Tutorial : will email

4x this semester

Final 75%
assignments 25%

Please take these seriously

- OK to do as a group (single write up alone)

- Declare if you work as a group (please!)

- Presentation matters (spend time on this 10%-20%)

Please scan your work to be legible
will not otherwise

<u>Reading</u> (Recommended)

- Hungerford "Algebra", (Chapters 1+2)
- Dummit and Foote "Algebra"
- Lecture notes (loosely inspiring this module)
  by Stefan Bergloft-Sails

Will study

- Group actions
- Group series (nested sequences of subgroups)
- solvable (nil potent groups)
- free groups (group presentation)
- Krull-Schmidt theorems
- Simple groups (A_n for $n \geq 5$)

Definition

A group is a set G with a binary operation $G \times G \to G$, written as $(g, h) \mapsto gh$, satisfying

(1) there exists e, the identity element, such that

$$eg = ge = g \quad \forall \in G g$$

(e_G if multiple groups involved)

(2) for all $g \in G$ there exists g^{-1} such that $gg^{-1} = g^{-1}g = e$

(3) for all $g, h, f \in G$

$$(gh)f = g(hf) \qquad \text{"assosiative"}$$

Example

$(n \in \mathbb{N})$

- $S_n = \{ f : \{1, \dots, n\} \to \{1, \dots, n\} \mid f \text{ bijective} \}$,

the group of permutation, i.e. symmetric group. The group operation is the composition of functions

- $C_m = \{0, \dots, m-1\}$

with operation $nk \mapsto n+k \pmod m$

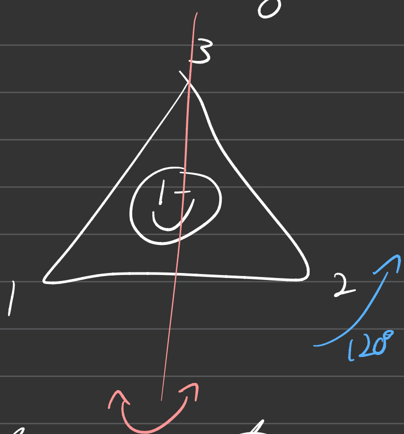
This group is Abelian, so $(m \in \mathbb{N})$

$(n,k) = (k,n) \quad \forall\ k,n \in C_m$

For Abelian groups, the operation is typically denoted "+", $n+k = (n+k) \bmod m$

Example

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under addition
- Symmetry groups (consider the symmetry over a regular triangle)

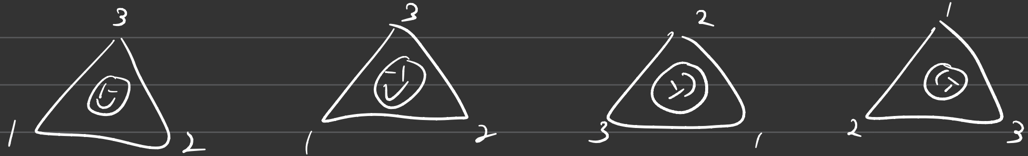


Let τ be the 120° rotation counter clockwise

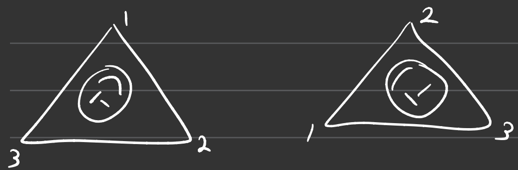
Let r be the reflection along the indicated axis

The symmetry group is written D_3 (Dihedral group) and consists of 6 elements composition left to right

id $\qquad r \qquad \tau \qquad \tau^2$



$r\tau \qquad r\tau^2$



Definition

A subgroup $H \le G$ is a subset st
$h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$

Example

$\{id, r\} \le D_3$ as $r^{-1} = r$

$\{id, \tau, \tau\} \le D_3$ $(\tau^2 = \tau^{-1})$

Definition

A subgroup $H \leq G$ is normal if

$gHg^{-1} = H$ for all $g \in G$

Denoted $H \trianglelefteq G$

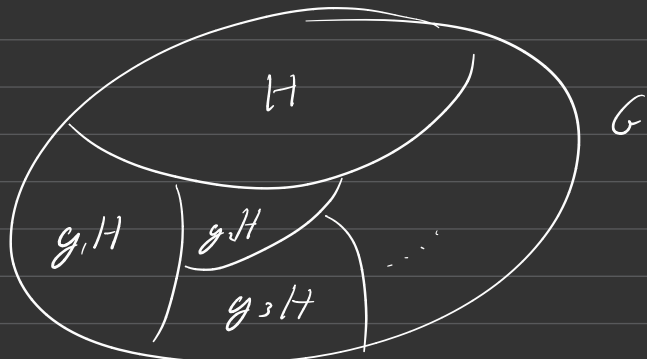
Definition

Let $H \leq G$. Consider the relations

$g \sim_L g' \iff gH = g'H$

$g \sim_R g' \iff Hg = Hg'$

This is an equivalence relation and the classes are called left ($\sim_L$), right ($\sim_R$) cosets.



If $H \trianglelefteq G$ then left and right cosets coincide, and the set of cosets form a group via the operation

$$(gH)(g'H) \longmapsto (gg'H),$$

called the quotient group, or the factor group

Definition

The order of a group G, $|G|$, is the number of elements

Fact:

(1) if $H \leq G$, $|H| \mid |G|$

(2) $|G/H| = \frac{|G|}{|H|}$

Definition

A a group homomorphism ("hom") is a map between groups G, G' st

$$f(gg') = f(g)f(g')$$

Definition

f is called a group monomorphism if f is injective ;

f is called a group epimorphism if f is surjective

f is called a group isomorphism if f is bijective

If $f\ G \to G'$ is a group isomorphism then G and G' are said to be isomorphism denoted $G \simeq G'$ ("relabelling")

Definition

$Ker(f) = \{g \in G \mid f(g) = e_H\}$

is the kernel of f

$Im(f) = \{f(g) \mid g \in G\}$

is the image of f

Isomorphism Theorems

Let $f: G \to H$ be a hom

Fact

$Ker f \trianglelefteq G$

$Im f \leq H$

Theorem (1st Isomorphism Theorem)

Let $f: G \to H$ be a hom

$G/Ker f \cong Im f$

Theorem (2nd Isomorphism Theorem)

Let $N \trianglelefteq G$, $H \leq G$

Let $NH = \{nh \mid n \in N, h \in H\} \leq G$ $(N \trianglelefteq NH)$

$$NH/N \cong H/H \cap N \quad (\text{NB } N \cap H \leq H$$

Theorem (3rd Isomorphism Theorem)

Let $H \leq K$, $H, K \leq G$

$$(G/H)/(K/H) \cong G/K$$

You should know the correspondence between subgroups of G/H and subgroups of G containing H!

__Fact__

If $H \trianglelefteq G$ and $H \leq K$ then $H \trianglelefteq K$

Direct Product

Let G, H be groups. Define the direct product to be the group on the set $G \times H$ with operation

$$(g,h)(g',h') = (gg', hh')$$

Example

$$C_2 \times C_3 = \{0,1\} \times \{0,1,2\} \simeq C_6$$

via $(1,1) \longmapsto (1)$

Fact

Identify G with $G \times \{e_H\}$ and H with $\{e_G\} \times H$

Then $G \trianglelefteq G \times H$, $H \trianglelefteq G \times H$

$G \cap H = \{e_{G \times H}\}$, $GH = G \times H$

$\{xy \mid x \in G \times \{e_H\},\ y \in \{e_G\} \times H\}$

$= \{(g, e_H)(e_G, h)\} = (g, h)$

Whenever G is a group admitting subgroups N_1, N_2

st $N_1, N_2 \trianglelefteq G$, $N_1 \cap N_2 = \{e\}$

$N_1 N_2 = G$ then

$G \simeq N_1 \times N_2$

The isomorphism is given by

$$G = N_1 N_2 \longrightarrow N_1 \times N_2$$
$$(n_1 n_2) \longmapsto (n_1, n_2)$$

Fact

Let G be an Abelian group,

$|G| < \infty$. Then

$$G \simeq C_{p_1^{e_1}} \times C_{p_2^{e_2}} \times \dots \times C_{p_n^{e_n}}$$

for (not nec distinct) primes p_i and $e_i \geq 1$

Example

- $|G| = 2$, $p_1 = 2$, $e_1 = 1$

$\Rightarrow G \simeq C_2$

- $G = 28 = 2^2 \times 7^1$

$C_2 \times C_2 = K_4 = \{e, (12)(34), (13)(24), (14)(23)\} \leq S_4$

$C_{2^2} = C_4$

$\Rightarrow$ (2 options)

(1) $C_2 \times C_2 \times C_7 = K_4 \times C_7 = C_2 \times C_{14}$

(2) $C_4 \times C_7 \cong C_{28}$

Group Actions

Definition

A group action of a group G on a set X is a function

$G \times X \to X$, usually written

$(g, x) = gx$ st (1) $ex = x$

(2) $g(hx) = (gh)x$

Note

We can think of the action of $g \in G$ on X as a function
$g: X \to X$

via $x \mapsto gx$

This function $g: X \to X$ is bijective

Proof

$$(g^{-1} \circ g)(x) = g^{-1}(g(x))$$
$$= (g^{-1}g)(x)$$
$$= e(x)$$
$$= x$$

$$(g \circ g^{-1})(x) = x \qquad \square$$

Thus a group action is a group homomorphism

$$\rho : G \to \mathrm{Sym}(X) = \{ f : X \to X \mid f \text{ bijective} \}$$

is $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$

Example

(1) S_n acting on $\{1, \dots, n\}$

$\rho : S_n \to \mathrm{Sym}(\{1, \dots, n\}) = S_n$

is the identity!

$$\underbrace{(24)(471)}_{g \in S_n}\underbrace{(1)}_{\in \{1, \dots, n\}} = 2$$

(2) G acts on itself (so $X = G$) by left multiplication

$$\rho : G \to \mathrm{Sym}(G)$$
$$g \mapsto \underbrace{(h \mapsto gh)}_{\in \mathrm{Sym}(G)}$$

Q. $\mathrm{Ker}(\rho) = \{g \in G \mid \rho(g) = \mathrm{id}\}$

so which g satisfy that $gh = h$ $\forall\, h \in G$

A. $g = e$! $gh = h \Rightarrow g = e$ ($\forall\, h$)

$\ker(\rho) = \{e\}$

Corollary

$$G/\ker(\rho) \cong \operatorname{Im}(\rho)$$

$\quad \cong$

$\quad G$

$\operatorname{Im}(\rho) \leq \operatorname{Sym}(G) \cong S_n$ for some n!

So every group is isomorphic to a subgroup of S_n

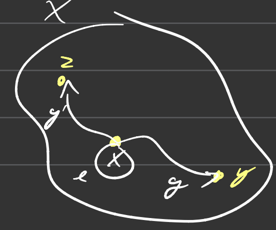
Group Actions

Let G act on a set X, we define the orbit of $x \in X$

$$G \longrightarrow \operatorname{Sym}(X)$$

Definition

$O_x = \{x, y, z\}$



The orbit of $x \in X$ is

$$O_x = \{gx \mid g \in G\}$$

The stabiliser of $x \in X$ is

$G_x = \{ g \in G \mid gx = x \}$

Fact

(G acts on X)

Consider the following relation on X

$x \sim y \iff \exists g \in G$ st $gx = y$

Then $\sim$ is an equivalence relation on X the equivalence classes are the orbits

Proof: Excercise

Example

S_3 acting S_3 by conjugation

First

Let G act on G by conjugation

$(g, x) = \underbrace{gx}_{\text{The element } g \in G \text{ acting on } x \in X (= G)} = g x g^{-1}$

Fact

This is a group action

$(ex = exe^{-1} = x)$

$$g(g'x) = g(g'xg'^{-1}) = gg'xg'^{-1}g^{-1} = (gg')x$$

Let's compute an orbit (if G acts on itself by conjugation, the orbits are the conjugacy classes) and stabilisers

$x = (132)$

$O_x = \{(123), (132)\}$

$exe^{-1} = x = (132)$

$S_3 = \{e, (132), (123), (12), (13), (23)\}$

$(23)x(23) = (231)$
$(12)x(12) = (123)$
$(13)x(13) = (123)$

$G_x = \{g \in S_n \mid gx = x\} = \{e, (123), (132)\}$

Proposition (Orbit stabiliser theorem)

$$|O_x| = [G : G_x] = \frac{|G|}{|G_x|} \Rightarrow |O_x| \cdot |G_x| = |G|$$

Example

S_n acting on S_n by conjugation

$|O_x| = 2$

$$\Rightarrow 2 = |O_x| = \frac{6}{3} = \frac{|G|}{|G_x|}$$

$|G_x| = 3$

$$= [G : G_x]$$

Fact

The stabiliser G_x (for any $x \in X$) is a subgroup

Proof

Define $G/G_x \xrightarrow{f} O_x$ by

$$gG_x \overset{f}{\longmapsto} gx$$

$G/G_x = \{eG_x, g_1 G_x, \ldots, g_n G_x\}$

(1) Well defined?

$$gG_x = g'G_x \iff g^{-1}g' \in G_x$$
$$\iff g^{-1}(g')x = x$$
$$\iff g(g^{-1}g')x = gx$$
$$\iff g'x = gx$$

$$gG_x \longrightarrow gx$$

<u>claim</u> surjective want some gG_x st

$f(gG_x) = g'x \quad \forall \; g'x$

$\quad\;\; \| $

$\quad\; gx$

Let $g' = g$

<u>claim</u> injective

$g'x = gx \Rightarrow gG_x = g'G_x$

<u>A</u> yes, see well defined

Corollary

$X = \bigcup X_i$ where X_i form a partition of X

$|X| = \sum |X_i|$

Recall that the equivalence classes form a partition

$X = \bigcup O_x$

$|X| = \sum |O_x|$

orbits disjoint

So assume that $O_{x_1}, O_{x_2}, \ldots, O_{x_n}$ are the disjoint orbits

Then $|X| = \sum_{i=1}^{n} |O_{x_i}| = \sum_{i=1}^{n} [G : G_{x_i}]$

$$= \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}$$

This is called the class equation

Claim

Let G act on itself by conjugation. Then this gives a homomorphism

$\rho : G \longrightarrow \mathrm{Aut}(G) = \{ f : G \to G \mid f \text{ is an isomorphism} \}$

is hom + bij

Need to show that

- $\rho(g)$ is hom
- $\rho(g)$ is bijective ✓ (Group action)

__For hom__

$\rho(g)(x_1 x_2) = g x_1 x_2 g^{-1}$

$= g x_1 g^{-1} g x_2 g^{-1}$

$= \rho(g)(x_1)\, \rho(g)(x_2)$ ✓

(1) Whats $\mathrm{Ker}(\rho)$?

