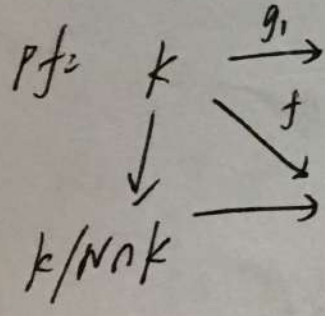
And when $f(N) = M$. which means $\underline{N = \ker\pi f}$

$\mathrm{Im}f \vee M = H$. which means $\pi(\mathrm{Im}f) = H/M$

$\therefore \pi f$ is epi- $\therefore$ by coro① on πf ✓.

③ Second Iso- theorem.

$K < G$. $N \lhd G$, then $K/N\cap K \cong NK/N$



$N\cap K \lhd K$ by Theorem.

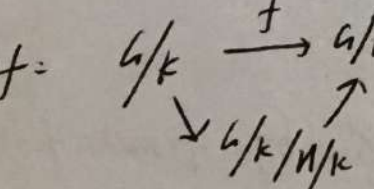
f is homo. with $\ker f = N\cap K$.

And $\forall nkN \in NK/N$. $nk = kn'$

$\therefore nkN = kn'N = kN = f(k)$

④ Third Iso- Theorem:

$N \lhd G$. $K \lhd G$. $K < N$. $\Rightarrow N/K \lhd G/K$. and $\frac{G/K}{N/K} \cong G/N$.



$N/K = \ker f$

Another form: $N \lhd G_1$, $\ker f \supseteq N$. $f: G_1 \to G_2$, epi-

then $G_1/N \cong G_2/f(N)$

Corollary: App to canonical projection: $G \to G/N$

$K/N < G/N \Leftrightarrow K < G$, $K/N \lhd G/N \Leftrightarrow K \lhd G$.

③ $f: G \to H$, epi-, then $f: K \mapsto f(K)$ 建立了 G 中包含 $\ker f$ 子群与 H 子群的一一对应，并保正规子群映至正规子群.

Pf: $\forall J < H$, $f^{-1}(J) < G$, $\therefore$ surjection.

$f^{-1}(f(A)) = A$, iff $A \supseteq \ker f$.

then injection. $\therefore$ bijection.

Normality remaining can be checked!

Lemma:

$f: G \to H$, homo.

$A < G$, $B < H$

then $f(A)$, $f^{-1}(B)$ is subset of H and G respectly.

pf: can be checked!

homo - remain structure of group!

④ **Cyclic groups**:

Def: G is a group. $X \subseteq G$. $\{H_i \mid i \in I\}$ is the family of all subgroups of G which contains X. $\bigcap_{i \in I} H_i$ is called the subgroup generated by X, denoted $\langle X \rangle$

即包含X的最小子群

If $|X|$ is finite, Assume $X = \{a_n\}$. Then $\langle X \rangle = \{\prod a_{i_n}^{k_n} \mid a_i \in X, k_i \in \mathbb{Z}\}$.

Note that $X \subset \langle X \rangle$!

Thm: (1) $H < G = \langle a \rangle$, $H \neq \{e\}$, then order of H is the minimal number above $\{k \mid a^k \in H\}$.

pf: Assume it's "m", $\langle a^m \rangle \subset H$.

$\forall a^l \in H$, $l = km + r$, then $a^r \in H$, $\therefore r = 0$.

(2) every infinite cyclic group $\cong \mathbb{Z}$ addictive group

(Note that the denumerable of generators)

every finite cyclic group $\cong \mathbb{Z}_m$, addictive group

(3) ~~Aut G is Abelian~~ (check!)

1. Symmetric. Alternating Group:

① Def: (1) cycle Denotion: $(i_1 i_2 \cdots i_r)$. $\{i_k\}_1^r \subseteq \{k\}_1^n$.

which are distinct! then maps: $i_1 \mapsto i_2 \cdots i_r \mapsto i_1$

$(i_1 \cdots i_r)$ is r-cycle with length r. 2-cycle is transposition

And whose inverse is $(i_r \cdots i_1)$

(2) symmetric group S_n is all bijection of $\{1,\cdots n\} \to \{1,\cdots n\}$.

(3) sign of permutation τ is $(-1)^k$. k is the number of transposition of τ. Denote "$\operatorname{Sgn}\tau$"

(4) a group is simple if it has no proper normal group.

单群 ←

② Theorem: (1) Cayley Thm:

G is a group. then. $G \cong$ 某个变换群. $\in S_n$ → ∴(n阶互不同构的群仅有限个 $\leq n!$)!

Pf: Let $S_n = \{l_a \mid a \in G\}$. def by $l_a(g) = ag$.

(即为"a左平移变换")

☆ ↓ 可将抽象群转化为具体变换群!

Note that $l_a^{-1} = l_{a^{-1}}$, $l_a l_b = l_{ab}$

$\therefore S_n < S$(变换群). 此时 $\varphi: G \to S_n$. 满一!

(2) $\forall \sigma \in S_n$. $\sigma \neq Id$. then σ is uniquely a product of disjoints cycle with length ≥ 2

Pf: A equivalent relation: $x, y \in I_n$. $x \sim y \Leftrightarrow x = \sigma^m(y)$

Let $\{B_i\}_1^s$ be the equivalent classes which are called "orbit" with length ≥ 2. Note that $B_i \cap B_j = \emptyset$.

Def: $\sigma_i = \begin{cases} \sigma, & x \in B_i \\ x, & x \notin B_i \end{cases}$ which is well-defined!

Moreover, σ_i is a cycle: 对 $x \in B_i$.

Let "d" be the least $\mathbb{Z}^+$ such that $\sigma_i^d(x) = \sigma_i^j(x)$. since I_n is finite!

对 $j \geq 1$, $\sigma_i^{d-j}(x) = x = \sigma_i^0(x)$. $0 < d-j < d$. contradict!

$\therefore \sigma_i^d(x) = x$. $\therefore \forall m$. $\sigma_i^m(x) \in \{\sigma_i^k\}_0^{d-1}$ $\therefore \sigma_i = (x\ \sigma(x) \cdots \sigma^{d-1}(x))$

Then. $\sigma = \prod_1^s \sigma_i$. the order of σ is $[m_1, m_2 \cdots m_s]$

m_i is the order of σ_i.

(思路对 $[1, 2, \cdots n]$ 作用若干次 σ, 寻找其所有循环轨道之并)

Corollary: $\forall \sigma$ in S_n. can be written as a product of transpotion.

Pf: $\forall$ cycle $(x_1 x_2 \cdots x_t) = (x_1 x_t)(x_1 x_{t-1}) \cdots (x_1 x_2)$

$\Rightarrow$ can be written as $\{(1\,2), (1\,3) \cdots (1\,n)\}$. $(n-1)$

Pf: $(1\,i)(1\,j)(1\,i) = (i\,j)$. $\forall i, j \in I_n$

$\Rightarrow$ Can be written as $\{(1,2), (2,3) \cdots (n-1\ n)\}$ $(n-1)$

Pf: $(1\,j-1)(j-1\ j)(1\,j-1) = (1\,j)$

(3) A_n is all even permutations of S_n.

$|A_n| = \frac{n!}{2}$ (By Symmetry). $A_n \triangleleft S_n$ of index 2 which is the only one.

pf: $f: S_n \longrightarrow \{1,-1\}$. $f(\sigma) = \operatorname{sig}\sigma$.

then $\ker f = A_n$. $S_n/A_n \cong \{1,-1\}$.

✡ Lemma of A_n: A_n is generated by

3-cycle $\{(rsk) \mid 1 \le k \le n\}$. $(=A)$

pf: 1) $\forall \sigma \in A_n$. $\sigma = (ab)(cd)$ or $(ab)(ac)$

$(ab)(cd) = (acb)(cad)$. $(ab)(ac) = (acb)$

2) Any 3cycle is the form (abc) (can be generate by A)

$(rsa)^2 = (ras)$. $(rab) = (rsb)(ras)$

$(sab) = (rsb)^2(rsa)$. $\therefore (abc) = (raf)(rsc)(sab)$ □

If $N \triangleleft A_n$. N contains a 3-cycle. then $N = A_n$

pf: $(rsk) = (rs)(ck)(rsc)^2(ck)(rs)$, $\exists c, \forall k$.

$= [(rs)(ck)]^{-1}$

(4) A_n is simple iff $n \neq 4$ (complicated)

→ corollary: A_n 无 $\frac{n!}{2}$ 阶正规子群!

(5) $D_n < S_n$. which is generate by

$a = (123\cdots n)$ and $b = \prod_{2 \le i \le n+3-i} (i\ n+2-i)$

is called Dihedral group of degree n

with the order $2n$. $D_n = \langle a, b \rangle = \{ a^i b^j \mid 0 \le i < n, 0 \le j < 1 \}$.

Property: $a^n = (1)$, $b^2 = (1)$, $ba = a^{n-1}b$

If G satisfies its property, then $G \cong D_n$.

Pf: By $ba = a^{n-1}b$, $\forall g = a^{n_1} b^{m_2} a^{n_3} b^{m_4} \cdots < a^i b^j$

then $f: a_i^i b_i^j \mapsto a^i b^j$, isophism!

Valuable conclusions

(1) All Groups of order 4:

Pf: i) It's generated by "a" which has a order "4". $\therefore G = \langle a \rangle$

ii) $G = \{e, a, b, c\}$. "a.b.c"'s order is 2, by Lagloge Theorem.

Then G is an Abelian group.

Figure out $ab = ?$ $ab \neq e, a, b$

$\therefore ab = c$, then $bc = a$, $ac = b$

$\Rightarrow$ We call G "Klein Four Group".

Extend: Group with order 6 is S_3 or cyclic!

✡ Lemma. If $\forall a \in G$ s.t. $a^2 = e$, then G is an Abelian group.

Pf: $\forall a \in G$, $a = a^{-1}$

then $(ab)^{-1} = e = abab$.

$\therefore a = bab$. $ba = ab$. □

$\Rightarrow$ Extend: G is an Abelian group $(\Leftarrow)$

$\forall a, b \in G$, $(ab)^2 = a^2 b^2$

Pf: "$\Rightarrow$" ✓ "$\Leftarrow$" $(=)$ $ab = ba$, obviously

→ Which can be used as a counter-example in the criterion of cyclic group! Because its 2-order group is unique!

(2) Ex. Extend Abelian Group Criterion:

G is Abelian $\Leftrightarrow \forall a, b \in G$, $(ab)^n = a^n b^n$ for three consecutive intergers holds.

Pf: $(ab)^n = a^n b^n$, $(ab)^{n+1} = a(ba)^n b = a^{n+1} b^{n+1}$

$\therefore (ba)^n = a^n b^n = b^n a^n$. Also, $a^{n+1} b^{n+1} = b^{n+1} a^{n+1}$.

→ If "2" is false!

$\therefore a^n b^n = (ab)^n = b^n a^n = (ba)^n$

$a^{n+1} b^{n+1} = (ab)^{n+1} = b^{n+1} a^{n+1} = (ba)^{n+1} \Rightarrow ab = ba$

(3) Little Lemma: the element "a" with order 2 appears single by $a^2 = e \Rightarrow a = a^{-1}$. when with order $\neq 2$. it appears pairly. by every $a_i \Rightarrow$ inverse a^{-1} also appears! (Since $a \neq a^{-1}$)

(4) The Inverse of Monoid:

b is a's Inverse in Monoid $\Leftrightarrow$

$aba = a$. $ab^2a = e$ → Alike with $a^{-1}ba = b$!

Pf: Note the structure "$aba = a$"

$ab = \underline{aba}b^2a = ab^2a = e$. □

$ba = ab^2\underline{aba} = ab^2a = e$

(5) Cancellation: (Note its structure by e.g!)

1. $\{a_k\}_1^n \subset G$. But $\{a_k\}_1^n$ probably not distinctive. Then $\exists\ 1 \le p \le q \le n$. st. $a_p a_{p+1} \cdots a_q = e$

Pf: Develop a set: $\{a_1, a_1a_2, \cdots, a_1a_2\cdots a_n\} = M$

Then $e \in M$ or $e \notin M$ → 2 ele is same!

2. G is finite group. S is a subset. st. $|S| > \frac{n}{2}$. then $\forall g \in G\ \exists a, b \in S$. st. $g = ab$

Pf: Develop gS^{-1}. its elem. is distinctive

$\therefore |gS^{-1}| = |S| > \frac{n}{2}$, $gS^{-1} \cap S \neq \emptyset$

~~(2)~~ $H_1 \cup H_2 = \langle H_1 \cup H_2 \rangle \Leftrightarrow H_1 \subseteq H_2$ or $H_1 \supseteq H_2$

Pf: $\forall h_1 \in H_1, h_2 \in H_2$, $h_1 h_2 \in \langle H_1 \cup H_2 \rangle$

$\therefore h_1 h_2 \in H_1$ or $h_1 h_2 \in H_2$ $\Rightarrow$ But not Arbitrary!

$\therefore h_1^{-1} h_1 h_2 = h_2 \in H_1$ or $h_1 h_2 h_2^{-1} \in H_2$

By Disproof: 对 $\exists a \in A, a \notin B, \exists b \in B, b \notin A$.

then $ab \notin A \cup B$, or $ab \in A$ or B.

$\therefore b \in A$ or $a \in b$! Contradiction!

~~(3)~~ $H < G$, $H \neq G$. Then $\langle G - H \rangle = G$. ⟶ H 在 G 中的补集也可生成 G!

Pf: 对 $\forall g \in G$, $g \notin H$, 则 $g \in G - H$.

对 $g \in H$, pick $a_i \notin H$, $G = H \cup a_1 H \cup a_2 H \cdots$

(陪集分解) $\therefore g = a_i^{-1}(a_i g) = (G-H)\cdot(G-H)$

since $a_i^{-1} \notin H$, $a_i g \in a_i H \neq H$, $\therefore g \in \langle G - H \rangle$!

(3) $\boxed{\mathrm{Aut}\, G}$ is the set of <u>all automorphisms of G</u>

(a) $\mathrm{Aut}\, G$ is a group. (by check $\sigma\tau^{-1} \in G$?) ⟶ 生成元的数量决定自同构的数量!

(b) $\mathrm{Aut}\, \mathbb{Z} \cong \mathbb{Z}_2$. $\mathrm{Aut}\, \mathbb{Z}_n \cong \mathbb{Z}_{\varphi(n)}$. φ is Euler func. $\mathbb{Z}$ 的生成元为 $\{1, -1\}$, $\mathbb{Z}_n$ 有 $\varphi(n)$ 个生成元. 设 $\{a_i\}_1^n$, 则 $f: a_1 \to a_i$ 为一个自同构!

(c) $\mathrm{Aut}\, \mathbb{Q} \cong \mathbb{Q}^*$ ($q \neq 0$)

(d) $G = (\mathbb{R}, +)$. then $\forall a, b \in G$, $\exists \varphi$. s.t. $\varphi(a) = b$

(e) $\mathrm{Aut}\, G$ can't be of odd order, if Aut is cyclic

Pf: (b) Take $\varphi \in \mathrm{Aut}\, \mathbb{Z}$. Assume $\varphi(1) = k$.

then $\exists l$. s.t. $\varphi(l) = 1$

$\therefore \varphi(l) = \varphi(1+1+1\cdots+1) = l\varphi(1) = lk = 1$

又 $l, k \in \mathbb{Z}$, $\therefore k = \pm 1$.

when $k=1$, φ is automorphism. $\therefore \mathrm{Aut}\,\mathbb{Z} = \{-\varphi, \varphi\} \cong \{1, 1\}$.

$k = -1$ $\varphi: \mathbb{Z}^+ \longrightarrow \mathbb{Z}^-$

Samely: 对于 $\mathrm{Aut}\,\mathbb{Z}_n \Rightarrow lk \equiv 1 \pmod n$

此时 $\{lk\}_{l=1}^{n}$. 当 $(n,k)=1$ 时, 若构成 mod n 的缩系.

$\therefore$ 必有 l, s.t. $lk \equiv 1 \pmod n$. 此时 k 有 $\varphi(n)$ 种选择

s.t. $(k,n)=1$, 且 $1 \le k < n$ $\therefore \mathrm{Aut}\,\mathbb{Z}_n \cong \mathbb{Z}_{\varphi(n)}$!

↘ Aut G is abelian 计 G is cyclic!

→ 实际上, 考察生成元组即可. 设 $\langle a\rangle_{i}^{\varphi(n)} = \{k\}_{i}^{\varphi(n)}$ 则令 $\tau_i(a) = a^{k_i}$, $\varphi: \{\tau_i\} \to \mathbb{Z}_{\varphi(n)}$ 同构! check!

(c) 作 $\sigma_r: (\mathbb{Q}, +) \longrightarrow (\mathbb{Q}, +)$ check it's isomorphism

$x \longmapsto rx$ $\therefore \sigma_r \in \mathrm{Aut}\,\mathbb{Q}$

Pick $\tau \in \mathrm{Aut}\,\mathbb{Q}$. Assume $\tau(1) = k$, $k \ne 0$

Then. $\forall \frac{m}{n} \in \mathbb{Q}$. (注: 此时取的 element 形式变化!)

$\therefore n\tau(\frac{m}{n}) = \tau(m) = m\tau(1) = mk$

$\therefore \tau(\frac{m}{n}) = \frac{m}{n} \cdot k$, $\therefore \tau(x) = kx$, $k \in \mathbb{Q}^*$

即 $\mathrm{Aut}\,\mathbb{Q} = \{\tau: x \mapsto kx \mid k \in \mathbb{Q}^*\} \cong \mathbb{Q}^*$

(同构必将n阶元映为n阶元!)
(同构对n阶封闭!)
(同构对任意集合都成立, 但内自同构仅对某一特定集合, 任取不成立)

Remark: $(\mathbb{Q}, +) \ncong (\mathbb{Z}, +)$. 否则设 φ is isomorphism

$\varphi(1) = 1$, then $\frac{1}{2} \in \mathbb{Q}$, but $\varphi(\frac{1}{2}) = \frac{1}{2}$, contradiction!

$(\mathbb{R}, +) \cong (\mathbb{R}, \cdot)$, by: $x \mapsto e^x$

(d) Pick $\varphi(x) = \frac{bx}{a}$. check $\varphi \in \mathrm{Aut}\,G$

(e) Since $|Inn G| < |Aut G|$. then $G/C(G)$ is cyclic. $\therefore G$ is Abelian

Now. Prove $\exists \varphi \in Aut G$. $|\varphi| = 2$. then $2 \mid |Aut G|$

If $\exists g \in G$. $|g| > 2$, then $\varphi: g \mapsto g^{-1}$ is well-def. And φ is of order 2.

If All elements in G is of order 2. then:

Let $\varphi(g_1) = g_2$, $\varphi(g_2) = g_1$

$\varphi(g) = g$. $g \in G$. $g \neq g_1, g_2$

$\therefore |\varphi| = 2$

武汉大学 数学与统计学院 School of Mathematics and Statistics

Date. No.

(f) $\sigma_a: G \to G$

$g \mapsto aga^{-1}$. $\forall g$

Denote $Inn G = \{\sigma_a \mid a \in G\}$.

Easily check $Inn G < Aut G$.

→ Moreover: $Inn G \trianglelefteq Aut G$!

Pf: $\sigma_a^{-1} \varphi \sigma_a(g)$

$= a^{-1} \varphi(\sigma_a(g)) a$

$= a^{-1} \varphi(aga^{-1}) a$

$= a^{-1} \varphi(g) \varphi(a) (a^{-1} \varphi(a))$

$= \sigma_{a^{-1}\varphi(a)}(\varphi(g))$

$\varphi \sigma_a \varphi^{-1}(g) =$

$\varphi(a \varphi^{-1}(g) a^{-1})$

$= \varphi(a) g \varphi^{-1}(a)$

$= \sigma_{\varphi(a)}(g)$

$\in Inn G$!

Note that $f: G \to Inn G$. epi-

$a \to \sigma_a$

$\forall g$.

$\ker f = \{a \mid \sigma_a(g) = g\} = \{a \mid aga^{-1} = g\} = \{a \mid ag = ga\}$

$= C(G)$. $\because C(G) \trianglelefteq G$. $\therefore Inn G \cong G/C(G)$

e.g. $C(S_n) = \{id\}$. 即 $Inn S_n \cong S_n$ ($n \geq 3$)

Pf: If $\sigma \in S_n$. $\sigma \neq id$. $\exists i$. s.t. $\sigma(i) = j \neq i$.

Pick $k \neq i, j$. $(\sigma \circ (ik))(k) = j$

However. $((ik) \circ \sigma)(k) = \begin{cases} k, & \sigma(k) = i \\ i, & \sigma(k) = k \\ \sigma(k) & \end{cases}$ since $\sigma(k) \neq j$, because $k \neq i$

$\therefore (ik) \circ \sigma \neq \sigma \circ (ik)$, $\therefore \sigma \notin C(S_n)$!

→ cor. If $G_1 \cong G_2$ then $Aut G_1 \cong Aut G_2$, $Inn G_1 \cong Inn G_2$

(Hint: $\varphi: G_1 \to G_2$ then: $\sigma_2 \cdot \varphi(a) \mapsto \varphi(\sigma_1(a))$, $\sigma_1 \in Aut G_1$)

(1) Little Lemma: $|c^{-1}ac| = |a| \Rightarrow |ab| = |ba|$

Since $ba = a^{-1}(ab)a$

(2) $f: G \to H$. homo. $|f(a)|$ finite. then

$|a|$ is infinite or $\frac{|a|}{|f(a)|} \in \mathbb{Z}^+$

Pf: $f(a^n) = f^n(a)$, when $a^n = e_G$.

then $f^n(a)$ must be e_H $\therefore \frac{|a|}{|f(a)|} \in \mathbb{Z}^+$ or $+\infty$!

(3) G is cyclic. then G/H. ($H < G$) is cyclic. When $H = \langle a^t \rangle$. then. G/H

$= \{H, aH, \cdots a^{t-1}H\}$. $|G/H| = t$.

Date.
No.

武漢大學 数学与统计学院
School of Mathematics and Statistics

3 The Criterion of Cyclic Group:

G is finite, $|G|=n$. then G is cyclic

$\Leftrightarrow \forall k|n$. at most exist a subgroup with order k.

Pf: "$\Rightarrow$" trivial. Now we prove "$\Leftarrow$"

Lemma. $\sum_{m|n} \varphi(m) = n$

Pf: Assume $|a|=n$. then Assume $|a^k|=m$.

Then $n=(k,n)m \therefore \frac{n}{m}=(k,n)$, $m|n$.

$\therefore k=\frac{n}{m}\cdot r$ $\frac{n}{m}=(\frac{n}{m}\cdot r, n)=\frac{n}{m}(r,m)$

$\therefore (r,m)=1$, 对每个不同的 m. r 有 $\varphi(m)$ 种选择. → 且 (m,r) 取好 对应不同的 k!

而 LHS 中的 k 有 $|\sim n$ 个, 则 $n=\sum_{m|n}\varphi(m)$

Lemma. Assume $[d_i]_{i=1}^{t}$ is the order of ele in G.

