Supplement on solvable groups:

(1) A finite solvable group admits a cyclic tower with the last term $= \{e\}$.

Pf: step (1) G abelian, finite.

(Induction on $|G|$)

Take any $x \neq e \in G$. Set $N = \langle x \rangle$

If $N = G$, then $G = N \rhd \{e\}$ is a cyclic tower

Otherwise, $|G/N| < |G|$ and by induction,

we get a cyclic tower ~~for~~ $G/N = \bar{G}_0 \supset \bar{G}_1 \supset \cdots \supset \bar{G}_n = \{\bar{e}\}$

Consider the canonical morphism

$$G \xrightarrow{\pi} G/N$$

Set $G_i = \pi^{-1}(\bar{G}_i)$, $0 \leq i \leq n$

Then $G_i/G_{i+1} \simeq \bar{G}_i/\bar{G}_{i+1}$ cyclic

Thus we get a tower

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = N \supset \{e\}$$

which is cyclic.

Step (2) G. solvable, finite.

By definition, G admits an abelian tower:

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\} \stackrel{\Delta}{=} G_{n+1}$$

Consider the canonical morphisms

$$\pi_i : \quad G_i \longrightarrow G_i / G_{i+1}, \qquad 0 \le i \le n$$

By step (1), since G_i / G_{i+1} abelian, finite,

we get a refinement of $G_i \supset G_{i+1}$ by

$$G_i \supset G_{i1} \supset \cdots \supset G_{i r_i} = G_{i+1}$$

which is cyclic.

Therefore, combining all refinements of $G_i \supset G_{i+1}$, $0 \le i \le n$,

we get a cyclic refinement of the original abelian tower.

(2) For finite groups, more than half groups are solvable.

(2.1) Theorem (Feit-Thompson)

$|G| = n$ odd, then G must be solvable!

(2.2) $|G| = 2^n$, Then G is solvable.

pf: use the class formula, to conclude $Z(G) \neq \{e\}$.

Then do induction on n.

\#

Lecture 4. cyclic groups, Permutation groups.

Part I: cyclic groups.

Prop: G cyclic. Then

$$G \cong \begin{cases} \mathbb{Z} \\ \mathbb{Z}/n\mathbb{Z}, & \text{for } n \in \mathbb{N} \end{cases}$$

pf: Take x to be a generator of G,

define $\mathbb{Z} \xrightarrow{f} G$

$n \longmapsto x^n$

then f is surjective, homomorphism.

if $\ker(f) = \{e\}$, then $\mathbb{Z} \simeq G$.

otherwise, claim: $\ker(f) = n\mathbb{Z}$, ~~for~~ some $n \in \mathbb{N}$.

pf of claim: Consider the subset

$\ker(f) \cap \mathbb{N} \subsetneq \mathbb{N}$

Let n be the least element in $\mathrm{Ker}(f) \cap \mathbb{N}$.

Then claim: $\forall\, m \in \mathrm{Ker}(f)$, $m = n \cdot q$

if $m < 0$, then $-m \in \mathrm{Ker}(f) \cap \mathbb{N}$.

Thus we assume $m \in \mathrm{Ker}(f) \cap \mathbb{N}$.

By assumption, $m \geq n$.

$\Rightarrow \quad m = n \cdot q + r, \qquad 0 \leq r \leq n-1$

Euclidean algorithm.

$\Rightarrow \quad r = m - n \cdot q \in \mathrm{Ker}(f) \cap \mathbb{N}$

n is minimal
$\Rightarrow r = 0 \iff m = n \cdot q$.

#.

<u>Prop</u>: (1) G cyclic, $|G| = n$. Then $\forall\, d \mid n$, $d > 0$. $\exists!$ subgroup H of G, $|H| = d$, which is again cyclic.

(2) G_i, $i = 1, 2$ cyclic, $|G_1| = m$, $|G_2| = n$, $(m, n) = 1$.