$\mathrm{Ker}(\rho) = \{ g \in G \mid gx = x \ \forall x \}$

$= \{ g \in G \mid g x g^{-1} = x \ \forall x \in G \}$

$= \{ g \in G \mid gx = xg \ \forall x \in G \}$

$= C(G) =$ centre of G

The map

$$G \longrightarrow Aut(G)$$

$$g \longmapsto (x \mapsto gxg^{-1})$$

has kernel $C(G)$ and the image, ie the automorphisms in $Aut(G)$ given by $f(x) = gxg^{-1}$ for some $g \in G$, are the inner automorphisms, $Inn(G)$

$$Inn(G) \leq Aut(G)$$

Let G act on itself by conjugation

$\rho : G \to Aut(G)$ is a homomorphism

with kernel $C(G) = \{g \in G \mid gh = hg \quad \forall h \in G\}$

Let $H \leq G$, Let G act on G/H

Definition

$$\rho : G \longrightarrow \mathrm{Sym}(G/H)$$

$$g(xH) = (gx)H$$

$G/H = \{eH, x_1H,$

Fact $\ker(\rho) \leq H$

check $\ker(\rho) = \{g \in G \mid \rho(g) = id_{G/H} = (xH \mapsto xH)\}$

$\rho(g)(eH) = (geH) = eH$

$g \in \ker(\rho)$

$\iff gH = H \iff g \in H$ (as $H \leq G$) $\Rightarrow \ker(\rho) \leq H$

Excercise Find G, H st $\ker(\rho) = H$

Corollary

If $H \leq G$ st H does not contain any non-trivial subgroups normal in G, then $G \simeq$ subgroup of S_m, where $m = [G:H]$

<u>Q</u> Is the assumption in the statement equivalent to H does not contain any non-trivial normal subgroups

Example

(Stupid) any non-normal subgroup of G
$H \trianglelefteq H$ for all H!

Proof

$$\rho : G \longrightarrow Sym\left(G/H\right)$$

$Ker(\rho) \leq H$, but $Ker(\rho) \trianglelefteq G$

So if H is as stated, then $Ker(\rho) \leq H$ must be trivial

$$\Rightarrow G/Ker(\rho) \simeq Im(\rho) \Leftrightarrow G \simeq Im(\rho) \leq S_m$$

for $m = [G:H]$

Fact Any subgroup of index 2 is normal

Proposition

Let p be the smallest prime in $|G|$ and suppose $H \leq G$ such that $[G:H] = p$. Then H is normal

Proof

Let G act on G/H

$$\rho : G \to \mathrm{Sym}(G/H) = S_p$$

(1) $|S_p| = p!$

(2) $\left| G/\ker(\rho) \right| \;\Big|\; |G|$

(3) $G/\ker\rho \simeq \mathrm{Im}(\rho) \leq S_p$

$\Rightarrow \left| G/\ker\rho \right| = |\mathrm{Im}(\rho)| \;\Big|\; 1 \cdot 2 \cdot \ldots \cdot p$

Now note that the prime divisors of $|G|$ are p + other primes ~~strictly~~ greater than p!

Since $\left|G/\mathrm{Ker}(\rho)\right| \,\big|\, |G|$, the prime divisors

of $\left|G/\mathrm{Ker}(\rho)\right|$ have to be a subset

of p + primes $> p$

Since $\left|G/\mathrm{Ker}\,\rho\right| \,\big|\, 1 \cdot 2 \cdot \ldots \cdot p$

the largest prime divisor would be p.

$\Rightarrow$ The only possible divisors of

$\cancel{G/\mathrm{Ker}(\rho)}$ are 1 and p

$\Rightarrow \left|G/\mathrm{Ker}(\rho)\right| = p^e$ (an $e > 1$? No!

$|S_p| = p!$ $p^2 \nmid p!$

Computation

$$\mathrm{Ker}(\rho) \leq H \leq G \Rightarrow \left|G/\mathrm{Ker}(\rho)\right| = \frac{|G|}{|\mathrm{Ker}(\rho)|} = \overset{p}{\frac{|G|}{|H|}} \, \overset{=1}{\frac{|H|}{|\mathrm{Ker}(\rho)|}} = p$$

$\Rightarrow [H : Ker\, \rho] = 1$

$\Rightarrow H = Ker(\rho) \trianglelefteq G$

Sylow's Theorem

Definition

Let G act on X. Consider the elements $x \in X$ whose orbits just x itself. Define

$$X_0 = \{x \in X \mid |O_x| = \{x\}\}$$
$$= \{x \in X \mid |O_x| = 1\}$$
$$= \{x \in X \mid gx = x \ \forall g \in G\}$$

$$O_x = \{gx \mid g \in G\}$$

Fact

Let H be a group of order p^n for p a prime and let G act on a set X. Then $|X| \equiv |X_0| \mod p$

Proof

$$|X| = \Sigma |O_{x_i}| \left(= \Sigma [G : G_{x_i}]\right)$$

$$= \sum_{|O_x|=1} |O_{x_i}| + \sum_{|O_{x_i}|>1} |O_{x_i}|$$

$$= |X_0| + \sum_{[G:G_{x_i}]>1} [G:G_{x_i}]$$

As $[G:G_{x_i}] \mid p^r \Rightarrow [G:G_{x_i}] = p^e$ for $0 \le e \le r$

As $[G:G_{x_i}] > 1$

$[G:G_{x_i}] = p^e$ for $1 \le e \le r$

In particular, $p \mid [G:G_{x_i}]$!

$\Rightarrow |X| = |X_0| + \underbrace{\cdots}_{\text{divides } p}$

$\Rightarrow |X| = |X_0| \mod p$

Theorem

Suppose $p \mid G$ for some group G. Then there exists

$g \in G$ st $|g| = p$

Proof

Let $X = \{(g_1, \dots, g_p) \in G^{\times p} \mid \prod g_i = e\}$

$|X| = n^{p-1}$ (choose $g_1, \dots, g_{p-1}$ arbitrarily)

$$g_p = (g_1, \dots g_{p-1})^{-1}$$

in particular $p \mid n^{p-1}$

Let $\mathbb{Z}_p$ act on X

$[1](g_1, \dots, g_p) = (g_p, g_1 \dots g_{p-1})$

if $(g_1, \dots, g_p) \in X_0$

then $[1](g_1, g_2, \dots, g_p) = (g_1, \dots, g_p)$

$\Rightarrow g_1 = g_2 = \dots = g_p$

In particular, if $(g_1, \dots g) \in X \Rightarrow g^p = e_0$

Since $(e, \dots, e) \in X_0$ and $|X_0| \equiv |X| \bmod p$,

$|X_0| \geq p$ and $p \mid x \Rightarrow |X_0| \equiv 0 \bmod p$

There is an element $(g, \dots, g) \in X_0$
st $g \neq e \Rightarrow |g| > 1 \Rightarrow |g| = p$

Theorem (Cauchy)

If a prime p divides $|G|$ then there $g \in G$ st $|g| = p$

Definition

A p-group is a group such that every element has order p^n (for p a prime)

Corollary

A finite group G is a p-group if and only if $|G| = p^n$

Proof

($\Leftarrow$) If $|G| = p^n$ then $|g| = p^k$ for $k \leq n$

($\Rightarrow$) Assume that $|G| \neq p^n$, so there exists a prime q st $q \mid |G|$

$\Rightarrow$ there exists $g \in G$ st

$|G| = q \neq p^k$ for any k

so G is not a p-group

Examples

First p-groups are hard ∵ No classification no hope thereof

$\boxed{p=2}$ • $|G| = 2^1 \Rightarrow G = \mathbb{Z}_2$

• $|G| = 2^2$

<u>Abelian</u>

so $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, $G = \mathbb{Z}_4$

• $|G| = 2^3$

<u>Abelian</u>

$\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

<u>Non-Abelian</u>

D_4 = dihedral group

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

st $i^2 = j^2 = k^2 = (-1)^2 = 1$

$ijk = 1$

$\boxed{p=3}$

- $|G| = 3$

$$G = \mathbb{Z}_3$$

- $|G| = 3^2$

$$G = \mathbb{Z}_3 \times \mathbb{Z}_3 \ , \quad G = \mathbb{Z}_9$$

- $|G| = 3^3$

$$G = \mathbb{Z}_{27}, \quad G = \mathbb{Z}_3 \times \mathbb{Z}_9$$

$$G = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

<u>Non-Abelian</u>

$$UT(3,3) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \ a, b, c \in \mathbb{F}_3 \right\}$$

$\mathbb{F}_2 = \{0,1\}$ $\quad 1+1=0$

$\mathbb{F}_3 = \{0,1,2\}$ $\quad 1+1+1=0$ $\quad (2)(2)=1$ in $\mathbb{F}_3$

group operation, Matrix Mult

<u>Non-Abelian</u>

$$G = \mathbb{Z}_9 \rtimes_\varphi \mathbb{Z}_3 \quad (\text{later})$$

$$\varphi : \mathbb{Z}_3 \longrightarrow \mathrm{Aut}(\mathbb{Z}_9)$$

Recall

If a group G acts on a set X

$|X| \equiv |X_0| \mod p$, $X_0 = \{x \in X \mid gx = x \ \forall g \in G\}$

Applications

$C(G)$ is non trivial

Center of a p-group

Proof

Let G act on itself by conjugation

Then $X_0 = C(G)$ and $|X_0| \equiv |G| = 0 \mod p$

$\Rightarrow |X_0| = \cancel{0}, p, 2p,$

as $e \in C(G)$

$\Rightarrow |C(G)| \geq p$ is non-trivial

Corollary

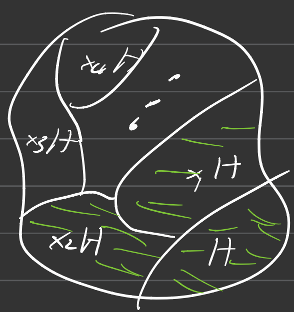
$$[N_G(H) : H] = [G : H] \bmod p,$$

normaliser

where H is a p-group and $H \leq G$,
$|G|$ not necessarily a p-group

Definition

Normaliser



$H \trianglelefteq H$

want largest N

st $H \trianglelefteq N$, $N \leq G$

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

~~Proof~~

Let H acts on $G/H = X$ by left multiplication. Then

$$X_0 = \{xH \mid hxH = xH \quad \forall h \in H\}$$

$\Rightarrow X_0 = \{xH \mid x \in N_G(H)\}$

$\Rightarrow X_0 = [N_G(H) : H] \equiv [G : H] \bmod p$

(Obvious Exercise)

If $x \in N_G(H)$, then $xh \in N_G(H)$ $\forall h \in H$

Definition

A p-subgroup is a subgroup which is a p-group

Definition

A Sylow p-subgroup P is a maximal p-subgroup, so if $P \leq H$ and H is a p-subgroup, then $P = H$

NB

If $|G| = p^k m$, $\gcd(p, m) = 1$, then

$H \leq G$ is a p-subgroup iff $|H| = p^l$
$l \leq k$

$H \leq G$ is a Sylow p-subgroup iff $|H| = p^k$

Fact

Let $H \leq G$ be a p-subgroup and let $p \mid [G:H]$

Then $N_G(H) \neq H$, so there exists $g \in G \setminus H$ st $gHg^{-1} = H$

$$[N_G(H):H] \equiv [G:H] \mod p$$

but $[G:H] \equiv 0 \mod p$

However

$$[H_G(H):H] \geq 1 \Rightarrow [N_G(H):H] \geq p$$

so in particular $H \neq N_G(H)$

Theorem (Sylow 1)

Let $|G| = p^k m$, $\gcd(p,m) = 1$. Then p-subgroups of order p^i for $i = 0, \dots, k$ exist and every such p-subgroup of order p^i is normal in a p-subgroup of order p^{i+1} (unless it is a Sylow)

Proof

By induction on i

$i = 0$ ✓

$i = 1$: By Cauchy's theorem, an element g of order p exists. Take $\langle g \rangle$

Suppose a p-subgroup of order p^i exists, say H. We will construct a p-subgroup p^{i+1} such that H is normal in it

Take $N_G(H)$. Recall $H \neq N_G(H)$

Issue: May not be of order p^{i+1}

Consider $N_G(H)/H$

<u>claim</u> $p \mid [N_G(H):H]$

Thus there exists an element

gH of order p

$\Rightarrow H' = \langle gH \rangle \leq N_G(H)/H$

By basic facts on quotient groups,

$H' = H_1/H$ $\quad H \trianglelefteq H_1 \leq N_G(H)$

$H_1 = H \cup gH \cup g^2H \cup \dots \cup g^{p-1}H$

$|X| = |X_0| \mod p$

Example

$6 = |S_4| = 2^3 \cdot 3$

$p = 2$

p-subgroup of order $p^0 = (id)$
$p^1 = 2^1$:

an element of order 2: (12)
Take the subgroup

$\langle (12) \rangle = \{(12), e\}$

For $2^2 = 4$, first find the normaliser of $\{e, (12)\} = H$

$N_{S_4}(H) = C_{S_4}(12) = \{id, (12), (34), (12)(34)\} = K_4$

Consider $N_{S_4}(H)/H = \{id\,H, (34)H\}$

Chose element of order 2 in $N_{S_4}(H)/H$
namely $(34)H$, $H' = \langle (34)H \rangle$

Here $H_1 = N_{S_4}(H)$

Given $H = \{id, (12), (34), (12)(34)\}$

(p subgroup of order 2^2)

want to build H_1 (p-subgroup of order 2^3)
st $H \trianglelefteq H_1$

• Take $N_{S_4}(H) = \{id, (12), (34), (12)(34),$

$(14)(23)\ (13)(24)$

$(1423)\ (1324)\}$

$\Rightarrow N_{S_4}(H) / H = \{H, (14)(23)H\}$

Pick element of order 2,

$(14)(23)H \Rightarrow H' = \langle (14)(23)H \rangle$

$\Rightarrow H_1 = N_{S_4}(H)$

Theorem (Sylow II)

Let H be a p-subgroup and P be any sylow p-subgroup of G. Then there exists $g \in G$ st

$$gHg^{-1} \leq P$$

Corollery

If H is sylow p-subgroup then

$$gHg^{-1} \leq P$$

and $|gHg^{-1}| = |P|$

$$\Rightarrow gHg^{-1} = P$$

and all sylow p-subgroups are conjugate!

