Algebra

Def: $(M, \circ_{M\times M\to M})$: magma ,

$(M, \circ_{M\times M\to M})$: unital magma :=

$\exists e_{\in M}\ \forall \sigma_{\in M}\quad \sigma\circ e = \sigma = e\circ\sigma$.

Theorem: $\exists! e_{\in M}\ \forall \sigma_{\in M}\ \sigma\circ e = \sigma = e\circ\sigma$.

Proof: $\forall \sigma_{\in M}, j_{\in\{1,2\}}\quad \sigma\circ e_j = \sigma = e_j\circ\sigma$

$\Rightarrow\quad e_1 = e_1\circ e_2 = e_2$ ∎

Ex: $M=\{0,1,2\}$, define $*_{M\times M\to M}$ such that

*	0	1	2
0	0	2	0
1	1	0	0
2	0	0	2

since $\forall e_{\in M}\ \exists \sigma_{\in M}\ \neg(\sigma * e = \sigma = e * \sigma)$

$0*1=2$, $1*2=0$, $2*1=0$

$(M,*)$: non-unital magma

also define $\otimes_{M\times M\to M}$ such that

⊗	0	1	2
0	0	1	2
1	1	1	2
2	2	2	0

so $e_\otimes = 0$

hence $(M,\otimes)$: unital magma .

Def: $(M, \circ_{M\times M\to M})$: semigroup :=

$\circ$: associative i.e.

$\forall x,y,z_{\in M}\quad (x\circ y)\circ z = x\circ(y\circ z)$.

Def: $(M, \circ_{M\times M\to M})$: commutative magma

$:= \forall x,y_{\in M}\quad x\circ y = y\circ x$.

Theorem: $\circ_{M\times M\to M}$: unital $\wedge$ $\otimes_{M\times M\to M}$: unital

$\wedge\ \forall x,y,\sigma,s \in M\ (x\otimes y)\circ(\sigma\otimes s) = (x\circ\sigma)\otimes(y\circ s)$

$\Longrightarrow\ \circ_{M\times M\to M} = \otimes_{M\times M\to M}$

$\wedge\ \circ = \otimes$: associative $\wedge$ commutative .

Proof: $e_\circ = e_\circ \circ e_\circ = (e_\otimes \otimes e_\circ)\circ(e_\circ \otimes e_\otimes)$

$= (e_\otimes \circ e_\circ)\otimes(e_\circ \circ e_\otimes) = e_\otimes \otimes e_\otimes$

$= e_\otimes$

So $e_\circ = e_\otimes$, define $e := e_\circ = e_\otimes$

Let $x,y \in M$,

$x\circ y = (x\otimes e)\circ(e\otimes y)$

$= (x\circ e)\otimes(e\circ y) = x\otimes y$

So $\circ_{M\times M\to M} = \otimes_{M\times M\to M}$

therefore $\circ = \otimes$: asso $\wedge$ comm

since $\forall x,y,z$

$(x\circ y)\circ z = (x\circ y)\circ(e\circ z)$

$= (x\circ e)\circ(y\circ z) = x\circ(y\circ z)$

$x\circ y = (e\circ x)\circ(y\circ e)$

$= (e\circ y)\circ(x\circ e) = y\circ x$ ∎

Def: $(S, \circ_{S\times S\to S})$: inverse semigroup :=

i. $\circ$: asso

ii. $\forall s_{\in S}\ \exists s^{-1}_{\in S}\quad s\circ s^{-1}\circ s = s \ \wedge\ s^{-1}\circ s\circ s^{-1} = s^{-1}$

Ex: $S = \{0,1,2\}$,

$\circ$	0	1	2
0	1	2	1
1	2	1	2
2	1	2	1

$\circ$: asso, so $(S,\circ)$: semigroup

$0\circ 0\circ 0 = 1\circ 0 = 2 \neq 0$ so $0^{-1}\neq 0$

$0\circ 1\circ 0 = 2\circ 0 = 1 \neq 0$ so $0^{-1}\neq 1$

$0\circ 2\circ 0 = 1\circ 0 = 2 \neq 0$ so $0^{-1}\neq 2$

So, since $\exists s^{(=0)}_{\in S}$ s: non-invertible,

$(S,\circ)$: not inv,

$K = \{0,1,2,3,4\}$,

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	0	0
2	0	0	0	1	2
3	0	3	4	0	0
4	0	0	0	3	4

$\otimes$: asso, so $(K,\otimes)$: semigroup

Also $\forall s_{\in K}$ s: inv

e.g. $2^{-1} = 3$

$2\otimes 3\otimes 2 = 1\otimes 2 = 2$

$3\otimes 2\otimes 3 = 4\otimes 3 = 3$

So $(K,\otimes)$: inv,

$*$	0	1	2
0	2	0	1
1	0	2	2
2	1	2	0

$*$: comm,

So $(S,*)$: comm magma.

Def: $(Q, \circ_{Q\times Q\to Q})$: quasigroup :=

$\forall x,y_{\in Q}\ \exists!\sigma,s_{\in Q}\ x\circ\sigma = y \wedge s\circ x = y$.

Ex: $Q = \{1,2,3,4,5,6,7\}$

∘	1	2	3	4	5	6	7
1	1	7	6	5	4	3	2
2	7	2	5	6	3	4	1
3	6	5	3	7	2	1	4
4	5	6	7	4	1	2	3
5	4	3	2	1	5	7	6
6	3	4	1	2	7	6	5
7	2	1	4	3	6	5	7

$(Q,\circ)$: quasigroup

e.g. for 2,5:

$2\circ 3 = 5 \wedge 3\circ 2 = 5$

or for 7,1:

$7\circ 2 = 1 \wedge 2\circ 7 = 1$,

$K = \{0,1,2\}$, $(K,\otimes)$: quasigroup

⊗	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

e.g. for 0,1:

$0\otimes 2 = 1 \wedge 1\otimes 0 = 1$.

Def: $(L, \circ_{L\times L\to L})$: loop :=

i. $(L,\circ)$: quasigroup

ii. $\exists e_{\in L}\ \forall l_{\in L}\ l\circ e = l = e\circ l$.

Ex: $L = \{1,2,3,4,5\}$

⊛	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

$(L,\circledast)$: quasigroup

e.g. for 2,4:

$2\circledast 3 = 4 \wedge 5\circledast 2 = 4$,

also $e_{\circledast} = 1$, so $(L,\circledast)$: loop.

Def: $(M, \circ_{M\times M\to M})$: monoid :=

i. $\circ$: asso

ii. $\exists e_{\in M}\ \forall x_{\in M}\quad x\circ e = x = e\circ x$.

Ex: $M = \{1,2,3,4\}$,

$\circ$	1	2	3	4
1	1	2	3	4
2	2	2	4	4
3	3	2	1	4
4	4	2	2	4

$e_\circ = 1$,

also $\circ$: asso

e.g. $(2\circ 3)\circ 3 = 4\circ 3 = 2$

$= 2\circ 1 = 2\circ(3\circ 3)$

So $(M,\circ)$: monoid

also $\circ$: non-comm

e.g. $2\circ 3 = 4 \neq 2 = 3\circ 2$

$K = \{0,1,2\}$,

$\otimes$	0	1	2
0	2	1	0
1	1	1	1
2	0	1	2

$e_\otimes = 2$,

$\otimes$: asso

e.g. $(0\otimes 0)\otimes 1 = 2\otimes 1 = 1$

$= 0\otimes 1 = 0\otimes(0\otimes 1)$

$\otimes$: comm

So $(K,\otimes)$: comm monoid

$\oplus$	0	1	2
0	2	0	0
1	0	1	2
2	0	2	2

$e_\oplus = 1$,

$\oplus$: asso

e.g. $(0\oplus 2)\oplus 0 = 0\oplus 0 = 2$

$= 0\oplus 0 = 0\oplus(2\oplus 0)$

$\oplus$: comm

So $(K,\oplus)$: comm monoid .

Def: $(G, \circ_{G\times G\to G})$: group :=

i. $\forall x,y,z_{\in G} \quad (x\circ y)\circ z = x\circ(y\circ z)$

ii. $\exists e_{\in G}\ \forall x_{\in G} \quad x\circ e = x = e\circ x$

iii. $\forall x_{\in G}\ \exists x^{-1}_{\in G} \quad x\circ x^{-1} = e = x^{-1}\circ x$.

Theorem: $\forall x_{\in G}\ \exists! x^{-1}_{\in G}$
$x\circ x^{-1} = e = x^{-1}\circ x$.

Proof: $\forall x_{\in G}, j_{\in\{0,1\}} \quad x\circ x_j^{-1} = e = x_j^{-1}\circ x$

$\Longrightarrow \quad x_0^{-1} = x_0^{-1}\circ e = x_0^{-1}\circ(x\circ x_1^{-1})$
$= (x_0^{-1}\circ x)\circ x_1^{-1} = e\circ x_1^{-1} = x_1^{-1}$

$\Longrightarrow x_0^{-1} = x_1^{-1}$ ∎

Theorem: $x_{\in G}\circ y_{\in G} = e \Longrightarrow x = y^{-1} \wedge y = x^{-1}$.