Then, $G_1 \times G_2$ is again cyclic

(3) G, finite abelian. If G is not cyclic, then there exists a prime p and a subgroup isomorphic to $C \times C$, where C is cyclic of order p.

pf: (1) $G \cong \mathbb{Z}/n\mathbb{Z}$.

$n = d \cdot k$

check: $k\mathbb{Z}/n\mathbb{Z} \leq \mathbb{Z}/n\mathbb{Z}$ has d elts.

on the other hand, <u>claim</u>: that any subgp in $\mathbb{Z}/n\mathbb{Z}$ is of form $k'\mathbb{Z}/n\mathbb{Z}$, $k' | n$.

pf of claim:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}/n\mathbb{Z} \\ & & \vee\!| \\ & & H \end{array}$$

$\pi^{-1}(H) \leq \mathbb{Z}$. The above argument shows that $\pi^{-1}(H) = k'\mathbb{Z}$, $k' \in \mathbb{N}$, and $k'\mathbb{Z} \supseteq n\mathbb{Z} \Rightarrow k' | n$

Thus $H = \pi(\pi^{-1}H) = \pi(k'\mathbb{Z}) = \frac{k'\mathbb{Z}}{n\mathbb{Z}}$. $k'|n$.

#

Thus, $\frac{k\mathbb{Z}}{n\mathbb{Z}}$ is the unique subgroup of ~~order~~ elts d, and it is clearly cyclic.

(2) $G_1 \cong \mathbb{Z}/m\mathbb{Z}$, $G_2 \cong \mathbb{Z}/n\mathbb{Z}$. $(m, n) = 1$

claim: $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/mn\mathbb{Z}$

pf of claim:

Consider $\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$k \bmod mn \longmapsto (k \bmod m,\ k \bmod n)$

ϕ is well-defined, Since

$k \equiv k' \bmod mn \Rightarrow k \equiv k' \bmod m,\ k \equiv k' \bmod n$

ϕ is clearly a group homomorphism.

$\ker(\phi) = \{ k \bmod mn \mid \underbrace{k \bmod m = 0}_{k=mr},\ \underbrace{k \bmod n = 0}_{k=nr'} \}$

$= \{ k \bmod mn \mid k = m \cdot n\, r'' \}$

$= \{ \bar{0} \}.$

i.e. ϕ is injective.

Note that $|\mathbb{Z}/mn\mathbb{Z}| = m \cdot n$, and $|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = m \cdot n$

$\Rightarrow \phi$ is an isomorphism.

#

(3) Take any $x \in G$, ~~G~~ non-cyclic $\Rightarrow \langle x \rangle \subsetneq G$.

We can assume $x^{\#} e$

(3) proof (I). By classification of finite abelian groups.

Theorem: G finite abelian. Then there is a uniquely determined set $\{p_1^{r_1}, p_2^{r_2}, \ldots, p_s^{r_s}\}$, where $\{p_1, \ldots, p_s\}$ prime numbers which may be equal, and $r_i \geq 1$, such that

$$G \cong \mathbb{Z}/p_1^{r_1} \times \cdots \times \mathbb{Z}/p_s^{r_s}.$$

Note: If $p_i \neq p_j$, $\forall i \neq j$, then G is cyclic by (2).

Thus, G is non-cyclic $\Rightarrow$ there are $i \neq j$, such that $p_i = p_j$.

Set $p = p_i = p_j$. Then $\mathbb{Z}/p \times \mathbb{Z}/p \leq \mathbb{Z}/p^{r_i} \times \mathbb{Z}/p^{r_j} \leq G$, as claimed.

Proof (II). $|G| = n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$, $\quad p_i \neq p_j$, $i \neq j$

Take any $x_1 \in G$ ($e \neq$), ~~such that~~ G non-cyclic $\Rightarrow \langle x_1 \rangle \lneq G$.

$\operatorname{ord}(x_1) = m \mid n$. assume $p_1 \mid m$.

Then replace x_1 by some power of x_1, we can assume that $m = p_1^{r_1'}$.