Proof

Let H act on G/P

$$|X| = [G:P] = \frac{|G|}{|P|} = \frac{mp^k}{p^k} = m$$

$$X_0 = \{gP \mid hgP = gP \ \forall \ h \in H\}$$

$= \{ gP \mid g^{-1}hg \in P \quad \forall h \in H \}$

$= \{ gP \mid g^{-1}Hg \le P \}$

$\Rightarrow |X| \equiv |X_0| \bmod p$

and $p \nmid |X|$ (i.e. $|X| \not\equiv 0 \bmod p$

$\Rightarrow |X_0| \not\equiv 0 \bmod p$ i.e. $|X_0| \neq 0$

So pick any $g \in G$ st $gP \in X_0$

$\Rightarrow g^{-1}Hg \le P$ $\square$

Corollary

All Sylow p-subgroups are conjugates
i.e. if $X = \{ P \le G \mid P$ a Sylow p-subgroup$\}$
then
$X = \{ gPg^{-1} \}$ for any Sylow p-subgroup

So if $|X| = 1$

$\Rightarrow gPg^{-1} = P \quad \forall g \in G$ i.e. $P \trianglelefteq G$

Theorem (Sylow III)

Let n_p be the number of Sylow p-subgroups of G. Then

(1) $n_p \mid |G|$

(2) $n_p \equiv 1 \mod p$

Proof

(1) Let G act on the set of Sylow p-subgroups by conjugation.

Recall from last time: All Sylow p-subgroups are conjugate

Let P be a Sylow p-subgroup

$$|\underbrace{\{xPx^{-1} \mid x \in G\}}_{\text{orbit of } P \text{ under the action, } O_P}| = n_p$$

$\Rightarrow n_p = |O_P| = [G : G_P]$ (Orbit Stabiliser)

$G_P = \{x \in G \mid xPx^{-1} = P\} = N_G(P)$

$$\Rightarrow n_p = [G : N_G(P)] = \frac{|G|}{|N_G(P)|}$$

$\Rightarrow n_p \mid |G|$

(2) Consider the action of P on $G/N_G(P)$

(We will use $|X_0| \equiv |X| \bmod p$ as P is a p-group)

Note that $|X| = [G : N_G(P)] = n_p$

We need to compute X_0

$X_0 = \{ xN_G(P) \mid pxN_G(P) = xN_G(P) \ \forall p \in P \}$

$\Rightarrow X_0 = \{ xN_G(P) \mid x^{-1}Px \leq N_G(P) \}$

claim $X_0 = \{ N_G(P) \}$

so if $x^{-1}Px \leq N_G(P)$ then $x \in N_G(P)$

For this we will need

$P \trianglelefteq N_G(P)$

and all Sylow p-subgroups are conjugate to P

Consider $xPx^{-1} \leq N_G(P)$. Note that xPx^{-1} is also a Sylow p-subgroup!
(of G and the normalizer)

How many Sylow P subgroups does $N_G(P)$ have?

Since <u>all</u> Sylow p-subgroups (of $N_G(P)$) are conjugate to P, they are of form

$$\underbrace{xPx^{-1}}_{=P} \text{ for } x \in N_G(P)$$

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

$\boxed{\text{Fact: If a Sylow } p\text{-subgroup is normal in } G, \text{ it is the unique Sylow } p\text{-subgroup!}}$

Thus $|X_0| = |\{N_G(P)\}| = 1$,

so $n_p \equiv 1 \bmod p$. This proves (2)

Corollary

The normalisers of Sylow p-subgroups are self normalising i.e.

$$N_G(N_G(P)) = N_G(P)$$

Proof ~~Exercise~~

Applications of Sylow Theorems

(1) Groups of order p^2 for a prime p

<u>claim</u>

Groups of order p^2 are Abelian, so either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$

<u>Proof</u>

The groups $\mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_p$ have order p^2

So let $|G| = p^2$. Then G is a p-group. We proved $C(G) \neq \{e\}$. If

$|C(G)| = p^2$, then

$G = C(G)$ and $C(G)$ is abelian

Assume $|C(G)| = p$

$\Rightarrow$ classification gives $G = \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$

[$x \in C(G) \iff xg = gx$

As $C(G) \trianglelefteq G$, can consider

$\left| G/C(G) \right| = p$ so $G/C(G)$ is cyclic

Fact

If $G/C(G)$ is cyclic then G is Abelian
(NB: Then $G = C(G)$ and $G/C(G) = \{e\}$)

Sketch

Every $g = x^n z$ for $\langle xC(G)\rangle = G/C(G)$, $z \in C(G)$

$$(x^n z)(x^m z') = (x^m z')(x^n z)$$

as all three commute!

$\Rightarrow G$ is Abelian so $G = \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$

(2) Groups of order pq for primes $p > q$

Let $|G| = pq$

There exist subgroups of order p (say P) and order q (say Q)

$|a| = p$ (largest prime)

$|b| = q$ (smallest prime)

$P = \langle a \rangle$ Let n_p = # of Sylow p-subgroups

$Q = \langle b \rangle$ Let n_q = # of Sylow q-subgroups

Claim

Option 1: $[G : P] = \frac{|G|}{|P|} = \frac{pq}{p} = q$

smallest prime in $|G|$

$\Rightarrow P \trianglelefteq G \Rightarrow n_p = 1$

Option 2: $n_p \mid |G| \Rightarrow n_p = 1, \cancel{p}, q, \cancel{pq}$

$n_p \equiv 1 \bmod p$ (can $q \equiv 1 \bmod p$ (No!))

So $P \trianglelefteq G$

Now consider $n_q \in \{1, p, \cancel{q}, \cancel{qp}\}$

and $n_q \equiv 1 \bmod q$

n_q?

$Q \trianglelefteq G$

$\Rightarrow G = P \times Q$ (ie Abelian)

$n_q = p \Leftarrow\Rightarrow p \equiv 1 \bmod q$

so $q \mid p-1$ a non abelian group

Let $|G| = pq$ for primes $p > q$

If $q \nmid p-1 \Rightarrow G$ is abelian,

$G = \mathbb{Z}_{pq} = \mathbb{Z}_p \times \mathbb{Z}_q$

If $q \mid p-1 \Rightarrow$ either G is abelian
or $G \cong K$, where

$K = \langle x, y \rangle$, $|x| = q$, $|y| = p$

$\forall$ $s \in \mathbb{N}$ st

$s \not\equiv 1 \bmod p$

$s^q \equiv 1 \bmod p$, $xyx^{-1} = y^s$

To prove K exist $\rightarrow$ defer to later (free groups)

Note

Any s satisfying these conditions results in the same group

$|a| = p \quad |a_1| = p \quad |y| = p$

$|b| = q \quad |b_1| = q \quad |x| = q$

Our plan

Exhibit elements $a_1, b_1 \in G$ st

$|a_1| = p_1, \quad |b_1| = q_1, \quad b_1 a_1 b_1^{-1} = a_1^s$

(for any given s satisfying the conditions)

Last time

$\exists\ a, b \in G$ st

$|a| = p, \ |b| = q, \ G = \langle a, b \rangle$ and

$ba b^{-1} = a^d$

~~Claim~~

$d \not\equiv 1 \bmod p$, $\quad bab^{-1} = a^d = a^{1+kp}$

~~Proof~~ G is not Abelian

$= a(a^p)^k = a$

$\Rightarrow ab = ba$

Claim $d^q \equiv 1 \mod p$

proof $b^q = e$, $b^{-q} = e$

$$a = eae = b^q a b^{-q} = b^{q-1}(bab^{-1})b^{-(q-1)}$$

$$= b^{q-1}(a^d)\, b^{-(q-1)}$$

$$= b^{q-2}(b a^d b^{-1})\, b^{-(q-2)}$$

$$(ba^ib^{-1}) = \underbrace{(bab^{-1})(bab^{-1})\dots(bab^{-1})}_{i \text{ factors}}$$

$$= (a^d)^i = a^{id}$$

$$= b^{q-2}(a^{d^2})\, b^{q-2} = (\dots) = a^{d^q}$$

$\Rightarrow a = a^{d^q} \Rightarrow d^q \equiv 1 \mod p = |a|$

This shows that the number of d satisfying $bab^{-1} = a^d$ (in G) satisfying

$d \not\equiv 1 \mod p$, $d^q \equiv 1 \mod p$

Number theory

Suppose $p > q$ are primes and $s \in \mathbb{N}$ satisfying $s \not\equiv 1 \bmod p$ and $s^q \equiv 1 \bmod p$. Then a solution exists say $s = k$ and all solutions (mod p) are of form

$$s = k, k^2, \ldots, k^{q-1}$$

So let K be a group as stated

$|a| = |a_1| = |y| = p$

$|b| = |b_1| = |x| = q$

So let K be a group as stated

$$xyx^{-1} = y^s$$

$\Rightarrow s = k^t$ for $1 \le t \le q$

for any solution k

Since d is such a solution

$$s = d^t \text{ for } 1 \le t < q$$

Let $a_1 = a$, $b_1 = b^t$

<u>want</u>: $b_1 a_1 b_1^{-1} = a_1^s$

check: $b_1 a_1 b_1^{-1} = b^t a b^{-t} = a^{(d^t)} = a^s$

$= a_1^s$

Recall

$|a_1| = p$, $|b_1| = q$ $\quad (t, q) = 1$ as $0 < t < q$

$$\Rightarrow G = \langle a_1, b_1 \rangle \longrightarrow K = \langle x, y \rangle$$

$$a_1 \longmapsto y$$
$$b_1 \longmapsto x$$

$b_1 a_1 b_1^{-1} = a_1^s$ $\qquad\qquad$ $x y x^{-1} = y^s$

<u>Example</u>

Let $|G| = 91 = 7 \cdot 13$

Is $7 \mid 13 - 1$? nope

$\Rightarrow G = \mathbb{Z}_7 \times \mathbb{Z}_{13} = \mathbb{Z}_{91}$

Example

If $|G| = 2 \cdot p$, p a prime $p > 2$

$\Rightarrow 2 \mid p-1$ ✓

$\Rightarrow G = K$ (K as before)

Note that $G = \mathbb{Z}_6$ or $G = S_3$

Every non-Abelian group of order $2 \cdot p$ must be D_{2p}

Frattini's argument

Theorem

Let P be a sylow p-subgroup and

$P < H \trianglelefteq G$. Then $G = N_G(P) H$

Proof

(1) The set of Sylow p-subgroups (for p, $|P| = p^t$) in G agrees with

~~the~~ set of Sylow-p-subgroups in H

~~Proof~~

$\{gPg^{-1}\}$ = Sylow p-subgroups in G

$gPg^{-1} \subseteq gHg^{-1} = H$ as $P \leq H$

$\Rightarrow$ gPg^{-1} is a subgroup of H, in fact a Sylow p-subgroup of H

$\{hPh^{-1}\}$ = ~~the~~ set of Sylow p subgroups in H

$gHg^{-1} = hPh^{-1}$, $\forall$ g

$\Rightarrow h^{-1}g \in N_G(P)$

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

$g = hn$ $\quad\quad h \in H,\ n \in N_G(P)$

$= nh'$

$\in N_G(P)H$

$H \trianglelefteq G$

Definition

A normal series for a group G is a sequence of nested normal subgroups starting at $\{e\}$, ending at G

$$\leq \quad G_0 = \{e\} \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$$

(Note $G_0, G_1, \dots, G_{n-1}$ may not be normal in G)

Definition

Let $(G_i \mid 0 \leq i \leq n)$ be a normal series. The length is n

Fact

Let $H \leq G$. Let $(G_i \mid 0 \leq i \leq n)$ be a normal series for G. Then $(G_i \cap H \mid 0 \leq i \leq n)$ is a normal series for G. Then $(G_i \cap H \mid 0 \leq i \leq n)$ is a normal series for H

Example

$$\{e\} \trianglelefteq \mathbb{Z}_3 \triangleleft \mathbb{Z}_{15} \triangleleft \underbrace{\mathbb{Z}_{15} \times \mathbb{Z}_2}_{\mathbb{Z}_{30}},$$

Definition

Let $a, b \in G$. The commutator of a, b is

$$[a,b] = aba^{-1}b^{-1}$$

The commutator subgroup is

$$[G,G] = \langle [a,b] \mid a, b \in G \rangle$$

Facts

$[G,G] \leq G$, $[G,G] \trianglelefteq G$,

factors through every homomorphism to an Abelian group

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & A \text{(abelian)} \\ G/[G,G] \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

if $f: G \to A$ is a hom, A is abelian, then there exists a map $\bar{f}: G/[G,G] \to A$

st $f = \bar{f} \circ \pi$

Notation

The commutator subgroup is also called the derived subgroup and written G' or $G^{(1)}$

Fact

If G/N is Abelian then $N \leq [G,G]$

The derived series

$$G \trianglerighteq \underbrace{[G,G]}_{G^{(1)}} \triangleright \underbrace{[\underbrace{[G,G]}_{G^{(1)}}, \underbrace{[G,G]}_{G^{(1)}}]}_{G^{(2)}} \triangleright \underbrace{[[[G,G], \dots}_{G^{(3)}}$$

Definition

$G^{(n)}$ = (commutator subgroup of)^n of G

Example

What is the derived series of $\mathbb{Z}_{15}$?