The the num of elements with order d_i is at most $\varphi(d_i)$

Pf: If $|a|=|x|=d_i$. Since exist at most 1 subgroup $\therefore \langle a\rangle=\langle x\rangle$. then $x=a^k$, but $(k,d_i)=1$.

$\therefore$ 共有 $\varphi(d_i)$ 种 x 的选择!

$\Rightarrow \sum_{d_i|n,\text{some } i} \varphi(d_i) = n = \sum_{m|n}\varphi(m) \therefore \exists d_i=n$.

2nd Criterion: $\forall$ subgroup of G can be written as $G^m=\{g^m \mid \forall g\in G\}$.

$\Leftrightarrow$ G is cyclic!

Case 1. If $|a|$ is infinite. Assume $\langle a\rangle = G^m$

$\exists b \in G$. s.t. $a = b^n$. Assume $\langle b\rangle = G^n$.

$\exists c \in G$. s.t. $b = c^n$. $c^n \in G^n$.

$\therefore \exists i$. s.t. $c^n = a^i = a^{mni}$ $\therefore m = 1$

Case 2. If $\forall a \in G$. $|a|$ is finite.

Then pick g with order p is prime. $p \mid |G|$

$\langle g\rangle = G^n$. then $\forall x \in G$. $x^{np} = e$. $|x| \le np$. which is bounded! (fix "p")

Then $\{p_i\}_1^n$ is element's prime order in G. (it holds!)

Note that $H < G$. then $H = G^t$

$\therefore xHx^{-1} = xG^t x^{-1} = \{xg^t x^{-1} \mid \forall g \in G\} = \{(xgx^{-1})^t \mid \forall g \in G\}$

$= \{g^t \mid \forall g \in G\} = G^t = H$. since $xgx^{-1} \in G$.

2) $\therefore$ $\forall$ subgroup of G is normal!

3) Assume g is an element with order p in G. p is a prime

We claim that $g \in C(G)$

If: $\forall x \in G$. $xgx^{-1} = g^i$. (Assume $\langle g\rangle = G^t$. $\langle g\rangle$ is normal!)

Also. $gxg^{-1} = x^j \Rightarrow gx^j = xg = g^i x$

$\therefore g^{i-1} = x^{j-1}$. since $(i-1, p) = 1$ $\therefore \exists k$.

s.t. $(g^{i-1})^k = g = x^{(j-1)k}$. then x, g can be commuted!

4) Assume h has order $|h|$. s.t. $\prod_1^n p_i \mid |h|$

And $|h|$ is the largest.

$\langle h\rangle = G^k$. $\therefore \exists\ h = a^k$ $|h| = |a^k| = \dfrac{|a|}{(|a|, k)}$

$\therefore (k, \prod_1^n p_i) = 1$ $\therefore |a|$ can be divided by $\prod_1^n p_i$ $\therefore |a| \le |h| \le |a|$

$\therefore (|a|, k) = 1$. $\exists u, v$ s.t. $u|a| + kv = 1$ by Bezout Theorem.

$\forall x \in G$. since $|x| \mid \prod_1^n p_i$ $\therefore (|x|, k) = 1$ $\therefore u|x| + vk = 1$ $\therefore x = x^{u|x| + vk} = (x^u)^k \in G^k$

$\therefore G \subseteq G^k \subseteq G$ $\therefore G^k = G = \langle h\rangle$

指 $\Sigma |x| \mid x \in G\}$. then: $|G|$ finite?

may be!

But $p_i < np$.

$\{p_i\}$ is finite!

Counter-example:

$\forall a \in G$. $|a|$ finite

But $|G|$ infinite:

$G = \bigcup_{i=1}^{\infty} G_i$. G_i 为 i 次单位根群.

(4) A group has a finite number of subgroup is finite.

Pf: Assume at G. we claim $|a|$ is finite. otherwise. $\langle a \rangle$ has an infinite number of subgroup. $\therefore G = \bigcup_{a \in G} \langle a \rangle$ is finite!

Not! (maximal proper subgroup)

(5) 一个无限循环群的极大子群 M:

不存在 B. s.t. $M < B < G$

此时. G 当且仅当. $M \cong p\mathbb{Z}$ (易证!)

$\Rightarrow$ Corollary: If $|G|$ finite. which has only one 极大子群. 则 $|G| = p^k$. p is a prime.

Pf: (…) $\Rightarrow G = \langle g \rangle$. If $|g| = pq$. $(p,q) = 1$.

then $\langle g^p \rangle, \langle g^q \rangle < G$. By Def:

$\langle g^p \rangle, \langle g^q \rangle < M$. $\therefore$ By Bezout. $\exists m, n$.

$mp + nq = 1$ $\therefore$ $g \in M$. $\therefore \langle g \rangle < M$. contradict!

(…): Since M is unique. $\therefore M$ is maximal

If $g \notin M$. $g \in G$. then

$G = \langle g \rangle$. or $\langle g \rangle < G$.

$\langle g \rangle < M$. contradict!

(6) G is an Abelian group. If $\forall a \in G$.

$|a|$ is finite. The maximal order is n.

Then $\forall a \in G$. $|a| \mid n$

Pf: Assume $g \in G$. $|g| = n$. Pick $b \in G$.

If $|b| \nmid |g|$. then $\exists p$. s.t. $p^k \| |g|$. $p^s \| |b|$

$k < s$, then $|g| = p^k g_1$. $|b| = p^s b_1$

$|g^{p^k} \cdot b^{b_1}| = p^s \cdot g_1 > p^k \cdot g_1$. contradiction!

(7) 唯一性构造: If a is the unqiue element in G.
with order 2. Then $a \in C(G)$

Pf: $\Leftrightarrow \forall x \in G.\ xa = ax$. Since $|xax^{-1}| = |a|$
then By the uniqueness. $xax^{-1} = a$!

⟶ 共轭构造法!
↓
$f: xGx^{-1} \mapsto G$. iso!
$xGx^{-1} \cong G$!

(8) $(|a|, |b|) = 2$. but $|ab| = 2k+1$. Prove: $\exists c$. s.t. $b = cac^{-1}$

Pf: Note that: $b(ab)^{2k+1} = (ba)\cdots(ba)(bab)a(bab)(bab)\cdots(bab)$
$= (ba)\cdots(ba)(bab)a[baba\cdots(bab)]^{-1}$ Since $a = a^{-1}$, $b = b^{-1}$

Remark: 上述两个元素共轭!

(9) Some conclusion about "HK"

(a). $H, K \subset G$ then $HK \subset G$. $\Leftrightarrow KH = HK$.

Pf: "$\in$" $\forall h_1k_1, h_2k_2 \in HK$. $(h_1k_1)^{-1}h_2k_2 = k_1^{-1}h_1^{-1}h_2k_2$
$\in k_1^{-1}HK = k_1^{-1}kH \in kH = HK$
"$\ni$" $\forall hk = (e\cdot h)\cdot(k\cdot e) \in kH$
$\forall kh = ((kh)^{-1})^{-1} \in (kH)^{-1} = H^{-1}k^{-1} = HK$

(b) $H, K < G$. with finite order.
And $[G:H]$, $[G:K]$ relatively prime. then $G = HK$.

Pf: $|G| = [G:H][H:H\cap K] = [G:K][K:H\cap K]$
$\therefore [G:K] \mid [H:H\cap K] \Leftrightarrow G = HK$!

(c) Dedekind Theorem: If $H, K, N < G$. $H < N$
Then $HK \cap N = H(K\cap N)$ (check!)

Corollary: $H, K, N \lhd G$, $H \subset K$, $H \cap N = K \cap N$, $HN = KN$
then $H = K$

(1) $|G| = p^s m$, $p \nmid m$, $H < G$, $|H| = p^s$, $K \subset G$, $|K| = p^t$
$t < s$, but $K \not\subset H$ Prove: $HK \neq G$.

Pf: If $HK < G$, $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p^{s+t}}{|H \cap K|}$
$\because \frac{|G|}{|HK|} \in \mathbb{Z}^+ \quad \therefore V_p(|HK|) \leq s \quad \therefore |H \cap K| \geq t = |K|$
since $K \subset HK$
$\therefore |H \cap K| = |K|$ 与 $K \not\subset H$ contradiction!

(2) 双陪集: $H < G$, $K \subset G$, $g \in G$, HgK称为
G的一个双陪集.

(a). $|HgK| = |H|[K : K \cap g^{-1}Hg] = |K|[H : H \cap g^{-1}Kg]$

(b) Use Double coset: Prove: $A < G$, $|A|$ is finite
$\exists \{g_i\}_1^n \subset G$, which can be the representives
of Left coset and right coset of G

Pf: (a). $HgK = \bigcup_1^t HgK_i$, see as right coset
of Hg, then $|HgK| = |H| \cdot t$.
Note that $\{k_i\}_1^t$ are the representives
of $K \cap g^{-1}Hg$, Because if $k \in K \cap g^{-1}Hg$
then $HgK = HHg = Hg \quad \therefore t = [K : K \cap g^{-1}Hg]$
$\therefore |HgK| = |H|[K : K \cap g^{-1}Hg]$

来积形式 ← 陪集分解法!

(b) Ref relation "$\sim$": $x \sim y \iff x \in HyK$

which can be easily checked it's equivalence!

$\therefore G = \bigcup_{g_i \in G_R} Hg_iK$. G_R is the set of representive!

$\therefore$ We can write G as $\bigcup_{g \in G_R} AgA$

(我们可将 AgA 拆为 $[A : A \cap g^{-1}Ag]$ 个左陪集

或右陪集之并!即: $AgA = \bigcup_1^t Aga_i = \bigcup_1^t b_igA$)

Note that $A = a_iA = Ab_i$. Since $a_i, b_i \in A$.

$\therefore AgA = \bigcup_1^t Ab_iga_i = \bigcup_1^t b_iga_iA$

Then $\bigcup_{g \in G_R} \{ b_{i(g)}\, g\, a_{i(g)} \mid 1 \le i \le t(g) \}$ is what we need!

(3) $H, K < G$, If $\exists a, b \in G$. s.t. $aH = bK$, Prove: $H = K$.

Pf: $a^{-1}bK = H$. (注意取单位元的意识, Pick $e \in K$).

$\Rightarrow a^{-1}b \in H$ $\therefore$ Assume $a^{-1}b = h$ $hK = H \Rightarrow K = h^{-1}H = H$.

(4) If $H_k < G$, $1 \le k \le n$, $[G : H_k]$ is finite. $\forall k$.

then $[G : H_1 \cap H_2 \cap H_3 \cdots \cap H_n]$ is finite!

Pf: 归纳 $[G : H_1 \cap \cdots H_{n-1}]$ is finite. Denote $H_1 \cap H_2 \cdots \cap H_{n-1} = H$.

Then Prove: $[G : H \cap H_n]$ is finite

Note that $\forall$ $H \cap H_n$ 的左陪集: $c(H \cap H_n) = cH \cap cH_n$

又 $\forall$ $aH \cap bH_n$ 非空. Pick $c \in aH \cap bH_n$, then.

$aH = cH$, $bH_n = cH_n$ $aH \cap bH_n = cH \cap cH_n = c(H \cap H_n)$

~~$\therefore$ 类 $H \cap H_n$ 的左陪集为 $\bigcup (aH \cap bH_n)$, 又 aH 反~~ ~~bH_n~~ ~~有限个!~~

$\therefore$ $H \cap H_n$ 的左陪集为 $\bigcup (aH \cap bH_n)$
$\hat{}$ G 关于 $\hat{}$ 分解

→ 关于 $H \cap H_n$ 的 left-coset 为 H, H_n left-coset 的交!

(1) If $N<G$, $[G:N]=2$, Then N is normal in G.

Pf: Note that $G=N\cup aN=N\cup Na$.

Since $N\neq Na$ $\therefore aN=Na$.

(2) Little Lemma. If $N_i\triangleleft G$, $1\leq i\leq n$ then $\cap N_i\triangleleft G$

(3) N is cyclic subgroup which is normal in G, then $\forall$ subgroup of N is normal in G.

Pf: Pick $\langle a^k\rangle<N=\langle a\rangle$. $\forall g\in G$. $a^{kn}\in\langle a^k\rangle$

$ga^{kn}g^{-1}=(gag^{-1})^{kn}=(a^t)^{kn}=(a^k)^{nt}\in\langle a^k\rangle$

Since $\langle a\rangle\triangleleft G$. $\therefore\langle a^k\rangle\triangleleft G$.

(4) $N\triangleleft G$. If N and G/N is finitely generated. Then G so is.

Pf: Assume $N=\langle b_1,\cdots b_m\rangle$. $G/N=\langle a_1N, a_2N\cdots, a_sN\rangle$

$xN\in G/N=\prod(a_{ik}N)^{t_k}=(\prod a_{sk}^{t_k})N$.

$\therefore\forall x=\prod a_{sk}^{t_k}\cdot n=\prod a_{sk}^{t_k}\prod b_{ij}^{t_{ij}}\in\langle\{a_s\}_1^s\cup\{b_i\}_1^n\rangle$

Prove: $N\triangleleft G$. $[G:N]=m$. $\forall a^m\in N$, $\forall a\in G$.

Pf: $\forall a\in G$. Since $G=N\cup a_1N\cup a_2N\cdots\cup a_{m-1}N$.

$a^m=(a_iN)^m=a_i^mN\Rightarrow a_i^m\in N$.

~~Note that $G/N=\{N, a_1N, a_2N\cdots a_{m-1}N\}$.~~

$|a_iN|\mid|G/N|$ $\therefore(a_iN)^m=eN$!

(6) $H<G$. 若关于H取两个左陪集之积仍为左陪集.

则 $H \triangleleft G$.

Pf: Trick: $aHa^{-1}H = cH$. Pick $a\cdot e\cdot a^{-1}\cdot e = ch$

$\therefore c = h^{-1}$ $\therefore aHa^{-1}H = H$. $aha^{-1}e = h' \in H$. □

(7) If G has unique subgroup with order n.

Then it's normal in G.

Pf: Note that $\forall a \in G$. if $H<G$, $|H|=n$.

By $a^{-1}Ha \cong H$. then $|a^{-1}Ha| = |H| = n$.

$\therefore a^{-1}Ha = H$. $H \triangleleft G$.

(8) $N \triangleleft G$. $|N| = m$. If exists $a \in G$. $\angle (n,m)=1$.

$|aN| = n$ in G/N. Then $\exists b \in G$.

$|b| = n$. s.t. $bN = aN$.

Pf: ($\Rightarrow$) $a^{-1}bN = N$. $\exists u, v$. $un+vm=1$ ⟶ By (*)!

$(aN)^n = N = a^nN$ $\therefore a^n \in N$.

$\therefore a = a^{un+vm} = (a^n)^u \cdot (a^m)^v = (a^m)^v \cdot a^{nu}$

Let $b = a \cdot a^{-nu}$!

$b^n = (a^{mv})^n = (a^n)^{mv}$, since $a^n \in N$ $\therefore b^n = e$.

If $\exists r<n$. s.t. $b^r = a^{mrv} = e$. $n \mid mrv$

$\because (mv, n) = 1$, $\therefore n \mid r$ $\therefore |b| = n$

Date.
No.

武漢大學 数学与统计
School of Mathematics and St

(9) (a). If $N \triangleleft G$, $[G:N]$ is finite and relatively prime
$H < G$, $|H|$

then $H < N$

(b) If $N \triangleleft G$, $[G:H]$ finite and relatively prime.
$H < G$ $|N|$

then, $N < H$.

Pf: (a). Way 1. Assume $[G:N] = n$, $|H| = m$, $(n,m) = 1$

$\therefore \forall h \in H$, $h^n \in N$. $\because \exists u, v$. $un + mv = 1$

$\forall g \in H$, $g = g^{un+mv} = (g^n)^u \in N$

(b) Way 2. Note that H isn't normal in G.

We change the way: $N \triangleleft NH < G$.

$\therefore [NH:H] \mid [G:H]$, $\because |NH|/|H|$

$= [NH:H] = \frac{|N|}{|H \cap N|}$

$\therefore [NH:H] \mid |N|$ $\therefore [NH:H] \mid ([G:H], |N|) = 1$

$\therefore NH = H$, $N < H$

($G/C(G) \times C(G) \cong G$?)

(12) (a) $G/C(G)$ is cyclic, then G is Abelian.

Pf: Note that $G/C(G) = \langle \bar{g} \rangle$

$\therefore \forall a, b \in G$. $a = g^m c_1$, $b = g^n c_2$, $c_1, c_2 \in C(G)$

$\therefore ab = ba$, check!

Remark: Note that $Inn(G) \cong G/C(G)$

If $Inn(G)$ is cyclic, $\Rightarrow$ G is Abelian

Remark: (1) 注意变换的几何直观!
(2) 逆映交换乘顺序，而同态保持顺序!
⇒ 联系Abel性!
(3) 注意 $a = g^{-1}\alpha(g) = g^{-2}$，只有保证：奇数阶Abel群可开方：$\beta: g \mapsto g^2$
若 $\beta(g_1) = \beta(g_2)$ ∴ $(g_1 g_2^{-1})^2 = e$，但 $\forall g \in G$，$|g| > 2$，∴ 仅 $g_1 = g_2$
∴ β 为单同态!
若 β^{-1} ∴ $\beta^{-1}(g^2) = g$ 为开方运算!

(11). $\alpha \in \mathrm{Aut}\,G$. 对 $\forall g \in G$, $\alpha(g) \neq g$, and $\alpha^2 = 1$, then G is Abelian with odd order!

→ 联系投影变换! $\varphi^2 = \varphi$
$\forall g = \underline{\varphi(g)} + \underline{g - \varphi(g)}$
投影　正交部分.
(而Abel性考虑到 $x \mapsto x^{-1}$ 即需证明 α 为逆?)
(注意 $\varphi \in \mathrm{Aut}\,G$，即知的正交/投影平面即为全空间.)

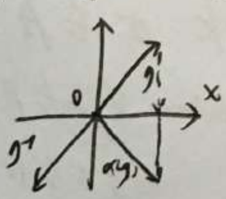
Pf: Develop: $H = \{g^{-1}\alpha(g) \mid \forall g \in G\}$. 将命题化为证明集合相等!

Then $H \supset G$. Since element is destinctive in H.

($Otherwise$, $\exists h^{-1}\alpha(g) = g^{-1}\alpha(g)$, ∴ $h^{-1}g = \alpha(h^{-1}g)$)

$a = g^{-1}\alpha(g)$ ∴ $\underline{\alpha(a) = \alpha(g^{-1})g = a^{-1}}$, And

$a \neq a^{-1}$ ∴ $|G|$ is odd!



$\alpha^2 = 1$ 可看作某个平面反射，而虚线向量：$g^{-1}\alpha(g)$ 恰好经 α 反射后为逆. ∴ 证明 $\{g^{-1}\alpha(g)\} = \{g\}$ 即可!

(12) (a) If $C(G) = \{e\}$, then $C(\mathrm{Aut}\,G) = \{id\}$.

Pf: Assume $\varphi \in C(\mathrm{Aut}\,G)$. But $\exists a$, s.t. $\varphi(a) = b \neq a$.

then $\tau_a \varphi = \varphi \tau_a \Rightarrow a^{-1}b\,\varphi(x) = \varphi(x)\,a^{-1}b$

$\varphi(x)$ is arbitrary. ∴ $a^{-1}b \in C(G)$ ∴ $a^{-1}b = e$. contradict!

(13) ☆ φ 为 G 到自身的 epi-, Prove: If G has a finite number of subgroups, then φ is auto-

Pf: 体会同构的意义. 取 $K = \ker\varphi$. Note that:

$G/\ker\varphi \cong G$. 将研究 G 转移至研究 G/K → 注意 φ 建立 G 中包含 K 子群与 G 的一一对应!

Note that $(g_1K)(g_2K)^{-1} \in H/K \overset{K \triangleleft G}{\Leftrightarrow}$

$g_1 g_2^{-1} K \in H/K \Leftrightarrow g_1 g_2^{-1} \in H$. namely $H < G$.

∴ G 与 G/K 含的子群数量相同!

If $\ker f \neq \{e\}$. $\{H_i/K\}_1^m$ 为 G/K 所有非单位子群. s.t. $K \subset H_i$

∴ $K \cup \{H_i\}_1^m$ 为 G 所有非单位子群. 再各补上单位子群 K 与 $\{e\}$.

两者数量不相等! 矛盾! ∴ $K = \{e\}$!

(1) Little Lemma. 设 $G < S_n$.

则要么 G 全为偶置换. 要么奇偶各占一半

Pf: Denote the set of odd permutation by A

Denote the set of even permution by B.

Pick $\sigma \in A$. $\varphi: \tau \longmapsto \tau\sigma$.

When $\forall \tau \in A$. φ is mono- between $A \to B$.

$\forall \tau \in B$. φ is mono- from $B \to A$.

$\therefore A \cong B$, namely $|A| = |B|$

(b) If $\sigma = (i_1 i_2 \cdots i_r) \in S_n$, $\tau \in S_n$.

then $\tau\sigma\tau^{-1} = (\tau(i_1)\ \tau(i_2) \cdots \tau(i_r))$

$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & & \tau(n) \end{pmatrix} \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_r & \cdots \\ i_2 & i_3 & i_4 & \cdots & i_1 & \cdots \end{pmatrix}$

$= \begin{pmatrix} i_1 & i_2 & \cdots & i_r \\ \tau(i_2) & \tau(i_3) & \cdots & \tau(i_1) \end{pmatrix} \begin{pmatrix} 1 & \cdots \\ \tau(1) & \cdots \end{pmatrix} = (\tau(i_1) \cdots \tau(i_r))\tau$

(which can be checked!) $\therefore \tau\sigma\tau^{-1} = (\tau(i_1) \cdots \tau(i_r))$

Corollary: S_n can be generated by $(1\,2\,3\cdots n)$ ($=\tau$) and $(1\,2)$ ($=\sigma$)

(By $\sigma_k = \tau\sigma_{k-1}\tau^{-1} = (k\ k+1)$) or $(1\,2)$, $(2\,3\cdots n)$

(2) Estimate: $C_{S_n}(\sigma) = \langle\sigma\rangle$ → 可推出 $C(S_n) = \{1\}$ since $|C_{S_n}(\sigma)| = |G|!$ Then $\forall \sigma \in C(S_n)$ 对 $\sigma \neq 1$!

Pf: $C_{S_n}(\sigma) = \{\tau \mid \sigma\tau = \tau\sigma, \tau \in S_n\}$.

Note that $\tau^{-1}\sigma\tau = \sigma = (\tau(i_1)\ \tau(i_2) \cdots \tau(i_r))$

$= (i_1\ i_2 \cdots i_r)$ 设 $\tau(i_1) = i_{k+1} \pmod n$

$\Rightarrow \tau = \sigma^k \in \langle\sigma\rangle$

(3) p is a prime. Then S_p has $(p-1)!$ elements with order p. $(p-2)!$ subgroups with order p.

Pf: Note that $\forall$ p-cycle's order is p. → p-cyc ∩ p-cyc = ∅.

There're $(p-1)!$ p-cycles. If $\sigma \in S_p$ which consists of r 条不相交的 cycle. $r \geq 1$.

then $\forall$ cycle's length $\leq p-2$, then order $< p$.

而 $|\sigma|$ 为 r 条 cycle 的最小公倍数阶. $\therefore |\sigma| \nmid p$.