Proof:

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

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

$\Longrightarrow x = y^{-1} \wedge y = x^{-1}$ ∎

Theorem: $(G, \circ)$: group,

$\sigma \circ x = \sigma \circ y \quad \vee \quad x \circ \sigma = y \circ \sigma \implies x = y$.

Proof:

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

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

■

Theorem: $o_2 x = x \implies x = e$.

Proof:

$$o_2 x = x$$
$$x \circ x = x$$
$$x \circ x = e \circ x$$
$$x = e$$

■

Theorem: $e^{-1} = e$.

Proof: $e \circ e = e = e \circ e^{-1}$

$$\implies e \circ e = e \circ e^{-1} \implies e = e^{-1}$$

■

Theorem: $(G, \circ)$: group, $(x^{-1})^{-1} = x$.

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

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

$(x^{-1})^{-1} = x$ ∎

Theorem: $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

Proof:
$$\begin{aligned}(x \circ y) \circ (y^{-1} \circ x^{-1}) &= x \circ (y \circ (y^{-1} \circ x^{-1})) \\ &= x \circ ((y \circ y^{-1}) \circ x^{-1}) \\ &= x \circ (e \circ x^{-1}) \\ &= x \circ x^{-1} \\ &= e \\ &= (x \circ y) \circ (x \circ y)^{-1}\end{aligned}$$

$\Longrightarrow y^{-1} \circ x^{-1} = (x \circ y)^{-1}$ ∎

Theorem: $(G, \circ)$: group $\Longrightarrow$

$(o_n x)^{-1} = o_n x^{-1} \wedge o_n x \circ o_m x = o_{n+m} x$

$\wedge\ o_n(o_m x) = o_{nm} x$.

Proof: i. Since $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$,

$(o_n x)^{-1} = (x \circ \dots \circ x)^{-1} = x^{-1} \circ \dots \circ x^{-1} = o_n x^{-1}$

ii. $o_n x \circ o_m x = (x \circ \dots \circ x) \circ (x \circ \dots \circ x)$

$= x \circ \dots \circ x \circ \dots \circ x = o_{n+m} x$

iii. $o_n(o_m x) = (o_m x) \circ \dots \circ (o_m x)$

$= x \circ \dots \circ x \circ \dots \circ x = o_{nm} x$ ∎

Def: $S_{\in G} \leq G :=$

$(G, \circ_{G\times G \to G})$: group $\wedge$

$(S, \circ_{|S\times S})$: group .

Theorem: $e_G = e_{S \leq G}$.

Proof: $e_S \circ e_S = e_S = e_S \circ e_G$

$e_S \circ e_S = e_S \circ e_G$

$e_S = e_G$ ■

Theorem: $S_{\in G} \leq G$

$\iff S \neq \emptyset \wedge \forall_{x,y \in S}\ x \circ y^{-1} \in S$.

Proof: $(\Rightarrow)$: $\forall_{\sigma \in S}\ \sigma^{-1} \in S$ so $\forall_{x,y \in S}$
$x \circ y^{-1}_{\in S} \in S$

$(\Leftarrow)$: since $S \neq \emptyset$, $\exists_{\sigma \in G}\ \sigma \in S$
by hypo $\sigma \circ \sigma^{-1} \in S$ i.e. $e_G \in S$ so
by hypo $e_G \circ \sigma^{-1} \in S$ i.e. $\sigma^{-1} \in S$ so
$\forall_{\Omega \in S}\ \Omega^{-1} \in S$,
$x, y \in S \Rightarrow x, y^{-1} \in S \Rightarrow x \circ (y^{-1})^{-1} \in S$
$\Rightarrow x \circ y \in S$

hence $(S, \circ_{|S\times S})$: group so $S \leq G$ ■

Theorem: $(G, \circ)$: finite group $\wedge$ $S = \{x_{\in G} \mid x \neq x^{-1}\}$
$\Longrightarrow |S|$: even .

Proof: $\forall x_{\in S}\ \exists x^{-1}_{\in S}\ x \neq x^{-1}$, note $(x^{-1})^{-1} = x$
also $\exists! x^{-1}\ x \circ x^{-1} = e_G$
so $S = \bigcup_{x \neq x^{-1}} \{x, x^{-1}\}$ hence $|S|$: even ■

Theorem: $(G, \circ)$: finite group,
$|G|$: odd $\Longrightarrow$ $|\{x_{\in G} \mid x = x^{-1}\}|$: odd
$|G|$: even $\Longrightarrow$ $|\{x_{\in G} \mid x = x^{-1}\}|$: even

Proof: let $S = \{x_{\in G} \mid x \neq x^{-1}\}$, note $|S|$: even
Since G: finite, $|G \setminus S| = |G| - |S|$
which concludes the result ■

Theorem: $(G, \circ)$: finite $\wedge$ $|G|$: even
$\Longrightarrow \exists x_{\in G} : x \neq e_G \wedge x = x^{-1}$.

Proof: since $|G|$: even,
$|\{x_{\in G} \mid x = x^{-1}\}|$: even,
also since $e_G \circ e_G = e_G = e_G \circ e_G^{-1}$
i.e $e_G = e_G^{-1}$,
there has to be at least
one more such element ■

Theorem: $(S,\circ) \leq (G,\circ) \wedge (T,\circ) \leq (G,\circ)$

$\Longrightarrow (S \cap T, \circ) \leq (G,\circ)$

Proof: $S \cap T$ closed under $\circ$:

$x,y \in S \cap T \Longrightarrow x,y \in S \wedge x,y \in T$

$\Longrightarrow (x \circ y) \in S \wedge (x \circ y) \in T$

$\Longrightarrow (x \circ y) \in S \cap T$

also $e_G (= e_S = e_T) \in S \cap T$

and $\forall x \in S \cap T \; x^{-1} (= x_G^{-1} = x_S^{-1} = x_T^{-1}) \in S \cap T$

also asso holds for $(S \cap T)_{\in G}$

so $(S \cap T, \circ) \leq (G,\circ)$ ∎

Def: $(G,\circ)$ group, $x \in G$

$\operatorname{ord}(G) = |G|$

$\operatorname{ord}(x) = \min\limits_{\substack{n \in \mathbb{N}_+ \\ \circ_n x = e_G}} n$.

Theorem: $(S,\circ) \leq (G,\circ)$, $(T,\circ) \leq (G,\circ)$

$(S \cup T, \circ)$: group $\iff S \subseteq T \vee T \subseteq S$

Proof: ($\Rightarrow$): suppose $S \not\subseteq T \wedge T \not\subseteq S$,

so $\exists x_{\in S}, y_{\in T}: x \notin T \wedge y \notin S$

since $x, y \in S \cup T$, $(x \circ y) \in (S \cup T, \circ)$

so $(x \circ y) \in S \vee (x \circ y) \in T$

suppose $(x \circ y) \in S$, since $(S,\circ)$: group

$\exists x^{-1}_{\in S}$ x^{-1}: inverse of $x_{\in S}$, so

$$x^{-1} \circ (x \circ y) = (x^{-1} \circ x) \circ y = e \circ y = y \in S$$

otherwise, similarly

$$(x \circ y) \circ y^{-1} = x \circ (y \circ y^{-1}) = x \circ e = x \in T$$

so $y_{\notin S} \in S \vee x_{\notin T} \in T$, which is a contradiction

hence $S \subseteq T \vee T \subseteq S$

($\Leftarrow$): $S \subseteq T \vee T \subseteq S$

$\Rightarrow T = S \cup T \vee S = S \cup T$

$\Rightarrow$ since both $(S,\circ)$ and $(T,\circ)$ is group

$(S \cup T, \circ)$: group ■

Theorem: $(G, \circ)$: group $\wedge$ $\mathrm{ord}(x_{\in G}) = m$

$\Rightarrow \forall s \; \exists!\, j_{\in\{0,\dots,m-1\}} \; x^s = x^j$.

Proof: $\forall s, m_{(>0)} \; \exists!\, q, r : 0 \le r < m$

$s = mq + r$ so $x^s = x^{mq+r} = x^{mq} \circ x^r$

$= (x^m)^q \circ x^r = e_G^q \circ x^r$

$= e_G \circ x^r = x^r$

so $\forall s \; \exists!\, r_{\in\{0,\dots,m-1\}} \; x^s = x^r$ ∎

Theorem: $(G, \circ)$: group $\wedge$ $\mathrm{ord}(x_{\in G}) = \infty$

$\Rightarrow \forall_{j_0, j_1 (\neq j_0)} \; x^{j_0} \neq x^{j_1}$.