$\mathbb{Z}_{15} \triangleright \{e\}$

Definition

A perfect group is a group G s.t. $G = [G, G]$

(A perfect group will not have any non-trivial homs to abelian groups)

Example

$[S_4, S_4] =$

(1) Explicit calculation

(2) $[S_4, S_4] \trianglelefteq S_4$

$\Rightarrow$ candidates are A_4, K_4

$\operatorname{sgn} : S_4 \longrightarrow \mathbb{Z}_2$

Definition

A cycle $C \in S_4$ is $C = (c_1\, c_2\, \dots\, c_n)$

Fact

Every permutation can be written as a product of disjoint cycles

Definition

$$\operatorname{sgn}((c_1\, c_2 \dots c_n)) = (-1)^{n-1}$$

$$\operatorname{sgn}((1\,2\,3)) = (-1)^{3-1} = +1$$

$$\operatorname{sgn}(1\,2) = -1$$

$$\underset{\substack{\uparrow \\ S_4}}{\operatorname{sgn}(\theta)} = \operatorname{sgn}(\underbrace{C_1 C_2 \dots C_m}_{\text{Each } C_i \text{ is a cycle}}) = \operatorname{sgn}(C_1)\operatorname{sgn}(C_2)\dots\operatorname{sgn}(C_m)$$

$$\operatorname{sgn}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 3 & 4 & 5 \end{pmatrix}$$

$$= \operatorname{sgn}((1\,6\,5\,4\,3)) = (-1)^{5-1} = +1$$

(<u>Question:</u> Given a random example of a commutator what is the probability that it is a 1 cycle)

$\text{sgn}: S_n \longrightarrow \mathbb{Z}_2$

$A_n = \text{Ker}(\text{sgn})$

<u>Recall</u>

$G/N \simeq$ Abelian then $N \subseteq [G,G]$

$\Rightarrow S_n / A_n \simeq \mathbb{Z}_2$ (abelian)

$\Rightarrow A_n \subseteq [G,G]$

$\Rightarrow$ as $[S_n : A_n] = 2 \Rightarrow [S_4, S_4] = A_4$

$[A_4, A_4] = K_4$ Explicit computation

$(123)(124)(321)(421) = \dots$

$[K_4, K_4] = \{e\}$

$\{e\} \triangleleft K_4 \triangleleft A_4 \triangleleft S_4$ is the derived series

Definition

A partial order on the set of normal series of a group G is given by the series

$$(H_i \mid 0 \le i \le n) \le (G_i \mid 0 \le i \le m)$$

if for all $0 \le i \le n$, $H_i = G_{j(i)}$ for some map j

Definition

The factors of a normal series are the quotients

$$G_i / G_{i-1}$$

(Another name for quotient group is a factor group)

Examples

$\{e\} \triangleleft \mathbb{Z}_3 \triangleleft \mathbb{Z}_{15} \triangleleft \mathbb{Z}_{30}$

Factors: $\mathbb{Z}_{30}/\mathbb{Z}_{15} \simeq \mathbb{Z}_2$, $\mathbb{Z}_{15}/\mathbb{Z}_3 \simeq \mathbb{Z}_5$

$\mathbb{Z}_3/\{e\} \simeq \mathbb{Z}_3$

$\{e\} \triangleleft \mathbb{Z}_2 \triangleleft K_4 \triangleleft A_4 \triangleleft S_4$

Factors: $S_4/K_4 \simeq \mathbb{Z}_2$

$A_4/K_4 \simeq \mathbb{Z}_3$

$K_4/\mathbb{Z}_2 \simeq \mathbb{Z}_2$

NB The factors are not allways cyclic groups

Definition

A composition series for G is a maximal normal series without repetitions

$\hookrightarrow (\{e\} \triangleleft \mathbb{Z}_{15}) \leq (\{e\} \triangleleft \mathbb{Z}_3 \triangleleft \mathbb{Z}_{15})$

$\{e\} \triangleleft \{e\} \triangleleft \mathbb{Z}_3 \triangleleft \mathbb{Z}_3 \triangleleft \mathbb{Z}_{15}$

not maximal

$(G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft G_3)$

$\leq (G_1 \underset{\neq}{\triangleleft} G_{1.5} \underset{\neq}{\triangleleft} G_2)$

Fact

A normal series is a composition series if and only if the factor groups do not admit non-trivial normal subgroups iff the factor groups are non-trivial simple groups

$G_1 \triangleleft G_{1.5} \triangleleft G_2 \iff G_1/G_1 \underset{\neq}{\triangleleft} G_{1.5}/G_1 \underset{\neq}{\triangleleft} G_2/G_1$

$\{e\} \triangleleft \mathbb{Z}_3 \triangleleft \mathbb{Z}_{15}$

Factors : $\mathbb{Z}_3, \mathbb{Z}_5$

$\{e\} \triangleleft \mathbb{Z}_5 \triangleleft \mathbb{Z}_{15}$

Factors : $\mathbb{Z}_3, \mathbb{Z}_5$

Theorem (Jordan-Holder)

Let G be a group and

$\{e\} \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G$

and $\{e\} \triangleleft H_1 \triangleleft \dots \triangleleft H_m = G$

be any composition series for G.

Then $n = m$ and there exists a permutation $\theta \in S_n$ such that

$$G_i / G_{i-1} \simeq H_{\theta(i)} / H_{\theta(i)-1} \quad \forall\ i = 1, \dots, n$$

(i.e. all compositions series have the same factors (up to isomorphism) but the orders of the factors may vary)

Proof

By induction (on the length of the composition series).

(If the length is 1, this is trivial (i.e. G is simple $\{e\} \lhd G$))

Now let

$$\{e\} \lhd G_1 \lhd G_2 \lhd \dots \lhd G_n = G$$

$$\{e\} \lhd H_1 \lhd H_2 \lhd \dots \lhd H_n = G$$

be composition series

We will prove $n = m$ (0)

$$G/H_{m-1} = H_m/H_{m-1} \simeq G_k/G_{k-1} \quad \text{for some } K \quad (1)$$

$$\overbrace{G_{k-1} \lhd G_k} \dots$$

$$G_k/G_{k-1} \simeq H_m/H_{m-1}$$

$$\dots \overbrace{H_{m-1} \lhd H_m} = G$$

$H_{m-1} = H$

$$\{e\} \triangleleft \underbrace{G_1 \cap H}_{x_1} \triangleleft \underbrace{G_2 \cap H}_{x_2} \triangleleft \cdots$$

$$\cdots \triangleleft \underbrace{G_{k-2} \cap H}_{x_{k-1}} \triangleleft \underbrace{G_k \cap H}_{x_{k-1}} \triangleleft \underbrace{G_{k+1} \cap H}_{x_k} \triangleleft \cdots$$

$$\cdots \triangleleft G_n \cap H = H$$

is a composition series for H (2)

and $X_i / X_{i-1} \simeq G_i / G_{i-1}$ $(i < k)$

$X_i / X_{i+1} \simeq G_{i+1} / G_i$ $(k < i < n)$

<u>Proof</u>

Lets start with (1). Recall that $H_{m-1} = H$. We need to show that there exist a k st

$$G/H \simeq G_k / G_{k-1}$$

Let $k = \min \{ i \mid G_i \notin H \}$

<u>Claim</u> $G_k \cap H = G_{k-1}$

Consider $(G_k \cap H) G_{k-1}$

$G_{k-1} \triangleleft G_k$

$\Rightarrow G_{k-1} \triangleleft (G_k \cap H) G_{k-1}$

Consider

$$G_{k-1}/G_{k-1} \trianglelefteq (G_k \cap H) G_{k-1} / G_{k-1} \trianglelefteq G_k / G_{k-1}$$

The series (G_i) is a composition series so

$$G_k / G_{k-1}$$

is simple ie does not admit non-trivial normal subgroups

$$\Rightarrow (G_k \cap H) G_{k-1} / G_{k-1} = G_{k-1}/G_{k-1} \quad \text{or} \quad G_k / G_{k-1}$$

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$(G_k \cap H) G_{k-1} = G_{k-1} \qquad (G_k \cap H) G_{k-1} = G_k$$

" $S/B \trianglelefteq M/B \trianglelefteq L/B$ "

if L/B is simple

$\Rightarrow M = S$ or $M = L$

$(G_n \cap H)\, G_{n-1} = G_{n-1}$

$\Rightarrow G_n \cap H \leq G_{n-1}$

If $(G_n \cap H)\, G_{n-1} = G_n$, $(G_n \cap H)\, G_n \leq G_n$

$\Rightarrow G_n \cap H = G_n$

Not allowed

$n = \min(G_n \not\leq H)$

Theorem (Jordan - Hölder)

Let

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_n = G$$

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots\dots \trianglelefteq H_m = H$$

be $\underbrace{\text{composition series}}_{\Leftrightarrow \; G_i/G_{i-1} \text{ is simple for } 1 \le i \le n}$ for a group G

Then $n=m$ and there exists $\sigma \in S_n$

st $\left(G_i/G_{i-1} \cong H_{\sigma(i)}/H_{\sigma(i)-1} \right)$ as a set of isomorphism classes allowing repetition the factors agree

Example

$G = \mathbb{Z}_{15}$

$\{e\} \trianglelefteq \mathbb{Z}_3 \trianglelefteq \mathbb{Z}_{15}$, $\{e\} \trianglelefteq \mathbb{Z}_5 \trianglelefteq \mathbb{Z}_{15}$

Factors $\mathbb{Z}_3, \mathbb{Z}_5$ $\qquad$ $\mathbb{Z}_5, \mathbb{Z}_3$

Here $\theta = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

Let $H = H_{m-1}$ and let $k = \min\{i \mid G_i \not\leq H\}$

claim

- $G/H \cong G_k/G_{k-1}$

- $\{e\} \trianglelefteq (G_0 \cap H) \trianglelefteq (G_1 \cap H) \trianglelefteq \overbrace{(G_{k-1} \cap H)}^{\text{omitted}}$
$\trianglelefteq (G_k \cap H) \trianglelefteq \dots \trianglelefteq (G \cap H) = H$

is a composition series for H st

$G_i \cap H / G_{i-1} \cap H \cong G_i / G_{i-1}$ (except for $i = k-1$)

Claim $G_k \cap H = G_{k-1}$

consider $(G_k \cap H) G_{k-1}$

$G_{k-1} \trianglelefteq (G_k \cap H) G_{k-1}$

$\Rightarrow (G_k \cap H) G_{k-1} / G_{k-1} \cong G_k \cap H / G_{k-1} \trianglelefteq G_k / G_{k-1}$

$\Rightarrow \underbrace{G_u \cap H = G_u}$ or $G_u \cap H = G_{u-1}$

$G_u = G_u \cap H \leq H$

$\Rightarrow G_u \leq H$ Contradiction to minimality of u

$\Rightarrow G_u \cap H = G_{u-1}$

If $i \geq K$ then $HG_i = G$

$H \trianglelefteq G$

Last time

$G_u \cap H = G_{u-1}$

$\{e\} \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_u = G$

$\{e\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_u = H$

, $K = \min\{i \mid G_i \not\leq H\}$

claim: $HG_j = G$ for $j \geq K$

$H \trianglelefteq G \Rightarrow H \trianglelefteq HG_j \Rightarrow HG_j/H \trianglelefteq G/H$

To see $HG_j/H \trianglelefteq G/H_i$

consider

$$HG_i/H \trianglelefteq HG_2/H \trianglelefteq HG_2/H \; \cdots$$

$$\cdots \trianglelefteq HG/H = G/H \leftarrow \text{simple} \quad H_m/H_{m-1}$$

As G/H is simple

$G_{n-1}/H \trianglelefteq G/H$ is either G/H or H/H

If $HG_{n-1}/H = H/H$ then $G_{n-1} \leq H$

if $HG_{n-1}/H = G/H$ then G_{n-1}/H is simple

by induction $HG_{j-1}/H = G/H$ (as $j \geq K$ by assumption)

$$\Rightarrow HG_j/H \trianglelefteq HG_{j+1}/H = G/H$$

$HG_j/H \trianglelefteq G/H$ ← simple

$\Rightarrow HG_j = H$ ($\Rightarrow G_j \leq H$, contradicting $j \geq k$)

<u>claim</u>

$G/H \cong G_k/G_{k-1}$

<u>proof</u> $G/H = HG_k/H \cong G_k/H \cap G_k = G_k/G_{k-1}$

<u>claim</u>

$H \cap G_i / H \cap G_{i-1} \cong G_i / G_{i-1}$ for $i < k$

<u>proof</u>

$H \cap G_i = G_i$ as $i < k \Leftrightarrow G_i \leq H \Rightarrow H \cap G_i = G_i$

$\Rightarrow H \cap G_i / H \cap G_{i-1} = G_i / G_{i-1}$

claim

$$H \cap G_i \big/ H \cap G_{i-1} \simeq G_i \big/ G_{i-1} \quad \text{for } i > k$$

claim 1

$G_i \cap H \nleq G_{i-1}$ for $i > k$

Recall $HG_i = G$,

$$G/H = HG_i \big/ H \simeq G_i \big/ G_i \cap H$$

simple   simple

If $G_i \cap H \leq G_{i-1} \trianglelefteq G_i \Rightarrow G_{i-1} \big/ G_i \cap H \trianglelefteq G_i \big/ G_i \cap H$

$G_{i-1} = G_i \cap H \Rightarrow G_{i-1} \leq H$ for $i-1 \geq k$, or

$G_{i-1} = G_i \Rightarrow$ violates that (G_i) is a composition series

Contradiction in either case so $G_i \cap H \nleq G_{i-1}$

Claim

$(G_i \cap H)G_{i-1} = G_i$ if $i > k$

$G_{i-1} \trianglelefteq (G_i \cap H)G_{i-1}$ (as $G_{i-1} \trianglelefteq G_i$, $G_{i-1} \trianglelefteq G_{i-1}$)

Consider $(G_i \cap H)G_{i-1} / G_{i-1} \trianglelefteq G / G_{i-1}$

$\Rightarrow (G_i \cap H)G_{i-1} = G_i$

or $(G_i \cap H)G_{i-1} = G_{i-1}$

$\Downarrow$ $G_i \cap H \leq G_{i-1}$

This is false by the previous claim

Claim

$G_i \cap H / G_{i-1} \cap H \cong G_i / G_{i-1}$ for $i > k$

$G_i / G_{i-1} = (G_i \cap H)G_{i-1} / G_{i-1} \cong G_i \cap H / G_{i-1} \cap G_i \cap H$

$$= \frac{G_i \cap H}{G_{i-1} \cap H}$$

Aschbacher Group Theory

{ Cantion

Solvable and nilpotent groups

Let G be a group. Then

$$C(G) = \{g \in G \mid gx = xg \quad \forall x \in G\}$$

is a normal subgroup of G.

Consider

$$C\left(\frac{G}{C(G)}\right) = \frac{C_2(G)}{C(G)} \qquad \text{for } C(G) \leq C_2(G) \leq G$$

Then inductively define

$$C\left(\frac{G}{C_i(G)}\right) = \frac{C_{i+1}(G)}{C_i(G)}$$

Nilpotent groups

Let G be a finite group, define

$C_1(G) = C(G) = \{ g \in G \mid gx = xg \quad \forall x \in G \}$

define

$$C_{i+1}(G) \big/ C_i(G) = C\left(G \big/ C_i(G) \right) \qquad \pi : G \to G/H, \quad g \mapsto gH$$

so $C_{i+1}(G) = \pi^{-1}\left(C\left(G \big/ C_i(G) \right) \right)$

Definition

A group G is nilpotent if $C_i(G) = G$ for some i

Example

D_4 Calculate the ascending central sequence

$$\{e\} \le C_1(G) \le C_2(G) \le \dots \le C_n(G)$$

(1) Calculate $C(D_4)$

claim $C(D_4) = \{ e, \tau^2 \}$ — rotation by $\pi = 180°$

$\tau^2 = (13)(24)$

proof

Just multiply elements out

$\langle \tau^i, r\tau^i$ for r = reflection

$r\tau r^{-1} = \tau^{-1}$ $\quad \tau^{-2} = \tau^2$ ✓

$\Rightarrow |C(D_4)| = 2$

$$\left| D_4 / C_1(G) \right| = \frac{|D_4|}{|C(D_4)|} = \frac{8}{2} = 4 = 2^2$$

$\Downarrow$

$D_4 / C(D_4)$ is abelian

$$C_2(D_4) / C_1(D_4) = C\left(D_4 / C_1(D_4) \right) = D_4 / C_1(D_4)$$

$\Rightarrow C_2(D_4) = D_4$

Since a group G is nilpotent if $C_i(G) = G$ for some i, conclude that D_4 is nilpotent

Theorem

Finite p-groups are nilpotent.