Note that subgroup with order p is cyclic!

then 任取 $p-1$ 条 p-cycles 与 id 构成 p 阶群. 共 $(p-2)!$ 种!

(4) Cayley Thm. Application:

k is odd. Then G with order $2k$ must have a subgroup with order k.

In the other words → $\exists\, \pi: G \to S_G$.

Pf: $G \cong S_G$. then. $|S_G| = 2k$. $\exists\, a$ with order 2 in G. Pick $\pi(a) g = ag$.

Pick $x_1 \in G$. $x_1 \neq a$. then $ax_1 \neq x_1$. Pick $x_2 \in G \setminus \{x_1, ax_1\}$ ∵ $|a|=2$ ∴ $\pi^2(a)_g = g, \forall g$.

then $ax_2 \neq a, ax_1, x_1$ --- Then $G = \{x_1 \cdots x_k, ax_1 \cdots ax_k\}$ Since $\pi(a)$ is iso- so that 无不动点!

$\therefore \exists\, \pi_a = \begin{pmatrix} x_1 & x_2 & \cdots & x_k & ax_k & \cdots & ax_1 \\ ax_1 & ax_2 & \cdots & ax_k & x_k & \cdots & x_1 \end{pmatrix} = (x_1\, ax_1) \cdots (x_k\, ax_k)$ ∴ $\pi(a)$ 为 k 个 2-cycle ∴ $\pi(a)$ is odd permutation!

which is an odd-permutations in S_G. Since $S_G \subset S_n$.

$\therefore$ in S_G, there're a set A which consists of all even-permutations in S_G with order $\frac{2k}{2} = k$. By Lemma(b)

(4) A_n is the only (normal) subgroup of S_n with index 2

Pf: If $N \trianglelefteq S_n$. $\forall (i_1 i_2 i_3) \in S_n$. By $[S_n : N] = 2$

$\therefore (i_1 i_2 i_3)^2 \in N$. $\Rightarrow (i_1 i_2 i_3)^{-1} \in N$.

$(i_1 i_2 i_3)$

$\therefore N = A_n$!

(1) $ab=ba$. $(|a|,|b|)=1$, then

i) $\langle a\rangle\cap\langle b\rangle=e$ ii) $\langle a,b\rangle=\langle ab\rangle$

Pf: i) is trivial. Since $|x|\mid(|a|,|b|)$ if $x\in\langle a\rangle\cap\langle b\rangle$

ii) $\langle a,b\rangle=\{a^ib^j\mid 0\le i\le|a|,\ 1\le j\le|b|\}$.

$\supseteq\langle ab\rangle$. $\because|\langle ab\rangle|=|a||b|=\langle a,b\rangle$

$\therefore\langle a,b\rangle=\langle ab\rangle$

(2) Somethings about Dihedral Group:

Lemma: By $ba=a^{-1}b$

$\Rightarrow a^ib=ba^{-i}$

(a) $\langle a\rangle$ is the ~~unique~~ normal subgroup of D_n. $D_n/\langle a\rangle\cong\mathbb{Z}_2$.

Normal subgroup: when n is even

$\langle a^k\rangle$, $d\mid n$. Lemma: $\{e,a^2,\cdots a^{2n-2}\}\cup\{b,a^2b,\cdots a^{2n-2}b\}$ (A)

$\{e,a^2,a^4,\cdots a^{2n-4}\}\cup\{ab,a^3b,\cdots a^{2n-1}b\}$ ← gene. form: $a^{2m}b$

n is odd: $\langle a^d\rangle$, $d\mid n$. (A) $\to\langle D_n\rangle$.

Pf: $|\langle a\rangle|=n$. $\langle a\rangle<D_n$. Note. $[D_n:\langle a\rangle]=2$

$\therefore\langle a\rangle\lhd D_n$. $D_n/\langle a\rangle=[\langle a\rangle,b\langle a\rangle]\cong\mathbb{Z}_2$.

If $\exists\ a^ib$. s.t. $a^{i_1}a^ib\,a^{-i_1}=a^{i_1+i_2}ba^{-i_1}$

$=a^{2i_1+i}b$. $\because i_1$ is arbitrary $\therefore\{a^{2i_1+i}b\}=\{a^ib\}$

But $\{a^ib\}^n\notin D_n$ $\therefore\langle a\rangle$ is unique!

(b) $C(D_n)=\{e\}$, n is odd; $C(D_n)=\{a^{\frac{n}{2}},e\}$, n is even.

Pf: 1) Assume $a^k\in C(D_n)$. $a^k\cdot a^ib=a^ib\,e^k$

$\Leftrightarrow k+j\equiv j-k\pmod n$ $\Leftrightarrow k=0$ or $\frac{n}{2}$

2) Assume $a^kb\in C(D_n)$. $a^kb\,a^ib=a^iba^kb$

$=a^{i-k}=a^{k-i}$ $\therefore 2k\equiv 2j\pmod n$. j is arbitrary

$\therefore a^kb\notin C(D_n)$!

(c) $D_n^* \cong D_n$.

Pf: Note that $\exists$ generator f = rotation $\frac{2\pi}{n}$ and g = reflection above diameter!

$\therefore f^n = e,\ g^2 = e,\ fg = gf^{-1}$

Structure of Group.

① **Action on Set by Group:** → induce a hom- to S_X!

(1). Find the homo: $\pi: G \longrightarrow S_X$ (permution on Set X)

⇒ Construct f: $G \times X \longrightarrow X$, $(g, x) \longmapsto \pi(g)x$. : $f(g, x) = \pi(g)x$.

which should satisfy: $\begin{cases} a.\ \pi(g_1g_2) = \pi(g_1)\pi(g_2) \\ b.\ \pi(g_1) \in S_X,\ \pi^{-1}(g_1) \in S_X \end{cases}$

⇒ $f(g_1g_2, x) = \pi(g_1g_2)x = \pi(g_1)\pi(g_2)x = f(g_1, \pi(g_2)x) = f(g_1, f(g_2, x)) \Rightarrow$ con. a.

$\pi(g_1)\pi^{-1}(g_1) = \pi(g_1g_1^{-1}) = \pi(e) = id \Rightarrow$ con. b. which mean. $f(e, x) = x$!

Then, we claim: $[f: G \times X \to X] \Longleftrightarrow [\pi: G \to S_X]$.

(which mean: give a "f", we can find "π". verse vise!)

(2) **Theorem:**

Lemma: i) $\overline{x} = \{gx \mid g \in h\}$ is the equivalent class which called orbit of x.

ii) $G_x = \{g \mid gx = x,\ g \in h\} < G$.

Theorem 1:

Then we have: $G/G_x \cong \bar{x}$ ($[G:G_x] = |\bar{x}|$) → can use $\frac{|G|}{|G_x|} = |\bar{x}|$ Find $|G_x|$!

Pf: $\varphi: gG_x \mapsto gx$. if $gx = hx \Leftrightarrow g^{-1}hx = x$.

$\Leftrightarrow g^{-1}h \in G_x \Leftrightarrow gG_x = hG_x$. then φ is well-def!

Check φ is bijection!

(such as: $C_G(x)$ $N_G(x)$ ...)

Corollary: if $\sum |\bar{x}_i| = |G|$. If let the action be conjugation. $\Rightarrow |G| = \sum [G:G_{x_i}] = |C(G)| + \sum [G:C_G(x_i)]$

(Let $K \subset G$. G act on G!)

(Note that $\sum \frac{1}{|G_x|} = 1$!)

Theorem 2: If G act on X st. $\forall x, y \in X$ → can be transitive!

$\exists g_0$ st. $y = g_0 x$. then $\bar{x} = \bar{y}$. and

which means in the same orbit, elements' stabilizers are conjugated! $G_x = g_0 G_y g_0^{-1}$

Pf: $\bar{x} = \bar{y}$ is trivial. $G_y = \{g \mid gy = y\} = \{g \mid gg_0x = g_0x\}$

$= \{g \mid g_0^{-1}gg_0x = x\}$. $= \{g \mid g_0^{-1}gg_0 \in G_x\} = g_0 G_x g_0^{-1}$

Proposition: i) $H < G$. $S = \{gH \mid g \in G\}$. If G act on S by left translation. then: kernel of: $G \xrightarrow{\varphi} A(S) < H$

(Act on (coset!))

ii) if $[G:H] = n$. no nontrivial normal subgroup of G is contained in H. then $G \cong$ a subgroup of S_n.

iii) $H < G$. G is finite. $|G/H| = p$ which is the smallest prime divides $|G|$. then $H \lhd G$.

Pf: i) G acts on its coset $\Rightarrow x g H = g H$. → which let kernel falls in H!
then let $g = e$. $\therefore x \in H$. $\therefore \ker \pi \in H$

ii) By i). $|S| = n$. And $\ker \pi \subset H$. $\therefore \ker \pi = \{e\}$
$\therefore G \cong S_n \cong G/\ker \pi$

iii) $|G/\ker \pi| \mid p!$. Since $G/\ker \pi$ is iso to a subgroup of S_p. And $[G:\ker \pi] = [G:H][H:\ker \pi]$
$[G:\ker \pi]|\ker \pi| = |G|$. Note that $|G/\ker \pi| \geq p$.
$\therefore |G/\ker \pi| = p$ $\therefore [H:\ker \pi] = 1$ $\therefore H = \ker \pi$!

Burnside Lemma: G acts on Ω which is a set. The orbits of Ω denoted by r. then $r = \frac{1}{|G|}\sum_{g \in G}|F(g)|$

$F(g) = \{x \mid g \circ x = x\}$.

Pf: 1°) $\Omega = \bigcup_{i}^{r} G(x_i)$. $|G(x_i)| = \frac{|G|}{|G_{x_i}|}$

which means the stabilizers of $G(x_i)$ with the same order. $\therefore G(x_i)$ 中所有元素共 $|G(x_i)|$ 个.
而稳定子有 $|G(x_i)||G_{x_i}| = |G|$ 个. (计重复)
(每个元素 每个稳定子元素)
$\therefore \sum_{1}^{r}|G| = \sum_{x \in \Omega}|G_x| = r|G|$

2°) 考虑 $S = \{(g, x) \mid g \circ x = x\}$. 1°)中为固定 x.
计算稳子个数 $\Rightarrow |S| = \sum_{x \in X}|G_x|$. 现固定 g
$\therefore |S| = \sum_{g \in G}|F(g)|$. $\therefore \frac{1}{|G|}\sum_{g \in G}|F(g)| = r$ □

g的稳定子 x x的稳定子.

Some inclusions:

① $\exists H < G$, $|G/H|$ is finite, then G contains a normal group of finite index, too.

Pf: Note that when discussing normal Consider the kernel of some homo-

$G \times [aiH \mid aiH$ is the representive of coset$)$.

$\longrightarrow [aiH)$. then $\exists \ker\varphi$.

$\varphi: G \longrightarrow A = S_n \cong S_{[aiH)}$. $|G/\ker\varphi| \mid n!$

$\therefore |G/\ker\varphi|$ is finite and $\ker\varphi \trianglelefteq G$!

remark: Or we can construct a normal group by N. Let $K = \bigcap x^{-1}Nx$. then $K \trianglelefteq G$. Then

$x \in G$ → the biggest normal group about G. included in N!

Prove $[G:K]$ is finite:

Lemma: $[G: g^{-1}Ng] = [G:N]$. By $xN \longmapsto xg \cdot g^{-1}Ng$

the map is bijection!

$\Rightarrow \forall x \in G$. $[G: x^{-1}Nx]$ is finite. Bwc $|G|$ is finite? $\therefore$ Consider $G/N_G(N)$. Note that $N < N_G(N) < G$. $[G: N_G(N)]$ is absolutely finite. $\therefore$ bec $x^{-1}Nx \neq N$, x is finite!

$\therefore [G: \bigcap x^{-1}Nx] = [G: \bigcap x^{-1}Nx]$ is finite!

$x \in G$ $\qquad$ $x \in G/N_G(N)$ finite

② Extend of Cayley Theorem:

$\forall G$ isom. to a subgroup of A_{2n}. where $|G|=n$.

Pf: Ref: $S_n \xrightarrow{i} A_{2n}$. by $i(\sigma) = \sigma\sigma'$.

$\sigma' = \begin{pmatrix} n+1 & n+2 & \cdots & 2n \\ \sigma(1)+n & \sigma(2)+n & \cdots & \sigma(n)+n \end{pmatrix}$, $\sigma' \cap \sigma = \emptyset$.

$\therefore$ "i" is homo-!

③ $N \trianglelefteq G$. $|N|=p$. $|G|=p^n$. then $N \leq C(G)$

→ N exists actually by the unique element "p" and Sylow

Pf: When noting that $N \trianglelefteq G$. Then we can consider G acts on N by conjugation.

Since $G \times N \to N$.

$\therefore |N| = \sum_1^r \frac{|G|}{|G_{n_i}|} = \sum_1^r \frac{|G|}{|C_G(n_i)|}$.

if $r>1$. Since $\frac{|G|}{|G_{n_i}|} = p^{k_{n_i}} \therefore k_{n_i} = 0$

$\therefore |N| = \sum_1^r \frac{|G|}{|G_{n_i}|}$. $C_G(n_i) = G \therefore N \leq C(G)$.

But we know: $e \in N$. $|O_e| = \left|\frac{|G|}{C_G(e)}\right| = 1$.

$\therefore r \geq 2$! which means $r=1$ can't happen!

→ Or consider $a \in N$. $a \neq e$. then $gag^{-1} \in N$. $|gag^{-1}| = p$. $\therefore |\langle gag^{-1} \rangle| = p$. $\therefore |G_a| = \frac{|G|}{|C_G(a)|} = 1$!

Remark: the set: $A = \{N_i \mid N_i \neq G\}$. then $p \mid |A|$. Note: $G \times A \to A$, $(g, N_i) \mapsto (g^{-1} N_i g)$

$\therefore |A| = \sum \frac{|G|}{|N_G(N_i)|}$. But $N_G(N_i) \neq G$.

Which implies: $N_i \trianglelefteq G$!

$\therefore p \mid \frac{|G|}{|N_G(N_i)|}$

(2) Sylow Theorem:

(1) Firstly: **Introduce some lemmas** All by Groups Action!

Lemma 1. Group H with order p^n acts on a finite set S. $S_0 = \{x \mid hox = x, \forall h \in H\}$

Then $|S_0| \equiv |S| \pmod p$

pf: $|S| = |S_0| + \sum \frac{|H|}{|H_x|}$. since $\frac{|H|}{|H_x|} > 1$. $\therefore p \mid \frac{|H|}{|H_x|}$

Lemma 2. $C(G)$ is nontrivial in a nontrivial p-group G

pf: $G \times G \xrightarrow{\text{conj}} G$. $|a| = |C(G)| + \sum \frac{|G|}{|G_x|}$. $|C(G)| \geq 1$

Lemma 3. $[G:H] \equiv [N_a(H):H] \pmod p$.

pf: S is the set of left cosets of G about H

$H \times S \subset \{aH \mid a \in G\}) \to S$

$haH = aH \Rightarrow a^{-1}ha \in H \therefore a^{-1}Ha = H$.

$\therefore a \in N_a(H)/H$. $\therefore [N_a(H):H] \equiv [G:H] \pmod p$

Since a/H may be a set. Then we choose $N_a(H)/H$ when then is a group!

(2) **Theorem 1.** Cauchy: If a finite group with order divisible by p, then there exists an element with order p.

pf: $S = \{(a_1, a_2, a_3 \cdots a_p) \mid \prod_1^p a_i = e, a_i \in G\}$.

Z_p acts on S by: $k \circ (a_1 \cdots a_p) = (a_{k+1} a_{k+2} \cdots a_p, a_1, \cdots, a_k)$

Note that Let $A = \prod_{k=1}^{p} a_k$ $B = \prod_{1}^{k} a_k$. $BA = e$. $\therefore AB =$

$ABAA^{-1} = AA^{-1} = e$. $\therefore$ $Z_p \times S \to S$. And $= (k_1 + k_2) \circ (a_1 \cdots a_p)$

$= k_1 \circ (k_2 \circ (a_1 \cdots a_p))$ $\therefore$ The action is well-def!

Then $(a_1 \cdots a_p) \in S_0 \iff a_1 = a_j$. Since $(e_1 \cdots e) \in S_0$.

$\therefore |S_0| \geq 1$. And $|S_0| \equiv |S| \equiv 0 \pmod p$ $\therefore \exists a \neq e$. $|a| = p$

Finite Sylow Theorem:

First: $|G| = p^l m$. then G contains a subgroup with order p^k $(0 \leq k \leq l)$. And each subgroup with order p^k is normal in some group with order p^{k+1}

Pf: By Induction on Cauchy Theorem:

$|H| = p^i$ $(1 \leq i < l)$ $\therefore [G:H] \equiv [N_G(H) : H] \equiv 0 \pmod p$

$\therefore p \mid |N_G(H)/H|$ which contains a subgroup $= H_1/H$

with order p. $\therefore |H_1| = |H_1/H||H| = p^{i+1}$. And $H \trianglelefteq N_G(H)$

$H_1 < N_G(H)$ $\therefore H \trianglelefteq H_1$

Remark: We can also use the Group Action Still:

$X = \{A \mid A \subset G, |A| = p^k\}$ (A is set!)

$G \times X \to X$ since $|gA| = |A|$. If $gA = A$

$(g, A) \mapsto gA$

$\Rightarrow g \in G_A$ (G_A is a group. Actually, we need $|G_A| = p^k$:) Then $G_A \times A \to A$

$\therefore A = \bigcup_{a \in A} G_A \cdot a$. And $G_A \subset A$. $\therefore |G_A||A| = p^k$

Note that $|X| = C_{p^l m}^{p^k} = \sum \frac{|G|}{|G_A|}$.

If $\forall A \in X$. $|G_A| \le p^{k+1}$. then $p^{l-k+1} \mid C_{p^l m}^{p^k}$

But $C_{p^l m}^{p^k} = \frac{p^l m (p^l m - 1) \cdots (p^l m - (p^k - 1))}{p^k (p^k - 1) \cdots (p^k - (p^k - 1))} \cdot \frac{p^l m - k'}{p^k - k'}$

$= \frac{p^l m - p^{k''} m'}{p^k - p^{k''} m'} = \frac{p^{l-k''} m - m'}{p^{k-k''} m - m'}$ can't be divided by p

$\therefore p^{l-k} \parallel C_{p^l m}^{p^k}$. contradiction!

Second: H is finite p-group of G. P is any sylow p-group of G. Then $\exists x$ such that $H < xPx^{-1}$

Pf: $H \times G/P \longrightarrow G/P$ (Then actions keep "P"!)

Note $|G/P|$ can't be divided by p. $\therefore |S_0| \neq 0$

$\therefore \exists xP \in S_0, \forall g$. $gxP = xP$ $\therefore x^{-1} g x \in P$.

$g \in xPx^{-1}$. $\forall g \in H$. $\therefore H < xPx^{-1}$

Third: The number of sylow-p-group of G is $kp+1$. And $kp+1 \mid |G|$

Pf: $\mathrm{Syl}_p(G)$ are the conjugations. So.

$G \times P \xrightarrow{\text{conj}} P$. P is the set of $\mathrm{Syl}_p(G)$

It's only one orbit $\therefore |P| = \frac{|G|}{|N_G(a)|}$. $a \in P$.

$\therefore$ the number divides $|G|$.

Then $Q \times P \xrightarrow{\text{conj}} P$. $R \in S_0 (= \{R\}) \Leftrightarrow xRx^{-1} = R$. $\forall x \in Q$.

$\therefore Q < N_G(R) < G$. since Q, R are sylp-group in G.

Then in $N_G(R)$. $R \trianglelefteq N_G(R)$ $\therefore Q = R$ $\therefore |S_0| = 1$.

($\because S_0 = \{Q\}$.) $\therefore |S| \equiv |S_0| \equiv 1 \pmod p$

Extend: Frobenius Theorem: By: (Wielandt) $|G| = p^\alpha m$.

Then the number of subgroup P with order $p^\beta = kp+1$

Pf: $\Omega = \{A \subseteq G \mid |A| = p^\beta\}$. $G \times \Omega \to \Omega$

$(g, A) \mapsto gA$.

Take an orbit O. $T \in O$. if $x \in T$. then

$x^{-1}T$ contains e. $\therefore \exists S \in O$. s.t. $e \in S$.

If $g \in G_S$. $gS = S$. $\therefore g \in S$. by $g \cdot e \in S$.

$\therefore G_S \subseteq S$. then:

Case 1. $G_S = S$. $\therefore S < G$ $|O| = \frac{|G|}{|S|} = p^{\alpha-\beta} m$

→ If $G_S \neq G$. then in G. all elements are subgrop of G? Of course not!

the O is the set of left cosets of G about S

Only an element is the subgroup of G.

Case 2. $G_S < S$. then $p^{\alpha-\beta+1} \mid |G|$. If $S \overset{\in O}{<} G$.

then $|G/S| = p^{\alpha-\beta}$. which contradicts!

Then there're no element in O being subgroup!

Now we count the orbits in Case 1. Suppose

there're k in Case 1.; l in Case 2.

$\therefore |\Omega| = \binom{p^\alpha m}{p^\beta} = kp^{\alpha-\beta} m + l \cdot p^{\alpha-\beta+1} m'$

Since $C_{p^{\alpha}m \cdot m'}^{p^{\beta}} / p^{\alpha-\beta} \equiv m^{-1}(km + lm'p) \pmod p$

$\equiv k$. we need prove: $C_{p^{\alpha}m}^{p^{\beta}} \cdot m^{-1} / p^{\alpha-\beta} \equiv 1 \pmod p$

$\Leftarrow$ $(p^{\alpha}m-1)\cdots(p^{\alpha}m-p^{\beta}+1) \equiv (p^{\beta}-1)(p^{\beta}-2)\cdots 2\cdot 1 \pmod p$

$p^{\alpha} \cdot q + (-1)^{\beta-1} \prod_{1}^{p^{\beta}-1} k$ $\because$ if $p \geq 3$, ✓.

if $p=2 \Rightarrow 0 \equiv 2 \cdot \prod_{1}^{2^{\beta-1}} k \pmod 2$ ✓.

Fourth: P is $\mathrm{Syl}_p(G)$, then $N_G(P) = N_G(N_G(P))$ → which can prove Syl III.

$[G : N_G(P)] \equiv [N_G(N_G(P)) : N_G(P)] \equiv 1 \pmod p$

pf: $N_G(P) \subset N_G(N_G(P))$ is obvious.

$\forall x \in N_G(N_G(P))$. $xN_G(P)x^{-1} = N_G(P)$

since $P \lhd N_G(P)$. $\therefore xPx^{-1} < N_G(P)$

$\therefore xPx^{-1} = P$ $\therefore x \in N_G(P)$ $\therefore N_G(P) \supset N_G(N_G(P))$

Remark: Consider **Frattini lemma**

If $N \lhd G$. $P \in \mathrm{Syl}_p(N)$, then $G = N_G(P)N$.

pf: $gNg^{-1} = N$. $\forall g$. Note that the structure of g: $g = hn$. $h \in N_G(P)$, $n \in N$. which means we just need prove $gn^{-1} \in N_G(P)$.