We can even assume, the following property

$$r_1' = \max\{ r \mid \mathrm{ord}(x) = p_1^r,\ x \in G \}. \qquad (*)$$

Now. Since $\langle x_1 \rangle \neq G$, we can take

$x_2 \notin \langle x_1 \rangle$.

Consider ~~$\langle x_1 \rangle \cap \langle x_2 \rangle$~~. $\mathrm{ord}(x_2)$

Case (i) $\exists\, q \neq p_1$, prime, $q \mid \mathrm{ord}(x_2)$

Say $q = p_2$. Then replace x_2 by some x_2-power,

we can assume $\mathrm{ord}(x_2) = p_2^{r_2'}$; and we can assume.

r_2' is maximal ~~among all p_2-power~~ in the sense of $(*)$.

Then $\langle x_1 \rangle \cap \langle x_2 \rangle = \{e\}$, and $\langle x_1 \rangle \times \langle x_2 \rangle \leq G$

cyclic subgp with ~~order~~ larger order.

Case (ii) $\mathrm{ord}(x_2) = p_1^{r'}$.

Then consider $\langle x_1 \rangle \cap \langle x_2 \rangle = \langle x \rangle$, and

$$\langle x \rangle \to \langle x_1 \rangle \times \langle x_2 \rangle \longrightarrow G$$

Claim: G contains a subgp, which is isomorphic to $\mathbb{Z}/p_1 \times \mathbb{Z}/p_1$.

It suffices to show the following Lemma

Lemma: $\mathbb{Z}/p^c\mathbb{Z} \overset{i_1}{\leq} \mathbb{Z}/p^a\mathbb{Z}$, $\mathbb{Z}/p^c\mathbb{Z} \overset{i_2}{\leq} \mathbb{Z}/p^b\mathbb{Z}$. Assume $a \leq b$.

Define
$$\mathbb{Z}/p^c\mathbb{Z} \xrightarrow{\ i\ } \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}$$
$$x \longmapsto (i_1(x),\ i_2(x))$$

then
$$\frac{\mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}}{i(\mathbb{Z}/p^c\mathbb{Z})} \cong \mathbb{Z}/p^{a-c}\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}$$

pf:

The proof of Lemma is left as an exercise. #

clearly; Lemma $\Rightarrow$ claim.

Conclusion: either we have already shown there exists a subgp ~~of~~ which is isomorphic to ~~type~~ $\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_1\mathbb{Z}$, or we find a subgp $\langle x_2 \rangle$ with the property:

$$\operatorname{ord}(x_2) = p_2^{r_2'}, \quad \text{where } r_2' = \max\{ r \mid \operatorname{ord}(x) = p_2^{r},\ x \in G \}.$$

~~That~~ Note that $\langle x_1 \rangle \times \langle x_2 \rangle \cong \mathbb{Z}/p_1^{r_1'} p_2^{r_2'}\mathbb{Z}$ which is cyclic.

Therefore, we can continue the above argument, until we ~~have~~ find a subgroup which is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for some prime p.

#

Proof (III). (I learnt this proof from my student):

Write $|G| = p_1^{r_1} \cdots p_s^{r_s}$

step 1: $\forall \overset{p_i}{p} \in \{p_1, \dots, p_s\}$.

There exists an element $x \in G$ with $\mathrm{ord}(x) = p_i$

pf: take an arbitrary $\underset{\ne}{\overset{e}{}} x \in G$,

Case (i). $p_i \mid \mathrm{ord}(x)$

Then, $\exists$ an elt of ord p_i in $\langle x \rangle \le \langle G \rangle$.

We're done.

Case (ii), $p_i \nmid \mathrm{ord}(x)$

Consider $\cancel{G} \xrightarrow{\pi} G/\langle x \rangle$.

Do induction on $|G|$. Then we can assume, there exists an elt $\bar{y}$ of order p_i in $G/\langle x \rangle$.