Proof

Let G be a p-group. Then

$|G| = p^n$ for some prime p

We proved that if G is a p-group

$C(G) \neq \{e\} \Rightarrow C_1(G) > 1$

By definition of the ASC

$$C_{i+1}(G)/C_i(G) = C\left(G/C_i(G)\right)$$

$$\neq C_i\left(G/C_i(G)\right) \Rightarrow C_i(G) \lneq C_{i+1}(G)$$

$\left(G/H \text{ is trivial} \Leftrightarrow G = H \right)$

$\Rightarrow |C_i(G)| < |C_{i+1}(G)|$

$\{e\} \lneq C_1(G) \lneq C_2(G) \lneq \qquad (\leq G)$

Since G is finite, this series must terminate in G, so

$C_i(G) = G$, so G is nilpotent

Theorem

Let H, K be nilpotent then $G = H \times K$ is nilpotent

Proof

Let the ASC be

$$\{e\} \leq C_1(K) \leq \dots \leq C_n(K) = K$$

$$\{e\} \leq C_1(K) \leq \dots \leq C_m(H) = H$$

Assume $m \geq n$

$$C_i(H \times K) = C_i(H) \times C_i(K)$$

Proof (By induction)

$$C_1(H \times K) = C_1(H) \times C_1(K)$$

Let $(h, k) \in C(H \times K)$

$$(h,k)(x,y) = (hx, ky) \qquad \forall\, (x,y) \in H \times K$$

$$(x,y)(h,k) = (xh, yk)$$

Since $(h,k) \in C(H \times K) \Rightarrow (hx, ky) = (xh, yk)$

$$\Rightarrow hx = xh \quad \forall\, x \in H \iff h \in C_1(H)$$

$$ky = yk \quad \forall\, y \in K \iff k \in C_1(K)$$

<u>Assume</u> $\quad C_i(H \times K) = C_i(H) \times C_i(K)$

$$\begin{tikzcd}
H \times K \arrow[r, "(\pi_H,\, \pi_K)"] \arrow[dr, bend right=60, "\pi"'] & H/C_i(H) \times K/C_i(K) \arrow[d, "f"] \\
& \cancel{\dfrac{H \times K}{C_i(H) \times C_i(K)}} = \dfrac{H \times K}{C_i(H \times K)}
\end{tikzcd}$$

$$f(hC_i, kC_i) = (h,k)(C_i(H) \times C_i(K))$$

<u>claim</u> $\quad \pi = f \circ (\pi_H, \pi_K)$

Proof

Write it out

Recall that

$$C_{i+1}(H \times K) = \pi^{-1}\left(C\left(H \times K \big/ C_i(H \times K)\right)\right)$$

Claim

Let $A \trianglelefteq H \quad B \trianglelefteq K$

$$C\left(\frac{H \times K}{A \times B}\right) = f\left(C\left(H/A\right) \times C\left(K/B\right)\right)$$

In general

$$H/A \times K/B \xrightarrow{f} H \times K \big/ A \times B$$

$$f(hA, kB) = (h, k)\, A \times B$$

$$C_{i+1}(H \times K) = \pi^{-1}\left(C\left(H \times K \big/ C_i(H \times K)\right)\right)$$

$$= (\pi_H, \pi_K)^{-1} f^{-1}\left(H \times K \big/ C_i(H \times K)\right)$$

$$= (\pi_H, \pi_U)^{-1}\left(C\left(H \times U \big/ C_i(H) \times C_i(U)\right)\right) \quad \text{by induction}$$

$$= (\pi_H, \pi_U)^{-1}\left(C\left(H \big/ C_i(H)\right) \times C\left(U \big/ C_i(U)\right)\right)$$

$$= \pi_H^{-1}\left(C\left(H \big/ C_i(H)\right)\right) \times \pi_U^{-1}\left(C\left(U \big/ C_i(U)\right)\right)$$

$$= C_{i+1}(H) \times C_{i+1}(U)$$

Theorem

A group G is nilpotent if and only if

$$G = P_{p_1} \times P_{p_2} \times \dots \times P_{p_n}$$

where $p_i \mid G$ are primes and

P_{p_i} = Sylow p_i-subgroups of G

Corollary

In a nilpotent group G, all Sylow p-subgroups are normal

Lecture on Fri 1 Dec to week

We need to prove, let $\{P_{p_i}\}$ be the set of Sylow p-subgroup

① $P_{p_i} \trianglelefteq G$

② $P_{p_i} \cap P_{p_j} = \{e\}$ if $i \neq j$

(3) $|G| = |P_{p_1}||P_{p_2}| \dots |P_{p_n}|$

<u>Proof</u>

$|G| = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n} = |P_{p_1}||P_{p_2}| \dots |P_{p_n}|$

① We need a lemma

<u>Lemma</u>

Let H be nilpotent and $K \lneq H$
Then
$$N_H(K) \neq K$$

<u>~~proof~~</u>

$\{e\} \leq C_1(H) \leq C_2(H) \leq \dots \leq C_j(H) = H$

<u>claim</u> there exists a largest i such that

$C_{i+1} \not\leq H$

Consider $a \in C_{i+1}(H) \not\leq K$

$a \in C_{i+1}(H) \Rightarrow aC_i(H)xC_i(H)$

$= xC_i(H)aC_i(H) \quad \forall x \in H$

Claim

$a \in N_H(K)$

Let $k \in K$, we want to show that

$aka^{-1} \in K$

We know that

$axC_i(H) = xaC_i(H) \quad \forall x \in H \Rightarrow \forall x \in K$

$\Rightarrow axa^{-1}x^{-1} \in C_i(H) \leq K$

$(axa^{-1})x^{-1} \in K$

Since $x^{-1} \in K$

$(axa^{-1}) \in K$

① Let H be nilpotent
If $K \subsetneq H$ then $N_H(K) \neq K$

Now consider $P = P_{p_i}$

We proved (in Lecture 5-7) that
$N_G(P) \neq P$

but that $\underbrace{N(N_G(P))}_{K} = N_G(P)$ is self normalizing

$\iff N_G(K) = K$ for $K = N_G(P)$

$\Rightarrow K = G$ (otherwise $N_G(K) \neq K \Rightarrow N_G(P) = G$

$\Rightarrow P \trianglelefteq G$

<u>Next</u> $P_{p_i} \cap P_{p_j} = \{e\}$

if $p_i \neq p_j$

since the elements in P_{p_i} have order

p_i^k the element in P_{p_j} have
order p_j^l

$\Rightarrow P_{p_i} \cap P_{p_j} = \{e\}$

Similarly $P_{p_1} P_{p_2} \cdots P_{p_{n-1}} \cap P_{p_n} = \{e\} \quad \forall n$

$$\Rightarrow |P_1 P_2 P_3 \cdots P_n| = \frac{|P_1||P_2|\cdots|P_n|}{|P_1 \cap P_2||P_1 P_2 \cap P_3| \cdots |P_1 P_2 \cdots P_{n-1} \cap P_n|}$$

$$= |P_1||P_2| \cdots |P_n|$$

$$\Rightarrow G = P_1 \times P_2 \cdots \times P_n$$

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

$$\parallel$$

$$\{hk \mid h \in H, k \in K\}$$

Fact

(1) every subgroup/quotient of a nilpotent group is nilpotent

(2) Let $m \mid |G|$, and G is nilpotent. Then there exists $K \leq G$ such that

$|K| = m$ (NB: not necessarily an element / an element g st $|g| = m$)

Solvable groups

Definition

A group G is solvable if the derived series terminates in $\{e\}$

$$G \rhd G' \rhd G^{(2)} \rhd \cdots$$

where $G' = [G, G]$

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

Theorem

Nilpotent groups are solvable

Solvable Groups

The derived series

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

$G \rhd G' \rhd G^{(2)} \rhd \cdots$ is the derived series

If $G^{(n)} = \{e\}$ then we say that G is solvable

Example

$S_4 \trianglerighteq A_4 \trianglerighteq K_4 \trianglerighteq \{e\}$

is the derived series, so S_4 is solvable

Fact

If G is a finite nilpotent group, then G is solvable

~~Proof~~

Recall G/N is abelian $\iff G' \leq N$

Let G be nilpotent so its ACS satisfies

$C_n(G) = G$ for some n

$$C_{i+1}(G) / C_i(G) = C\left(G / C_i G\right)$$

Since $C(\text{Any group})$ is abelian

$C_{i+1}' \leq C_i$ (I will omit "(G)" in $C_i(G)$)

Since $C_n = G$, $C_n' = G' \leq C_{n-1}$

$G^{(2)} = (G')' \leq (C_{n-1})' \leq C_{n-2}$

$H \leq K$
$\Rightarrow H' \leq K'$
$\langle [h,h'] \rangle \leq \langle [k,k'] \rangle$

$\Rightarrow G^{(n)} \leq C_{n-(n-1)} = C_1' = \underbrace{C(G)}_{\text{Abelian}}' = \{e\}$

$[g,g'] = gg'g^{-1}(g')^{-1} = gg^{-1}g'(g')^{-1} = e$

Theorem

G is solvable iff G admits a solvable series, ie a normal series

$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G$

with G_i / G_{i-1} abelian for all i

Proof

$(\Rightarrow)$ $\{e\} = G^{(n)} \triangleleft G^{(n-1)} \triangleleft \ldots \triangleleft G^{(1)} \triangleleft G$

is a normal series

Since $\underbrace{G^{(i+1)} = (G^{(i)})'}_{(G^{(i)})' \leq G^{i+1}} \Rightarrow G^{(i-1)} / G^{(i)}$ is Abelian

($\Leftarrow$) Let

$\{e\} \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G$

be a solvable series

Since G_{i+1} / G_i is Abelian

$\Rightarrow (G_{i+1})' \leq G_i \quad \forall i \qquad (*)$

We want to show that

$G^{(n)} = \{e\}$

$G' = (G_n)' \leq G_{n-1}$

$G^{(2)} = (G')' \leq (G_{n-1})' \qquad (\text{as } G' \leq G_{n-1})$

$\leq G_{n-2} \qquad (\text{by } *)$

by induction

$G^{(n)} \leq G_{n-n} = G_0 = \{e\}$

so $G^{(n)} = \{e\}$

Theorem (Feit-Thompson)

Groups of odd order are solvable

Theorem (Burnside)

Groups of order $p^i q^j$ for primes p, q are solvable

Fact (Hall)

Let G be solvable and let

$|G| = mn$

where $(m,n) = 1$

Then

(1) G contains a subgroup of order m, called a Hall subgroup

(2) All subgroups of order m are conjugate

(3) If $l \mid m$ and H is a subgroup of order l, then $H \leq K$ for a hall subgroup K, (so $|K| = m$)

Definition

A subgroup $H \leq G$ is characteristic denoted

H char G

if $\varphi(H) = H \quad \forall \quad \varphi \in Aut(G)$

Characteristic Subgroups

H char $G \iff \varphi(H) = H$ for all automorphisms

$\varphi \in Aut(G) = \{f : G \to G \mid f \text{ iso}\}$

Example

$Aut(Z_4)$, $Z_4 = \langle x \rangle$

x^1	x^2	x^3	e
4	2	4	1

If $\varphi \in Aut(Z_4)$

$\varphi(e) = e$, $\varphi(x^2) = x^2$

$\varphi(x) = x \qquad (\Rightarrow \varphi = id)$

or $\varphi(x) = x^3 = x^{-1}$

$\Rightarrow \varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$

$= \varphi(a)\varphi(b)$

is the $\underbrace{\text{involution}}_{f\circ f = id}$ $\quad \varphi : G \to G$, $g \mapsto g^{-1}$

is indeed an isomorphism if G is abelian

$\Rightarrow Aut(\mathbb{Z}_4) = \mathbb{Z}_2 = \{id, g \mapsto g^{-1}\}$

Example

$C(G)$ char G

$[G,G]$ char G

$f([a,b]) = f(aba^{-1}b^{-1})$

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

$= [f(a), f(b)]$

Properties

If H char K, K char G

$\Rightarrow$ H char G

Recall

(2) $\alpha_g(x) = gxg^{-1}$ is an automorphism

$\alpha_g : G \to G$, $g \in G$

(inner automorphism)

If $\alpha(H) = H$ for all inner automorphism
then $H \trianglelefteq G$

(1) H Char G $\Rightarrow$ $H \trianglelefteq G$

(3) If H Char K, $K \trianglelefteq G$ $\Rightarrow$ $H \trianglelefteq G$

(4) If G is finite $\Rightarrow$ G' char G

Proof

(2) Let H char K, K char G

To show H char G, need ~~to~~ show

$\varphi(H) = H \quad \forall \; \varphi \in Aut(G)$

Let $\varphi \in Aut(G)$

$\varphi(K) = K$ as K char G

$\Rightarrow \varphi|_K$ is an automorphism of K

$\varphi|_K(H) = H = \varphi(H)$ as H char K

and as $H \leq K$

Note

G' char G

$G^{(2)} = (G')'$ char G'

$G^{(3)} = (G^{(2)})'$ char $G^{(2)}$

$\vdots$

$\Rightarrow G^{(n)}$ char G

Theorem

If G is solvable, then G contains a normal Abelian non-trivial subgroup

Semidirect Product

Recall that G is the internal direct product if there exists $H, K \trianglelefteq G$ such that

(1) $G = HK$ $(\Leftrightarrow |G| = |H||K|)$

(2) $H \cap K = e$

In particular

$$\underbrace{h k h^{-1}}_{\in K} k^{-1} \in H \cap K \Rightarrow hkh^{-1}k^{-1} = e$$

with $k h^{-1} k^{-1} \in H$

$$\Leftrightarrow hk = kh$$

so elements in H and K commute

Note if we relax the condition $H, K \trianglelefteq G$ to merely require one of them to be normal, so say

$N \trianglelefteq G$, $H \leq G$

st $NH = G$, $N \cap H = \{e\}$

then we find the following examples

Example

D_{2n} ($= D_n$) a group of $2n$ elements

$= \langle r, \tau \rangle$ where $|r| = 2$

$|\tau| = n$

Let $N = \langle \tau \rangle$, $H = \langle r \rangle$

$N \cap H = \{e\}$ as $r \neq \tau^i$ for any i

$N \trianglelefteq D_{2n}$ as $[D_{2n} : N] = 2$

$NH = D_{2n} = \{r\tau^i\} \cup \{\tau^i\}$

$= HN$

Example

S_5

$N = A_5$

$H = \langle (12) \rangle$ (or any (ab) $a \neq b$))

$NH = S_5$ $\left(\begin{matrix} |N| = 60, \ |H| = 2 \\ |S_5| = 120 \end{matrix} \right)$

$N \cap H = \{e\}$

$\Big(\varepsilon\,(12) = -1$, but $\varepsilon(A_5) = \{+1\}$)