$\Rightarrow gPg^{-1} < N$. Note that gPg^{-1} and P $\in \mathrm{Syl}_p(N)$ $\therefore$ conjugate! $\therefore \exists n \in N$.

s.t. $n^{-1}gPg^{-1}n = P$ $\therefore n^{-1}g \in N_G(P)$

$\therefore g \in N_G(P)N$! $G < N_G(P)N < G$!

Another pf: $P < N_G(P) < M \lhd N_G(M)$;

Sylp(M) ⊂ Sylp(G), obviously

$\therefore N_G(M) = M$, $N_G(P) = M$.

Cor. If $P \in Syl_p(G)$, $N_G(P) < M < G$, then $N_G(M) = M$.

pf: $\forall x \in N_G(M) \Rightarrow x^{-1}Mx = M > N_G(P) > P$.

$\therefore M > xPx^{-1}$. since $P \in Syl_p(M)$, too

so xPx^{-1} is $\Rightarrow \exists m \in M$, s.t. $mxPx^{-1}m^{-1} = P$.

$\therefore mx \in N_G(P) < M \quad \therefore x \in m^{-1}m = M$.

$\Rightarrow$ Let $G = N_G(N_G(P))$, $N = N_G(P) \lhd G$

$\longrightarrow xPx^{-1} = P$. $gxg^{-1}gPg^{-1}gx^{-1}g^{-1}$
$= gPg^{-1}$
Or by $N_G(P)$ is the kernel of $G \times Syl_p(G) \to Syl_p(G)$ $\xrightarrow{conj}$ $\{\}$.

(3) Infinite Sylow Theorem:

If $|G| = +\infty$, then the Sylow Theorem above will not effect! (include I, II, III)

(Tarski Monster Counterexamples)

$\longrightarrow$ Prüfer p-group: $C_{p^\infty} = \bigcup_{k \geq 0} \{ e^{\frac{2\pi i k}{n}} \mid n = p^k, k \geq 0 \}$.

We claim: If G is an infinite p-group, then either G has a subgroup of order p^n, $n \geq 1$ or $\exists m$, $\forall$ finite subgroup of G with order p^k, $k \leq m$

pf: Def "$\leq$" on the set $S = \{ P \mid P < G \}$.

If $P_1 \leq P_2$. ($\Leftrightarrow$) $|P_1| \mid |P_2|$. $P_1 < P_2$

Then $(S, \leq)$ is a poset.

Take a chain C. then $\bigcup_{P \in C} P$ is the upper bound in C. $\therefore$ By Zorn's lemma:

$\exists$ maximal elements in $(S, \leq)$.

(4) Some conclusions:

① $|G| = p^n t$. $p \nmid t$. $\mathrm{Syl}_p(G)$. p^β subgroup in G is the same as order p^β subgroup in P (mod p)

Pf: $S = \{H \mid H < G, |H| = p^\beta\}$. $P \times S \xrightarrow{\text{conj}} S$, if $|O_H| = 1$ then $pHp^{-1} = H$. $\forall p \in P < N_G(H)$, $P \in \mathrm{Syl}_p(N_G(H))$

$\therefore \exists x \in N_G(H)$. $H < xPx^{-1} \Rightarrow x^{-1}Hx = H < P$.

$\therefore |O_H| = 1 \Leftrightarrow H < P$. If $|O_H| > 1$, then $P \mid |O_H|$ which means we can omit it!

② N, G/N are p-subgroup. ($N \triangleleft G$) then. G is p-subgrp.

Pf: $|N| = p^s$. $|G/N| = p^t$. $\therefore \forall g \in G$ $gp^t \in N$. $\therefore (gp^t)^{p^s} = e$

Remark: generally, $N \triangleleft G$. $H < G$. which are both p-subgroup, then HN is p-grp too!

Pf: By $HN/N \cong H/H \cap N$

③ G is finite p-group. $H \triangleleft G$. $H \neq \langle e \rangle$, then $H \cap C(G) \neq e$

Pf: $G \times H \xrightarrow{\text{conj}} H$. $|H| = |C_G(H)| + \sum \frac{|G|}{|G_{h'}|}$

$|G_h(H)| \geq 1$. $|C_G(H)| \equiv 0 \pmod p$

Which means $\exists h' \in H$. $\frac{|G|}{|G_{h'}|} = 1 \therefore h' \in H \cap C(G)$

Date.
No.

① $\exists N_i \trianglelefteq G$. $|G| = p^n$. s.t. $G > N_{p^1} > N_{p^{n-1}} \cdots > N_1 > \langle e \rangle$.
$|N_i| = p^i$.

Pf: By Induction: then since $p \mid |C(G)|$.

Pick a subgroup of $C(G)$ with order p.

Remote $= N_1$. then $|G/N_1| = p^{n-1}$.

$\therefore$ $G/N_1 > N_{p^1}/N_1 > N_{p^2}/N_1 \cdots > N_1$

$\pi: H \longrightarrow H/N_1$. canonical projection.

then. $G > \pi^{-1}(N_{p^1}/N_1) > \cdots > \pi^{-1}(N_{p^{n-1}}/N_1) > N_1 > \langle e \rangle$

② If $\forall G \in Sylp(G)$. $G \trianglelefteq G$. $\forall p$. then
G is the direct product of syl-subgroups

Pf: $|G| = \prod_1^k p_i^{n_i}$. $|P_i| = p_i^{n_i}$, $P_i \trianglelefteq G$. ⟶ By Lagrange!.

then $P_i \cap P_j = \langle e \rangle$. since $\prod_{i \neq j}^{k} P_i < G$ $\because \prod_1^k P_i = P_1 \times P_2 \cdots \times P_k$

$\prod_{i \neq j}^{k} P_i \cap P_j = \langle e \rangle$ $\therefore G = P_1 \times P_2 \cdots P_k$

since $|G| = \prod P_i^{n_i}$.

⑥ Every Aut of S_φ is Inn-aut. then $S_\varphi \cong Aut S_\varphi$

Pf: $C(S_\varphi) = \langle e \rangle$ $\therefore S_\varphi \cong Aut S_p \cong Inn S_\varphi$.

We only prove: $S_\varphi \cong Aut S_p$.

Firstly. Note that $\Sigma = [\langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle]$.
is the set of $Syl_3(S_4)$. $|\Sigma| = 4$. then:

$Aut S_4 \times \Sigma \to \Sigma$, since $\sigma \in Aut S_4$. which transforms
$(\sigma, \langle x \rangle) \to \sigma(\langle x \rangle)$ 3-order-subgrp to 3-order-subgrp!

$\therefore$ Induce a map: $Aut S_4 \xrightarrow{f} S_4$

Date.
No.

① $\exists N_i \trianglelefteq G$. $|G| = p^n$. s.t. $G > N_{p^1} > N_{p^{n-1}} \cdots > N_1 > \langle e \rangle$.
$|N_i| = p^i$.

Pf: By Induction: then since $p \mid |C(G)|$.

Pick a subgroup of $C(G)$ with order p.

Remote $= N_1$. then $|G/N_1| = p^{n-1}$.

$\therefore$ $G/N_1 > N_{p^1}/N_1 > N_{p^2}/N_1 \cdots > N_1$

$\pi: H \longrightarrow H/N_1$. canonical projection.

then. $G > \pi^{-1}(N_{p^1}/N_1) > \cdots > \pi^{-1}(N_{p^{n-1}}/N_1) > N_1 > \langle e \rangle$

② If $\forall G \in Sylp(G)$. $G \trianglelefteq G$. $\forall p$. then
G is the direct product of syl-subgroups

Pf: $|G| = \prod_1^k p_i^{n_i}$. $|P_i| = p_i^{n_i}$, $P_i \trianglelefteq G$. ⟶ By Lagrange!.

then $P_i \cap P_j = \langle e \rangle$. since $\prod_{i \neq j}^{k} P_i < G$ $\because \prod_1^k P_i = P_1 \times P_2 \cdots \times P_k$

$\prod_{i \neq j}^{k} P_i \cap P_j = \langle e \rangle$ $\therefore G = P_1 \times P_2 \cdots P_k$

since $|G| = \prod P_i^{n_i}$.

⑥ Every Aut of S_φ is Inn-aut. then $S_\varphi \cong Aut S_\varphi$

Pf: $C(S_\varphi) = \langle e \rangle$ $\therefore S_\varphi \cong Aut S_p \cong Inn S_\varphi$.

We only prove: $S_\varphi \cong Aut S_p$.

Firstly. Note that $\Sigma = [\langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle]$.
is the set of $Syl_3(S_4)$. $|\Sigma| = 4$. then:

$Aut S_4 \times \Sigma \to \Sigma$, since $\sigma \in Aut S_4$. which transforms
$(\sigma, \langle x \rangle) \to \sigma(\langle x \rangle)$ 3-order-subgrp to 3-order-subgrp!

$\therefore$ Induce a map: $Aut S_4 \xrightarrow{f} S_4$

Suppose $bab^{-1}=a^r$, $r\not\equiv 1 \pmod p$. Or it will be Abelian

$\Rightarrow b\cdot bab^{-1}b^{-1}=ba^rb^{-1}=a^{r^2}\rightarrow \therefore b^2ab^{-2}=a^{r^2}$ ⟶ Significant step!

In particular, $j=q$, then $r^q\equiv 1 \pmod p$

the order of r is q exactly, since $|r|\mid q$.

then $|r|=1$ or q, but $r\not\equiv 1 \pmod p$ $\therefore |r|=q$

$\therefore \{r^0\}_0^{q-1}\equiv\{k\}_0^{q-1} \pmod p$, which means r^k are discriminative!

$\therefore G$ generated by a, b, $|a|=p$, $|b|=q$, $ba=a^rb$, $r\not\equiv 1 \pmod p$, $r^q\equiv 1 \pmod p$

(2) The nonabelian group G of order 8:

Case 1. If $\forall a\in G$, $|a|=2$, then G is Abelian.

$\therefore \exists a\in G$, $|a|=4$. (Otherwise not 8. → cyclic!)

$\therefore \langle a\rangle \lhd G$, $|G/\langle a\rangle|=2$, if $\exists b\neq a\in G$.

$\Rightarrow b^2\in\langle a\rangle$ if $b^2=a$ or a^3. $\Rightarrow |b^2|=4$

$\therefore |b|=2, 4$ or 8 → $|b|=8$. Contradiction!

$\therefore b^2=a^2$ or e. Using the normality:

$bab^{-1}=a^i$. $i=3$ only! since $i^2\equiv 1 \pmod 4$

$\therefore bab^{-1}=a^{-1}$, $G=\{b^ja^i\mid -\}$. determined by $b^2=a^2$ or e!

$\therefore G\cong D_4$ or Q_8

Remark: $D_4\not\cong Q_8$. Since the number of element with order 2 isn't same. But if the number of element and subgroup with the same order is same, between G_1 and G_2, $G_1\not\cong G_2$ as well.

The famous counterexample is Heisenburg group.

(3) The nonabelian group of order 12.

Pf: Consider the $Syl_3(G)$.

If $P \in Syl_3(G)$. $|P|=3$, $[G:P]=4$

$G \times G/P \to G/P$. then $\chi: G \to A(S_4)$

Case1. $\ker\chi = \langle e\rangle$ or P. if $G \to S_4$. mono-

when $\ker\chi=\langle e\rangle$. Since $|G|=12$,

$\therefore G \cong A_4$, Since A_4 is the only grop index 2

Case2. If $\ker\chi = P$. $P \trianglelefteq G$. P is the unique

syl-3-subgroup. $\therefore$ Only 2 elements with order 3

$G \times P \xrightarrow{conj} P \quad \therefore |P| = \sum \frac{|G|}{|C_G(c)|} + 1$

$\frac{|G|}{|C_G(c)|} = 1$ or $2 \Rightarrow |C_G(c)| = 6$ or 12.

$\therefore \exists\, b \in C_G(c)$. $|b|=2$. $\therefore |bc|=6$ → Normality is significant!

$\therefore \langle bc\rangle \trianglelefteq G$. Let $a=bc$. $d \in G$. $d \neq h$.

$d^2 \in \langle a\rangle$. ··· the same as (2)

$\therefore G \cong D_6$ or generated by $|a|=6$. $b^2=a^3$. $ba=a^5b$

(4) The nonabelian group of order p^3. $p \geq 3$.

Pf: Lemma. $C(G) = \langle [aba^{-1}b^{-1} \mid a,b \in G]\rangle$

$|G/C(G)| = p$ or p^2. G is nonabelian

$\therefore |C(G)|=p$. $|G/C(G)| = p^2$ $\therefore$

$G/C(G)$ is abelian and $G/C(G) \cong \langle \bar{a}\rangle \oplus \langle \bar{b}\rangle$

~~$|\bar{a}|=|\bar{b}|=p \Rightarrow a^p, b^p \in C(G)$~~

In other words, note that $G' \trianglelefteq \langle e \rangle$.

$G' < C(G)$ since $G/C(G)$ is abelian

then $|G'| = |C(G)| \therefore C(G) = G'$

Date
No.

Note that $a^i C(G) \cdot b^j C(G) = b^j C(G) \cdot a^i C(G)$

$\Rightarrow a^i b^j C(G) = b^j a^i C(G) \therefore a^{-i} b^{-j} a^i b^j \in C(G)$

Since $a^i \cdot b^j \in G - C(G)$. If $a, b \in C(G) \to e \in C(G)$!

$\therefore C(G) = \langle \{ aba^{-1}b^{-1} \mid a, b \in G \} \rangle$

Let $c = aba^{-1}b^{-1} \therefore C(G) = \langle c \rangle$ Since G is cyclic

Case 1. If there's no elements with order p^2. $\therefore |\langle a \rangle| = |\langle b \rangle| = p$.

$\Rightarrow G = \langle a \rangle, \langle b \rangle, \langle c \rangle$, $ac = ca, bc = cb, ab = cba$.

Case 2. If there's an element with order p^2.

Assume it's d. By sylow theorem:

$\langle d \rangle \trianglelefteq G$. And $|G/\langle d \rangle| = p$. Assume

$\langle \bar{b} \rangle = G/\langle d \rangle \therefore b^p \in \langle d \rangle$. By:

$bdb^{-1} = d^k \Rightarrow b^j d b^{-j} = d^{k^j}$

$\therefore k^p \equiv 1 \pmod{p^2}$. By Fermat Theorem:

$k^{p-1} \equiv 1 \pmod{p} \therefore k^p = pmk + k$

$= p^2 m' + 1 \therefore k \equiv 1 \pmod{p}$

找到一个合适的数!

Assume $k = pt + 1$. $\because (t, p) = 1$. $\therefore \exists j$ st. $jt \equiv 1 \pmod{p}$

$\Rightarrow b^j a b^{-j} = a^{k^j} = a^{(pt+1)^j} = a^{jpt+1} = a^{p+1}$

Let b^j replace b $|b^j| = |b|$ Since $(j, p) = 1$. $b^j \notin \langle a \rangle$

$\therefore \boxed{bab^{-1} = a^{p+1}}$. Assume $b^p = a^r$. $|b^p| \le p$.

Since $|b| \le p^2$. $\therefore b^p = a^{rp}$.

the only relation of a, b!

Test $= (ba^{-r})^p = b^p a^{-r(1 + (1+p) \cdots + (1+p)^{p-1})} \to \frac{(p+1)^p - 1}{p} = p + p^2 m$

may be $(a^r)^p$?

$= b^p a^{-rp} = 1$. Let $c = ba^{-r}$. $|c| = p$.

And $cac^{-1} = a^{1+p}$. $\therefore G$ generated by $|a| = p^2, |c| = p$.

④ (1) **Nilpotent Group**:

-※- **Commutator**: $[H,K]=\langle hkh^{-1}k^{-1} \mid h\in H, k\in K\rangle$ → not a subgroup! If not "$\langle\cdot\rangle$"

generally if $[H,K]=e$, moreover $H,K<G$.

$\Rightarrow K\lhd C_G(H)$, $H<C_G(K)$.

→ Access the Level of Abelian!

1. Note that $[H,K]<H\cap K$, if $H\lhd G$.

$K\lhd G \Rightarrow [H,K]\lhd G$.

A. $[ab,c]=a[b,c]a^{-1}[a,c] \Rightarrow$

$[ab,c][a,c]^{-1}=a[b,c]a^{-1} \therefore [H,K]\lhd HVK$

(※) By Def:

$cg\in C_{n+1}(G)$

$=gc\in C_{n+1}(G)$, $c\in C_n(G)$

$\therefore [G,C_{n+1}(G)]<C_n(G)$

Def: $C_1(G)=C(G)$, $\pi_1: G\to G/C(G)$

$\cdots C_2(G)=\pi_1^{-1}(C(G/C(G)))$ ---

$C_n(G)=\pi_{n-1}^{-1}(C(G/C_{n-1}(G)))$, $\pi_{n-1}: G\to G/C_{n-1}(G)$

1. Note that $C(G/C_{n-1}(G))\lhd G/C_{n-1}(G)$

$\therefore \pi_{n-1}^{-1}(C(G/C_{n-1}(G)))\lhd G \Rightarrow$ By Induction:

π_k is a canonical projection.

2. And $C_{n-1}(G)<C_n(G)$, since $\pi_{n-1}(C_n(G))=\bar{e}$

$\Rightarrow$ Ascending central series: $\langle e\rangle<C_1(G)<\cdots<C_n(G)$

G is nilpotent iff $C_n(G)=G$, for some n.

Remark: Another definition of nilpotent group:

$G^k=[G^{k-1},G]$, then $G>G^2>G^3\cdots>G^n$.

G is nilpotent iff $G^n=\langle e\rangle$ for some n.

Now we prove the definitions are equivalent:

Lemma: σ is a homomorphism. $\sigma([H,K]) = [\sigma(H), \sigma(K)]$.

Pf: Note that $\sigma([h,k]) = \sigma(hkh^{-1}k^{-1}) = \sigma(h)\sigma(k)\sigma^{-1}(h)\sigma^{-1}(k)$
$= [\sigma(h), \sigma(k)]$. Then $\sigma([H,K]) = [\sigma(H), \sigma(k)]$.

Pf: (必): [对 $\exists n$. $C_n(G) = G \Rightarrow [G,G] = G^2 = [C_n(G), G]$
$< [C_{n+1}(G), G]$. $G^3 = [G^2, G] = [[C_n(G), G], G] < [C_{n+1}(G), G]$
✗ $[[C_{n+1}(G), G], G] \subsetneq [C_{n+1}(G), G]$ (wrong!)]

By: let $\sigma = \pi$ (canonical projection)

$[C_n(G)/C_{n+1}(G),\ G/C_{n+1}(G)] = \bar{e}$

$\therefore [\pi^{-1}(C_n(G)/C_{n+1}(G)),\ G] < C_{n+1}(G)$

$\therefore [C_n(G), G] < C_{n+1}(G)$

∴ Another way: $C_n(G)/C_{n+1}(G) = \pi(C_n(G)) = C(G/C_{n+1}(G))$

$\therefore \forall \bar{g} \in C_{n+1}(G)/C_{n+1}(G)$. $\forall \bar{h} \in G/C_{n+1}(G)$. $\bar{g}\bar{h} = \bar{h}\bar{g}$

$\therefore ghg^{-1}h^{-1} \in C_{n+1}(G)$ $\because [C_n(G), G] < C_{n+1}(G)$

$\therefore [G, [G,G]] = [G, [C_n, G]] < [G, C_{n+1}(G)]$

$\therefore G^3 < [C_{n+1}(G), G] \cdots, G^{n+2} < [\langle e\rangle, G] = \langle e\rangle$

$\therefore G^{n+2} = \langle e\rangle = [G^{n+1}, G]$ $\therefore G^{n+1} < C(G)$

(⇑) 对 $\exists n$ s.t. $G^n = \langle e\rangle = [G^{n-1}, G]$ $\therefore G^{n-1} < C(G)$

$G^{n-1} = [G^{n-2}, G] < C(G)$, $[\pi(G^{n-2}), \pi(G)] < \bar{e}$

$\therefore G^{n-2}/C(G) < C_2(G)/C(G)$ $\therefore G^{n-2} < C_2(G)$

$\cdots \therefore G < C_n(G) < G$ $\therefore C_n(G) = G$.

Cor. every subgroup and quotient group of nilpotent group are nilpotent.

Pf: $H < G$. Since $H^n < G^n$. obviously!

If $N \triangleleft G$. N is nilpotent. Note that

$Z[G,G] = Z(G^1) = [Z(G), Z(G)]$

$= Z^1(G)$. By Induction: $Z(G^n)$

$= Z^n(G)$ $\therefore Z(G^n) = (G/N)^n = \pi(\bar{e}) = \bar{e}$

$\therefore (G/N)^n = N$

(Remark: If N, G/N are nilpotent. $\longrightarrow$ the problem: $(G^n)^k = [G^n, (G^n)^k]$

G won't be nilpotent possibly. (check S_3) $\overset{0}{=} \langle e \rangle$!

But If $N < C(G)$, then $G^n \trianglelefteq [G^n, G]$

$\langle [N, G] = e \rangle \therefore G^{n+1} = \langle e \rangle$)

Theorem: A finite product of nilpotent group is nilpotent.

Pf: By Induction: $G = H \times K$. $C(G) = C(H \times K)$

$= C(H) \times C(K)$. then we find: $\pi: G \to G/C_1(G)$

Firstly: $C_2(G) = C_2(H) \times C_2(K)$ By Induction assumption.

$$G = H \times K \xrightarrow{\pi_H \times \pi_K} H/C_1(H) \times K/C_1(K) \xrightarrow[\text{iso-!}]{\psi} \frac{H \times K}{C_1(H) \times C_1(K)}$$

$= G/C_1(G)$. $\therefore C_{n+1}(G) = \pi^{-1}(C(G/C_n(G)))$

$= (\pi_H \times \pi_K)^{-1} \psi^{-1}(C(G/C_n(G))) = (\pi_H \times \pi_K)^{-1}(C(H/C_n(H) \times K/C_n(K)))$

$= (Z_m \times Z_k)^{-1} C(H/(G\times H)) \times C(K/(G\times K)) = C_{i+1}(H) \times C_{i+1}(K)$

$\therefore C_i(G) = C_i(H) \times C_i(K)$. holds for $\forall i$.

Then $\exists N \geq \max\{n_1, n_2\}$. $C_N(G) = K \times H = G$.

Theorem ☆: A finite group is nilpotent $\Leftrightarrow$ it's the product (direct) of sylp-groups.

Lemma 1. p-group is nilpotent.

Pf: $G/Z(G)$ is p-group $\therefore |C(G)/Z(G)| > 1$

$\therefore C_1(G) < C_{i+1}(G)$. strictly! And G is finite

$\therefore C_n(G)$ must be G. for some n.

$\Rightarrow$ Then ($\in$) holds!

Lemma 2. If $H < G$, G is nilpotent finite group. H is proper subgroup. then $H < N_G(H)$ strictly.