Take an $y \in G$, such that $\pi(y) = \bar{y}$

Consider the canonical map

$$\langle y\rangle \xrightarrow{\pi} \langle \bar{y}\rangle$$

As $|\langle \bar{y}\rangle| = p_i$, it follows that

$p_i \mid \langle y\rangle$, and therefore, there exists an order p_i elt in $\langle y\rangle \leq G$. We're done.

#

Step 2: $\forall \overset{p_i}{\overset{\shortparallel}{p}} \in \{p_1, \ldots, p_s\}$.

If there exists NO subgp isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ in G, then there must exist an elt $x \in G$ with $\mathrm{ord}(x) = p_i^{r_i}$,

pf: By step (1), take $x \in G$, with $\mathrm{ord}(x) = p_i$.
If $r_i = 1$, there is nothing to prove. Assume then $r_i \geq 2$.
Consider $G \xrightarrow{\pi} G/\langle x\rangle$

Note $|G/\langle x\rangle| = p_1^{r_1} \cdots p_i^{r_i - 1} \cdots p_s^{r_s}$

$r_i - 1 \geq 1$. $\Rightarrow \exists\ \bar{y} \in G/\langle x\rangle$, with $\mathrm{ord}(\bar{y}) = p_i$.

Take $y \in G$, with $\pi(y) = \bar{y}$. $\Rightarrow y^{p_i} \in \langle x\rangle$

Case (i) $y^{p_i} = e$, i.e. $\langle y\rangle \cong \mathbb{Z}/p_i\mathbb{Z}$.

But $\langle x\rangle \cap \langle y\rangle \leq \langle y\rangle$, $\overset{|\langle y\rangle| = p_i}{\Rightarrow}$ $\langle x\rangle \cap \langle y\rangle = \{e\}$ or $\langle x\rangle = \langle y\rangle$

Clearly $y \notin \langle x \rangle \Rightarrow \langle x \rangle \cap \langle y \rangle = \{e\}$

Thus
$$\langle x \rangle \times \langle y \rangle \xrightarrow{\phi} G$$
$$(x^i, y^j) \longmapsto x^i y^j$$

The natural morphism ϕ is injective.

Therefore G contains a subgroup isomorphic $\mathbb{Z}/p_i\mathbb{Z} \times \mathbb{Z}/p_i\mathbb{Z}$. Contradiction!

Case (ii) $y^{p_i} \neq e$ i.e. $\operatorname{ord}(y) = p_i^2$. (note $x = y^{p_i}$ in this case).

In this case, we can continue the above argument by considering

$$G \to G/\langle y \rangle. \quad \cancel{(\text{note } \langle x \rangle \subseteq \langle y \rangle)}$$

However, there is one case which requires the Lemma in ~~the~~ the second method, namely, $\exists\ z \in G$, s.t

$\operatorname{ord}(z) = p_i^2$, $z^{p_i} \in \langle y \rangle$. Then $\langle z \rangle \cap \langle y \rangle \cong \mathbb{Z}/p_i\mathbb{Z}$

This case is left to the students, to get a contradiction.

Step 3. By step 2, if $\forall i$, there is no $\mathbb{Z}/p_i\mathbb{Z} \times \mathbb{Z}/p_i\mathbb{Z}$ subgp in G,

we get $x_i \in G$, s.t $\operatorname{ord}(x_i) = p_i^{r_i}$, $1 \le i \le s$.

Thus
$$\langle x_1 \rangle \times \cdots \times \langle x_s \rangle \xrightarrow{\phi} G$$
$$(x_1^{i_1}, \ldots, x_s^{i_s}) \longmapsto x_1^{i_1} \cdots x_s^{i_s}$$
must be an isomorphism, which is impossible, because LHS is cyclic.