$(12) \in A_5 \Big)$

Example

$G = \{ A \in GL_3(\mathbb{R}) \mid A \text{ upper triangular} \}$

$$N = \left\{ \begin{pmatrix} 1 & x & x \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

$$H = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \;\middle|\; abc \neq 0 \right\}$$

$$N \cap H = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

Last time

Suppose $N \trianglelefteq G$, $H \leq G$, $NH = G$, $N \cap H = \{e\}$

- D_{12} (order 12)
- S_5
- Upper triangular matrices

Definition

Let N H be groups. Let $\varphi : H \longrightarrow \mathrm{Aut}(N)$
We will write

$\varphi_h = \varphi(h)$ ($\varphi_h : N \to N$ a bijective hom)

Since φ is a homomorphism

$\varphi_h(\varphi_{h'}(n)) = \varphi_{hh'}(n)$

We define the semidirect product group

$N \rtimes_\varphi H$

to be the group operation $N \times H$, with group operation

$(n,h)(n',h') = (n\varphi_h(n'), hh')$

Fact

$N \rtimes_\varphi H$ is a group

~~proof~~

$$(e_N, e_H)(n, h) = (e_N \varphi_{e_H}(n), e_H h)$$

$$(n, h)(e_N, e_H) = (n\varphi_h(e_N), he_H)$$

$$= (ne_H, he_H) = (n, h)$$

$\Rightarrow (e_N, e_H)$ is the identity

The inverse of (n,h) is $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$
(evaluate)

Theorem

Let G be a group, $N \trianglelefteq G$, $H \leq G$,
$NH = G$, $NH = G$, $N \cap H = \{e\}$. Then

$$G \cong N \rtimes_\varphi H$$

where $\varphi_h : n \longmapsto hnh^{-1}$, so $\varphi_h(n) = hnh^{-1}$

~~Proof~~

As $G = NH$, every $g \in G$ can be

written as $g = nh$ uniquely

Define $G \xrightarrow{f} N \rtimes_\varphi H$ via $nh \mapsto (n,h)$
Then f is a bijection. To see it is a homomorphism

$$f(gg') = f(nhn'h') = f(n\underbrace{hn'h^{-1}}_{\varphi_h(n') = hn'h^{-1}}hh')$$

$$= f((\underbrace{nhn'h^{-1}}_{\in N})\underbrace{hh'}_{\in H})$$

$$= (n\varphi_h(n'), hh')$$

$$= (n,h)(n',h')$$

$$= f(g)f(g')$$

Corollary

- $D_{12} \cong C_6 \rtimes_\varphi C_2$ $\qquad C_6 = \langle \tau \rangle$ rotation, $C_2 = \langle r \rangle$ reflection

where $\varphi_r(\tau^i) = r\tau^i r^{-1} = \tau^{-i}$

so $(\tau^i, r^j)(\tau^k, r^l) = \begin{cases} (\tau^{i-k}, r^{j+l}) & \text{if } j = 1 \\ (\tau^{i+k}, r^{j+l}) & \text{else} \end{cases}$

$$S_5 = A_5 \rtimes_{\varphi} C_2 = \langle (12) \rangle$$

$$\varphi_{(12)}(\theta) = (12)\theta(12)$$

$$\varphi_e(\theta) = \theta$$

- $\left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \middle| \det \neq 0 \right\}$

$$= \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \rtimes_{\varphi} \left\{ \begin{pmatrix} a & & 0 \\ & b & \\ 0 & & c \end{pmatrix} \middle| \det \neq 0 \right\}$$

where $\varphi_M(N) = MNM^{-1}$

Fact

- $N \cong \{(n, e_H) \mid n \in N\}$, $H \cong \{(e_H, h) \mid h \in H\}$
- $(e_N, h)(n, e_H)(e_H, h)^{-1} = (\varphi_h(n), e_H)$

Fact

N, H be groups, $\varphi : H \longrightarrow \mathrm{Aut}(N)$
$f \in \mathrm{Aut}(H)$. Then

$$N \rtimes_{\varphi} H \cong N \rtimes_{\varphi \circ f} H$$

$$\begin{tikzcd} H \arrow[r, "f"] \arrow[rr, bend right, "\varphi \circ f"'] & H \arrow[r, "\varphi"] & \mathrm{Aut}(N) \end{tikzcd}$$

Proof

$$(n, h) \longmapsto (n, f^{-1}(h))$$

Theorem (Jordan)

A_n is simple if $n \geq 5$, so A_n has no normal subgroups

Corollary

A_n is not solvable if $n \geq 5$

Proof Outline

- A_n is generated by 3-cycles
- $N \trianglelefteq A_n$ and 3-cycle $\in N \Rightarrow N = A_n$
- $N \trianglelefteq A_n$, $N \neq \{e\} \Rightarrow$ 3-cycle $\in N$

Fact

(1) $\theta \in S_n \Rightarrow \theta$ is a product of transpositions

(2) $\theta \in S_n \Rightarrow \theta = c_1 c_2 \ldots c_k$ for disjoint cycles

(3) $\theta \in A_n \Leftrightarrow \mathrm{sgn}(\theta) = +1 \Leftrightarrow \theta$ is a product of an even number of transpositions

Lemma

Pick $r \neq s$, $1 \leq r, s \leq n$. Then A_n is generated by

$(r\, s\, k)$ for $1 \leq k \leq n$, $k \neq r$, $k \neq s$

Exercise

- $r=1,\ s=2,$

Then $A_5 = \langle (1\,2\,3), (1\,2\,4), (1\,2\,5) \rangle$

- $r=4,\ s=1$

Then $A_6 = \langle (4\,1\,2), (4\,1\,3), (4\,1\,5), (4\,1\,6) \rangle$

$A_n = \langle (r\,s\,k) \rangle$

Proof

Let $\theta \in A_n$, Then

$\theta = (a_1, b_1)(a_2\ b_2) \dots (a_m, b_m)$ (even number)

so sufficient to consider $\theta = (a\,b)(c\,d)$

3 cases

- $|\{a,b,c,d\}| = 2 \Rightarrow \theta = (a\,b)(a\,b) = e$
- $|\{a,b,c,d\}| = 3 \Rightarrow \theta = (a\,b)(a\,c) = (a\,c\,b)$
- $|\{a,b,c,d\}| = 4 \Rightarrow \theta = (a\,b)(c\,d) = (a\,c\,b)(c\,d\,a)$

So it is sufficient to prove that any 3-cycles is a product of the 3-cycls in the generating set

Let $(a\,b\,c)$ be a 3-cycle

3 cases

(1) $r, s \in \{a, b, c\}$

$(a, b, c) = (r\,s\,c)$ or $(r\,c\,s)$

If $(a\,b\,c) = (r\,c\,s) = (r\,s\,c)^2$

(2) $r \in \{a, b, c\} \not\ni s$

Then $(r\,a\,b) = (r\,s\,b)(r\,s\,a)(r\,s\,a)$

(3) $s \in \{a, b, c\} \not\ni r$

Then $(s\,a\,b) = (r\,s\,b)(r\,s\,b)(r\,s\,a)$

(4) $s, r \notin \{a, b, c\}$

$(a\,b\,c) = \underbrace{(r\,c\,a)}_{\text{case 2}}\underbrace{(r\,a\,b)}_{\text{case 2}}$

Lemma

If $N \trianglelefteq A_n$ $(n \geq 5)$ and $(a\,b\,c) \in N \Rightarrow N = A_n$

~~Proof~~

Let $(a\,b\,c) = (r\,s\,k)$ (as r, s were arbitrary in the previous Lemma)

Let $i, j \notin \{r, s, k\}$ (possible as $n \geq 5$)

$$(i\,j\,k)^{-1}\underbrace{(r\,s\,k)}_{\in N}(i\,j\,k) = (r\,s\,j) \in N$$

$$\underbrace{(i\,j\,k)}_{\in A_n}$$

$\Rightarrow$ every element $(r\,s\,j)$ in the generating set of A_n is in $N \Rightarrow N = A_n$

Theorem (Jordan)

A_n is simple if $n \geq 5$

~~Proof~~

We showed that if $\{e\} \neq N \trianglelefteq A_n$, then N contains a 3-cycle, and apply the lemma

There is $\theta \in N$ such that $\theta \neq e$

Then $\theta = c_1 c_2 \dots c_n$ where c_i are disjoint cycles

5 cases

(1) θ = 3-cycle

(2) Some c_i is a r-cycle for $r \geq 4$

(3) $\theta = c_1 c_2 f$ where c_1, c_2 are 3-cycles and f consists of 2-cycles and 3-cycles

(4) $\theta = c_1 f$ where c_1 is a 3-cycle and f consists of 2-cycles

(5) θ is a product of 2-cycles

---

(1) ✓

(2) Let $\theta = (a_1 \dots a_r) c_2 \dots c_m$ $(r \geq 4)$

$\delta = (a_1 a_2 a_3) \in A_n$

$$[\theta^{-1}, \delta] = \underbrace{\underbrace{\theta^{-1}}_{\in N} \underbrace{\delta \theta \delta^{-1}}_{\in N}}_{\in N}$$

$= c_m^{-1} \cdots c_2^{-1} (a_r a_{r-1} \cdots a_1)(a_1 a_2 a_3) c_2 \cdots c_m (a_1 a_2 \cdots a_r)(a_3 a_2 a_1)$

$= (a_r a_{r-1} \cdots a_1)(a_1 a_2 a_3)(a_1 a_2 \cdots a_r)(a_3 a_2 a_1)$

$= (a_1 a_3 a_r)$

(3) Let $\theta = c_1 c_2 f$ (f a product of 3, 2-cycles

$\theta = (a_1 a_2 a_3)(a_4 a_5 a_6) f$.

Let $\delta = (a_1 a_2 a_4)$, compute $[\theta^{-1}, \delta]$

$N \ni \theta^{-1} \delta \theta \delta^{-1}$

$= f^{-1} (a_6 a_5 a_4)(a_3 a_2 a_1)(a_1 a_2 a_4)(a_1 a_2 a_3)(a_4 a_5 a_6) f (a_4 a_2 a_1)$

$= (a_1 a_4 a_2 a_6 a_5)$ $\rightsquigarrow$ reduces to case 2

(4) $\theta = (a_1 a_2 a_3) f$, f a product of 2-cycles

$\theta^2 = (a_1 a_3 a_2)$ $\rightsquigarrow$ Case (1)

(5) $\theta = (a_1 a_2) \cdots (a_{2m-1} a_{2m})$

Subcase a) θ fixes a_k $\Rightarrow a_k \notin \{a_1 \ldots a_{2m}\}$

Then $(a_1 a_2 a_k) \theta (a_1 a_2 a_k)^{-1} \in N$ ($N \trianglelefteq A_n$)

Compute

$(a_1\, a_2\, a_n)\,\theta\,(a_n\, a_2\, a_1)$

$= (a_1\, a_2\, a_n)(a_1\, a_2)(a_3\, a_4)\dots(a_{2m-1}\, a_{2m})(a_n\, a_2\, a_1)$

$= (a_2\, a_n)(a_3\, a_4)\dots(a_{2m-1}\, a_{2m})$

$\theta(a_1\, a_2\, a_n)\theta(a_n\, a_2\, a_1) = (a_1\, a_2\, a_n) \rightsquigarrow$ reduces to case 1

Subcase b)

$\theta = (a_1\, a_2)\dots(a_{n-1}\, a_n)$ and $n = 4m$

$\delta = (a_1\, a_2\, a_3\, a_4\, a_5)$ $(n \geq 5)$

$\theta\delta\theta\delta^{-1} = (a_1\, a_6\, a_3)(a_2\, a_4\, a_5) \rightsquigarrow$ reduces to case 3

$K_4 \trianglelefteq A_4$

Free groups

Let S be a (finite) set

$S = \{s_1, s_2, \ldots, s_n\}$

s_i^{-1} are just symbols and have no algebraic properties

Define $S^{-1} = \{s_1^{-1}, s_2^{-1}, \ldots, s_n^{-1}\}$

Definition

Let T be a set. Let $T = \{t_\alpha\}$ be a word in T (on T) is a finite sequence of elements in T, so

$w = t_{\alpha_1} t_{\alpha_2} \ldots t_{\alpha_n}$ (so $w : [n] \to T$)

Example

$T = \{a, b, c, \ldots, z, A, B, \ldots, Z\}$

$w = alphabet$

$w : [8] \longrightarrow T$

$1 \longmapsto a \qquad 5 \longmapsto a$
$2 \longmapsto l \qquad 6 \longmapsto b$
$3 \longmapsto p \qquad 7 \longmapsto e$
$4 \longmapsto h \qquad 8 \longmapsto t$

Example

$T = \{x, y\}$

$w = xyxyyxxy$

$[0] := \emptyset$
$[n] := \{1, \dots, n\}$

Definition

The length of a word $w : [n] \to T$ is $|w| = n$

Definition

The empty word is $w : \emptyset \to T$

Definition

Let w be a word in $S \cup S^{-1}$. We say that w is reduced if w contains no subwords of form ss^{-1} or $s^{-1}s$, where a subword w' of w is a sequence

$$[k] \xrightarrow{w'} S \cup S^{-1}$$

such that $w'(i) = w(k+i)$

for some k and all $1 \leq i \leq |w'|$

Example

hahahahahahahahahahaaaa $= w$

subwords?			
$w'(i) = w(k+i)$	hh	no	aaah no
for $k=0$	$w' =$ ha	yes
(or $k = 2, 4, \ldots$)	aa	yes
	hahah	yes

Example

$S = \{x, y\}$

$xyxx^{-1}yy^{-1}x$ is not reduced, as xx^{-1} is a subword

If w is not reduced we may reduce it by deleting the subword ss^{-1} or $s^{-1}s$ from w

Example

$xyxx^{-1}yy^{-1}x \rightsquigarrow xyyy^{-1}x \rightsquigarrow xyx$

The deletion of a single occurrence of ss^{-1} or $s^{-1}s$ is called an elementary reduction denoted $w \rightsquigarrow w'$

Definition

Let $w \rightsquigarrow w_1 \rightsquigarrow w_2 \rightsquigarrow \dots \rightsquigarrow w_n$

and $w' \rightsquigarrow w_1' \rightsquigarrow w_2' \rightsquigarrow \dots \rightsquigarrow w_m'$

be sequence of elementary reductions such that w_n, w_m' are reduced

Theorem

$$w_n = w_m' \qquad (n = m)$$

Corollary

Denote the reduction of w to be w_n, write

$$\overline{w} = w_n$$

Proof

By induction (on length of the word)

$w \rightsquigarrow w_1$

$w \rightsquigarrow w_1'$

If there exists $w \neq w'$, then w must contain at least two occurences of subwords ss^{-1} or $s^{-1}s$