Pf: $C_0(G) = \langle e \rangle$. $C_N(G) = G$. $\therefore \exists$ maximal k. s.t. $C_k(G) < H$. but $C_{k+1}(G) \not< H$.

choose $a \in C_{k+1}(G)$ but $a \notin C_k(G)$. then

$aC_k(G)\, hC_k(G) = ahC_k(G) = hC_k(G)\, aC_k(G)$

$= haC_k(G)$, $\forall h \in H$ $\therefore ha \in ahC_k(G)$

$\therefore ha = ahh'$. $h' \in C_k(G)$ $\therefore a^{-1}ha = hh' < H$.

since $h' \in C_k(G) < H$

$\Rightarrow$ Then $\exists P \in Sylp(G)$, then $N_G(P) = G$

Otherwise. $N_G(P) < N_G(N_G(P))$. contradiction!

$\therefore P \trianglelefteq G$. $\therefore$ $\forall$ sylow-p-group is normal group! $\rightarrow$ Product!

Remark: The criterion by Wielandt.

a finite group is nilpotent $\Leftrightarrow$

every maximal proper subgroup of G is normal

Pf: ($\Rightarrow$) If H is the maximal proper subgroup.

then $H \leq N_G(H)$, $N_G(H)$ must be G.

$\therefore H \trianglelefteq G$

($\Leftarrow$) If $\exists$ Sylp-subgroup P isn't normal.

Then $N_G(P)$ is the proper subgroup.

$N_G(P) < H < G$. By Frattini Lemma

$N_G(H) = H = G$, contradiction!

Some conclusions:

① $N \neq \langle e \rangle \trianglelefteq G$. G is finite nilpotent, then $N \cap C(G) \neq \langle e \rangle$

Pf: $\exists n$, $C_n(G) = G$. $N \cap G = N$

$\therefore \forall g \in G$, $n C_n(G) \cdot g C_n(G) = g C_n(G) \cdot n C_n(G)$ ⟶ Lemma: $[N, G] < N \Leftrightarrow N \trianglelefteq G$.

$\Rightarrow n g n^{-1} g^{-1} \in C_n(G)$, $n g n^{-1} g^{-1} \in [N, G] < N$

$\therefore n g n^{-1} g^{-1} \in C_n(G) \cap N$. If $C_n(G) \cap N = \{e\}$

$\therefore N < C(G)$ $\therefore C_n(G) \cap N = N_1 \neq \{e\}$

Or $C_n(G) \cap N \neq \{e\}$. $N_1 = C_n(G) \cap N$; then $G/C_n(G)$ ⋯ $N_n = C(G) \cap N \neq \{e\}$.

Cor. every minimal normal group of G (above) is contained in $C(G)$ with prime order ⟶ Since $N \subset C(G)$, N is Abelian and simple!

~~Pf: Since $N \cap C(G) \neq \langle e \rangle$, $N \cap C(G) = N$~~

Or $N \cap C(G) \leq N$, $N \cap C(G) \trianglelefteq G$. Contradict!

↓ Since $C(G) \trianglelefteq G$. Obvious by!

Date.
No.

② Somethings about D_{2n} ($|a|=n$, $|b|=2$)

i) $[D_{2n}, D_{2n}] = \langle a^2 \rangle$, then if n is odd

$[D_{2n}, D_{2n}] \cong \mathbb{Z}_n$. if n is even, $[D_{2n}, D_{2n}] \cong \mathbb{Z}_{\frac{n}{2}}$

ii) D_{2n} is nilpotent $\Leftrightarrow |D_{2n}| = 2^{k+1}$ (which means $n = 2^k$)

iii) D_{2n} is solvable

Pf: i) $g_1 g_2 g_1^{-1} g_2^{-1} = a^i b^\delta a^{-i} b^\delta b^{-\delta} a^{-i} b^{-\delta} a^{-i}$

$= a^{2i}$ $\therefore [D_{2n}, D_{2n}] = \langle a^2 \rangle$

ii) ($\Rightarrow$) If $\exists p \geq 3$, $p \mid |D_{2n}|$, then $p \mid n$

Note that $|\langle a^{\frac{n}{p}} \rangle| = p$ belongs to $\mathrm{Syl}_p(G)$

$\langle b \rangle$ belongs to $\mathrm{Syl}_2(G)$ (which means there're contained in syl-group!)

But $a^{\frac{n}{p}} b \neq b a^{\frac{n}{p}}$, contradict!

→ The problem is the D_{2n}!

($\Leftarrow$) when $n = 2^{k+1}$, note that

$C(D_{2n}) = \{e, a^{2^k}\}$, By Induction:

$k=1$ obviously. By assumption:

Note that $D_{2n}/C(D_{2n}) \cong D_{2^k}$,

$\therefore D_{2n}/C(D_{2n})$, $C(D_{2n})$ is nilpotent.

$\Rightarrow D_{2n} = D_{2^{k+1}} \Rightarrow$ nilpotent!

iii) $D_n^{(1)} = \langle a \rangle$, $\langle a \rangle$ is abelian.

(2) **Solvable**:

- $G^{(i)} = (G^{(i-1)})' = [G^{(i-1)}, G^{(i-1)}]$, then
  $G \triangleright G^{(1)} \triangleright G^{(2)} \cdots \triangleright G^{(i)}$. If $\exists n$.
  s.t. $G^{(n)} = \langle e \rangle$. then G is solvable

- [Characteristic: $f: G \to G$, auto-, $H < G$. If $f(H) < H$. then H is c...
  Fully invariant: $f: G \to G$, endo-, $H < G$, If $f(H) < H$, then H is f...

Remark: 1. Fully invariant $\longrightarrow$ Characteristic $\longrightarrow$ normal
(f = inj.)

2. Notice even Aut (or Inn-Aut) can't let H
$\to H$ possibly. We talk it on subgroup but not map!

Proposition: If $G' \triangleleft G$. If G/G' is abelian
and if G/N is abelian. then $G' < N$.

Pf: i) G' is the fully invariant subgroup of G.

ii) $(ab)(ba)^{-1} \in G' \Rightarrow ab \in (ba)G'$

$\therefore abG' = baG'$

If $abN = baN \Rightarrow aba^{-1}b^{-1} \in N$, obviously!

Remark: 1. Every nilpotent group is solvable.

Pf: By: $G^n > G^{(n)}$ Or by $G^{(a)}$

$= [G, G] = [G, C_n(G)] < C_{n-1}(G)$

$\Rightarrow G^{(i)} < C_{n-i}(G)$

Date.
No.

2. $G^{(i)}$ is the full-invariant subgroup of G.

Pf: By Induction: $i=1$ ✓.

Lemma: $f(G^{(i)}) = f^{(i)}(G)$

Pf: $f(G^{(i)}) = f((G^{(i-1)})') = (f(G^{(i-1)}))' = (f^{(i-1)}(G))' = f^{(i)}(G)$. By Induction!

$\Rightarrow f(G^{(i)}) = f^{(i)}(G) < G^{(i)}$

Then $\underline{G^{(i)} \trianglelefteq G}$!

→ Cor: $f(G)$ is solvable $\Leftrightarrow G$ is solvable.

↓

C. Cor. G/N, N solvable. $N \trianglelefteq G$. then G solvable

Pf: By $(G/N)^{(n)} = f(G^{(n)}) = N \therefore G^{(n)} < N$

$\therefore (G^{(n)})^{(k)} < N^{(k)} = \langle e \rangle$

Lemma. i) G is a finite group. $N \trianglelefteq G$. $H < G$.

If H is a characteristic subgroup of N.

then $H \trianglelefteq G$

→ Inparticularly, $G_{[P]}$

ii) Every normal sylp-subgroup of G is fully invariant subgroup.

iii) G solvable. $N \trianglelefteq G$. which is the minimal normal subgroup. then N is abelian group with prime order

Pf: i) Note that $N \longrightarrow gNg^{-1}$, $\forall g$.

$\therefore gHg^{-1} < H$. $\forall g \in G$

ii) $P \in Sylp(G)$. $|G| = p^k m$. $|P| = p^k$

Note that P is the unique sylp-group.

By sylow Theorem. $\forall H < G$. $|H| = p^k \Rightarrow H < P$.

∴ If we want to prove $f(p) < P$.

Only check $|f(g)| = p^k$?

Note that $\forall g \in P$, $g^{p^l} = e$.

$\therefore f(g^{p^l}) = f(g)^{p^l} = f(e) = e$

$\therefore \forall f(g)$, $|f(g)| \mid p^l \therefore \langle f(g) \rangle < P$

$\therefore f(p) < \langle \bigcup_{g \in P} \langle f(g) \rangle \rangle < P$.

i) Consider N' which is fully invariance in N. $\Rightarrow N' \trianglelefteq G$.

$\therefore N' = \langle e \rangle$ or N. Since G is solvable

$\Rightarrow N$ is solvable $\therefore N' \neq N$. $\therefore N' = \langle e \rangle$

$\therefore N$ is Abelian. $P \in Syl_p(N)$. then

$P \trianglelefteq N$ since N is Abelian

$\therefore P$ is fully-invariance by i) $\therefore P \trianglelefteq G$.

Then $P < N$ $\therefore P = N$

✡

The difference-proving

Proposition:

P. Hall Theorem:

G is finite, solvable. With order mn. $(m, n) = 1$, then

i) G contains a subgroup of order m.

ii) Any two subgroups of order m are conjugated

iii) $H < G$. $|H| = k \mid m$. then $H < |H|$. H is a subgp of order m

Pf: Which is more than complicated!

Since $G'' \lhd C(G')$, by: $G' \times G'' \to G''$
then $G'/C(G') \cong$ subgrp $(g, a^z) \mapsto gag^{-1}$
G'' subgrp of $ga^zg^{-1} = a^z = (gag^{-1})^z$
武漢大學 數學與統計學院 School of Mathematics and Statistics $\Leftrightarrow g \in C(H(a))$

Date.
No.

Some conclusions:

① something about S_4:

i) $S_4' = A_4$. $A_4' = K_4$. $K_4' = \langle e \rangle$. $\therefore S_4$ is solvable

ii) S_4 isn't nilpotent, since $C(S_4) = \{e\}$.

iii) There's no G, s.t. $G' = S_4$.

Pf: i) note that $\sigma\tau\sigma^{-1}\tau^{-1}$ is even permutation
$\therefore \forall \sigma\tau\sigma^{-1}\tau^{-1} \in A_4$. Note that K_4 is the unique normal subgrp of A_4.
But $(12)(13)(12)^{-1}(13)^{-1} = (123) \notin K_4$.
$\therefore S_4' = A_4$. $\therefore S_4 > A_4 > K_4 > \langle e \rangle$.

ii) $C(S_4) = \{e\}$. $\therefore S_4$ isn't nilpotent.

iii) Lemma. If $G^{(1)}/G^{(2)}$, $G^{(2)}/G^{(3)}$ are cyclic, then $G^{(2)} = \langle e \rangle$. ($G$ is solvable)

Pf: Assume $G^{(2)} = \langle e \rangle$. Or we can module $G^{(2)}$ at the same time. Then $G^{(2)}$ is cyclic then $G^{(4)} = \langle e \rangle$ ($\Leftrightarrow$) $G^{(1)}$ is abelian ($\Leftrightarrow$) $G^{(1)}/C(G^{(1)})$ is cyclic, $G^{(2)}/C(G^{(1)}) \cong G^{(2)}/G^{(3)}/C(G)/G^{(3)}$

② H is the maximal proper subgrp of finite solvable group G, the $[G:H] = p^k$.

Pf: By Induction on the order:
$|G| = 2$ is obvious. Then Take the minimal normal subgrp of G by iii) or by Lemma.
Denote N. Then H/N is still the maximal proper subgrp of G/N $\therefore [G/N : H/N] = p^k$.
Note that $\frac{G/N}{H/N} \cong G/H$ $\therefore [G:H] = p^k$

Remark: S_n isn't solvable ($n \geq 5$). Note that A nonabelian simple group is commutator! $A_n = A_n'$!

Remark: A group is complete when $C(G) \cong$ Aut $G \cong$ Inn $G \cong G$

If G is complete, $G' \neq G$, then G isn't a commutator ($\exists H' = G$)

Pf: Since $C_G(a) = \langle e \rangle$
$\therefore G \cap C_H(G) = \{e\}$.
By complete. $H = G \times C(H(G))$
$\Rightarrow H' = (G \times C(H(G)))'$
$= G' \times \langle e \rangle$
$C(H(G)) \cong H/G$ is Abelian
Since

Existence? If $G' \neq \langle e \rangle$ then $G' \lhd G$. If $G' = \langle e \rangle$ $\Rightarrow G$ is Abelian. $H < G$ $\therefore H \lhd G$.

③ $\forall G$, $C(G)$ is characteristic but not necessarily subgroup.

pf: The former is easy. Then we take a counterexample: $GL_2(\mathbb{Q})$

if $A \in GL_2(\mathbb{Q})$. Denote $|A| = \frac{b}{a} \cdot 2^{r(A)}$, $(a,b)=1$, a,b are odd.

then $|AB| = |A||B| \therefore r(AB) = r(A)+r(B)$

$\varphi: A \longmapsto \begin{pmatrix} 1 & r(A) \\ 0 & 1 \end{pmatrix}$. endo-

$\left(\varphi(AB) = \begin{pmatrix} 1 & r(A)+r(B) \\ 0 & 1 \end{pmatrix} = \varphi(A)\varphi(B)\right)$

But $\varphi\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ which isn't center. but $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ is!

④ G is nonabelian nilpotent group. A is the maximal element in the set of normal group of G. And A is Abelian.

Then $C_G(A) = A$

pf: 1') $C_G(A)$ is normal: $a \in C_G(A)$. $x \in A$

$gag^{-1}x \overset{?}{=} xgag^{-1}$. $\forall g \Leftrightarrow ga^{-1}g^{-1}x^{-1}gag^{-1}x = e$! $\in A$

$\therefore g(g^{-1}x^{-1}g)a^{-1}ag^{-1}x = e$, $\therefore C_G(A) \triangleleft G$

2') $A < C_G(A)$ $\therefore C_G(A) = A$ or G.

If $C_G(A) = G$. A is contained in $C(G)$

$\therefore C(G) = A$ or G. But G is not abelian.

$\therefore C(G) = A$. G/A is of prime order

since A is the maximal normal grp.

and $Z_1(C_G(G/C_G(G))) = C_G(G) \supsetneq C(G)$

because G is nilpotent $\therefore C_G(G) = G$.

$\therefore G/A$ is abelian. then G/A

can't contain a proper subgroup.

But $\because |G/A| = p \Rightarrow G$ is abelian. contradiction!

Remark: when concerning above the maximal or minimal. consider construct a smaller or bigger group. like G' or $C_G(A)$...

(determined by descend or ascend!)

(5) Normal and Subnormal Series.

- $G \triangleright G_1 \triangleright G_2 \cdots \triangleright G_n \cdots$ is a series

  if $G_i \triangleleft G$ for all $i \longrightarrow$ normal series

  if $G_i \triangleleft G_{i+1}$ for all $i \longrightarrow$ subnormal series.

$\Rightarrow$ The length of series determined by the strictly inclusions or nontrivial G_i/G_{i+1}

- composition series: A subnormal series with each factor G_i/G_{i+1} is simple
- solvable series: A subnormal series with each factor G_i/G_{i+1} is abelian.

- Refinement: Add a subgroup N to the series which keeps its property!

Remark: Any refinement of composition series is equivalent to itself!

Since it has no proper refinement $\Leftrightarrow$ A subnormal series is a composition series.

Theorem. i) Every finite group G has a composition series. By choosing G_{i+1} to be the maximal normal proper subgroup of G_i (Hence: $G = G_0$)

ii) Every refinement of solvable series is solvable series.

Pf: $G_{i+1} \triangleleft H \triangleleft G_i$. G_i/G_{i+1} is abelian

Note that $\dfrac{G_i/G_{i+1}}{H/G_{i+1}} \cong G_i/H$

H/G_{i+1} is abelian since $H/G_{i+1} < G_i/G_{i+1}$

Propositions i) G is solvable

ii) Exist a normal series of G

iii) Exist a subnormal series of G, s.t. G_i/G_{i+1} is abelian.

iv) Exist a composition series of G whose factors G_i/G_{i+1} with prime order

There're equivalent.

Pf: i) $\rightarrow$ ii) $\rightarrow$ iii) by $G > G^{(1)} > G^{(2)} \cdots > G^{(n)} > \langle e \rangle$

Date.
No.

iii) ⇒ iv) Take the maximal series in iii)

If $\exists G_{i+2}, G_{i+1}$, $|G_i/G_{i+1}|$ isn't prime.

By Theorem of Sylow: $\exists \bar{H} \triangleleft G_i/G_{i+1}$.

Since G_i/G_{i+1} is abelian, then:

$\pi: G_i \longrightarrow G_i/G_{i+1}$, $H = \pi^{-1}(\bar{H})$

$H \underset{\neq}{\triangleleft} G_i$ still and $H \underset{\neq}{\triangleright} G_{i+1}$

∴ it's a proper refinement, contradiction!

iv) ⇒ i) $G_n = \langle e \rangle$ is solvable. G_{n-1}/G_n is prime-abelian. ∴ it's solvable ∴ G_{n-1} is solvable

Then by Induction: G is solvable

iii) ⇒ ii) By $G_n > G^{(n)}$, iv) ⇒ iii) is obviously!

ii) ⇒ iv) Add $\{H_i\}$ to (G_{i+2}, G_{i+1}): $G_i \triangleright H_1 \triangleright H_2 \cdots \triangleright H_k \triangleright G_{i+1}$

Denote $G_i = H_0$, $G_{i+1} = H_{k+1}$. Choose H_j is the maximal normal group of H_{j+1}, then H_{j+1}/H_j is simple and abelian so it's prime order.

Zassenhaus Lemma: $A, B < G$. $A^* \triangleleft A$, $B^* \triangleleft B$.

Then i) $A^*(A \cap B^*) \triangleleft A^*(A \cap B)$

$B^*(A^* \cap B) \triangleleft B^*(A \cap B)$

ii) $A^*(A \cap B)/A^*(A \cap B^*) \cong B^*(A \cap B)/B^*(A^* \cap B)$

Pf: 1°) $A \cap B^* = (A \cap B) \cap B^* \triangleleft A \cap B$ ∴ $(A \cap B^*)(A^* \cap B)$

$A^* \cap B = A^* \cap (A \cap B) \triangleleft A \cap B$ $= D \triangleleft A \cap B$

2°) Def: $A^*(A\cap B) \xrightarrow{\pi} (A\cap B)/D$

$\pi(ac) = Dc$. $a\in A^*$, $c\in A\cap B$. check if well-def?

$ac_1 = ac_2 \Rightarrow c_1c_2^{-1} = a^{-1}a_2 \in A^*\cap A\cap B$.

$\therefore c_1c_2^{-1} \in A^*\cap(A\cap B) = A^*\cap B < D$.

$\therefore c_1D = c_2D$ ($Dc_1 = Dc_2$)

3°) And π is surjective, then check homo-?

$\pi(a_1c_1a_2c_2) = \pi(a_1a_3c_1c_2) = Dc_1c_2 = Dc_1\cdot Dc_2$

$= \pi(a_1c_1)\pi(a_2c_2)$

4°) Then $a\in \ker\pi \Leftrightarrow c\in D \Leftrightarrow c = a_1c_1$

$a_1\in A^*\cap B$. $c_1\in A\cap B^* \Leftrightarrow ac = (aa_1)c$

$\in A^*(A\cap B^*)$ $\therefore A^*(A\cap B^*) = \ker\pi$

The same as $B^*(A^*\cap B)$ is kernel of

$B^*(A\cap B) \longrightarrow (A\cap B)/D$. $\therefore$ Normal!

And $A^*(A\cap B)/A^*(A\cap B^*) \cong A\cap B/D \cong B^*(A\cap B)/B^*(A^*\cap B)$

Ps

Schreier Theorem: Any two N or SN series. has refinements are equivalent

Pf: $G = G_0 > G_1 > \cdots > G_n$. $H = H_0 > H_1 > \cdots > H_m$. $G_{n+1} = H_{m+1} = \langle e\rangle$

Then $G_i = G_{i+1}(G_i\cap H_0) > G_{i+1}(G_i\cap H_1) > \cdots$

$> G_{i+1}(G_i\cap H_{m+1}) = G_{i+1}$.

$\therefore$ the length of refinement is $(n+1)(m+1)$

The same as $G=H_0>\cdots>H_{n+1}$ which has the same length.

By Zassenhaus Lemma, the operations keep the properey of series, and produce a one-to-one-response:

$$\frac{G_{i+1}(G_i\cap H_j)}{G_{i+1}(G_i\cap H_{j+1})} \cong \frac{H_{j+1}(G_{i+1}\cap H_j)}{H_{j+1}(G_{i+1}\cap H_j)}$$

→ Remark: the composition series has the max length.

* **Jordan Hölder Thm:** Any two compositions of G is equivalent. Then every group has a composition series determine a unique list of simple groups (factors)

Some conclusions:

① If $N\trianglelefteq G$, N is simple, G/N has a composition series, then G has a composition series

pf: $G_0/N > G_1/N \cdots > G_k/N$, then $\pi: H \to H/N$

$G > \pi^{-1}(G_1/N) > \pi^{-1}(G_2/N) \cdots > \pi_k^{-1}(G_k/N) > N$

② [1. An abelian group has a composition series $\Leftrightarrow$ it's finite
2. A solvable group with finite composition series, is finite.

pf: ($\Rightarrow$) Note that an abelian group is simple $\Rightarrow$ the order is prime $\therefore |G_k/G_{k+1}|$ is finite.

And $|G| = \prod |G_k/G_{k+1}|$ finite.

(⇐) By Induction on the order.

Choose the max proper subgroup G_1.

2) By theorem ⇒ ∃ composition series

s.t. $|G_k/G_{k+1}| = p$. ∴ $|G| = \prod |G_k/G_{k+1}|$ is finite

(Remark: A solvable group may not be finite)

③ Any simple group of order 60 $\cong A_5$

Pf: 1) If ∃ H, $H \leq_{*} G$. $G \times G/H \longrightarrow G/H$

$(g_1, g_2H) \longmapsto g_1g_2H$

the ker φ: $\varphi: G \longrightarrow A(G/H)$

$\ker\varphi \trianglelefteq G$. ∴ $\ker\varphi = G$ or $\langle e\rangle$

if $\ker\varphi = G$. Note that $\ker\varphi < H$.

∴ $G = H$, contradiction! ∴ $\ker\varphi = \langle e\rangle$

∴ $|G| \mid |G/H|!$ then $\underline{|G/H| \geq 5}$ ···①

2) The purpose is to find a group H of order 12. Then $|G/H| = 5$.

Then $G \cong \bar{G} < S_5$. since $\ker\varphi = \langle e\rangle$

∴ $\bar{G}$ is A_5 since $|\bar{G}| = 60$

3°) Now we count the sylp-group of G

- sylp-group: 6个 → element of order 5 = 4×6 = 24个
- sylp-group: 4或10个
- sylp-group: 5或15个.

(△ since the intersection of sylow-group with prime order is null set)

If syl$_2$-subgroup have 5 one:

Note that the syl$_p$-subgroup is an orbit. by:

$G \times$ syl$_5$-subgroup $\longrightarrow$ syl$_5$-group $\quad \therefore \frac{|G|}{|N_G(P)|} = 5$

$(g, P) \longmapsto g^{-1}Pg$

If syl$_2$-subgroup has 12 one:

then $\exists\ H_1, H_2 \in$ syl$_2$. $H_1 \cap H_2 \neq \langle e \rangle$. $H_1 * H_2$

Otherwise: $24 + 3\times 15 > 60$. Contradict!