Proof: suppose $j_0 \neq j_1$ and $x^{j_0} = x^{j_1}$,

say $j_0 > j_1$, so $x^{j_0} \circ x^{-j_1} = e_G$

so $x^{j_0 - j_1} = e_G$ hence $\mathrm{ord}(x) = j_0 - j_1$

which is a contradiction ∎

Theorem: $(G, \circ)$: finite group

$\Rightarrow \forall x_{\in G} \; \mathrm{ord}(x) \in \mathbb{N}$.

Proof: if $\exists \sigma_{\in G} \; \mathrm{ord}(\sigma) = \infty$, $\forall i, j_{(\neq i)} \; \sigma^i \neq \sigma^j$

since $\forall q \; \sigma^q \in G$, G would be infinite ∎

Theorem: $(G, \circ)$: group; $x, y \in G$

i. $\text{ord}(x) = 1 \iff x = e_G$

ii. $\text{ord}(x) = \text{ord}(x^{-1})$

iii. $\text{ord}(x \circ y) = \text{ord}(y \circ x)$.

Proof: i. ($\Rightarrow$): $\text{ord}(x) = 1$ i.e. $x^1 = e_G$

so $x = e_G$

($\Leftarrow$): $\min_{\substack{n \in \mathbb{N}_+ \\ x^n = e_G}} n = \min_{\substack{n \in \mathbb{N}_+ \\ e_G^n = e_G}} n = 1$

i.e. $\text{ord}(x) = 1$

ii. Say $\text{ord}(x) = n$ so $x^n = e_G$

So $(x^{-1})^n = (x^n)^{-1} = e_G^{-1} = e_G$

So $\text{ord}(x^{-1}) \leq n$, if $\text{ord}(x^{-1}) = m < n$

$(x^{-1})^m = e_G$ so $x^m = e_G^{-1} = e_G$

So $x^m = e_G$ where $m < n$: contradiction

So $m = n$ i.e. $\text{ord}(x^{-1}) = \text{ord}(x)$

Say $\text{ord}(x) = \infty$, if $\exists m$ $\text{ord}(x^{-1}) = m$

i.e $(x^{-1})^m = e_G$ then $x^m = e_G^{-1} = e_G$

So $x^m = e_G$ where $m < \infty$

which is a contraduction, so $\text{ord}(x^{-1}) = \infty$

Proof cons: iii. say $\text{ord}(x \circ y) = n$

i.e. $(x \circ y)^n = e_G$,

since $(x \circ y)^n \circ x = (x \circ y) \circ \ldots \circ (x \circ y) \circ x$

$= x \circ (y \circ x) \circ \ldots \circ (y \circ x)$

$= x \circ (y \circ x)^n$

So $x \circ e_G = e_G \circ x = (x \circ y)^n \circ x$

$= x \circ (y \circ x)^n$

So $(y \circ x)^n = e_G$ so $\text{ord}(y \circ x) \leq n$

Say $\text{ord}(y \circ x) = m$ similarly $\text{ord}(x \circ y) \leq m$

hence $\text{ord}(x \circ y) = \text{ord}(y \circ x)$

Say $\text{ord}(x \circ y) = \infty$,

if $\exists m$ $\text{ord}(y \circ x) = m$

then, as shown above, $\text{ord}(x \circ y) = m < \infty$

which is a contradiction,

So $\text{ord}(x \circ y) = \text{ord}(y \circ x)$ ∎

Def: $(G, \circ)$: abelian $:=$ $\circ$: comm .

Theorem: $(G, \circ)$: abelian

$$\iff \forall_{x,y \in G} \; (x \circ y)^{-1} = x^{-1} \circ y^{-1} .$$

Proof: $(\Longrightarrow)$: $(x \circ y)^{-1} = y^{-1}_{\in G} \circ x^{-1}_{\in G} = x^{-1} \circ y^{-1}$

$(\Longleftarrow)$: $(x \circ y)^{-1} = x^{-1} \circ y^{-1}$

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

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

$$x \circ y = y \circ x \qquad \blacksquare$$

Theorem: $(G, \circ)$: group $\wedge$

$$\forall_{x,y \in G} (x \circ y)^2 = x^2 \circ y^2 \Longrightarrow (G, \circ) : \text{ab}$$

Proof:

$$(x \circ y)^2 = x^2 \circ y^2$$

$$(x \circ y) \circ (x \circ y) = (x \circ x) \circ (y \circ y)$$

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

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

$$e_G \circ (y \circ x) \circ e_G = e_G \circ (x \circ y) \circ e_G$$

$$y \circ x = x \circ y \qquad \blacksquare$$

Theorem: $(G,\circ)$: group $\wedge$ $\forall x_{\in G}\ x = x^{-1}$

$\Longrightarrow (G,\circ)$: ab .

Proof: let $x, y \in G$;

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

$= ((y \circ x)^{-1})^{-1} = y \circ x$ ■

Theorem: $(G,\circ)$: ab $\wedge$ $H = \{x_{\in G} \mid x = x^{-1}\}$

$\Longrightarrow H \leq G \wedge (H,\circ)$: ab .

Proof: $\forall x,y_{\in H}\ x \circ y = x^{-1} \circ y^{-1} = (y \circ x)^{-1}$

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

so H: closed under $\circ$

i.e. $\circ(H \times H) \subseteq H$

also $e_G \in H$ as $e_G = e_G^{-1}$

since $e_G \circ e_G^{-1} = e_G = e_G \circ e_G$

also $\forall x_{\in H}\ \exists x^{-1}_{\in H\ (=x)}$ x^{-1}: inv of x

also $\circ$: asso by hypo

so $(H_{\leq G}, \circ)$: group so $H \leq G$

also $\circ$: comm by hypo

so $(H,\circ)$: ab ■

Def: $(G, \circ)$: group, $S, T \leq G$;

$$S \circ T := \{ x \circ y \mid x \in S \wedge y \in T \}$$

Theorem: $(G, \circ)$: ab $\wedge$ $S, T \leq G$

$$\Longrightarrow (S \circ T, \circ) \leq_{ab} G$$

Proof: since $S, T \subseteq G$

and G : closed under $\circ$, $S \circ T \subseteq G$

let $a, b \in S \circ T$, since $\circ$: comm

$$a \circ b = (x_1 \circ y_1) \circ (x_2 \circ y_2)$$

$$= (x_1 \circ x_2)_{\in S} \circ (y_1 \circ y_2)_{\in T} \in S \circ T$$

so $S \circ T$: closed under $\circ$

also $e_G \in S \circ T$ since $e_G = e_{G \in S} \circ e_{G \in T}$

let $a \in S \circ T$,

$$a^{-1} = (x \circ y)^{-1} = y^{-1} \circ x^{-1}$$

$$= x^{-1}_{\in S} \circ y^{-1}_{\in T} \in S \circ T$$

so $(S \circ T, \circ) \leq_{ab} G$. ■

Theorem: $(G, \circ)$: non-ab $\implies |G| \geq 5$

Proof: suppose $(G, \circ)$: non-ab

so $\exists a, b \in G \quad a \circ b \neq b \circ a$

$a \neq e_G$: otherwise $b \neq b$ as $e_G \circ b \neq b \circ e_G$

$b \neq e_G$: otherwise $a \neq a$ as $a \circ e_G \neq e_G \circ a$

$a \neq b$: otherwise $a^2 \neq a^2$ and $b^2 \neq b^2$

so $\{e_G, a, b\} \subseteq G$

$a \circ b \neq a$: otherwise $b = e_G$

$a \circ b \neq b$: otherwise $a = e_G$

$b \circ a \neq a$: otherwise $b = e_G$

$b \circ a \neq b$: otherwise $a = e_G$

if $a \circ b = e_G$ and $b \circ a = e_G$

then $e_G \neq e_G$

also $a \circ b = e_G \iff b \circ a = e_G$

since $a = b^{-1} \iff a^{-1} = (b^{-1})^{-1}$

$\iff a^{-1} = b$

so $a \circ b \neq e_G$ and $b \circ a \neq e_G$

so $\{e_G, a, b, a \circ b, b \circ a\} \subseteq G$ ∎

Def: $(S_n, \circ)$: sym group, where

$$S_n = \{\sigma^{bij}_{\{1,\dots,n\}\to\{1,\dots,n\}}\}$$

$$\sigma_1 \circ \sigma_2 (x) = \sigma_1(\sigma_2(x)) .$$

Theorem: $|S_n| = n!$.