<u>case 1</u> $(\ldots)ss^{-1}(\ldots)t^{-1}t(\ldots)$

<u>case 2</u> $(\ldots)ss^{-1}s(\ldots)$

<u>Case 2</u> $(\ldots)\underbrace{ss^{-1}}s(\ldots) \rightsquigarrow (\ldots)s(\ldots)$

$(\ldots)s\underbrace{s^{-1}s}(\ldots) \rightsquigarrow (\ldots)s(\ldots)$

$\Rightarrow w_1 = w_1'$

<u>case 1</u>

$(\ldots)ss^{-1}(\ldots)t^{-1}t(\ldots)$

$\rightsquigarrow (\ldots)(\ldots)t^{-1}t(\ldots) = (\ldots)\underbrace{t^{-1}t}(\ldots)$

$\rightsquigarrow (\ldots)$

Similarly for ss^{-1}

$\Rightarrow w_1 = w_1'$

<u>Exercise</u>

$\overline{\overline{\alpha\beta}\gamma} = \overline{\alpha(\overline{\beta\gamma})}$

Free Groups

Let S be an alphabet,

let $F(S) = \{$ reduced words on $S, S^{-1}\}$

Claim

$F(S)$ is a group with a group operation given by

$$(w, w') \longmapsto \overline{ww'}$$

Identity: 1 (empty word)

Inverse of $s_{i_1}^{\varepsilon_{i_1}} s_{i_2}^{\varepsilon_{i_2}} \cdots s_{i_n}^{\varepsilon_{i_n}}$ is

$$s_{i_n}^{-\varepsilon_{i_n}} s_{i_{n-1}}^{-\varepsilon_{i_{n-1}}} \cdots s_{i_1}^{-\varepsilon_{i_1}}$$

so the inverse of $xyxy^{-1}$ is $yx^{-1}y^{-1}x^{-1}$

Fact

$$\overline{w_1 \overline{w_2 w_3}} = \overline{\overline{w_1 w_2}\, w_3}$$

This group is the free group on the set S, we say the rank of $F(S)$ is the cardinality of S (typically finite)

Facts

- $|S| = |S'|$

$\Rightarrow F(S) \simeq F(S')$

$s_{i_1}^{\varepsilon_{i_1}} \cdots s_{i_n}^{\varepsilon_{i_n}} \longmapsto s_{i_1}'^{\varepsilon_{i_1}} \cdots s_{i_n}'^{\varepsilon_{i_n}}$ for $s_i' = f(s_i)$ for $f: S \to S'$ bijection

Proof

$(\Rightarrow)$ $|S| = |S'| \Rightarrow$ see map stated

$(\Leftarrow)$ $F(S) \cong F(S')$

Consider $N = \langle w^2 \mid w \in F(S) \rangle$

$N' = \langle w^2 \mid w \in F(S') \rangle$

$$\Rightarrow F(S)/N \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{|S| \text{ factors}}$$

similarly $$F(S')/N' \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{|S'| \text{ factors}}$$

- $F(\{x,y\})/N = \mathbb{Z}_2 \times \mathbb{Z}_2$

$= \{N, xN, yN, xyN\}$

$xNyNxN = (xNxN)\,yN = yN$

$\quad \parallel$

$xyxN = xN$

$\Rightarrow$ write $xyxy^{-1}$ = product of squares

(~~try~~ try this!)

- $F(\{x\}) = \mathbb{Z}$

$\quad \parallel$

$\{1, x, x^{-1}, \underset{\substack{\parallel \\ x^2}}{xx}, \underset{\substack{\parallel \\ x^{-2}}}{x^{-1}x^{-1}}, \ldots\}$

$x^i \longmapsto i$

- Subgroups of free groups are free (Hard)
- If $|S| \geq 2$, then $F(S)$ contains subgroups of any arbitrary finite rank

Theorem

Let H be a free group, $\varphi : S \to H$. Then there exists a unique extension

$\tilde{\varphi} : F(S) \to H$, a group homomorphism

$$\begin{tikzcd} S \arrow[r, hook, "i"] \arrow[dr, "\varphi"'] & F(S) \arrow[d, "\tilde{\varphi}"] \\ & H \end{tikzcd}$$

$$\left(i(s) = s \,,\quad \tilde{\varphi} \circ i = \varphi \right)$$

commutes

$\longrightarrow$ map

$\hookrightarrow$ injection

$\twoheadrightarrow$ surjection

Example

$S = \{x, y\}$	$F(\{x,y\}) \xrightarrow{\tilde{\varphi}} H$
$H = \mathbb{Z}_3$	$\tilde{\varphi}$ is a hom
$\varphi(x) = 1$	$\tilde{\varphi}(x) = 1$
$\varphi(y) = 0$	$\tilde{\varphi}(y) = 0$

$w = xyxyx^{-1}$

$$\tilde{\varphi}(w) = \varphi(x)\varphi(y)\varphi(x)\varphi(y)\varphi(x)^{-1}$$

$$= 1 + 0 + 1 + 0 + 2$$

$$= 1$$

Proof

$$\tilde{\varphi}(s_{i_1}^{\varepsilon_{i_1}} s_{i_2}^{\varepsilon_{i_2}} \cdots s_{i_n}^{\varepsilon_{i_n}}) = \varphi(s_1)^{\varepsilon_{i_1}} \cdots \varphi(s_{i_n})^{\varepsilon_{i_n}}$$

- Clearly unique
- Well defined

$$ss^{-1} \xmapsto{\tilde{\varphi}} e_H$$

$$s^{-1}s \xmapsto{\tilde{\varphi}} e_H$$

" $F(S)$ is a free object in the category of groups "

Group presentations

Let G be a group

$G = \langle S \rangle$

where S is a generating set of G

$$\begin{aligned} S &\xmapsto{\varphi} G \\ s &\longmapsto s \end{aligned}$$

$S_{12} = \langle (12), (13) \dots, (1\ 12) \rangle$

$S = \{(12), (13) \dots, (1\ 12)\} \longrightarrow F(S)$

$(1, a) \longmapsto (1, a)$

$$\begin{tikzcd} S \arrow[r, hook, "i"] \arrow[dr, "\varphi"'] & F(S) \arrow[d, "\tilde{\varphi}"] \\ & G = \langle S \rangle \end{tikzcd}$$

(1) $\tilde{\varphi}$ is surjective as it maps onto the generating set of G

(2) $G = \operatorname{Im} \tilde{\varphi} \cong F(S) / \operatorname{Ker} \tilde{\varphi}$

$\ker \tilde{Q} \leq F(S)$, so $\ker \tilde{Q}$ is free, with

$\ker \tilde{Q} = F(R)$

for R a set of words in $F(S)$

Let $\ker \tilde{Q} = \underbrace{\text{normal closure of } R}_{\text{intersection of all normal subgroups containing } R}$

Define a group presentation as

$G = \langle S \mid R \rangle$

generators

relators

where $G \cong F(S) / N(R)$

normal closure

Example

$C_n = \langle x \mid \underbrace{xxx\ldots x}_{\text{length } n} \rangle = \langle x \mid x^n \rangle$

Group Presentations

$$G = \langle S \mid R \rangle = F(S)/N$$

N normal closure of R (is the smallest normal subgroup containing $R \subseteq F(S)$)

is $N = \bigcap\limits_{\substack{N_\alpha \text{ normal} \\ R \subseteq N_\alpha}} N_\alpha$

Notation

Example

- $\langle s_1, s_2, \dots, s_n \mid r_1, \dots, r_m \rangle$ "$\langle x \mid xxx \rangle$" $\cong \mathbb{Z}_3$

generators relators

- $\langle s_1, \dots, s_n \mid r_1 = e, r_2 = e, \dots, r_m = e \rangle$
- $\underbrace{\langle s_1, \dots, s_n \mid r_1 = r_1', r_2 = r_2', \dots, r_m = r_m' \rangle}$

$\iff$

$r_1' r_1^{-1} = e$

$\iff$

$r_1' r_1^{-1}$

- $\langle x \mid \underbrace{xxxxx = xx}_{x^5 = x^2} \rangle$

Definition

In $F(S)$, $a^n = \underbrace{aa \ldots a}_{n \text{ juxtapositions}}$ for $a \in F(S)$

Theorem (Fundamental Theorem of Group Presentations)

Let $G = \langle S \mid R \rangle$. Let $\varphi : S \longrightarrow H$, a map of sets. Then φ extends to a map

$\tilde{\varphi} : G \longrightarrow H$

iff $\bar{\varphi}(r) = e \in H \quad \forall r \in R$ $\quad \left(\begin{array}{l} \bar{\varphi} : F(S) \longrightarrow H \\ \text{always exists} \end{array} \right)$

$$
\begin{tikzcd}
S \arrow[r, hook] \arrow[dr, "\varphi"'] & F(S) \arrow[r, "\pi"] \arrow[d, "\bar{\varphi}"] & F(S)/N = G \arrow[dl, "\tilde{\varphi}"] \\
& H &
\end{tikzcd}
$$

Lemma

Let G be a group, $N \trianglelefteq G$, $\varphi : G \to H$. Then φ descends to a map G/N if and only if $N \leq \operatorname{Ker}\varphi$

Proof

$$\hat{\varphi} : G/N \longrightarrow H$$

$$\hat{\varphi}(gN) = \varphi(g)$$

$$gN = g'N \iff g'g^{-1} \in N$$

$$\iff \varphi(g) = \hat{\varphi}(gN) = \hat{\varphi}(g'N) = \varphi(g')$$

if $g'g^{-1} \in N$

$$\iff \varphi(g'g^{-1}) = e_H \text{ if } g'g^{-1} \in N$$

$$\iff N \leq \operatorname{Ker}\varphi$$

$$\Rightarrow \hat{\varphi} : G/N \longrightarrow H$$

$nN = e_{G/N}$, so

$e_H = \hat{\varphi}(nH) = \varphi(n) \Rightarrow n \in \operatorname{Ker}\varphi$

$\Rightarrow N \subseteq \operatorname{Ker}\varphi$

<u>Proof of theorem</u>

Extend φ to $\bar{\varphi} : F(S) \longrightarrow H$. $\bar{\varphi}$ descends to

$$\tilde{\varphi} = \hat{\bar{\varphi}} : F(S)/N \longrightarrow H \quad \text{iff} \quad N \subseteq \operatorname{Ker}\bar{\varphi}$$

When $N \subseteq \operatorname{Ker}\bar{\varphi}$?

If $\bar{\varphi}(r) = e \Rightarrow r \in \operatorname{Ker}\bar{\varphi} \quad \forall\, r \in R$

$\Rightarrow N \subseteq \operatorname{Ker}\bar{\varphi}$

If $N \subseteq \operatorname{Ker}\varphi \Rightarrow r \in \operatorname{Ker}\varphi$ as $r \in N \ \forall\, r \in R$

<u>Examples</u>

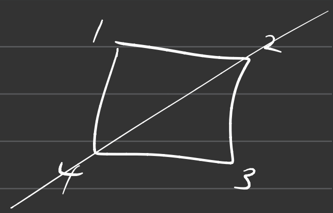
- $\langle x \mid x^n \rangle = \mathbb{Z}_n$ (Exercise $F(\{x\}) \cong \mathbb{Z}$)
- $\underbrace{\langle a, b \mid a^4, b^2, (ab)^2 \rangle}_{G} \simeq D_4$

Step 1

$G \twoheadrightarrow D_4$ using previous theorem

Step 2

$|G| \leq 8$



(1) $\varphi : \{a, b\} \longrightarrow D_4$

$a \longmapsto 90^\circ$ Rot $= (1\,2\,3\,4)$

$b \longmapsto$ flip $\Rightarrow (13)$

We need to check

$\bar{\varphi} : F(S) \twoheadrightarrow D_4$ if

$\bar{\varphi}(a^4) = \bar{\varphi}(b^2) = \bar{\varphi}((ab)^2) = e$

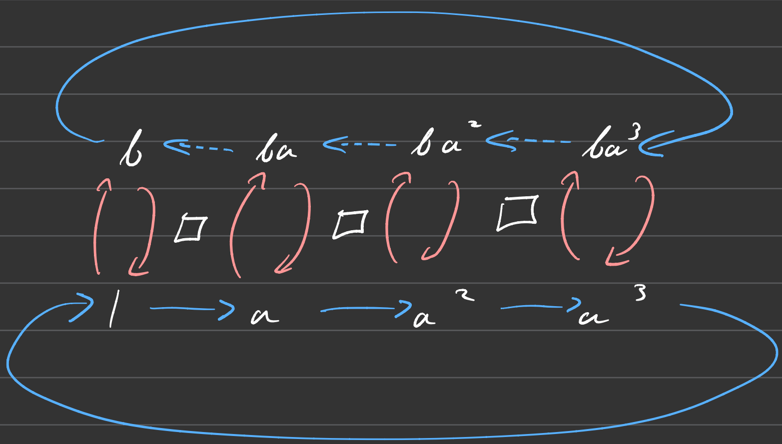
(2) We will draw a graph

$$\begin{tikzcd}
 & bw & \\
a^{-1}w \arrow[r] & w \arrow[u, "b"] \arrow[r, "a"] & aw \\
 & b^{-1}w \arrow[u] &
\end{tikzcd}$$

$w \longleftrightarrow wN \in F(S)/N = G$

If we can draw such a graph containing the identity, then G has at most order the number of vertices of the graph

pick wN, arbitrary in $F(S)/N$, start at identity, follow the edge labels in w, until you find the vertex representing N



$(ab)^2 = abab$

$$\begin{tikzcd}
bw \arrow[r] & abw \arrow[d] \\
1w \arrow[u] & babw \arrow[l]
\end{tikzcd}$$

$1w = ababw$

This forces the dashed arrows!