$\left[\left[\begin{array}{l} H_1 = [e, a, a^2, a^3] \\ H_2 = [e, b, b^2, b^3] \end{array}\right.\right.$ the only possibility is: $a^2 = b^2$ $\Big]$ → need not to be cyclic!

Note 2^2 order group is abelian.

$\therefore H_1, H_2 < C(k)$. $k = H_1 \cap H_2 \neq \langle e \rangle$ (*)

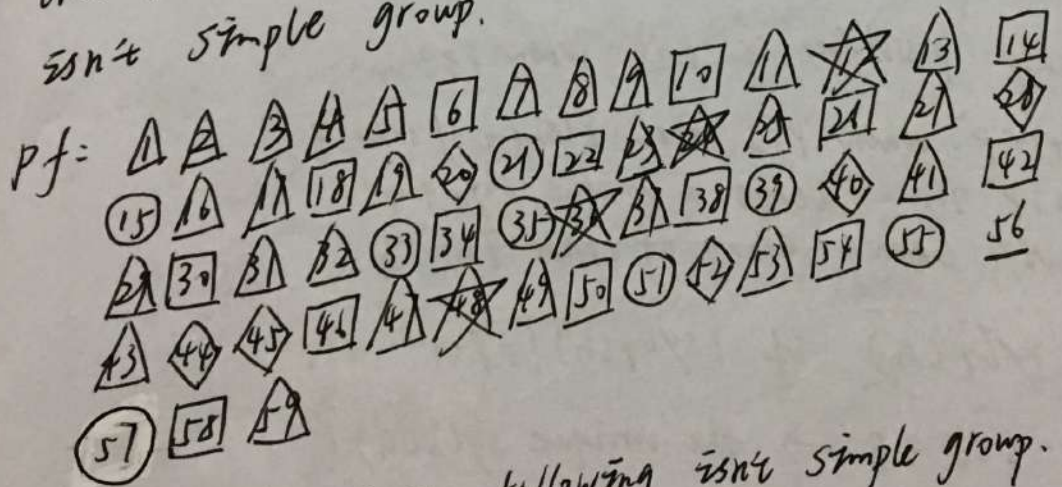
$\therefore 4 \mid |C(k)| \cdot |C(k)| > 4 \quad \therefore |C(k)| \neq 12, 20, 60$

But 对 $H \leq G$. $|H| \leq \frac{60}{5} = 12$. $\therefore |C(k)| = 12$ or 60

If $C(k) = G \Rightarrow k \triangleleft C(k) \quad \therefore |C(k)| = 12$.

(*) Since we can't construct a subgroup. We can use the subgroup at the process. Such as $N_G(H)$, $C_G(H)$, kernel ---

④ the nonabelian group with order < 60 isn't simple group.

Pf: 

Lemma: The group following isn't simple group.

i) P-group. mark by "△"

~~ii) $|G| = 2k$. k odd = 口~~

iii) $|G| = pq$. p, q are prime. ○

iv) = $|G| = p^l m$. $p > m$. ◇

or $p \nmid m-1$

i) Consider kernel. $|G| = p^l m$.

if $p+1 \le m \le 2p$ and G has $p+1$

个 sylp-subgroups. Suppose $m = p+1$

(*) Then Pick $P \in$ sylp-subgroup.

$G \times G/P \to G/P$. $\therefore \frac{|G|}{|\ker\lambda|} \Big| (p+1)!$

$\therefore$ if $l \ge 2$. then $\ker\lambda \ne \langle e \rangle$

$\therefore |G| = p^l(p+1)$. $l \ge 2$. G isn't simple. ☆

vi) $p^2 q$ group. (Moreover. it's solvable.)

Pf: $p \ge q$. obvious. if $p < q$. and $q \mid p^2-1$

$\Rightarrow q \mid (p+1)(p-1)$ $\therefore q \mid p+1$, but $p+1$ is even

$\Rightarrow q \mid \frac{p+1}{2}$. contradict! $\therefore kq+1 = 1, p, p^2$

the only possibility is $k=0$. when $p \ge 3$.

Or $kq+1 = p^2$. when $p=2$. then element of order q $= (q-1)p^2 \cdot 7$. $\therefore$ leave a unique syl_p-grp!

vii) Now we leave group of order (72). 56

Count $syl_7(G)$. if $|syl_7(G)| = 7+1$

$\Rightarrow 56 - 6 \times 8 = 8 \to$ the unique $syl_2(G)$!

(Remark: 72 阶群 → 不妨设 $|syl_3(G)| = 4$ → 当个数很小. G 的阶足够大!

→ 作用 conjugate: $\frac{|G|}{|\ker\lambda|} \Big| 4!$ $\therefore \ker\lambda \ne \langle e \rangle$)

↓ the same as (*)

⑥ Category : (pre-)

-X-

(1) A category $\nearrow$ 1. a class C of objects together with
$\searrow$ 2. a class of disjoint sets denoted $\hom(A,B)$ ~~check!~~ It's natural. Since A,B won't be different.
for each pairs of object in C.
i.e. $\varphi \in \hom(A,B)$, then $\varphi: A \to B$, called morphism form $A \to B$.

Satisfies 1 the composition: for (A,B,C) of objects of C
operation : $\hom(A,B) \times \hom(B,C) \longrightarrow \hom(A,C)$
$(f, g) \longmapsto f \circ g$

has 2 axioms : 1) Associativity: $h \circ (g \circ f) = (h \circ g) \circ f$
2) Identity: $1 \circ f = f$. $g \circ 1 = g$.

$\Rightarrow$ A morphism called an equivalence : $f: A \longrightarrow B$.
when $\exists$ unique, obviously! $g: B \to A$ $f \circ g = 1_B$. $g \circ f = 1_A$, then A,B is equivalent!

Remark: Construct a larger category $\mathcal{D}$ from C.:
Let morphisms from C to be objects in $\mathcal{D}$.
Then $\hom(f,g) = \{(\alpha, \beta) \mid \alpha: A \longrightarrow C, \beta: B \to D, \text{mor-}\}$

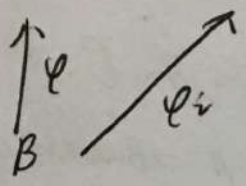
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ C & \xrightarrow{g} & D \end{array}$$
(Diagrams) check Axioms!

(2) Product = $[A_i \mid i \in I]$ a family of objects of C.
A product for it is an object P with
a family of morphisms $[\pi_i: P \to A_i]$

st. $\forall$ objece B with $[\varphi_i | B \to A_i, i\in I]$. $\to$ or induce a φ!

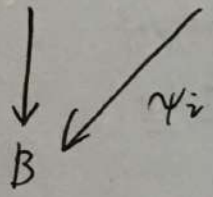
$\exists!\ \psi = B \to P$. st. $\pi_i \circ \psi = \varphi_i$. $\forall i \in I$.

Diagram: $P \xrightarrow{\pi_i} A_i$. P often denoted by $\prod_{i\in I} A_i$.



A coproduce (or sum) with morphisms which are inverse arrows. denote $\coprod_{i\in I} A_i = S$

Diagram: $S \xleftarrow{l_i} A_i$



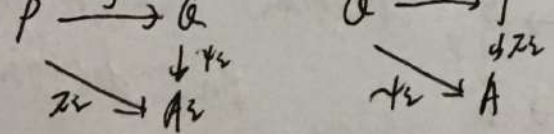
Remark: 1. produce or coproduce doesn't exist always.

2. The proceed above like constructing a new objece!

Duality Theorem: If $(P, [\pi_i])$, $(Q, [\psi_i])$ are produces or coproduces for the same family $[A_i | i\in I]$.

Then P, Q are equivalence.

pf: 1) $P \xrightarrow{f} Q$, $Q \xrightarrow{g} P$



compose: $P \xrightarrow{g\circ f} P$ since $g\circ f$ is unique

$\Rightarrow g\circ f = 1_P$ (and $f\circ g = 1_Q$)

the same as produce, when in coproduct!

Remark: the product is absolutely different from coproduct.

For example: Set $\{X_i\}$: product $= \prod X_i$, but coproduct: $\dot{\bigcup} X_i = [\bigcup X_i \times I]$.

Vector space $\{X_i\}$: pro: $\prod X_i$, copro: $\dot{\bigoplus} X_i = [\bigoplus X_i \times I]$.

(3) Concrete category: A category C with a function σ for each object A: $\xrightarrow{\sigma}$ $\sigma(A)$, a underlying set!

satisfy that: the morphisms in C is a function in $\{\sigma(A) \mid A \in C\}$. keeping their property. (axioms)

Remark: 1. In concrete category: morphisms $\rightleftarrows$ map in underlying set ($\nexists$ sometimes)

2. Now we can consider object in the concrete sets!

$\Rightarrow$ X is a nonempty set. F a object in C.

F is free on X: $\forall A \in C$. with map $f: X \to A$. induces a unique morphism $\bar{f}: F \to A$ such that $\bar{f} i = f$

Diagram:

$$\begin{array}{ccc} X & \xrightarrow{i} & F \\ & \searrow^{f} & \downarrow \bar{f} \\ & & A \end{array}$$

Duality Theorem $F, F' \in C$, F is free on X. F' is free on X'. then if $|X| = |X'| \Rightarrow F \cong F'$

Pf:

$$\begin{array}{ccccc} F & \xrightarrow{p} & F' & \xrightarrow{\psi} & F \\ i \uparrow & \nearrow_{if} & \uparrow j & \nearrow_{jf'} & \uparrow i \\ X & \xrightarrow[f]{} & X' & \xrightarrow[f']{} & X \end{array}$$

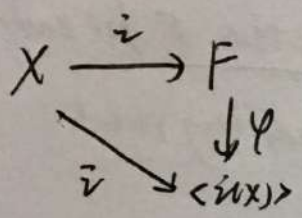
(objections)

By uniqueness

$\Rightarrow p\psi = 1$ $\therefore$ F equal to F'

$\psi p = 1$

① e.g. In group category. free set X for $F \in C$. then $i(X)$ is the generator of group F.

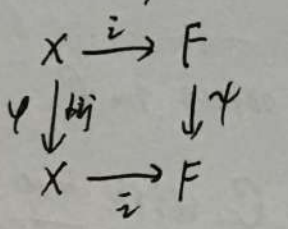


Pf: $i: X \to F$. construct i: $X \to \langle i(X) \rangle$. then $\varphi i = i$, $\varphi = 1$. by uniqueness $\therefore F = \langle i(X) \rangle$

② If in a concrete category. C which contains an object whose u-s contains more than at least 2 elements. then $\forall F \in C$. F free on X. $X \xrightarrow{i} F$. i is injective.

Pf: If $|X|=1$, obviously.

If $|X| \geq 2$.



then $\psi i = i\varphi$. Since φ is injective $\Rightarrow i$ is injective!

④ I in C is universal (initial). If $\forall C \in C$. $\exists!$ morphism $\varphi: I \to C$

T is couniversal (terminal) if $\forall C$. $\exists!$ $\psi: C \to T$

⇓ Any 2 universal or couniversal object are equivalent:

Pf: $I \xrightarrow{f} J \xrightarrow{g} I$, $fg = gf = 1$

Remark: 1) $\langle e \rangle$ is universal and couniversal object in group category.

2) the product/coproduct is determined up to the equivalence (which means it's unique!)

① Direct product and coproduct.

(1) Define: Direct product: $\{G_i | i \in I\}$.

then it's $\prod_{i \in I} G_i$ with an operation in $\prod_{i \in I} G_i$

Operation: define elements in $\prod_{i \in I} G_i$. $f \in \prod G_i$.

$f: I \to \bigcup G_i$, $f(i) \in G_i$, 对 $g \in \prod G_i$

$fg: I \to \bigcup G_i$, by: $f(i)g(i)$. (Image) Denote

$f = [a_i]_{i \in I}$, 对 $f(i) = a_i$

$\Rightarrow$ Then: $\prod G_i$ is a group.

Def: canonical projection: $\pi_k: [a_i] \longmapsto a_k$.

Then $\prod G_i$ is product in group category. → see group as set then check homo-!

(2) (External) weak direct product:

of $\{G_i | i \in I\}$. Denote $\prod^w G_i$.

$\forall f \in \prod^w G_i$, $f(i) = e_i$ for all but finite i.

$\Rightarrow \prod^{w}_{i\in I} G_i \triangleleft \prod_{i\in I} G_i$. If we define $l_i : G_i \to \prod^{w} G_i$

then $l_i(G_i) \Rightarrow \{(a_i)_{i\in I} \mid a_i \neq e\}$. $a_i \neq e$.

for $k \neq i$. $a_k = e$. then $l_i(G_i) \triangleleft \prod G_i$

l_i is called canonical injection.

Remark: If in a category of abelian group. then $\prod_{i\in I} G_i$ denoted by $\sum G_i$. which will be the coproduct!

Pf: $\psi : \sum A_i \to B$. $\forall B \in$ category.

$\varphi((a_i)) = \sum_{i\in I} \psi_i(a_i)$. which will be homo- since B is abelian!

(3) Internal weak direct product:

$\{N_i\}_{i\in I}$ a family of normal group of G.

such that $G = \langle \bigcup_{i\in I} N_i \rangle$ st. $N_i \cap \langle \bigcup_{\substack{k\neq i \\ k\in I}} N_k \rangle = \langle e \rangle$

$\Rightarrow$ then $G \cong \prod^{w}_{i\in I} N_i$

Pf: i) We can denote $(a_i)_{i\in I} \in \prod^{w} N_i$ by

$(a_i)_{i\in I_0}$. I_0 is the finite set. since only finite $a_i \neq e$. then $\prod_{i\in I_0} a_i$ is also well-def in G. since $a \in N_i$. $b \in N_j$. $\to ab = ba$

2°) Def: $\varphi = \prod^W N_i \longrightarrow G$. by $[a_i] \mapsto \prod_{i\in\mathbb{Z}} a_i$ (and $\varepsilon \mapsto e$)
such that $\varphi(\iota_i(a_i)) = a_i$

3°) φ is epi- : $\forall a \in G$. $a = \prod_{i\in\mathbb{Z}} a_i$. then
$\prod_{i\in\mathbb{Z}} \iota_i(a_i) \in \prod^W N_i$, $\varphi(\prod \iota_i(a_i)) = \prod a_i = a$

4°) φ is mono- : $\varphi([a_i]) = \prod a_i = e$. then
$a_1^{-1} = \prod_{i\neq 1} a_i \in N_1 \cap (\vee N_i) = \langle e \rangle \therefore n_1 = e$
$\Rightarrow$ By Induction. $a_k = e$!

Theorem: G is internal product for family of normal group $\{N_i\}_{i\in\mathbb{Z}} \Leftrightarrow a \in G$. $a \neq e$. a is the unique product $a_{i_1} a_{i_2} \cdots a_{i_m}$ st. $a_{i_k} \in N_{i_k}$.

→ Or replace it by: $a_i a_j = a_j a_i$ $i \neq j$. $a_i \in N_i$. $a_j \in N_j$

pf: ($\Rightarrow$) By $G \cong \prod^W N_i$. $a = a_{i_1} \cdots a_{i_m} = a_{i_1} \cdots a_{i_m}$
then $\prod a_{i_k} = \prod a_{i_k} \Leftrightarrow a_{i_k} = a_{i_k}$. $\therefore$ unique!
($\Leftarrow$) $\prod^W N_i \longrightarrow G$ is well-defined.
and obviously epi-. And $\varphi(\prod a_i) = \prod a_i = e$.
since $e = e \cdot e \cdots e$ $\therefore a_i = e$ by uniqueness!

Remark: 1. $\prod^W G_i$ is the internal product for $\{\iota_i(G_i) \mid i \in \mathbb{Z}\}$
2. internal and external will be omitted. Since there're equivalent.

(4) Homo- of product:

$\{f_i: G_i \to H_i \mid i \in I\}$ $f = \prod f_i : \prod G_i \to \prod H_i$.

$f(\{a_i\}) = \{f_i(a_i)\}$. then $\mathrm{Im} f = \{\mathrm{Im} f_i\}$.

$\ker f = \prod \ker f_i$

$\Rightarrow$ If $N_i \triangleleft G_i$. $\prod N_i \triangleleft \prod G_i$ or $\prod^W N_i \triangleleft \prod^W G_i$

$\Rightarrow$ $\prod G_i / \prod N_i \cong \prod G_i / N_i$, $\prod^W G_i / \prod^W N_i \cong \prod^W G_i / N_i$.

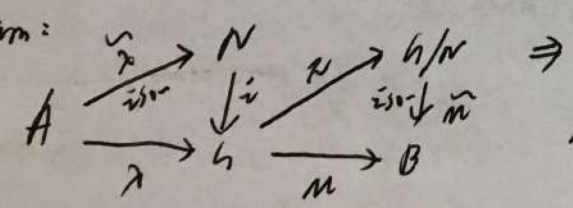
(5) Group Extension:

Consider decompose a Group into small group. Or put small groups together to be a large group.

Ref: If $N \triangleleft G$. $N \cong A$. $G/N \cong B$.

then: G 为 B 过 A 的扩张.

Diagram:



$\Rightarrow \lambda = i\tilde{\lambda}$. mono-

$\mu = \tilde{\mu}\pi$. epi-

Note that $\mathrm{Im}\lambda = \lambda(A) = \ker \mu$, named exact (正合) on G.

$\Rightarrow$ Short exact sequence:

$$\{1\} \longrightarrow A \longrightarrow G \longrightarrow B \to \{1\}.$$

~~s.t. the former image is kernel of latter homo-~~

Proposition: 对 $G \cong G'$, then $\Leftrightarrow$ the exact sequences are same.

Pf: ($\Rightarrow$) It's obvious!

($\Leftarrow$)
$$\begin{array}{ccccccccc} \{1\} & \longrightarrow & A & \xrightarrow{\lambda} & G & \xrightarrow{\mu} & B & \longrightarrow & \{1\} \\ & & \downarrow id & & \downarrow f & & \downarrow id & & \\ \{1\} & \longrightarrow & A & \xrightarrow{\lambda'} & G' & \xrightarrow{\mu'} & B & \longrightarrow & \{1\}. \end{array}$$

By duality. only prove f is mono- $\longrightarrow$ To be Commutative.

$x \in G$. $f(x)=e \Rightarrow \mu'(f(x)) = e = \mu(x)$

$\therefore x \in \ker\mu = \mathrm{Im}\lambda$. $\therefore x = \lambda(y)$

$\therefore f(\lambda(y)) = f(x) = e = \lambda'(y)$ $\therefore y = e$ by λ' mono-

$\therefore x = \lambda(e) = e$ $\therefore f$ is mon-

Now, $\forall N \triangleleft G$. whether H exists, st $H < G$.

$G = HN$. then it's the semidirect product (internal) of G. denote: $G = H \rtimes N$

对 H exists. then: $\mu|_H : H \longrightarrow B$, absolutely homo-

Is it mono-? $\ker(\mu|_H) = \ker\mu|_H = \ker\mu \cap H = N \cap H = \langle e \rangle$

Is it epi-? Note $\forall b \in B$. $\exists g \in G = HN$. $\mu(g) = b$.

And $g = hn$ $\therefore \mu(hn) = \mu(h) = b$. then $h = gn^{-1}$

Then find H ($\Leftarrow$) find a homo-: $\eta : B \longrightarrow G$, st. $\eta(B) \cap N = \langle e \rangle$

and η is mono-. since $\exists M$. $M\eta = 1$

Moreover, 对 $\eta(B) \triangleleft G$. then $G = N \times \eta(B)$ 为 the direct product.

Remark: 1. H can be seen as the complement of N in G. which is equivalent to G/N.

2. External semiproduct: G, H are group. $\theta: H \to Aut\, G$. the $G \times_\theta H$ is the set $G \times H$ and an operation: $(g,h)(g',h') = (g[\theta(h)g'], hh')$

Theorem

$\Rightarrow$ Conversely, give two groups A, B. there must exist an unique direct product of A, B.

pf: $G = A \times B = \{(a,b) \mid a \in A, b \in B\}$.

operation: $(a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2)$

Ref: $A \xrightarrow{\lambda} G \xrightarrow{\pi} B$ And A, B unique up to equivalent!

$a \overset{\lambda}{\longmapsto} (a, 1_B)$

$(a,b) \overset{\pi}{\longmapsto} b$

$(1_A, b) \overset{\eta}{\longleftarrow} b$

Some conclusions:

① $\mathbb{Z}, S_n$ can't be decomposed. And $\mathbb{Z}_k$ can't be decomposed $\Leftrightarrow k = p^w$

pf: 1) The subgroup of $\mathbb{Z}$ can be expressed by $\langle k \rangle$. [If $\mathbb{Z} = \langle k_1 \rangle \langle k_2 \rangle \cdots \langle k_n \rangle$ then $\mathbb{Z}$ is finite! contradiction!] $\longrightarrow$ Wrong. $\mathbb{Z}$ is still infinite!

Or by $\hat{\prod}_{i=1}^{n} k_i \in \hat{\bigcap}_{i=1}^{n} \langle k_i \rangle$,

2°) $n \neq 4$. only $A_n \trianglelefteq S_n$. $n=4$. $A_4, K_4 \trianglelefteq S_n$. $\therefore S_n$ can't be decomposed! (Simple group must be indecomposable)

3°) ($\Leftarrow$) the proper subgroup $= \langle p^i \rangle$ $(1 \le i \le n-1)$

But $\langle p^{n-1} \rangle < \langle p^{n-2} \rangle \cdots < \langle p \rangle$

($\Rightarrow$) if $k = mn$. $(m,n) = 1$. $m, n > 1$

then $Z_m, Z_n \trianglelefteq G$. $Z_m \cap Z_n = \langle e \rangle$

$|Z_m \cdot Z_n| = |G|$ $\therefore G = Z_m \times Z_n$. Contradict!

Remark: A lemma: $Z_k \oplus Z_r \cong Z_{kr} \Leftrightarrow (k,r) = 1$

Pf: ($\Leftarrow$). By 3°). ($\Rightarrow$) only prove the existence of the element with order kr:

choose $(1,1)$. $kr(1,1) = (kr, kr) = (0,0)$

if $n(1,1) = (n,n) = (0,0)$. then $k|n$. $r|n$.

$\therefore kr|n$ $\therefore n = kr$ (suppose n is order of $(1,1)$)

② G is the semi (or direct) product of H, K

then $G/H \cong K$. $G/K \cong H$

Pf: by $G/H = HK/H \cong K/H \cap K = K/\langle e \rangle = K$

③ Refine: complete decomposed group: can be decomposed to be the direct product of simple group.

Refine: direct factor: H. $H \trianglelefteq G$. if exists $K \trianglelefteq G$.

s.t. $H \times K = G$.

Then (1) If H is direct factor of K, K is direct factor of G, then H is the direct factor of G.

若 $N<H$ ← then $N<G$!

Pf: $K = H \times H_1$, $G = K \times H_2 \Rightarrow G = H \times H_1 \times H_2$

$\therefore G = H \times (H_1 \times H_2)$, since $(H_1 \times H_2) \triangleleft G$.