Proof: every $\sigma \in S_n$ has the form :

$$\sigma = \begin{pmatrix} 1 & \dots & n \\ x_1 & \dots & x_n \end{pmatrix}$$

where x_j vary over $\{1,\dots,n\} \setminus \{x_1,\dots,x_{j-1}\}$

since $\sigma \in S_n$: bij

which produce $n!$ distinct ordering ∎

Def: $(S_X, \circ)$: perm group on X, where

$$S_X = \{\sigma^{bij}_{X\to X}\}, \quad \sigma_1 \circ \sigma_2 (x) = \sigma_1(\sigma_2(x)) .$$

Def: $D_n = \langle \alpha, \beta : \alpha^n = \beta^2 = e, \beta\alpha\beta = \alpha^{-1} \rangle$

Theorem: $G_\omega = \{\sigma \in S_\Omega \mid \sigma(\omega) = \omega\}$

$\Longrightarrow G_\omega \leq S_\Omega$

Proof: let $\sigma_1, \sigma_2 \in G_\omega$,

then $\sigma_1 \circ \sigma_2(\omega) = \sigma_1(\sigma_2(\omega))$

$= \sigma_1(\omega) = \omega$

so $\sigma_1 \circ \sigma_2 \in G_\omega$ i.e. G_ω: closed under $\circ$

also, $id \in G_\omega$ since $id(\omega) = \omega$

also, $\sigma(\omega) = \omega$ implies

$\sigma^{-1}(\sigma(\omega)) = \sigma^{-1}(\omega)$ so $\omega = \sigma^{-1}(\omega)$

so $\sigma^{-1} \in G_\omega$,

hence $(G_\omega \leq S_\Omega, \circ)$: group

so $G_\omega \leq S_\Omega$ ∎

Def: $\sigma \in S_X$: k-cycle $:= \exists S \subseteq X$:

$\sigma(s_i) = s_{i+1} \quad 0 \leq i < k \;\wedge$

$\sigma(s_{k-1}) = s_0 \quad \wedge \quad \sigma_{|X \setminus S} = id$.

Def: $(a_1 \dots a_n), (b_1 \dots b_m)$: disjoint :=

$\forall i \in \{1,\dots,n\}, j \in \{1,\dots,m\} \quad a_i \neq b_j$.

Theorem: $n \geq 3 \Rightarrow (S_n, \circ)$: non-ab .

Proof: consider $(1\,2), (1\,3) \in S_n$,

$$(1\,2) \circ (1\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2)$$

$$(1\,3) \circ (1\,2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$$

So $(1\,2) \circ (1\,3) \neq (1\,3) \circ (1\,2)$

Since $(1\,3\,2) \neq (1\,2\,3)$

So $(S_n, \circ)$: non-ab ■

Theorem: α, β : disjoint $\Longrightarrow \alpha \circ \beta = \beta \circ \alpha$.

Proof: let $\alpha = (a_1 \dots a_s)$ and $\beta = (b_1 \dots b_t)$

note, by hypo, $\forall i_{\in\{1,\dots,s\}}, j_{\in\{1,\dots,t\}}\ a_i \neq b_j$

also note

$$\alpha(x) = \begin{cases} x, & \forall i\ x \neq a_i \\ a_i \end{cases} \qquad \beta(x) = \begin{cases} x, & \forall j\ x \neq b_j \\ b_j \end{cases}$$

consider $\alpha \circ \beta$ and $\beta \circ \alpha$

i. $x \neq a_i \wedge x \neq b_j \Longrightarrow \alpha \circ \beta(x) = \alpha(\beta(x))$

$= \alpha(x) = x = \beta(x) = \beta(\alpha(x)) = \beta \circ \alpha(x)$

ii. $x = a_{i_0} \wedge x \neq b_j \Longrightarrow \alpha \circ \beta(x) = \alpha(\beta(x))$

$= \alpha(x) = a_{i_1} = \beta(a_{i_1}) = \beta(\alpha(x))$

$= \beta \circ \alpha(x)$

iii. $x \neq a_i \wedge x = b_{j_0} \Longrightarrow \alpha \circ \beta(x) = \alpha(\beta(x))$

$= \alpha(b_{j_1}) = b_{j_1} = \beta(x) = \beta(\alpha(x))$

$= \beta \circ \alpha(x)$

iv. $x = a_{i_0} \wedge x = b_{j_0} \Longrightarrow a_{i_0} \neq b_{j_0}$ by hypo

So $\alpha \circ \beta = \beta \circ \alpha$ ■

Theorem: α, β : disjoint

$$\Longrightarrow \forall m>0 \quad (\alpha \circ \beta)^m = \alpha^m \circ \beta^m \ .$$

Proof: $\alpha \circ \beta = \beta \circ \alpha$ since α, β : disjoint

so $(\alpha \circ \beta)^m = (\alpha \circ \beta) \circ \ldots \circ (\alpha \circ \beta)$

$= (\alpha \circ \ldots \circ \alpha) \circ (\beta \circ \ldots \circ \beta)$

$= \alpha^m \circ \beta^m$ ∎

Theorem: α, β : disjoint $\wedge$ $\varepsilon := id_{\{1,\ldots,n\}}$

$\wedge$ $\alpha \circ \beta = \varepsilon \Longrightarrow \alpha = \beta = \varepsilon$.

Proof: suppose $\alpha \neq \varepsilon$,

so $\exists x_{\in\{1,\ldots,n\}}\ \alpha(x) \neq x$, so by def of α

$\exists i_0\ \alpha(x) = a_{i_0}$ where $a_{i_0} \neq x$

i.e. $\exists i_1\ x = a_{i_1}$ i.e. $\forall j\ x \neq b_j$

so $\beta(x) = x$ so $\alpha(\beta(x)) = \alpha(x) = a_{i_0}$

so $\alpha \circ \beta(x) = a_{i_0 (\neq x)}$: contradicts hypo

so $\alpha = \varepsilon$

Proof cont'd: suppose $\beta \neq \varepsilon$,

so $\exists x_{\in\{1,\dots,n\}}\ \beta(x) \neq x$

so, by def of β, $\exists j_0\ \beta(x) = b_{j_0}$

where $b_{j_0} \neq x$, since $\alpha(b_{j_0}) = b_{j_0}$

$$\alpha(\beta(x)) = \alpha(b_{j_0}) = b_{j_0}$$

so $\alpha \circ \beta(x) = b_{j_0(\neq x)}$: contradicts hypo

so $\beta = \varepsilon$

hence $\alpha = \beta = \varepsilon$ ∎

Theorem: $\sigma_{\in S_n} \neq id_{\{1,\dots,n\}} \Longrightarrow \sigma = \prod_j c_j$.

c_j: cycle
c_i, c_k: disjo
finite

Proof: by hypo $\exists x\ \sigma(x) \neq x$,

let $a_1 = \min_{\sigma(x)\neq x} x$ so $\exists a_{2(\neq a_1)}\ \sigma(a_1) = a_2$

so $\sigma(a_2) \neq a_2$, as σ: bij and $a_2 \neq a_1$:

if $\sigma(a_2) = a_1$, say $c_0 = (a_1 a_2)$

if not, with same process,

$a_1 \to a_2 \to \dots \to a_k \to a_1$, say $c_0 = (a_1 \dots a_k)$

if c_0: n-cycle, already $\sigma = c_0$

or if c_0: k-cycle but $\sigma_{|\{1,\dots,n\}\setminus\{a_1,\dots,a_k\}} = id_{\{1,\dots,n\}}$

then again $\sigma = c_0$

Proof cont'd : if not,

i.e. c_0 : k-cycle and $\exists y_{\in \{1,\dots,n\}\setminus\{a_1,\dots,a_k\}}$

such that $\sigma(y) \neq y$;

let $b_1 = \min_{\substack{\sigma(y)\neq y \\ y\in\{1,\dots,n\}\setminus\{a_1,\dots,a_k\}}} y$, via same way

$c_1 = (b_1, \dots, b_q)$: q-cycle where $2 \leq q \leq n-k$

note $b_2 \notin c_0$ since $\sigma^{-1}(b_2) = b_1 \notin c_0$

Similarly $\forall_j\ b_j \notin c_0$ so c_0, c_1 : disjoint

if $q = n-k$:

$$\sigma = \begin{pmatrix} a_1 \dots a_k\ b_1 \dots b_q \\ a_2 \dots a_1\ b_2 \dots b_1 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 \dots a_k\ i_{k+1} \dots i_n \\ a_2 \dots a_1\ i_{k+1} \dots i_n \end{pmatrix} \circ \begin{pmatrix} i_1 \dots i_k\ b_1 \dots b_q \\ i_1 \dots i_k\ b_2 \dots b_1 \end{pmatrix}$$

$$= c_0 \circ c_1$$

if not, produce c_2 which is of course disjoint from both c_0 and c_1 in the way c_0, c_1 : disjoint,

so, either $\sigma = c_0 \circ c_1 \circ c_2$ or

$\sigma = \circ_j c_j$

Def: c : transposition := c : 2-cycle

Theorem: $|\{ \tau_i \mid_{i \in \mathbb{N}} \tau_i : tra_{\{1,\dots,n\}} \wedge \tau_j \neq \tau_k \}|$

$$= \sum_{k=1}^{n-1} k \quad .$$

Proof: every transposition will be

of the form $(a\,b)$,

set $a=1$, then $\forall b_{\neq 1}\,(1\,b) : tra$,

set $a=2$, then $\forall b_{\neq 2, \neq 1}\,(2\,b) : tra$

note $(2\,1)_{(=(12))}$ not included

so when $a=k$, $n-k$ tra

of the form $(k\,b)$ exist where $k < b \leq n$

producing total nuber of

$\sum_{k=1}^{n-1} k$ distinct transpositions ∎

Theorem: $(a\,b) : \mathrm{tra} \wedge \varepsilon = id_{\{1,\dots,n\}}$

$\Longrightarrow (a\,b) \circ (a\,b) = \varepsilon$.