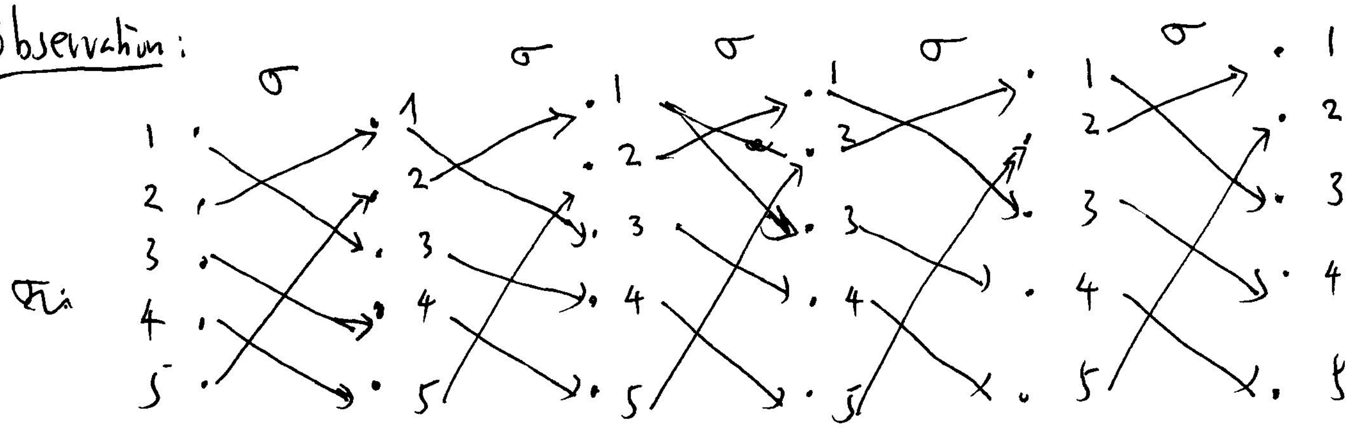
part II: symmetric group

Def (cycle)

$[i_1, i_2, \dots, i_r] \in S_n$ means

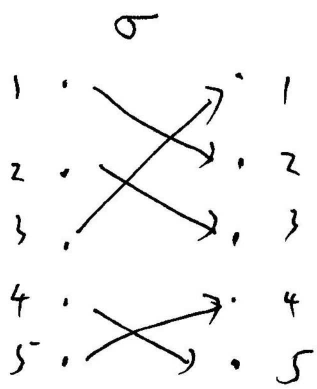
$$i_1 \to i_2 \to i_3 \to \cdots \to i_r \to i_1$$

Observation:



$$1 \to 3 \to 4 \to 5 \to 2 \to 1$$

$\sigma = [1, 3, 4, 5, 2]$



$1 \to 2 \to 3 \to 1$

$4 \to 5 \to 4$

$\sigma = [1\,2\,3] \cdot [4\,5]$

Prop: $\forall \sigma \in S_n$

σ is the product of disjoint cycles.

Here, we say two cycles $\sigma_1 = [i_1, \ldots, i_r]$ disjoint,
$\sigma_2 = [j_1, \ldots, j_s]$

if $\{i_1, \ldots, i_r\} \cap \{j_1, \ldots, j_s\} = \phi$.

pf: obvious.

#

Note: $[i_1, \ldots, i_n] = \underbrace{[i_1 i_n] \cdots [i_1 i_3][i_1 i_2]}_{(n-1) \text{ transposition}}$

Conclusion: Any permutation $\sigma \in S_n$ is written into product of transpositions.

~~Proposition~~ and Definition:

Let $\sigma = \prod_{k=1} \cancel{(i_k, j_k)}\ (i_1, j_1) \cdots (i_r, j_r)$

$= (i_1', j_1') \cdots (i_s', j_s')$.

Then $s \equiv r \mod 2$.

If ~~s~~ even number, then we say σ is even permutation; otherwise σ is odd permutation.

proof: postponed.

#

Def: $A_n \leq S_n$ is the subgp of S_n consisting of even permutations, called the alternating group.

Note: $S_n = A_n \amalg A_n (ij)$.