Remark: $H \xrightarrow{f} G$, homo- can be extended

$G \xrightarrow[\text{endo-}]{\pi} G$ by $\pi(h,k) \mapsto (f(h), 0)$

if mono-, then $\pi(h,k) \mapsto (f(h), k)$, auto-

(2) the normal subgroup of completely decomposable group are direct factors.

Pf: $G = \prod_1^n G_i$, G_i is simple.

Since $N \triangleleft G$, $N \cap G_i \triangleleft G_i$.

then $N \cap G_i = G_i$ or $\langle e \rangle$

若 $N \cap G_i = G_i$, then $NG_i = N$.

we the G_i off. 若 $N \cap G_i = \langle e \rangle$

$\therefore NG_i = N \times G_i \Rightarrow N G_{i_1} \cdots G_{i_k} \cap G_k' \triangleleft G_k$.

induce

then we can also cut G_k' off 若 intersection is G_k' or let $N G_{i_1} \cdots G_{i_k} G_k'$

$= N G_{i_1} \cdots G_{i_k} \times G_k'$. $\Rightarrow G = N \times G_{i_1} \cdots \times G_{i_k}$

then $H = \prod_1^k G_{i_k} \triangleleft G$. $G = N \times H$

~~Remark: the subgroups which are normal~~

or quotient groups are completely decomposable!

pf: $G = N \times G_{i1} \cdots \times G_{ir}$. and $N' \times G_{i1} \cdots \times G_{ir} = G$.

N' is the product of diverse factors about G_{ik}.

then $N \cong N'$ (by Krull Theorem) $\cong G/\prod_{1}^{r} G_{ik}$

$G/N \cong \prod_{1}^{r} G_{ik} \cong H$!

④ Notice: 1. $G_1 \cong G_2$. $G_1/H_1 \cong G_2/H_2 \not\Rightarrow H_1 \cong H_2$

(When $G_1 \neq G_2$, $H_2 \trianglelefteq G_2$)

e.g. $\mathbb{Z}_2 \times \mathbb{Z} \cong \mathbb{Z}$. $\mathbb{Z}_2 \times \mathbb{Z}/\mathbb{Z}_2 \cong \mathbb{Z}/\langle e \rangle$

but $\mathbb{Z}_2 \ncong \langle e \rangle$

2. $G_1 \cong G_2$, $H_1 \cong H_2 \not\Rightarrow G_1/H_1 \cong G_2/H_2$

e.g. $\mathbb{Z} \cong \mathbb{Z}_2 \times \mathbb{Z}$. $\mathbb{Z} \cong \mathbb{Z} \not\Rightarrow \mathbb{Z}/\mathbb{Z} \cong \langle e \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}_2$

3. $H_1 \cong H_2$, $G_1/H_1 \cong G_2/H_2 \not\Rightarrow G_1 \cong G_2$

e.g. $\mathbb{Z}_2 \oplus \mathbb{Z}_2/\mathbb{Z}_2 \cong \mathbb{Z}_4/\mathbb{Z}_2$, $\mathbb{Z}_2 \cong \mathbb{Z}_2$

but $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \ncong \mathbb{Z}_4$!

4. $H_1 \times H_2 \cong K_1 \times K_2 \not\Rightarrow H_1 \cong K_1$ or K_2, $H_2 \cong K_1$ or K_2

e.g. $\mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_5 \times \mathbb{Z}_6$ (Not completely decompose!)

Remark: If $G_1 \cong G_2$, then $G_1 \xrightarrow{f} G_2$, f is iso.

$H_1 \trianglelefteq G_2$, $H_1 \cong H_2$, need: $H_1 \xrightarrow{f} H_2$, also

then $f(H_1) = H_2 \Rightarrow G_1/H_1 \cong G_2/f(H_1)$

Or $G_1/H_1 \cong G_2/H_2$, $H_1 \cong H_2$, If need: $G_1 \cong G_2$

then: $G_1 \cong G_1/H_1 \times H_1 \cong G_2/H_2 \times H_2 \cong G_2$

which means it should satisfy direct product rules!

⑧ Free Group and Free Product.

(1) Free Group:

given a set X, construct a group F free on X.

1) 若 $X=\emptyset$, $F=\langle e\rangle$.

2) 若 $X\neq\emptyset$, Define adjacent relation:

若 $\begin{cases} W_1 = u_1 x_i x_i^{-1} u_2 \\ W_2 = u_1 u_2 \end{cases}$ then $W_1 \smile W_2$

若 $u_1=W_1, u_2, u_3 \cdots u_n=W_2$, u_i is adjacent with u_{i+1}, then $W_1 \backsim W_2$.

Then prove the relation is equivalent relation and satisfy the congruent relation:

1. $W = W\cdot 1 \backsim W\cdot x x^{-1}\cdot 1 \backsim W\cdot 1 = W$

2. 若 $W_1 \backsim W_2$, $u_1=W_1, u_2 \cdots u_n=W_2$

$\Rightarrow V_1=W_2, V_2=u_{n-1} \cdots V_n=W_1 \therefore W_2 \backsim W_1$

3. $W_1 \backsim W_2$, $W_2 \backsim W_3$, then $\Rightarrow$

$u_1=W_1, u_2 \cdots u_n=W_2=V_1, V_2 \cdots V_m=W_3 \therefore W_1 \backsim W_3$

4. 若 $u_1 \backsim u_2$, $W_1 \backsim W_2$

$\Rightarrow u_1 W_1 \backsim u_2 W_1 \backsim u_2 W_2$ -- Congruent!

3°) Construct X^{-1} (or not F is monoid or semi-group)

$F = X \cup X^{-1} \cup \{1\}$ (disjoint), the elements in F is the reduced words (*) $= (x_1^{\lambda_1}, x_2^{\lambda_2} \cdots x_n^{\lambda_n}, 1 \cdots 1)$

$\lambda_i = \pm 1$, and replace xx^{-1} by 1 on "$\backsim$" relation.

(*) or the group is too big!

define the binary operation: (just juxtaposition) → may not cancellation if not necessary

$(x_1^{\lambda_1}\cdots x_n^{\lambda_n})(y_1^{\mu_1}\cdots y_m^{\mu_m}) = x_1^{\lambda_1}\cdots x_n^{\lambda_n} y_1^{\mu_1}\cdots y_m^{\mu_m}$

+) check the associativity:

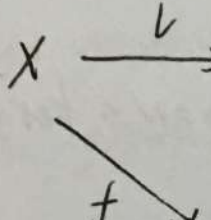
def: $|x^\delta|$ is the map: $F \xrightarrow{|x^\delta|} F$, $y \longmapsto x^\delta y$

then x^δ is a permutation. $F_0 = \langle |x^\delta| \mid x^\delta \in F \rangle$

def: $x_1^{\delta_1}x_2^{\delta_2}\cdots x_n^{\delta_n} \xrightarrow{\varphi} |x_1^{\delta_1}||x_2^{\delta_2}|\cdots|x_n^{\delta_n}|$

$\therefore \varphi$ is the iso-! then $F \cong$ subgrp of $(A(F))$

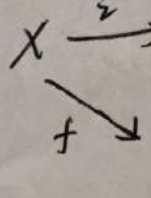
Theorem: $X \xrightarrow{\iota} F$, ι is inclusion map; f is a map, then $\exists$ unique homo- $\bar{f}$. s.t. $\bar{f}\iota = f$.



pf: Def: $\bar{f}(1) = e$, $\bar{f}(x_1^{\delta_1}x_2^{\delta_2}\cdots x_n^{\delta_n}) = f(x_1)^{\delta_1} f(x_2)^{\delta_2}\cdots f(x_n)^{\delta_n}$, well-def-!

⇒ Every group is the homo-image of free group.

pf: X is the generators of G. then $\bar{f}$ is epimorphism.



with the kernel, denote N.

s.t. $W = x_1^{\delta_1}x_2^{\delta_2}\cdots x_n^{\delta_n} \in N$

then $W \xrightarrow{\bar{f}} e$, denote $W = e$

which is the "relation": (among x_i!)

Denote the generators of N is set Y

↓

of reduced words on X!

then $G \cong F/N$. and said $\langle X|Y\rangle$ is the presentation of G. G is the group def by the generator X and relation $W=e. W\in Y$

⇓

Van Dyck Theorem X, Y is the set of reduced words on X is set

G def by generator X and relation $W=e. W\in Y$.

if $H=\langle X\rangle$. satisfying all relation $W=e$,

then $\exists f: G \xrightarrow[f]{epi} H$.

Pf: Note that $Y \subset \ker\bar{f}$. $\therefore \langle Y\rangle = N < \ker\bar{f} \therefore F/N \xrightarrow[epi]{\bar{f}} H$

$\bar{f}: F \xrightarrow{\bar{f}} H$ ⇒ then $G \cong F/N \xrightarrow[f]{} H$. epi!

$i \uparrow \quad \nearrow f$

X

Remark: 1. free is relation free!

2. if $|H|$ is finite. we can estimate $|G| \geq |H|$, and $\underline{|F/N|} = h$. → Count elements in F/N!
by epimorphism and $G \cong F/N$

(2) Free Product:

collect a family of Groups $[G_i | i\in I]$.

(relabel (if $\exists G_i = G_j$) elements). Then

$\prod_{i\in I}^{*} G_i = G_1 * G_2 * G_3 \cdots * G_n$. Operation is the juxtaposition with cancellation.

if we add relation $a_i a_j = e$. $a_i \in G_i$. then ⇒ product?

If $|G_i| \geq 2$ ⇒ free product is infinite group.

Then the product is the coproduct:

$[G_i | i\in I]$ a family of groups. $[\psi_i: G_i \to H | i\in I]$.

then $\exists! \psi: \prod^* G_i \to H$, s.t. $\psi\iota_i = \psi_i$.

pf: Def $\psi(a_1 a_2 \cdots a_n) = \psi_1(a_1)\cdots\psi_n(a_n)$

which is well-def homo!

(3) **Some conclusions:**

① A free group is free product of infinite cyclic group. → 可作自由群拆分!

pf: $X = [x_i | i\in I]$ since $x_i * e \Rightarrow |x_i| = +\infty$.

$X = \bigcup_{i\in I}[x_i]$ $\therefore F(X) = \prod_{i\in I}^*[x_i]$ with operation about juxtaposition! since $F(X) = \langle \bigcup_{i\in I}\langle x_i\rangle\rangle$

② N is the normal subgroup of $A*B$ generated by A

$\Rightarrow A*B/N \cong B$

pf: $\forall\, g\in A*B$. $g = a_1 b_1 a_2 b_2 \cdots a_n b_n$.

$\Rightarrow g = a_1 b_1 a_2 b_1^{-1}\, b_1 b_2 a_3 b_2^{-1} b_1^{-1}\, b_1 b_2 b_3 \cdots a_n \tilde{\prod_1} b_i$

$\in A \tilde{\prod_1} b_i$, then $Ag \xrightarrow{t} b$, 证毕!

$A*B/N \to B$

③ $(X\cup Y | R_1 \cup R_2) \cong (X|R_1) * (Y|R_2)$, R_1, R_2 is relation word

④ $\begin{cases} G_1 \xrightarrow{f} G_2 \\ H_1 \xrightarrow{g} H_2 \end{cases}$ f, g are homo- $\Rightarrow \exists!$ homo- h:

$G_1 * H_1 \longrightarrow G_2 * H_2$, such that $h|_{G_1} = f$, $h|_{H_1} = g$.

Pf: $G_1 * H_1 \xrightarrow{\varphi} G_2 * H_2$

$\uparrow i_1 \circ k_1$ $\nearrow$ $\uparrow i_2 \circ k_2$

$G_1 \amalg H_1 \xrightarrow{f \amalg g} G_2 \amalg H_2$

$\psi_1 : G_1 \longrightarrow G_2 * H_2$, $\psi_1 = i_1 \circ f$

$\psi_2 : H_1 \longrightarrow G_2 * H_2$, $\psi_2 = i_2 \circ g$

$\therefore \exists$ unique $\varphi : G_1 * H_1 \longrightarrow G_2 * H_2$

Def: $\varphi(G_1 * H_1) = f(h_1) * g(H_1)$

φ is homo-, check. $g \in G_1 * H_1$

$\Rightarrow g = g_1 h_1 g_2 h_2 \cdots g_n h_n$. $g_i \in G_1, h_i \in H_1$

Remark: If f, g are iso- $\not\Rightarrow$ φ is iso-

⑨ Free Abelian Groups:

(1) Def: the conditions follows, equivalent.

Definitions:

i) F is an free abelian group.

ii) F has a nonempty basis

iii) $F \cong \sum_{i \in I} \mathbb{Z}$

iv) F is free object in category of abelian, which has universal property. (Then $\forall$ abelian group G is image of free abelian group of rank $|X|$, X is the generator of G)

Lemma An abelian group G is simple
$\Leftrightarrow |G| = p$ or $+\infty$

Pf: 1) 对 $|G| = pq$. 由 sylp-subgroup $\trianglelefteq G$.
Note $\forall$ subgroup of abelian group is normal.

2) Pick $a \in G$. 对 $|a|$ is finite.
then $\langle a \rangle \trianglelefteq G$. 对 $|a|$ is infinite.
$\Rightarrow \langle a^2 \rangle \trianglelefteq \langle a \rangle \trianglelefteq G$.

Define basis for abelian group F is set X. s.t. $\longrightarrow |\chi_i| = +\infty, \forall i$
1) $F = \langle X \rangle$ 对 $\sum_{\chi_i \in X} \lambda_i \chi_i = 0 \Leftrightarrow \lambda_i = 0, \forall i$.

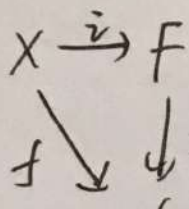
Remark: the basis is different from the basis in vector space.
1. 对 $|F| = n$. Not every L-I-E sets X are the basis of F. e.g. $n=1$, $X = \{k\}$, $k \neq 1$.
$\Rightarrow F = \langle k \rangle = k\mathbb{Z} \neq \mathbb{Z}$!

2. Can't be basis extended sometimes.
e.g. $\{n\}_1^k$ is basis. then $\{i+n\}_1^{k+1}$ can't be extended!

3. Not every generate set contains a basis. $\longrightarrow$ 对 generate by n elements. rank $\leq n$
e.g. $\{n\}_1^k$ basis. then $\{2n\}_1^k \cup \{2i+1+n\}_1^k$!
Note finite basis $\neq$ finite generate in general grp.

Pf: 1)$\Rightarrow$2) $\langle \chi_i \rangle \trianglelefteq F$. $|\langle \chi_i \rangle| = +\infty$. 对 $\langle \chi_i \rangle \cap \langle \bigcup_{k \neq i} \chi_k \rangle \neq Q$. then $\exists n \chi_i = \sum_{k \neq i} \lambda_k \chi_k$. $\exists n \neq 0$.
contradict with L-I-E!

(iii) ⇒ (ii)



define $\bar{f}(\sum n_i x_i) = \sum n_i f(x_i)$

$\bar{f}$ is unique homo-!

(ii) ⇒ (iii)

$\sum \mathbb{Z}$ is the free object on bases $\{\theta_x \mid x \in X\}$.

$|\{\theta_x \mid x \in X\}| = |X| \therefore \sum \mathbb{Z} \cong F$ by duality.

$(\theta_x = \{u_x \mid x \in X\},\ u_x = 1,\ \text{other} = 0\})$

Theorem: Any two bases of F have same cardinality.

pf: If F has finite bases, then

$F/2F \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cdots \oplus \mathbb{Z}_2$ (m summands) $\cong \mathbb{Z}_2 \oplus \cdots \mathbb{Z}_2$ (n summands)

$\therefore m = n$

If F has infinite bases.

the $|F(A)| = |A| = |F|$

by $F = \bigcup_{n \in \mathbb{N}^+} \langle x_1, x_2 \cdots x_n \rangle$, $x_i \in A$.

$|F| \geq |A|$ obviously. $|F| \leq |\cup A^n| \, |\langle x_1 \cdots x_n \rangle|$

$= |A| \aleph_0 = |A|$

$\Rightarrow F_1(X_1) \cong F_2(X_2) \iff |X_1| = |X_2|$

For analysing the structure of abelian grp:

Thm: If F is free abelian on X. X is finite.
$|X|=n$. $G<F$. $G\neq\langle 0\rangle$. then $\exists\ \{x_i\}_1^r$
$\in X$. $1\le r\le n$, $\{d_i x_i\}_1^r$ is basis of G.
such that $d_1|d_2\cdots|d_r$

pf: Lemma = $\{x_i\}_1^n$ is basis of $F \Rightarrow \{x_1 x_2\cdots x_j+ax_i\cdots x_n\}$
is also the basis of F.

Now by Induction on n. $n=1$, obvious!
Assume $<n$ holds. Let S be set such
that $\forall$ element $=\sum_1^n k_i y_i$ in G (of basis $\{y_i\}_1^n$ of F)
then $\{k_i\}_1^n \subset S$. $S\neq\emptyset$ since $G\neq\langle 0\rangle$
then $\exists$ minimal positive integer d_1
$\Rightarrow v=d_1y_1+\sum_2^n k_iy_i$. $k_i=q_id_1+r_i \Rightarrow$
$v=d_1(y_1+\sum_2^n q_iy_i)+\sum_2^n r_iy_i$ $\therefore r_i=0$ since $r_i<d_1$
$\therefore v=d_1x_1\in G$. $x_1=y_1+\sum_2^n q_iy_i$. $\{x_1,y_2\cdots y_n\}$ is basis!

Since $F=\langle x_1\rangle\oplus\langle y_2,\cdots y_n\rangle=\langle x_1\rangle\oplus H$
$G=\langle x_1\rangle\oplus(G\cap H)$, by induction
$G\cap H$ is free abelian with basis $\{d_i\}_2^r$
by $d_2>d_1$. $d_2=qd_1+r_1$. $d_1x_1+d_2x_2=d_1(x_1+qx_2)+r_1x_2$
$\therefore r_1=0$. $\therefore d_1|d_2$ $\therefore G$ has basis of $\{d_ix_i\}_1^r$

Remark: subgrp of F with basis may not
contained in the basis of F. e.g. $F=\mathbb{Z}$.
by $\{1\}$. by $n\mathbb{Z}<\mathbb{Z}$. by $\{n\}$.

(2) **Some conclusions:**

① The direct sum of free abelian group is free abelian, but direct product not

Pf: more than free abelian group is the direct sum of infinite cyclic group.

But $\prod_{z\in\mathbb{Z}} \mathbb{Z}$. may be uncountable. So it will not have a basis.

② F free group on X. G on Y.

$F' = \langle \{aba^{-1}b^{-1} \mid a,b\in F\}\rangle$. $G' = \langle \{aba^{-1}b^{-1} \mid a,b\in G\}\rangle$

then $F \cong G \iff |X| = |Y|$

Pf: ($\Leftarrow$) by universal property of free objects.

($\Rightarrow$) $\varphi: F \cong G$. then $\varphi: F' \cong G'$

$\therefore F/F' \cong G/G'$. $|F/F'| = |X| = |G/G'| = |Y|$

(F/F', G/G': free abelian)

(10) Finite generated abelian Group.

Proposition: $\forall$ finite generated abelian group $\cong$ a direct sum of infinite group or finite cyclic summands of order $m_1, m_2 \cdots m_n$.

$m_1 | m_2 | m_3 \cdots | m_n$

Pf: $F \xrightarrow{f} G$. epi. $\therefore \exists \ker f < F$. if basis of F is $\{x_i\}_1^n$

the basis of $\ker f$ is $\{d_i x_i\}_1^r$ $\therefore \ker f = \sum_1^r \langle d_i x_i \rangle$

$F/\ker f \cong G$. $\therefore G \cong \mathbb{Z}d_1 \oplus \mathbb{Z}d_2 \cdots \oplus \mathbb{Z}d_r \oplus \mathbb{Z} \cdots \oplus \mathbb{Z}$.

($d_i \neq 0$ or 1. if $d_i = 1 \Rightarrow \mathbb{Z}/d_i\mathbb{Z} = \langle 0 \rangle$)

Remark: 1. Finite generated Abelian group is free
($\Leftrightarrow$ every element is infinite order.

→ if infinite generated then it's wrong: e.g. $\mathbb{Q}$ is not free since no basis!

2. Now $\mathbb{Z}_d = \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \cdots \oplus \mathbb{Z}_{p_k^{r_k}}$

we can decompose G with prime power order

And clearly know $\exists H < G. \forall |H| \mid |G|$

Theorem: The deposition of finite generated abelian group is unique.

Pf: lemma. if $\varphi: G \cong H$. then $\varphi: G(p) \cong H(p)$

$\varphi: G_t \cong H_t$. (G_t, H_t are torsion group)

then $G/G_t \cong H/H_t$

$\Rightarrow$ Prove: $G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \cdots \oplus \mathbb{Z}_{m_t} \oplus F$, F is free abelian

$\cong \mathbb{Z}_{p_1^{s_1}} \oplus \mathbb{Z}_{p_2^{s_2}} \cdots \oplus p_k^{s_k} \oplus F$ is unique test

1') the rank of F is constant - by $F \cong G/G_t \cong H \oplus F/G(H)$

2') if $G \cong \sum_1^r \mathbb{Z}_{n_i} \oplus F \cong \sum_1^s \mathbb{Z}_{k_j} \oplus F'$, n_i, k_j are power of prime.

$\Rightarrow (\sum_1^r \mathbb{Z}_{n_i})(p) \cong (\sum_1^s \mathbb{Z}_{k_j})(p)$

$\therefore \sum_1^r \mathbb{Z}_{p^{\alpha_i}} \cong \sum_1^s \mathbb{Z}_{p^{\beta_i}}$ $(\sum_1^r \mathbb{Z}_{p^{\alpha_i}})[p] \cong (\sum_1^s \mathbb{Z}_{p^{\beta_i}})[p]$

$\because \sum_1^r \mathbb{Z}_p \cong \sum_1^s \mathbb{Z}_p \quad \therefore r=s.$

Let: $p^{av} G(p) \cong \sum_1^r \mathbb{Z}_{p^{a_i - a_v}} \cong \sum_1^r \mathbb{Z}_{p^{c_i - a_v}}$

$\Rightarrow$ must $a_v = c_i$!

Remark: G, H, K are finitely generated abelian groups. then:

$G \oplus G \cong H \oplus H \Rightarrow G \cong H$ (consider elementary divisors!)

$G \oplus H \cong G \oplus K \Rightarrow H \cong K$

But if G is infinite generated. it will be wrong:

e.g. $G = \sum_1^\infty \mathbb{Z}$. $G \oplus \mathbb{Z} \oplus \mathbb{Z} \cong G \oplus \mathbb{Z}$. but $\mathbb{Z} \oplus \mathbb{Z} \ncong \mathbb{Z}$!

Some conclusions:

① If a finite abelian p-group satisfies:

i) only a subgroup with order p. Or.

ii) only a subgroup with index p.

Then. it's a cyclic group.

Pf: The structure is $\mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \cdots \oplus \mathbb{Z}_{p^{k_s}}$

Then it's clear! if $s \geq 2$. Contradict!