Proof: say $\sigma = (a\,b)$,

$\sigma \circ \sigma\,(a) = \sigma(\sigma(a)) = \sigma(b) = a$

$\sigma \circ \sigma\,(b) = \sigma(\sigma(b)) = \sigma(a) = b$

$\sigma \circ \sigma\,(x \neq_b^{\neq a}) = \sigma(\sigma(x)) = \sigma(x) = x$

So $\sigma \circ \sigma = \varepsilon$ ■

Theorem: $(a\,b), (b\,c) : \mathrm{tra} \wedge a \neq b \neq c$

$\Longrightarrow (a\,b) \circ (b\,c) = (a\,b\,c)$.

Proof: say $\sigma_0 = (a\,b)$ and $\sigma_1 = (b\,c)$

$\sigma_0 \circ \sigma_1\,(a) = \sigma_0(\sigma_1(a)) = \sigma_0(a) = b$

$\sigma_0 \circ \sigma_1\,(b) = \sigma_0(\sigma_1(b)) = \sigma_0(c) = c$

$\sigma_0 \circ \sigma_1\,(c) = \sigma_0(\sigma_1(c)) = \sigma_0(b) = a$

So $\sigma_0 \circ \sigma_1 = (a\,b\,c)$ ■

Theorem: C : s-cycle

$$\Longrightarrow C = \underset{j\in[s-1]}{\circ} (a_s a_j)$$

Proof: define

$$\sigma_0 = \underset{j\in[s-1]}{\circ} (a_s a_j)$$

compute: $\sigma_0(a_i)$, where $i \neq s$:

$$\sigma_0(a_i) = \underset{j\in[s-1]}{\circ} (a_s a_j)(a_i)$$

$$= (a_s a_{s-1}) \circ \dots \circ (a_s a_1)(a_i)$$

since $\forall_{q\in[i-1]} (a_s a_q)(a_i) = a_i$,

$$= (a_s a_{s-1}) \circ \dots \circ (a_s a_i)(a_i)$$

since $(a_s a_i)(a_i) = a_s$,

$$= (a_s a_{s-1}) \circ \dots \circ (a_s a_{i+1})(a_s)$$

since $(a_s a_{i+1})(a_s) = a_{i+1}$,

$$= (a_s a_{s-1}) \circ \dots \circ (a_s a_{i+2})(a_{i+1})$$

since $\forall_{\omega\in[i+2,s]} (a_s a_\omega)(a_{i+1}) = a_{i+1}$,

$$= a_{i+1}$$

so $\forall_{i\neq s}\ \sigma_0(a_i) = a_{i+1}$

Proof cont'd: also compute

$$\sigma_0(a_s) = \underset{j\in[s-1]}{\circ} (a_s a_j)$$

$$= (a_s a_{s-1}) \circ \dots \circ (a_s a_1)(a_s)$$

Since $(a_s a_1)(a_s) = a_1$,

$$= (a_s a_{s-1}) \circ \dots \circ (a_s a_2)(a_1)$$

Since $\forall k_{\in[2,s]} (a_s a_k)(a_1) = a_1$,

$$= a_1$$

So $\sigma_0(a_s) = a_1$

hence $\sigma = \sigma_0$ ∎

Def: $\sigma_{\in S_n} := \circ_K t_i$ where t_i: tra

$$\text{sign}(\sigma) := \begin{cases} 1, & K \in 2\mathbb{Z} \\ -1, & K \in \mathbb{Z} \setminus 2\mathbb{Z} \end{cases}$$

Theorem: $\varepsilon_{\in S_n} = \underset{\substack{i \in [K] \\ t_i : \text{tra}}}{\circ} t_i \Longrightarrow \exists \{s_i\}_{[K-2]} : \varepsilon = \underset{\substack{i \in [K-2] \\ s_i : \text{tra}}}{\circ} s_i$

Proof:

pick $x_{\in [K]}$ such that $\exists i \; t_i = (x \; *)$

define $j := \max_{t_i = (x *)} i$ so $\exists a_{\in [K]} \; t_i = (x \; a)$

say $t_{j-1} = (y \; b)$,

i. $y = x \wedge b = a$,

i.e. $t_{j-1} = t_j$ so $t_{j-1} \circ t_j = \varepsilon$;

$$\varepsilon = \left(\underset{i \in [j-2]}{\circ} t_i \right) \circ \underbrace{\left(t_{j-1} \circ t_j \right)}_{(=\varepsilon)} \circ \left(\underset{i \in [j+1, K]}{\circ} t_i \right)$$

$$= \underset{i \in [K] \setminus \{j-1, j\}}{\circ} t_i$$

ii. $y = x \wedge b \neq a$,

i.e. $t_{j-1} = (x \; b)$, so

$$t_{j-1} \circ t_j = (x b) \circ (x a) = (b x) \circ (x a)$$

$$= (b \; x \; a) = (x \; a \; b)$$

$$= (x a) \circ (a b)$$

note $(b x a) \equiv a^{G_x} b \equiv (x \; a \; b)$

Proof cont'd : so $t_{j-1} \circ t_j = (x\,a) \circ (a\,b)$

so $\varepsilon = \left(\underset{i \in [j-2]}{\circ} t_i\right) \circ (x\,a) \circ (a\,b) \circ \left(\underset{i \in [j+1,\kappa]}{\circ} t_i\right)$

but now, $j-1 = \max_{t_i = (x\,*)} i$

iii. $y \neq x \wedge b = a$,

i.e. $t_{j-1} = (y\,a)$, so

$t_{j-1} \circ t_j = (y\,a) \circ (x\,a) = (y\,a) \circ (a\,x)$

$= (y\,a\,x) = (x\,y\,a)$

$= (x\,y) \circ (y\,a)$

note $(y\,a\,x) \equiv {}^{x}_{y}\!\circlearrowleft_{a} \equiv (x\,y\,a)$

so $t_{j-1} \circ t_j = (x\,y) \circ (y\,a)$

so $\varepsilon = \left(\underset{i \in [j-2]}{\circ} t_i\right) \circ (x\,y) \circ (y\,a) \circ \left(\underset{i \in [j+1,\kappa]}{\circ} t_i\right)$

but now, $j-1 = \max_{t_i = (x\,*)} i$

iv. $y \neq x \wedge b \neq a$,

i.e. $t_{j-1} = (y\,b)$, so

$t_{j-1} \circ t_j = (y\,b) \circ (x\,a) = (x\,a) \circ (y\,b)$

so $t_{j-1} \circ t_j = (x\,a) \circ (y\,b)$

so $\varepsilon = \left(\underset{i \in [j-2]}{\circ} t_i\right) \circ (x\,a) \circ (y\,b) \circ \left(\underset{i \in [j+1,\kappa]}{\circ} t_i\right)$

but now, $j-1 = \max_{t_i = (x\,*)} i$

Proof cont'd :

applying ii, iii, iv shifts $(x\ *)$

to one left, once i applies

the claim gets concluded

Suppose $t_2 = (x\ \omega)$ after some

number of ii, iii, iv ; i.e. $\max_{t_i=(x\,*)} i = 2$,

note $\max_{t_i=(x\,*)} i \neq 1$ holds always,

because otherwise $x = \varepsilon(x) = \omega \neq x$,

then $\varepsilon = (*\ *) \circ (x\ \omega) \circ (\bigcirc_{i\in[3,\kappa]} t_i)$

so $x = \varepsilon(x) = (*\ *) \circ (x\ \omega)(x)$

$= (*\ *)(\omega)$

hence $t_1 = (x\ \omega)$ so the conclusion

via i, so say i has applied to $h, h-1$

then $\varepsilon = \bigcirc_{i\in[\kappa]\setminus\{h-1,h\}} t_i$ ∎

Theorem: $\text{sign}(\varepsilon) = 1 \wedge \text{sign}(\varepsilon) \neq -1$.