Thus $A_n \triangleleft S_n$, $\Leftarrow [S_n : A_n] = 2$

Exercise: check the def. of alternating group coincides with the one given before, namely:

$$A_n = \mathrm{Ker}(\phi : S_n \longrightarrow \{\pm 1\})$$
$$\sigma \longmapsto \det(e_{\sigma(1)} \cdots e_{\sigma(n)})$$

Theorem: A_n is a simple group, $n \geq 5$.

Corollary: S_n is non-solvable, if $n \geq 5$.

Key: 3-cycles!

Observation:

$\tau \in S_n$, $\sigma = [i_1, \dots i_r][j_1 \dots j_s] \cdots [k_1, \dots, k_t]$

$$\tau \sigma \tau^{-1} = [\tau(i_1), \dots, \tau(i_r)][\tau(j_1) \dots \tau(j_s)] \cdots [\tau(k_1), \dots, \tau(k_t)]$$

pf: $\sigma_1 \triangleq [i_1, \dots i_r]$, $\sigma_2 \triangleq [j_1, \dots, j_s]$, $\dots$, $\sigma_n = [k_1, \dots, k_t]$

Then $\tau \sigma \tau^{-1} = \tau(\sigma_1 \cdots \sigma_n)\tau^{-1}$

$$= (\tau \sigma_1 \tau^{-1})(\tau \sigma_2 \tau^{-1}) \cdots (\tau \sigma_n \tau^{-1}).$$

Thus, it suffices to verify, e.g.

$$\tau [i_1, \dots, i_r] \tau^{-1} = [\tau(i_1), \dots, \tau(i_r)].$$

Indeed: for $j \notin \{i_1, \dots, i_r\}$,

$$(\tau \cdot [i_1, \dots i_r])(j) = \tau(j)$$

$$([\tau(i_1), \dots, \tau(i_r)]\,\tau)(j) = [\tau(i_1), \dots \tau(i_r)](\tau(j)) = \tau(j).$$

for $j = i_\ell$, $1 \leq \ell \leq r$,

$$(\tau [i_1, \dots i_r])(i_\ell) = \tau(i_{\ell+1 \bmod r})$$

$$([\tau(i_1), \dots, \tau(i_r)] \cdot \tau)(i_\ell) = \tau(i_{\ell+1 \bmod r})$$

Thus: $\tau [i_1, \dots i_r] = [\tau(i_1), \dots, \tau(i_r)] \cdot \tau$

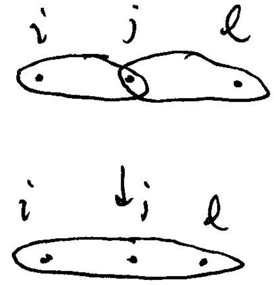
#

Step 1: A_n is generated by 3-cycles.

pf: Consider $[ij][kl]$:

Case (i) $\{ij\} \cap \{kl\} \neq \phi$

then $[ij][kl] = \begin{cases} id \\ \text{a 3-cycle} \end{cases}$

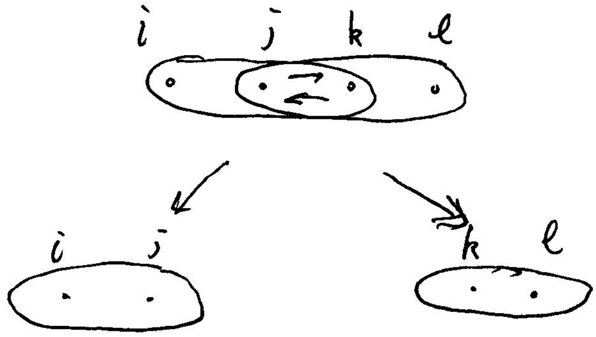


In fact: $[ij][jl] = [jli]$

$l \neq i$

Case (ii) $\{ij\} \cap \{kl\} = \phi$.

$$[ij][kl] = [ij\underline{k}] \cdot [\underline{j}kl]$$



#

Step 2: $n \geq 5$, all 3-cycles are conjugate in A_n

pf: Given $[ijk]$, $[i', j', k'] \in A_n$,

$\gamma [ijk] \gamma^{-1} = [i', j', k']$, for some $\gamma \in S_n$, s.t

$\gamma(i) = i'$, $\gamma(j) = j'$, $\gamma(k) = k'$.