Remark: If finite p-group only has a subgroup with an index p. then it's cyclic.

Pf: $|C(G)| \geq p$. By Induction on order p^n. n.

$\Rightarrow (G/C(G) : H/C(G)) = p \quad \therefore G/C(G)$ is cyclic

$\therefore G$ is abelian!

⊙ G is finite abelian group and x has maximal order. then $\langle x\rangle$ is the direct sum factor

pf: Lemma. Let G is p-group. We show it holds.

pf: If G is cyclic. obvious. if it's not.

By Induction on $|G|$'s "n". $|G|=p^1$ obviously!

1°) Note $|G|=p^n$. G has more than 1 subgroup with order p, while $\langle x\rangle$ only have a subgroup with order p. $\therefore \exists H. |H|=p$.

$H\cap\langle x\rangle=\emptyset$ $\therefore \langle x\rangle+H/H=\langle x\rangle$

$\Rightarrow$ Then in G/K: $\forall g+k$ with order divids $|g|$.

$\therefore x+k$ is still most-order-element.

2°) By assumption of induction: $G/K\cong\langle x+k/K\oplus H'$

for some $H'<G/K$. $\therefore K<\pi^{-1}(H')<G$.

$\therefore G/K\cong\langle x+k/K\oplus\pi^{-1}(H')/K$

$\therefore G=\langle x\rangle+k+\pi^{-1}(H')$. since $K<\pi^{-1}(H')$

$\therefore G\cong\langle x\rangle\oplus\pi^{-1}(H')$

Then $G(p_1)\cong\langle a_1\rangle\oplus H_1$. $\forall p_1$, a_1 has maximal order in $G(p_1)$ $\Rightarrow^{by}G\cong\sum G(p_i)$

$\therefore G\cong(\langle a_1\rangle\oplus\langle a_2\rangle\cdots\oplus\langle a_m\rangle)\oplus(H_1\oplus\cdots H_n)$

$\langle a\rangle=\langle a_1\rangle\oplus\langle a_2\rangle\cdots\langle a_m\rangle$. since $(p_1,p_2\cdots p_n)=1$

$\therefore a$ has maximal order!

$\Rightarrow G\cong\mathbb{Z}_{m_1}\oplus\mathbb{Z}_{m_2}\oplus\cdots\mathbb{Z}_{m_n}$, $m_1|m_2|\cdots|m_n$

$\therefore$ [(1,1,1⋯1),(0,1,1⋯1),(0,0,1⋯1)⋯(0,0⋯0,1)] set of max order elements!

Remark: $\forall$ F-A p-group is generated by the maximal elements.

④ G is torsion free group. Then

i) $G \cong \sum G(p)$

ii) If H is another torsion free,

$G \cong H \Leftrightarrow G(p) \cong H(p)$, $\forall p$.

Pf: i) 1') $G(p_1) \cap G(p_2) = \langle 0 \rangle$. by Lagrge.

2) $\forall u \in G$. $|u| = \prod_1^n p_i^{k_i}$ =

Note that $(\frac{|u|}{p_1^{k_1}}, \frac{|u|}{p_2^{k_2}} \cdots \frac{|u|}{p_n^{k_n}}) = 1$

$\therefore \exists c_i \quad \sum c_i \frac{|u|}{p_i^{k_i}} = 1$

$\Rightarrow u = \sum c_i \cdot (\frac{|u|}{p_i^{k_i}} u) \in G(p_i)$

$\in \sum G(p_i)$ $\therefore G = \sum G(p_i)$

ii) ($\not\Leftarrow$) Consider elementary element

Remark: Note that $\bar{y} \in G/\langle x \rangle$, x is the maximal-order-element in F-A p-grp G.

then $\exists y \in G$. $|y| = |\bar{y}|$. By Induction:

$|y| \geq |\bar{y}|$ $\quad G(p)/\langle x \rangle \cong \sum \langle \bar{x}_i \rangle \Rightarrow G(p) \cong \sum \langle x_i \rangle \oplus \langle x \rangle$

$\langle y \rangle \subset \langle y \rangle$!

Then we can also have the structure Theorem.

④ Count subgroups of order p^2 in $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$

Pf: i') $p^2 \frac{1}{\eta} z = kx + ty$ (Assume (x, y) is basis)

$p^2 | pk, p^2 | pt \Rightarrow \begin{cases} t = pt'. & 0 \leq t' \leq p-1 \\ k = p^2 k'. & 0 \leq k' \leq p-1 \end{cases}$ but $(k', t') \neq 0$

$\therefore \frac{1}{\eta} p^2 - 1 \eta$.

2) p^2阶元：可通过计算p^3阶元间接得到：

$p^3 \mid p^3k$, $p^2 \mid p^3t$, and $p \nmid k, t$.

$\therefore k = r_1p + k'$, $t = r_2p + t'$ → 不影响，取 $0 \le t \le p^2-1$

$r_1 = 0 \sim p^2-1$ $\therefore$ 共 $p^2 \cdot p^2(p-1)$ 个

$\therefore p^2$阶元 $= p^5 - p^4(p-1) - (p^2-1) - 1 = p^2(p^2-1)$

$\Rightarrow$ 而p^2阶循环群有 $p(p-1)$ 个p^2阶元，$\therefore p(p+1)$ 个p^2阶循环群.

注意 p阶元 p^2-1 个，而p^2阶群至少 p^2-1 个 $\therefore$ 1个非循环群

$\therefore$ 共 p^2+p+1 个！

② $G = Z_p \oplus Z_p \Rightarrow G$有$p$阶自同构.

Pf: G中p阶元 $= p^2-1$ 个. $\begin{cases} \tau(x) = ix + jy \\ \tau(y) = kx + ty \end{cases}$ $\tau \in \mathrm{Aut}G$.

$\{x, y\}$ is basis of G. then (i, j) 共 $m(k, t)$！$(0 \le m \le p-1)$ → 完备！

固定 (i, j) 共 p^2-p 个 $\therefore (p^2-1)(p^2-p)$ 为 $|\mathrm{Aut}G|$

By sylow Thereen $\Rightarrow \exists u \in \mathrm{Aut}G$ $|u| = p$.

③ $|G| = p^aq^b$, $\mathrm{Aut}G$ 中无p阶元. $\Rightarrow a = 0$ or 1

Pf: Note that $\mathrm{Inn}G < \mathrm{Aut}G$. $G/C(G) \cong \mathrm{Inn}G$

$\therefore p \nmid |G/C(G)|$ $\therefore p^a \mid\mid |C(G)|$ $\therefore$

$\exists P \in \mathrm{Syl}_p(G)$. s.t. $P \in \mathrm{Syl}_p(C(G))$

$\therefore P < C(G)$ $\therefore P \trianglelefteq G$, P is unique!

Since $Q \in \mathrm{Syl}_q(G)$, $|PQ| = p^aq^b$.

P is contained in $C(G)$ $\therefore Q \trianglelefteq G$.

$P \cap Q = \langle e \rangle$ $\therefore G = P \times Q$.

If $Z_p \oplus Z_p < P$, $\Rightarrow$ 有P阶元在Aut(G).

$\therefore P = Z_{p^a}$, 对于 $a>1$, then $p^{a-1}+1$

$P = \langle x \rangle$, $x \in Aut(G)$, $x(x) = x^{p^{a-1}+1}$

$\therefore |x| = P$. contradiction!

(13) The Krull-Schmidt Theorem

Def: ACC, DCC $\Rightarrow$ 可不断分为proper subgrp!

Remk: finite group satisfies both conditions

步

(1) **Theorem:** If G satisfies ACC or DCC on normal group then G is direct product of finite number of indecomposable subgrp.

pf: the idea is sprang from "suppose $G = G_1 \times G_2 \cdots \times G_n \cdots$ is infinite number of I-subgrp", then.

$G_1 \trianglelefteq G_1 \times G_2 \trianglelefteq G_1 \times G_2 \times G_3 \cdots \trianglelefteq \hat{\prod} G_i$ or

$G \trianglelefteq G/G_1 \trianglelefteq G/G_1 \times G_2 \cdots$

That means. firstly collect the groups G such that G is direct factor and is direct product of infinite normal subgroups. then

$G = H \times T_H$, $H = K_H \times J_H$ $\cdots$ decompose!

(2) Lemma. $\dot{X}$ normal endo- $= af(b)a^{-1} = f(aba^{-1})$, $\forall a,b \in G$.

If G satisfies ACC / DCC on normal subgrp.

f is endo- / normal endo- of G. Then f is auto-

$\Leftrightarrow$ f is epi- / mono-

Pf: 1) $\langle e \rangle < \ker f < \ker f^2 \cdots < \ker f^n \cdots$

$\therefore \exists n.\ \ker f^n = \ker f^{n+1}$.

If $a \in G$. $f(a) = e$. Since f epi- $\Rightarrow f^n$ epi-

$\therefore a = f^n(b)$ $\therefore f^{n+1}(b) = e = f^n(b)$. Since $b \in \ker f^n = \ker f^{n+1}$

$\therefore a = e$. $\therefore f$ mono-

2) $G > \mathrm{Im} f > \mathrm{Im} f^2 > \cdots > \mathrm{Im} f^n > \cdots$

($\mathrm{Im} f^k$ is normal since f is normal endo-)

$\Rightarrow \mathrm{Im} f^n = \mathrm{Im} f^{n+1}$ $f^n(a) = f^n(f(b))$ $\therefore a = f(b)$, $\forall a$.

Since f is mono- $\therefore f$ is epi-!

dd

Cor: If G satisfies both on normal subgrp.

f normal endo- of G. $\Rightarrow G = \ker f^n \times \mathrm{Im} f^n$ for some n.

Pf: By Lemma. $\mathrm{Im} f^k = \mathrm{Im} f^n$. $\ker f^k = \ker f^n$. $\forall k \geq n$.

Claim: $\mathrm{Im} f^n \cap \ker f^n = \langle e \rangle$

$\forall c \in G$. express $c = \mathrm{Im} f^n \times \ker f^n$

$c = f^n(d) \times \ker f^n \Rightarrow$ $c f^n(d^{-1}) \in \ker f^n$

$\Rightarrow f^n(c) f^{2n}(d^{-1}) = e \Rightarrow f^n(c) = f^{2n}(d)$

$\therefore d = f^n(c)$ $\therefore c \in \mathrm{Im} f^n \times \ker f^n$

Cor. If G is indecomposable, satisfies ACC and DCC on normal subgroup, f is normal endo- of G.

$\Rightarrow f$ is nilpotent or auto!

Pf: $\Rightarrow \ker f^n = \langle e \rangle$ or $\mathrm{Im} f^n = \langle e \rangle$

$\Rightarrow \ker f = \langle e \rangle$ or $f^n(a) = e. \forall a \in G.$

By Lemma $\Rightarrow$ auto- or nilpotent.

Lemma: Pf: $f+g = a \overset{G \to G}{\longmapsto} f(a)g(a)$ → may not a endo!

If "—", f is normal nilpotent endo- of G, $\sum_1^r f_{ik}$ is endo-

then $\sum_1^n f_i$ is nilpotent.

Pf: By Induction. $n=2$: If f_1+f_2 is not nilpotent.

since f_1+f_2 is also normal $\therefore f_1+f_2$ is auto-

then $\exists (f_1+f_2)^{-1} = g \therefore g(f_1+f_2) = 1 = (f_1+f_2)g$

$\Rightarrow g_1 = f_1 g,\ g_2 = f_2 g. \Rightarrow x = [g_1(x^{-1})\ g_2(x^{-1})]^{-1}$

$\therefore g_1+g_2 = g_2+g_1 = 1 \therefore g_1 g_2 = g_2 g_1$

$(g_1+g_2)^m = \sum C_i^m g_1^i g_2^{m-i}$, but g_1, g_2 nilpotent.

$\Rightarrow$ for large enough m, $(g_1+g_2)^m(x) = e. \forall x \in G.$

Remark: replace nilpotent by auto-

If $\sum_1^r f_{ik} \neq 0$, then $\sum_1^n f_i$ is auto-

(3) Krull-Schmidt Theorem.

G satisfies ACC and DCC on normal subgroups.

If $G \cong G_1 \times G_2 \cdots \times G_s \cong H_1 \times H_2 \cdots \times H_t$. then $s=t$. (H_i, G_i are simple subgps!)

and $H_i \cong G_i$. and $\forall r$. $G \cong G_1 \times G_2 \cdots \times G_r \times H_{r+1} \cdots \times H_t$.

Pf: It state the uniqueness of decompose of simple groups!

1) By Induction on r. Consider π_i on $G_1 \times G_2 \cdots \times G_s$.

and π'_i on $G_1 \times \cdots G_{r-1} \times H_r \times \cdots \times H_t$. check projections are normal(X) $\Rightarrow$ Consider l_i and l'_i on $G_1 \times \cdots G_s$ and

$G_1 \times \cdots G_{r-1} \cdots \times H_t$, $\varphi_i = l_i \pi_i$. $\varphi'_i = l'_i \pi'_i$. check normal endo!

2) Now $\varphi_r = \varphi_r(\sum_i^t \varphi'_i) = \varphi_r\varphi'_r + \varphi_r\varphi_{r+1} + \cdots \varphi_r\varphi'_t \to$ normal.

And $\varphi_r|_{G_r}$ is normal auto., G_r satisfies ACC or DCC.

$\Rightarrow \exists$ some $j \geq r$. s.t. $\varphi_r\varphi'_j$ is auto., so $(\varphi_r\varphi'_j)^{n+1}$ is!

$(\varphi_r\varphi'_j)^{n+1} = \varphi_r(\varphi'_j\varphi_r)^{n}\varphi'_j$ $\therefore \varphi'_j\varphi_r : H_j \to H_j$ can't be nilpotent.

$\therefore \varphi'_j\varphi_r$, $\varphi_r\varphi'_j$ are both auto. $\to$ $\begin{cases} \varphi'_j|_{G_r} : G_r \to H_j \\ \varphi_r|_{H_j} : H_j \to G_r \end{cases}$ are iso-!

$\therefore G_r \cong H_j$!

Then def $\theta : G_1 \cdots \times G_{r-1} \times H_r \times \cdots \times H_t \to G_1 \times \cdots G_r \times H_{r+1} \cdots \times H_t$ by φ'_j, φ_r!

Some conclusions:

① a) $G = H \times K$ satisfies ACC or DCC. so do H and K

b) $G \cong F$. G satisfies ACC or DCC, so do F

Pf: a) obvious chains of H, K contained in G.

b) $H_1 > H_2 \to H_n \cdots$, $H_i < F$. then

$H_i = f(G_i)$. $G_i < G$. $G_1 > G_2 \cdots > G_n \cdots$

$\exists n$. $\forall k \geq n$. $G_n = G_k \Rightarrow H_n = H_k$ ✓

Date.
No.

② f, g are normal endo- of G.

check i) fg so ii) $H \trianglelefteq G \Rightarrow f(H) \trianglelefteq G$

③ Somethings about $Z(p^\infty)$

i) $Z(p^\infty) = \{ \frac{\bar{a}}{p^n} \mid n \in \mathbb{Z} \}$. $\frac{\bar{a}}{p^n} = \{ \frac{k}{p^n} \mid (k, p) = 1,\ 1 \le k \le p^n \}$.

ii) $Z(p^\infty) < \mathbb{Q}/\mathbb{Z}$ (additive.)

iii) the proper subgrp of $Z(p^\infty)$ is $C_n = \langle \frac{1}{p^n} \rangle$, $n \in \mathbb{Z}^+$

iii) $Z(p^\infty) \cong \varinjlim \langle \{ x_n \mid |x_n| = p^n \} \rangle$ (abelian)

iv) $Z(p^\infty)$ satisfies DCC but not ACC

Note that: $(ij)(kl) \in A_n$

- $(ij)(ij) = 1$ --- ①
- $(ij)(ik) = (kji)$ -- ②
- $(ij)(kl)$ --- ③

For the case ③. we can construct a bridge.
Since. there's not bond between (ij) and (kl)

note that $(jk)(jk) = 1 \therefore (ij)(jk)(jk)(kl)$
$= (jki)(ljk)$. So that $\underline{A_n = \langle \{3\text{-cycles}\} \rangle}$

3') Lemma: the k-cycles are conjugated mutually (Next. we prove: $k=3$)

pf: $\forall (ijk)$. $(ijk) = \sigma(123)\sigma^{-1}$. $\sigma \in S_n$
$= (\sigma(1)\ \sigma(2)\ \sigma(3))$, then $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$ --

Anyway. $\underline{\text{if } n \geq 5}$. $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ i & j & k & i_5 & i_6 & \cdots & i_n \end{pmatrix}$

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ i & j & k & i_6 & i_5 & \cdots & i_n \end{pmatrix}$. then either

$\sigma_1 \in A_n$. or $\sigma_2 \in A_n$

Remark: ① If $N \trianglelefteq \underline{A_n}$. which contains a cycle-3 then $N = A_n$

The thinking of the proof of:

A_n is simple. when $n \neq 4$.

1°) If we want to find a normal group of G. we will find a kernel of homo-. since we regard the normal group as a kernel.
But we can also do the steps. follow:

① Take the generators of G.

② Check the conjugations.

↳ Normal group is consists of conjugations!

If we want to prive that $\forall N \trianglelefteq A_n$.
then $N = A_n$. which is equivalent to say: the generators of A_n are conjugated mutually!

2') So firstly. observe the generators of A_n:

⑧ There's a partition of S_n about conjugations:

Let $\sigma_1 = (a_1 a_2 \cdots a_{l_1})\cdots(q_1 q_2 \cdots q_{l_k})$. $\tau\sigma_1\tau^{-1} =$

$(\tau(a_1)\tau(a_2)\cdots\tau(a_{l_1}))\cdots(\tau(q_1)\cdots\tau(q_{l_k}))$. $n = l_1 + l_2 + \cdots + l_k$

After conjugating, it contains the partition of n.

∴ the number of conjugations of S_n = the kinds of $\sum a_i = n$.

4) Suppose $H \neq \langle e \rangle \triangleleft A_n$. We prove: A 3-cycle exists in H eventually. Pick $\sigma = (a_1 \cdots a_r)\tau$. Denote a_r with k

We have: $\sigma = (123\cdots r)\tau$

Case 1. If $r \neq 4$. Pick $(123) \in A_n$.

$(123)\sigma(123)^{-1}\sigma^{-1}$ → for offsetting the τ!

$= (2314\cdots r)\tau\sigma^{-1} = (124)$ the whole is commutator which has double conjugations!

Case 2. If the cycles of σ with length $= 3$, then: $\sigma = (123)(456)\tau$

$\sigma = (123)\tau$, τ is the product of transpositions

$\sigma = (12)(34)\tau$

∴ Case 2.1. $\sigma = (123)(456)\tau$

Pick $(124) \in A_n$. $(124)\sigma(124)^{-1}\sigma^{-1} = (12534)$

connect $(123)(456)$ → Case 1 ✓

Case 2.2. $\sigma = (123)\tau$, then $\sigma^2 = (123)^2 = (132)$

Case 2.3. $\sigma = (12)(34)\tau$. If we still combine a cycle with 1.2.3.4. it will not produce a 3-cycles or more. Attempt to use (125).

$(125)\sigma(125)^{-1}\sigma^{-1} = (125)(12)(125)^{-1}(125)(34)(125)^{-1}(12)(34)$

$= (25)(34)(12)(34) = (152)$ □

① Complete Group:

In the Group Extension, we find G such that $K \triangleleft G$. and $G/K = Q$, $Q < G$. Now we will find a special normal subgroup K. s.t. for arbitary quotient group Q. extend a unique G.

Proposition: Above is equivalent to find all $K \triangleleft G$. for arbitrary G. $\boxed{K \text{ is direct factor}}$

Theorem: It's equivalent that $Z(G) = \langle e \rangle$. $\mathrm{Inn}G = \mathrm{Aut}G$

pf: ($\Leftarrow$) If $\exists Q < G$. s.t. $G = K \times Q$, then $Q < C_G(K)$

$\Rightarrow K \cap Q < K \cap C_G(K) = Z(K)$

And $G = KQ = KC_G(K)$ $\therefore \forall g \in G.\ k_1 \in K,\ g k_1 \in C_G(K)$

$\therefore g k_1 k k_1^{-1} g^{-1} = k \Rightarrow k_1 k k_1^{-1} = \underline{g^{-1} k g}$ ↗ $\gamma_g|_K \in \mathrm{Aut}K$

$\therefore \gamma_g|_K \in \mathrm{Inn}K$, then If $Z(K) = \langle e \rangle$

$\mathrm{Inn}K = \mathrm{Aut}K$. $\Rightarrow G = K \times Q = K \times C_G(K)$

($\Rightarrow$) For $g^{-1} k g = \gamma_g(k)$. $\gamma_g \longmapsto \mathrm{Aut}K$ is

surjective: $\varphi(k) = k_0 k k_0^{-1} = gkg^{-1}$. see k, g as the permutations of k, then $k = Lk$. left-translation $gLkg^{-1} = L_{\varphi(k)}$. G contains Lk and a subgroup of Aut_k $\therefore G = \langle Lk, Aut_k \rangle = Hol(k)$

for letting G small possibly, then $k \cap G_1(k) = \langle e \rangle$

② The Probelm: If G is solvable. $G^{(1)}/G^{(2)}$, $G^{(2)}/G^{(3)}$ are cyclic, then $G^{(2)} = G^{(3)}$, which means $G^{(2)} = \langle 0 \rangle$

Pf: Let $X = G/G^{(3)}$. $X' \cong G^{(1)}/G^{(3)}$ $X^{(2)} \cong G^{(2)}/G^{(3)}$

$X^{(3)} = \langle e \rangle$. Note: $X/_{C_X(X^{(2)})} \times X^{(2)} \xrightarrow{\text{conj}} X^{(2)}/\square$

Since $X^{(2)} \trianglelefteq X$. $\therefore X/_{C_X(X^{(2)})}$ embedded in Aut $X^{(2)}$ which is abelian, $\therefore X/_{C_X(X^{(2)})}$ abelian.

$\therefore X' < C_X(X^{(2)})$, $X^{(2)} < C(X')$

$\therefore X'/_{C(X')} \cong X'/X^{(2)}/(C(X')/X^{(2)})$ which is cyclic!

$\therefore X'$ is abelian, $\Rightarrow X^{(2)} = \langle e \rangle$ $\therefore G^{(2)} = G^{(3)} = \langle e \rangle$

P-Group:

Property: If H is the maximal subgroup in G. then $|G/H|=p$. and $H \trianglelefteq G$.

$\Rightarrow$ Proposition: If G is p-group. G/G' is cyclic, then G is abelian

Pf: ($\Leftarrow$) Prove: if G is nonabelian. then G/G' is noncyclic.

Pick H is the maximal subgrp of G then H is unique. Since $\forall x \in G/H$. $\langle x \rangle$ is the subgroup of G. $\langle x \rangle \nsubseteq H$. $\therefore \langle x \rangle = G$

But G is nonabelian. then $\exists H_1, H_2$, which are both the maximal subgrp of G $\therefore$ in G/G'. H_1/G' and H_2/G' are the maximal subgrp. Sin $G' < H_1, H_2$. By $|G/H_1| = |G/H_2| = p$. $\therefore G/G'$ will not be cyclic!