Proof: $\varepsilon = \underset{i \in [2]}{\circ} t_i = (a\,b) \circ (a\,b)$

since $2 \in 2\mathbb{Z}$, $\text{sign}(\varepsilon) = 1$

also $\text{sign}(\varepsilon) \neq -1$

since otherwise following contradiction would be reached:

suppose $\varepsilon = \underset{i \in [k]}{\circ} t_i$ where $k \in \mathbb{Z} \setminus 2\mathbb{Z}$

since $\forall \sigma \in S_n : \sigma = \underset{i \in [q]}{\circ} t_i \Longrightarrow \sigma = \underset{i \in [q] \setminus \{q_0, q_1\}}{\circ} t_i$

applying that $\frac{k-1}{2}$ times implies that

$\varepsilon = \underset{i \in [1]}{\circ} t_i = t_1 = (a\,b)$

but $a = \varepsilon(a) = t_1(a) = b \neq a$

implies the contradiction referred above ∎

Theorem: $\sigma \in S_n$

$\Longrightarrow$ $\text{Sign}(\sigma) = 1$ $\veebar$ $\text{Sign}(\sigma) = -1$

Proof: Suppose otherwise,

say $\sigma = \circ_1^{\kappa} t_i$ and $\sigma = \circ_1^{j} u_i$

where $\kappa \in 2\mathbb{Z}$ and $j \in \mathbb{Z} \setminus 2\mathbb{Z}$

note $\sigma^{-1} = (\circ_1^{j} u_i)^{-1} = \circ_1^{1} u_i^{-1}$,

So $\varepsilon = \sigma \circ \sigma^{-1} = (\circ_1^{\kappa} t_i) \circ (\circ_1^{1} u_i^{-1})$

$= \circ_1^{\kappa + j} s_i$

Since $\kappa_{\in 2\mathbb{Z}} + j_{\in \mathbb{Z} \setminus 2\mathbb{Z}} \in \mathbb{Z} \setminus 2\mathbb{Z}$,

$\text{Sign}(\varepsilon) = -1$

but it has shown that

$\text{Sign}(\varepsilon) \neq -1$ ∎

Theorem: $\sigma \in S_n$: s-cycle

$$\Longrightarrow \operatorname{sign}(\sigma) = \begin{cases} 1, & s \in \mathbb{Z} \setminus 2\mathbb{Z} \\ -1, & s \in 2\mathbb{Z} \end{cases}$$

Proof: say $\sigma = (\alpha_1, \ldots, \alpha_s)$

so $\sigma = \alpha_1^{s-1}(\alpha_s \alpha_i)$

so $\operatorname{sign}(\sigma) = \begin{cases} 1, & s-1 \in 2\mathbb{Z} \\ -1, & s-1 \in \mathbb{Z} \setminus 2\mathbb{Z} \end{cases}$

so $\operatorname{sign}(\sigma) = \begin{cases} 1, & s \in 2\mathbb{Z} \\ -1, & s \in \mathbb{Z} \setminus 2\mathbb{Z} \end{cases}$ ∎

Theorem: α, β : cycle

$$\Longrightarrow \operatorname{sign}(\alpha \circ \beta) = \begin{cases} 1, & \operatorname{sign}(\alpha) = \operatorname{sign}(\beta) \\ -1, & \operatorname{sign}(\alpha) \neq \operatorname{sign}(\beta) \end{cases}$$

Proof: say α : k-cycle

and β : j-cycle so $\alpha \circ \beta$: $(k+j)$-cycle

if $\operatorname{sign}(\alpha) = \operatorname{sign}(\beta)$,

either $k, j \in 2\mathbb{Z}$ or $k, j \in \mathbb{Z} \setminus 2\mathbb{Z}$

so $k + j \in 2\mathbb{Z}$ so $\operatorname{sign}(\alpha \circ \beta) = 1$

if $\operatorname{sign}(\alpha) \neq \operatorname{sign}(\beta)$,

either $k \in 2\mathbb{Z} \wedge j \in \mathbb{Z} \setminus 2\mathbb{Z}$ or vice versa

so $k + j \in \mathbb{Z} \setminus 2\mathbb{Z}$ so $\operatorname{sign}(\alpha \circ \beta) = -1$ ∎

Def: $(A_n, \circ)$: alternating group :=

$$A_n \leq S_n = \{\sigma \in S_n \mid \operatorname{sign}(\sigma) = 1\}$$

Theorem: $A_n \leq S_n$.

Proof: let $\sigma, \gamma \in A_n$, say $\sigma = \circ_1^k t_i$

and $\gamma = \circ_1^j u_i$ so $\sigma \circ \gamma = \circ_1^{k+j} s_i$

where $k+j \in 2\mathbb{Z}$ so $\operatorname{sign}(\sigma \circ \gamma) = 1$

so $(\sigma \circ \gamma) \in A_n$

so A_n: closed under $\circ$,

also $\varepsilon \in A_n$ since $\operatorname{sign}(\varepsilon) = 1$ as shown

also $\forall \sigma_{\in A_n} \sigma^{-1} \in A_n$, since otherwise :

suppose $\sigma^{-1} \notin A_n$ so $\operatorname{sign}(\sigma^{-1}) = -1$

say $\sigma = \circ_1^k t_i$ and $\sigma^{-1} = \circ_1^j u_i$

so $\varepsilon = \sigma \circ \sigma^{-1} = \circ_1^{k+j} s_i$

note $k+j \in \mathbb{Z} \setminus 2\mathbb{Z}$ so $\operatorname{sign}(\varepsilon) = -1$

but actually $\operatorname{sign}(\varepsilon) \neq -1$: contradiction

so $A_n \leq S_n$ ■

Theorem: $|A_n| = |S_n \setminus A_n| = \frac{n!}{2}$.

Proof: define $B_n := S_n \setminus A_n$

define $f : A_n \to B_n$, fixing $\omega_{\in B_n}$: tra

$$f(\sigma) = \omega \circ \sigma$$

f: inj ; let $\sigma_1, \sigma_2 \in A_n$

$$f(\sigma_1) = f(\sigma_2)$$

$$\omega \circ \sigma_1 = \omega \circ \sigma_2$$

since $\circ$: group op

$$\sigma_1 = \sigma_2$$

f: surj ; let $\gamma \in B_n$, then $\omega \circ \gamma \in A_n$

note $\omega \circ \omega = \varepsilon$,

so $f(\omega \circ \gamma) = \omega \circ \omega \circ \gamma = \varepsilon \circ \gamma = \gamma$

so $\exists s^{(=\omega\circ\gamma)}_{\in A_n} : f(s) = \gamma$

so $f_{A_n \to B_n}$: bij , also note $|S_n| = n!$

so $|A_n| = |B_n| = \frac{n!}{2}$ ■

Theorem: α, β : s-cycles

$$\Longrightarrow \exists \sigma_{\in S_n} \forall i_{\in [s]}\ \sigma(a_i) = b_i$$

Proof: define $\sigma_{[n]\to[n]}$:

$$\sigma(x) = \begin{cases} b_i\ , & \exists i_{\in[s]}\ x = a_i \\ \xi(b_j) & \exists j_{\in[s]}\ x = b_j \wedge \forall i_{\in[s]}\ x \neq a_i \\ x\ , & \forall i_{\in[s]} : x \neq a_i \wedge x \neq b_i \end{cases}$$

define $\mathcal{A} = \{ x \mid \alpha(x) \neq x \}$

$$\mathcal{B} = \{ x \mid \beta(x) \neq x \}$$

$$\mathcal{A}^- = \mathcal{A} \setminus \mathcal{B} \qquad \mathcal{B}^- = \mathcal{B} \setminus \mathcal{A}$$

$$C = [n] \setminus (\mathcal{A} \cup \mathcal{B})$$

note $\sigma_{|\mathcal{A}} : b_{ij}$ and $\sigma_{|C} : b_{ij}$

and $\sigma_{|\mathcal{B}^-} = \xi_{\mathcal{B}^- \to \mathcal{A}^-}$

define $\psi_{0\ \{j \mid b_j \in \mathcal{B}^-\} \to [|\mathcal{B}^-|]}$: $\psi_0(j) = \max\limits_{\substack{\forall S \in S_{\subseteq \mathcal{B}^-} \\ s \leq j}} |S|$

and $\psi_{1\ [|\mathcal{A}^-|] \to \{i \mid a_i \in \mathcal{A}^-\}}$:

$$\psi_1(m) = i : \max_{\substack{\forall s \in S_{\subseteq \mathcal{A}^-} \\ s \in i}} |S| = m$$

define $\xi(b_j) = a_{\psi_1 \circ \psi_0(j)}$ so $\xi : b_{ij}$

so $\sigma : b_{ij}$ so $\sigma \in S_n$ ∎

Def: $\sigma \in S_n$, $\alpha_{\in S_n}$: cycle ;

$\rho_{\in S_n} = \sigma \circ \alpha \circ \sigma^{-1}$: conjugate of α by σ ...

Theorem: α, β : s-cycles $\wedge$ $\forall i_{\in [s]}\ \sigma_{\in S_n}(a_i) = b_i$

$\Longrightarrow \beta = \sigma \circ \alpha \circ \sigma^{-1}$.