Case (i) $\gamma \in A_n$,

we're done

Case (ii), $\gamma \notin A_n$.

Then $n \geq 5$, $\Rightarrow$ $\exists \{r,s\} \cap \{i,j,k\} = \phi$.

Then replace γ by $\gamma[rs] \in A_n$, and

$\gamma[rs][ijk][rs]\gamma^{-1}$

$= \gamma \underbrace{[rs]\cdot[rs]}_{= e} \cdot [ijk]\gamma^{-1}$

$= \gamma [ijk] \gamma^{-1} = [i',j',k']$ #

Step 3. $\forall n \geq 5$, $\forall N \lhd A_n$, There must a 3-cycle in N.

Take $\sigma \in N$ with the maximal fixed ~~pts.~~ numbers.
number of

i.e. $\forall \tau \in S_n$ define $F_\tau \triangleq \{ i \in \{1, \ldots, n\} \mid \tau(i) = i \} \subseteq \{1, \ldots, n\}$.

Then $|F_\sigma| \geq |F_\tau|$, $\forall \tau \in N$.

Claim: $|F_\sigma| = n-3$

Note : $|F_\sigma| = n-3 \Leftrightarrow \sigma$ is a 3-cycle.

write

$$\sigma = [a_1, \dots a_{i_1}][b_1 \dots b_{i_2}] \cdots [\cdot\ \cdot]$$

into product of disjoint cycles. See

We assume $[a_1, \dots a_{i_1}]$ is the longest cycle in the product.

Case (1). $|F_\sigma| = n-4$.

i.e σ moves 4 numbers.

Certainly, we can assume σ moves $\{1, 2, 3, 4\}$.

Since σ is even, it follows that

$\sigma \overset{\text{Conjugate}}{\sim} [12][34]$. We assume $\sigma = [12][34]$

Consider $\sigma' = [345]\big[[12][34]\big][345]^{-1} \in N$

$$= [12][45]$$

Then $\sigma \cdot \sigma' = [34][45] = [345] \in N$

Case (2) $|F_\sigma| \leq n-5$

Case (2.1) σ Contains a cycle of length ≥ 4.

i.e. $i_1 \geq 4$.

Take $\beta = [a_2\, a_3\, a_4] \in A_n$

Then $\sigma' = \beta \cdot \sigma \cdot \sigma^{-1}$

$$= [a_1\, a_3\, a_4\, a_2 \cdots a_{i_1}][b_1, \cdots b_{i_2}] \cdots [\quad] \in N$$

Note: $|F_{\sigma' \cdot \sigma^{-1}}| = n-3$. (The moving numbers of $\sigma' \cdot \sigma^{-1}$ are a_1, a_2, a_4).

Case (2.2) σ contains a cycle of length $= 3$, which is the largest length. i.e. $i_1 = 3$.

Write $\sigma = [a_1\, a_2\, a_3][b_1\, b_2 \cdots] \cdot [\cdots]$.

Note σ moves at least 5 numbers $\Rightarrow$ σ is not a 3-cycle

σ even $\Rightarrow$ σ moves at least 6 numbers

Thus take $\beta = [a_2\, a_3\, b_1] \in A_n$

~~$\sigma = [a_1\, a_2\, a_3][b_1\, b_2\, b_3] \cdots [\quad]$~~

$$\sigma' = \beta \cdot \sigma \cdot \beta^{-1} = [a_1\, a_3\, b_1][a_2\, b_2 \cdots] \cdots [\quad]$$

But $\sigma' \cdot \sigma^{-1}$ moves at most 5 numbers. Contradiction!

Case (2.3). $i_1 = 2$.

σ even $\Rightarrow$ σ moves at least 6 numbers.