$aba^{-1}baaabN = ba^3N$

$abN = ba^3N$

$aba^{-1}ba^3bN$

$\Rightarrow G \cong D_4$

Tietze Transformations

The following operations preserve groups given by presentation

(1) Add a generator that is a word in the other generators

Example

$$\langle s_1, \ldots, s_n \mid \underbrace{r_1, \ldots, r_m}_{\in F(s_1, \ldots, s_n)} \rangle = \langle s_1, \ldots s_n, x \mid r_1, \ldots, r_n, x = r_{n+1} \rangle$$

(2) Remove a generator ie remove inverse of (1)

(3) Add a relation that "follows" from the other relations ie

$$\langle s_1, \ldots, s_n \mid r_1, \ldots, r_n \rangle = \langle s_1, \ldots, s_n \mid r_1, \ldots, r_n, r_{n+1} \rangle$$

where $r_{n+1} \in \langle r_1, \ldots, r_m \rangle$

(4) Remove a relation, inverse of (3)

Example

$\langle s_1, s_2 \mid s_1^2, s_2^2, s_1 s_2 s_1 = s_2 s_1 s_2 \rangle$

$= \langle s_2, s_3 \mid s_2^3, s_3 s_2 = s_3^{-1} s_2 s_3 \rangle$ $\left(\begin{array}{l} \text{add } s_3 = s_1 s_2 \\ \text{remove } s_1 \end{array}\right)$

The outer automorphism of S_6

Recall

$\mathrm{Aut}(G) = \{ f : G \to G \mid f \text{ bijective group hom} \}$

with group operation given by composition

$\mathrm{Inn}(G) = \{ x \longmapsto g x g^{-1} \} \leq \mathrm{Aut}(G)$

g fixed $\forall\, x \in G$

$G/Z(G) \cong \mathrm{Inn}(G)$

$g \in Z(G) \quad x \longmapsto g x g^{-1} = x g g^{-1} = x$

so $x \longmapsto g x g^{-1}$ is the identity

$Z(S_n) = \begin{cases} \{e\} & n \geq 1 \\ S_2 & n = 2 \end{cases} \Rightarrow \mathrm{Inn}(S_n) \cong S_n \quad \forall\, n \geq 3$

Definition

Let G be a group. The outer automorphism group is

$$\mathrm{Out}(G) = \mathrm{Aut}(G) / \mathrm{Inn}(G)$$

so an outer automorphism is a coset, represented by a (non-inner) automorphism

$$\mathbb{Z}_3 \longmapsto \mathbb{Z}_3$$
$$x \longmapsto x^{-1}$$

$$\mathrm{Inn}(\mathbb{Z}_3) = \mathbb{Z}_3 / Z(\mathbb{Z}_3) = \mathbb{Z}_3 / \mathbb{Z}_3 = \{e\}$$

every non-trivial automorphism of Abelian groups is outer

Theorem

If $n \neq 6$ then $Out(S_n) = \{e\}$

$(\Rightarrow Aut(S_n) = Inn(S_n) = S_n, \quad n \geq 3)$

Proof

Next time

Theorem

Let $f : S_n \to S_n$ be an Automorphism.
Then f is inner if and only if it maps transpositions to transpositions

$(\Rightarrow)$ f inner $\Rightarrow$ f maps conjugacy classes to themselves.

As transpositions form a conjugacy class, this proves the claim

$(\Leftarrow)$ Claim

There exist $a, b_2, \dots, b_n$ st

$$f((1\ i)) = (a\ b_i)$$

$S_3 \quad Aut(S_3) = S_3 = \langle (12), (123) \rangle$

all such maps are homomorphism and bijective

so $|Aut(S_3)| \leq 6$

$Inn(S_3) = |S_3| / |Z(S_3)| = \frac{6}{1} = 6 \Rightarrow Aut(S_3) = Inn(S_3)$

Proof of Claims

- automorphism preserve order

$(1\ i)(1\ j) = (j\ i\ 1)$

$f((1\ i)(1\ j)) = f((j\ i\ 1))$ has order 3

$f((1\ i)) f((1\ j)) = (r\ s)(r'\ s')$ where $(1\ i) \overset{f}{\mapsto} (r\ s)$
$(1\ j) \overset{f}{\mapsto} (r'\ s')$

as f preserves transpositions

So $|(r\ s)(r'\ s')| = 3$ so cannot be a product of distinct transpositions

$\Rightarrow |\{r, s, r', s'\}| = 3$ say $r = r' = a_{\{i,j\}}$

$s = b_i$

$s' = b_j$

$f((1\ i)) = (r\ s) = (a_{\{i,j\}}\ b_i)$

$f((1\ j)) = (a_{\{i,j\}}\ b_j)$

$f(12) = (4\ 20)$
$f(13) = (4\ 64)$

$f(12) = (20\ 4)$
$f(17) = (20\ 22)$

We need to prove $a_{\{i,j\}} = a_{\{i',j'\}}$

It's sufficient $a_{\{i,j\}} = a_{\{j,k\}}$

$\Rightarrow f(1\ i) = (a_{\{i,j\}}\ b_i)$ | $f(1\ j) = (a_{\{j,k\}}\ b_j')$

$f(1\ j) = (a_{\{i,j\}}\ b_j)$ | $f(1, k) = (a_{\{j,k\}}\ b_k')$

$(a\ b) = (1\ a)(1\ b)(1\ a) = (i\ a)(i\ b)(i\ a)$ $i \neq a, b$

$f(i\ j) = f((1\ i)(1\ j)(1\ i)) = (b_i\ b_j)$

$f(i\ k) = f((1\ i)(1\ k)(1\ i))$

$$= \underbrace{(a_{\{i,j\}}\ b_i)(a_{\{j,k\}}\ b'_k)}_{\text{disjoint}}(a_{\{i,j\}}\ b_i)$$

<u>claim</u>

$$a_{\{i,j\}} = a_{\{i,j\}}$$

<u>Proof</u>

If not, then

$$f(i,j) = (a_{\{i,j\}}\ b_i) = (a_{\{j,k\}}\ b'_j)$$

and $a_{\{i,j\}} \neq a_{\{j,k\}}$

then $a_{\{i,j\}} = b'_j \neq b'_k$

$$a_{\{j,k\}} = b_j \neq b_i$$

To show that $(a_{\{i,j\}}\ b_i)(a_{\{i,j\}}\ b'_k)$

$$= (a_{\{j,k\}}\ b'_k)(a_{\{i,j\}}\ b_j)$$

If $b'_k = b_i \Rightarrow f(1\ k) = (a_{\{j,k\}}\ b'_k)$

$$= (a_{\{j,k\}}\ b_i) = (b_j\ b_i)$$

$f(i\ j) = f((1\ i)(1\ j)(1\ i)) = (b_j\ b_i)$

f is injective so contradiction

We proved that if $a_{\{i,j\}} \neq a_{\{j,k\}}$ then the 1st 2 cycles are disjoint

$= (a_{\{j,k\}}\ b_k) = f(1\ k)$

contradicts injectivity

$\Rightarrow a_{\{i,j\}} = a_{\{j,k\}}$

and our original claim is proven

<u>Last time</u>

There exists a, b_i st

$f(1\ i) = (a\ b_i) \quad \forall\ 1 \le i \le n$

(assumption: f maps transposition to transposition)

<u>claim</u>: f is inner

Consider $\theta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a & b_2 & b_3 & \cdots & b_n \end{pmatrix}$

$f(x) = \theta x \theta^{-1}$

Sufficient to check on the set $\{(1\ i)\}$ since it generates $S_n = \langle \{(1\ i)\} \rangle$

$f(1\ i) = \theta (1\ i) \theta^{-1} : a \xmapsto{\theta^{-1}} 1 \xmapsto{(1\ i)} i \mapsto b_i$

$b_i \xmapsto{\theta^{-1}} i \xmapsto{(1\ i)} 1 \mapsto a$

$\quad \shortparallel \qquad\qquad \shortparallel$

$(a\ b_i) \quad (a\ b_i)$

If $k \neq i \Rightarrow \theta (1\ i) \theta^{-1} : k \mapsto k$

$\quad \neq 1$

$\Rightarrow f$ is inner

Corollary

If $n \neq 6$, then $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$

Proof

Automorphisms preserve the order of elements

$n \neq 6 \Rightarrow$ Automorphisms preserves the cycle type cycle type

$\Rightarrow \theta \in S_n$, $\theta = (r_1 \dots r_n)(s_1 \dots s_m)(t_1 \dots t_k) \dots (z_1 \dots z_s)$

for r_i, s_i, t_i, z_i all distinct

cycle type: $(n)(m)(k) \dots (s)$

order $= 2 \Rightarrow$ cycle type either

2 or $(2)(2)$ or $(2)(2)(2)$

<u>Lets count them</u>

S_8 cycle	(ab) 2	$(ab)(cd)$ $(2)(2)$	$(ab)(cd)(ef)$ $(2)(2)(2)$	$(ab)(cd)(ef)(gh)$
# elements	28	$\binom{8}{2}\binom{6}{2}/2$	$\dfrac{\binom{8}{2}\binom{6}{2}\binom{4}{2}}{2\cdot 3}$	$\dfrac{\binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2}}{4!}$

S_6	2	$(2)(2)$	$(2)(2)(2)$
	15	$\dfrac{15\cdot\binom{4}{2}}{2} = 42$	$\dfrac{15\cdot 6\cdot 1}{6} = 15$

If $n \neq 6$ then

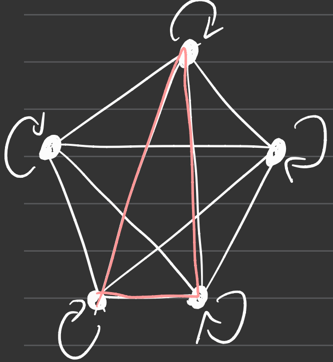
$$\binom{n}{2} \neq \frac{\binom{n}{2} \cdots \binom{n-2k}{2}}{k!}$$ (check it)

If $n=6$ then

transpositions = # of product of 3 transpositions

$\Rightarrow$ all automorphisms of S_n ($n \neq 6$) must map transpositions to transpositions

$\Rightarrow$ all automorphisms are inner



(loopless complete graph on 5 vertices)

Complete graph on 5 vertices
I want to colour the edge st each color forms a cycle of length 5, such that

- all edge are coloured
- each edge has only 1 colour

Definition

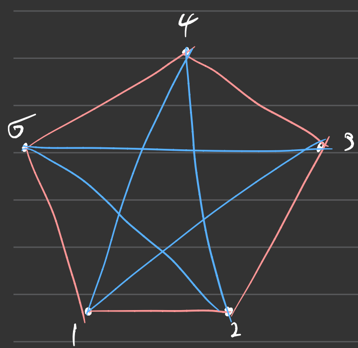
An edge of a graph with vertex set $\{v_1, \dots, v_n\}$ is $\{v_i, v_j\}$. If $v_i = v_j$ the edge is called a loop

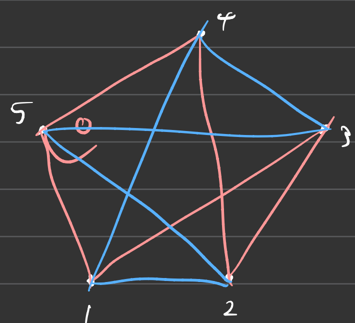
Length = # of edges in cycles

Definition

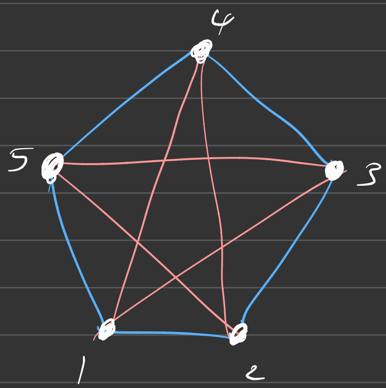
A cycle is a subset of the edges st $\{v_i, v_j\}, \{v_j, v_k\}, \dots, \{v_t, v_i\}$

" mystic pentagon "





Fish with mouth at 5 ... Fish with mouth at i



$B = \{\{1,2\}, \{2,3\}, \{3,4\}, \{4,5\}, \{5,1\}\}$

$R = \{\{1,4\}, \{4,2\}, \{2,5\}, \{5,3\}, \{3,1\}\}$

Action of S_5

$(12)A = ?$

Let $\sigma \in S_5$

$\sigma(v_i) = v_{\sigma(i)}$

$\sigma(\{v_i, v_j\}) = \{v_{\sigma(i)}, v_{\sigma(j)}\}$

$(12)A$

$(12)\{1,2\} = \{(12)1, (12)2\}$

$= \{1,2\}$

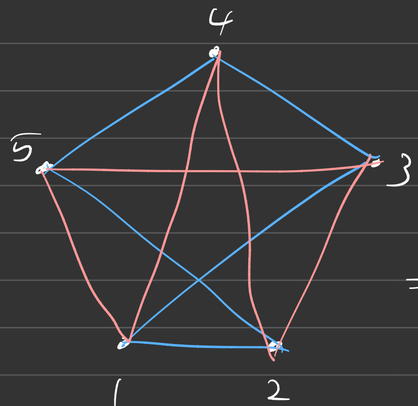
$(12)\{3,4\} = \{3,5\}$

$(12)\{1,5\} = \{2,5\}$

$(12)\{2,3\} = \{1,3\}$

<u>Fact</u>

Cycles are preserved under the S_5 action



$= F_4$

$(23)A = F_5$

$g : S_5 \to S_6$

$(34)A = F_1$

$(45)A = F_2$

$(51)A = F_3$

F_i = "fish with mouth at i"

We get action

$$S_5 \text{ on } \{A, \underset{\overset{\|}{D}}{F_1}, \underset{\overset{\|}{E}}{F_2}, \underset{\overset{\|}{F}}{F_3}, \underset{\overset{\|}{B}}{F_4}, \underset{\overset{\|}{C}}{F_5}\}$$

Claim: This action has trivial Kernel

$$f : S_5 \longrightarrow Perm(X) = S_6$$

Normal subgroups of S_6 : $A_6, S_6, \{e\}$

let $\theta = (123) = (12)(23)$

Claim: acts non-trivially

$$\theta A = (12)(23) A$$

$$= (12) F_5$$

$$= F_1$$

$\Rightarrow \theta \neq id$!

$\Rightarrow \theta$ act non trivially

$\Rightarrow Ker(f) = \{e\}$

$\Rightarrow \operatorname{Im}(f) \cong S_5$

The action is transitive, so

$\operatorname{Im}(f) \neq \operatorname{Stab}_i(S_6)$

consider the cosets of $\operatorname{Im}(f)$ in S_6

$H = \operatorname{Im}(f) =$

$S_5 = \langle (12), (23), (34), (45), (51) \rangle$

$\Rightarrow$ Image of this generating set

$\Rightarrow \operatorname{Im} f = \langle \underbrace{(A\ F_4)(F_5\ F_1)(F_2\ F_3)}_{f(12)},$

$\ldots\ (A F_3)(F_4\ F_5)(F_1\ F_2) \rangle$

The cosets of H in S_6 are

$S_6 / H = \{ H, (12)H, (13)H, (14)H, (15)H \}$

~~proof~~ Many Computations

Recall that if $K \trianglelefteq G$, then G acts on G/K by

$$g(xk) = (gx)k$$

Recall that $\operatorname{Ker} K \trianglelefteq K$

$\Rightarrow$ Consider S_6 acting on

$S_6/H \Rightarrow \operatorname{Ker} \leq H = \operatorname{Im} f \Rightarrow \operatorname{Ker} = \{e\}$

$\Rightarrow \operatorname{Ker} = S_6, A_6, \{e\}$

$$|\operatorname{Ker}| \leq |\operatorname{Im} f| = 5! = 120$$

$\Rightarrow \operatorname{Ker} \neq 360, 720$

$\Rightarrow \operatorname{Ker} = \{e\}$