Proof: note $\forall i_{\in [s]}\ \sigma^{-1}(b_i) = a_i$ as $\sigma_{\in S_n}$: bij ,

if $i \in [s-1]$,

$$[\sigma \circ \alpha \circ \sigma^{-1}](b_i) = [\sigma \circ \alpha](a_i)$$

$$= \sigma(a_{i+1}) = b_{i+1}$$

if $i = s$,

$$[\sigma \circ \alpha \circ \sigma^{-1}](b_s) = [\sigma \circ \alpha](a_s)$$

$$= \sigma(a_1) = b_1$$

assume $x \notin \{b_i\}_{i \in [s]}$, say $\sigma^{-1}(x) = y$

note $y \notin \{a_i\}_{i \in [s]}$, otherwise say $y = a_j$

$b_j = \sigma(y) = x_{\notin \{b_i\}_{i \in [s]}}$: contradiction

so $[\sigma \circ \alpha \circ \sigma^{-1}](x) = [\sigma \circ \alpha](y)$

$$= \sigma(y) = x$$

so $\sigma \circ \alpha \circ \sigma^{-1} = \beta$ ■

Theorem: $\alpha = (ab) \Longrightarrow ord(\alpha) = 2$.

Proof: note $ord(\sigma) = 1$ iff $\sigma = \varepsilon (= e_{S_n})$

so $ord(\alpha) \geq 2$ as $(ab) \neq \varepsilon$

also $ord(\alpha) \leq 2$ since $\alpha^2 = \varepsilon$

so $ord(\alpha) = 2$ ∎

Theorem: α : s-cycle $\Longrightarrow ord(\alpha) = s$ ..

Proof: $ord(\alpha) \leq s$ since $\forall_{i \in [s]} \alpha^s(a_i) = a_i$

assume $ord(\alpha) = m < s$

i.e. $\alpha^m = \varepsilon$ but $\alpha^m(a_1) = a_{m+1}$

since $a_1 \neq a_{m+1}$, $\alpha^m \neq \varepsilon$: contradiction

so $ord(\alpha) = s$ ∎

Def: $lcm(\{x_i\}) = \min_{\forall i\ x_i | m} m$

$gcd(\{x_i\}_i) = \max_{\forall_i d | x_i} d$

$q_0 | q_1 := \exists s\ q_1 = s q_0$

$x \equiv_n y := n | (x - y)$

Theorem: $\sigma \in S_n = \prod_{\substack{c_j:\text{cycle} \\ c_i, c_k:\text{disjo} \\ \text{finite}}} c_j$

$\Rightarrow \operatorname{ord}(\sigma) = \operatorname{lcm}(\{\operatorname{ord}(c_j)\}_j)$

Proof: denote $\forall j \; m_j = \operatorname{ord}(c_j)$

say $m = \operatorname{ord}(\sigma)$,

$\varepsilon = \sigma^m = (\prod_j c_j)^m = \prod_j c_j^m$

so $\forall j \; c_j^m = \varepsilon$,

$\forall j \; \exists \omega_j, r_j : 0 \le r_j < m_j$

$m = \omega_j m_j + r_j$

so $\varepsilon = c_j^m = c_j^{\omega_j m_j + r_j} = c_j^{\omega_j m_j} \circ c_j^{r_j}$

$= (c_j^{m_j})^{\omega_j} \circ c_j^{r_j} = \varepsilon^{\omega_j} \circ c_j^{r_j}$

$= \varepsilon \circ c_j^{r_j} = c_j^{r_j}$

so $c_j^{r_j} = \varepsilon$ but $r_j < m_j$ so $r_j = 0$

so $\forall j \; m_j \mid m$

so $m = \operatorname{lcm}(\{m_j\}_j)$ ∎

Def: $f_{(G,\cdot)\to(H,*)}$: homomorphism :=

$\forall x,y \in G \quad f(x\cdot y) = f(x) * f(y)$.

Prop: $f_{(G,\cdot)\to(H,*)}$: homo $\Longrightarrow f(e_G) = e_H$.

Proof: $e_G \xrightarrow{f} e_H$:

$$e_H * f(e_G) = f(e_G) = f(e_G \cdot e_G)$$
$$= f(e_G) * f(e_G)$$
$$\Longrightarrow e_H = f(e_G)$$

■

Prop: $f_{(G,\cdot)\to(H,*)}$: homo $\Longrightarrow \forall x \in G \quad f(x^{-1}) = [f(x)]^{-1}$

Proof: $x \in G$,

$$f(x^{-1}) * f(x) = f(x^{-1}\cdot x) = f(e_G)$$
$$= e_H = [f(x)]^{-1} * f(x)$$
$$\Longrightarrow f(x^{-1}) = [f(x)]^{-1}$$

■

Prop: $f_{(G,\cdot)\to(H,*)}$: homo $\Longrightarrow \forall x \in G \quad f(x^n) = [f(x)]^n$

Proof: $x \in G$,

$$f(x^n) = f(\cdot_n x) = *_n f(x) = [f(x)]^n$$

■

Prop: $f_{G\to H}$: homo $\wedge$ $S \le G \implies f(S) \le H$.

Proof: $f(S)$: closed under $*$,

otherwise, $\exists \omega_0, \omega_1 \in f(S)$: $\omega_0 * \omega_1 \notin f(S)$

note $\forall \omega_i \in f(S)\ \exists s_i \in S$: $f(s_i) = \omega_i$

so $\exists s_0, s_1 \in S$ $f(s_0) * f(s_1) \notin f(S)$

so $f(s_0 \cdot s_1)\ (= f(s_0) * f(s_1)) \notin f(S)$

also, since S: closed under $\cdot$ as $S \le G$

$s_0 \cdot s_1 \in S$ so $f(s_0 \cdot s_1) \in f(S)$: contradiction

also, since $e_G \in S$ as $S \le G$,

$e_H\ (= f(e_G)) \in f(S)$,

also, $\forall \omega \in f(S)\ \exists s \in S$: $f(s) = \omega$

so $\exists \omega^{-1}\ (= f(s^{-1}))$:

$\omega * \omega^{-1} = e_H = \omega^{-1} * \omega$,

hence $f(S) \le H$ ■

Prop: $f_{G \to H}$: homo $\wedge$ $\Omega \leq H$

$\Longrightarrow$ $f^{-1}(\Omega) \leq G$.

Proof: $x, y \in f^{-1}(\Omega)$,

so $f(x), f(y) \in \Omega$, note since $\exists [f(y)]^{-1}_{\in \Omega}$:

$[f(y)]^{-1}$: inv of $f(y)$ as $\Omega_{\leq H}$: group

$f(y^{-1})_{(=[f(y)]^{-1})} \in \Omega$

so $f(x) * f(y^{-1}) \in \Omega$ as $\Omega_{\leq H}$: closed under $*$

so $f(x \cdot y^{-1})_{(= f(x) * f(y^{-1}))} \in \Omega$

so $x \cdot y^{-1} \in f^{-1}(\Omega)$

hence $f^{-1}(\Omega) \leq G$ ■

Def: $\ker(f_{G \to H}) := f^{-1}(\{e_H\})$.

Prop: $f_{G \to H}$ homo $\Longrightarrow$ $\ker(f) \leq G$.

Proof: $\ker(f) \neq \emptyset$ since $e_G (= f^{-1}(e_H)) \in \ker(f)$

Let $x, y \in \ker(f)$;

$$\begin{aligned} f(x \cdot y^{-1}) &= f(x) * f(y^{-1}) \\ &= f(x) * [f(y)]^{-1} \\ &= e_H * e_H^{-1} \\ &= e_H * e_H \\ &= e_H \end{aligned}$$

so $f(x \cdot y^{-1}) = e_H$ so $x \cdot y^{-1} \in \ker(f)$

hence $\ker(f) \leq G$ ■

Def: $f_{G \xrightarrow{=} H}$: monomorphism := f : inj

Def: $f_{G \xrightarrow{=} H}$: epimorphism := f : surj

Prop: $f_{G \xrightarrow{=} H}$: mono $\iff$ $\mathrm{Ker}(f) = \{e_G\}$.

Proof: ($\Longrightarrow$): let $x \in \mathrm{Ker}(f)$

so $f(x) = e_H (= f(e_G))$, note f : inj as f : mono

so by inj of f, $x = e_G$

hence $\mathrm{Ker}(f) = \{e_G\}$

($\Longleftarrow$): let $x, y \in G$,

suppose $f(x) = f(y)$, then

$$e_H = f(x) * [f(x)]^{-1} = f(x) * [f(y)]^{-1}$$

$$= f(x) * f(y^{-1}) = f(x \cdot y^{-1})$$

so $f(x \cdot y^{-1}) = e_H$

so $x \cdot y^{-1} \in \mathrm{Ker}(f) (= \{e_G\})$ so $x \cdot y^{-1} = e_G$

so $x = y$ so f : inj

hence f : mono ■

Def: $f_{G \xrightarrow{\cong} H}$: isomorphism := f : bij

Prop: $f_{G \to H}$: iso $\Longrightarrow$ $f^{-1}{}_{H \to G}$: iso .