$\sigma = [a_1 a_2][b_1 b_2] \cdots$

Take ~~agai~~ $\beta = [a_2\, b_1 b_2] \in A_n$.

$$\sigma' = \beta \cdot \sigma \cdot \beta^{-1} = [a_1 b_1][b_2 a_2] \cdots$$

Then $\sigma \cdot \sigma'^{-1}$ moves at ~~mo~~ 4 numbers. Contradiction!

#

Lecture 5. Group action on a set.

G = Group, X = set

A G-action on X is a map

$$G \times X \xrightarrow{\Phi} X \quad \text{satisfying}$$
$$(g, x) \longmapsto \Phi(g, x)$$

(i) $\Phi(g_1 \cdot g_2, x) = \Phi(g_1, \Phi(g_2, x))$, $\forall g_1, g_2 \in G$, $\forall x \in X$

(ii) $\Phi(e, x) = x$, $\forall x \in X$.

If we write $\Phi(g, x)$ ~~by~~ $g \cdot x$, then

(i) formally looks like the ~~comp~~ associativity:

$$(g_1 \cdot g_2) x = g_1 (g_2 \cdot x)$$

(ii) formally looks like $e \cdot x = x$

Prop: A G-action on X is equivalent to a homomorphism $G \longrightarrow Perm(X)$.

Pf: for a G-action Φ on X, define

$$G \longrightarrow Perm(X)$$
$$g \longmapsto \Phi_g : x \longmapsto \Phi(g, x)$$

Note: $\Phi_g : X \to X$ is a bijection, because

$$\Phi_{g^{-1}} \circ \Phi_g = \Phi_g \circ \Phi_{g^{-1}} = \Phi_e = Id_X.$$

Easy to check the above map is a group homo.

Conversely, for given a morphism

$$\phi : G \longrightarrow Perm(X).$$

define $G \times X \xrightarrow{\Phi} X$ by

$$(g, x) \longmapsto \phi_g(x)$$

Easy to check Φ is a G-action.

#

Important Examples:

(1) Conjugation.

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ \downarrow & & \downarrow \\ (g, x) & \longmapsto & gxg^{-1} \end{array}$$

Notation: $C_g(x) = gxg^{-1}$

Check: it is a G-action.

Note: if we define $g \cdot x$ by $g^{-1}xg$, then it is NOT a group action.

It induce other conjugation actions:

(i) X = set of subsets of G, then

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ \downarrow & & \downarrow \\ (g, S) & \longmapsto & gSg^{-1} \end{array}$$

(ii) X = set of subgps of G, then

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ \downarrow & & \downarrow \\ (g, H) & \longmapsto & gHg^{-1} \end{array}$$

Note $g \cdot H = H \iff H$ is normal

(2) Translation.

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

Notation: $T_g(x) = g \cdot x$

Easy to check it is a G-action.

Note: $(g, x) \mapsto x \cdot g$ is NOT a G-action. But $(g, x) \mapsto x \cdot g^{-1}$ is a G-action.

A difference of C_g and T_g :

Note the conjugation define a homo

$$G \xrightarrow{\phi} \mathrm{Aut}(G), \quad \text{with } \mathrm{Ker}(\phi) = Z(G).$$

$\mathrm{im}(\phi) \leq \mathrm{Aut}(G)$ called the inner automorphism.

But the translation is NOT a group automorphism, in general.

It is just a permutation.

(3). Examples from linear Algebra.

V/K : Vector space over K.

$G = GL(V)$ = group of linear automorphisms of V.

Then $G \times V \longrightarrow V$ is naturally a G-action on V.

$(g, v) \longmapsto g.v$

Definition (G-sets and G-maps).

A set is called a G-set if we specify a G-action on X

(note the trivial action of G on X ~~always~~ exists !).

A map $f : X_1 \to X_2$ between G-sets is said to be a G-maps

if $f(gx) = gf(x)$, $\forall g \in G$, $x \in X_1$.