Proof: let $h_0, h_1 \in H$,

since f : bij, f : surj so $\exists g_0, g_1 \in G$:

$f(g_0) = h_0 \wedge f(g_1) = h_1$,

so $f^{-1}(h_0 * h_1) = f^{-1}(f(g_0) * f(g_1))$

$= f^{-1}(f(g_0 \bullet g_1))$

$= g_0 \bullet g_1$

$= f^{-1}(f(g_0)) \bullet f^{-1}(f(g_1))$

$= f^{-1}(h_0) \bullet f^{-1}(h_1)$

so f^{-1} : homo,

also f^{-1} : bij since f : bij

hence f^{-1} : iso ■

Prop: $id_{G \to G}$: iso .

Proof: let $g_0, g_1 \in G$, $id(g_0 \bullet g_1) = g_0 \bullet g_1 = id(g_0) \bullet id(g_1)$

so id : homo, also id : bij, so id : iso ■

Prop: $f_{H \to K}$: iso $\wedge$ $g_{G \to H}$: iso

$\Longrightarrow f \circ g_{G \to K}$: iso .

Proof: let $\omega_0, \omega_1 \in G$,

$$\begin{aligned} f \circ g(\omega_0 \cdot \omega_1) &= f(g(\omega_0 \cdot \omega_1)) \\ &= f(g(\omega_0) * g(\omega_1)) \\ &= f(g(\omega_0)) \otimes f(g(\omega_1)) \\ &= f \circ g(\omega_0) \otimes f \circ g(\omega_1) \end{aligned}$$

so $f \circ g$: homo

also $f \circ g$: bij as f : bij and g : bij

hence $f \circ g$: iso ■

Prop: $\cong$: equivalence relation .

Proof: i. $G \underset{id}{\cong} G$

ii. $G \underset{f}{\cong} H \Longrightarrow H \underset{f^{-1}}{\cong} G$

iii. $G \underset{g}{\cong} H \wedge H \underset{f}{\cong} K \Longrightarrow G \underset{f \circ g}{\cong} K$ ■

Theorem: $G: ab \wedge H: non\text{-}ab$

$\Longrightarrow G \not\cong H$.

Proof: since $H: non\text{-}ab$,

$\exists h_0, h_1 \in H : h_0 * h_1 \neq h_1 * h_0$

Suppose $\exists f_{G \to H}\ f: iso$,

since $f: surj$ as $f: bij$, $\exists g_0, g_1 \in G$:

$f(g_0) = h_0 \wedge f(g_1) = h_1$

Since $G: ab$, $g_0 \cdot g_1 = g_1 \cdot g_0$

so $f(g_0 \cdot g_1) = f(g_1 \cdot g_0)$

also, $f(g_0 \cdot g_1) = f(g_0) * f(g_1)$

$= h_0 * h_1$

$\neq h_1 * h_0$

$= f(g_1) * f(g_0)$

$= f(g_1 \cdot g_0)$

so $f(g_0 \cdot g_1) \neq f(g_1 \cdot g_0)$: contradiction

hence $G \not\cong H$ ■

Theorem: $(G, \circledast) \cong (G^{\bullet}, \circ)$,

$$G^{\bullet} := \{ \sigma_{\omega} \mid \omega \in G \wedge \forall_{g \in G}\, \sigma_{\omega}(g) := \omega \bullet g \}$$

Proof: $G^{\bullet} \subset S_G$:

let $\sigma_{\omega\, G \to G} \in G^{\bullet}$, then σ_{ω}: bij;

σ_{ω}: inj; let $x, y \in G$

$$\sigma_{\omega}(x) = \sigma_{\omega}(y) \implies \omega \bullet x = \omega \bullet y$$

$$\implies x = y$$

σ_{ω}: surj; let $y \in G$ then $\exists x_{(= \omega^{-1} \bullet y)}^{\in G}$:

$$\sigma_{\omega}(x) = \sigma_{\omega}(\omega^{-1} \bullet y) = \omega \circledast \omega^{-1} \circledast y$$

$$= e_G \circledast y = y$$

$G^{\bullet} \leq S_G$:

i. $G^{\bullet}$: closed under $\circ$; let $\sigma_{\omega_0}, \sigma_{\omega_1} \in G^{\bullet}$,

$$(\sigma_{\omega_0} \circ \sigma_{\omega_1})(x) = \sigma_{\omega_0}(\sigma_{\omega_1}(x))$$

$$= \sigma_{\omega_0}(\omega_1 \circledast x)$$

$$= \omega_0 \circledast \omega_1 \circledast x$$

$$= \sigma_{\omega_0 \bullet \omega_1}(x)$$

Proof cont'd:

ii. $e_G \bullet = \sigma_{e_G}$;

$$\begin{aligned}(\sigma_\omega \circ \sigma_{e_G})(x) &= \sigma_\omega(\sigma_{e_G}(x)) = \sigma_\omega(e_G \otimes x) \\ &= \sigma_\omega(x) \\ &= e_G \otimes \sigma_\omega(x) = \sigma_{e_G}(\sigma_\omega(x)) \\ &= (\sigma_{e_G} \circ \sigma_\omega)(x)\end{aligned}$$

iii. $[\sigma_\omega]^{-1} = \sigma_{\omega^{-1}}$;

$$\begin{aligned}(\sigma_\omega \circ \sigma_{\omega^{-1}})(x) &= \sigma_\omega(\sigma_{\omega^{-1}}(x)) = \sigma_\omega(\omega^{-1} \otimes x) \\ &= \omega \otimes \omega^{-1} \otimes x = e_G \otimes x \\ &= x \\ &= e_G \otimes x = \omega^{-1} \otimes \omega \otimes x \\ &= \sigma_{\omega^{-1}}(\omega \otimes x) = \sigma_{\omega^{-1}}(\sigma_\omega(x)) \\ &= (\sigma_{\omega^{-1}} \circ \sigma_\omega)(x)\end{aligned}$$

Proof cont'd: let $f_{G \to G^\bullet}$: $f(\omega) = \sigma_\omega$

i. f: bij ;

i. f: inj ;

$$f(\omega_0) = f(\omega_1) \Longrightarrow \sigma_{\omega_0}(x) = \sigma_{\omega_1}(x)$$

$$\Longrightarrow \omega_0 \circledast x = \omega_1 \circledast x \Longrightarrow \omega_0 = \omega_1$$

ii. f: surj ;

$$y \in G^\bullet \Longrightarrow \exists \omega_{\in G}\ y = \sigma_\omega$$

$$\Longrightarrow f(\omega)_{(=\sigma_\omega)} = y$$

ii. f: homo ;

$$f(\omega_0 \circledast \omega_1) = \sigma_{\omega_0 \circledast \omega_1}(x)$$

$$= \omega_0 \circledast \omega_1 \circledast x$$

$$= \omega_0 \circledast \sigma_{\omega_1}(x) = \sigma_{\omega_0}(\sigma_{\omega_1}(x))$$

$$= (\sigma_{\omega_0} \circ \sigma_{\omega_1})(x)$$

$$= f(\omega_0) \circ f(\omega_1)$$

hence f: iso,

so $(G, \circledast) \underset{f}{\cong} (G^\bullet, \circ)$ ■

Def: $f_{G \xrightarrow{\cong} G}$: automorphism .

Prop: G : ab $\wedge$ $\mu_{G \to G} : x \mapsto x^{-1}$

$\Longrightarrow$ μ : auto .

Proof: μ : bij ;

μ : inj ; $\mu(x) = \mu(y) \Longrightarrow x^{-1} = y^{-1}$

$\Longrightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Longrightarrow x = y$

μ : surj ; $y \in G \Longrightarrow \exists x_{(= y^{-1}) \in G}$:

$\mu(x)_{(= (y^{-1})^{-1})} = y$

μ : homo ; $x, y \in G \Longrightarrow$

$\mu(x \cdot y) = (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$

$= x^{-1} \cdot y^{-1} = \mu(x) \cdot \mu(y)$

hence $\mu_{G \to G}$: iso , implies μ : auto . ■

Def: $Aut(G) := \{ \mu_{G \to G} \mid \mu : \text{auto} \}$.

Prop: $Aut(G) \leq S_G$.

Proof: i. $Aut(G)$: closed under $\circ$;

$f, g \in Aut(G) \Longrightarrow f_{G \to G} : \text{iso} \wedge g_{G \to G} : \text{iso}$

$\Longrightarrow f \circ g_{G \to G} : \text{iso} \Longrightarrow f \circ g \in Aut(G)$

ii. $e_{Aut(G)} := \varepsilon_{(= e_{S_G})}$, since $id : \text{iso}$

$\varepsilon_{(:= id_{G \to G})} : \text{iso}$; so $\varepsilon \in Aut(G)$

iii. $f \in Aut(G) \Longrightarrow f_{G \to G} : \text{iso}$

$\Longrightarrow f^{-1}_{G \to G} : \text{iso} \Longrightarrow [f]^{-1}_{(= f^{-1}_{G \to G})} : \text{iso}$

$\Longrightarrow [[f]]^{-1} \in Aut(G)$ ■

Def: $i_{\omega\, G \to G} : \text{inner auto} := i_\omega(g_{\in G}) = \omega g \omega^{-1}$.

Prop: $i_{\omega\, G \to G} : \text{inner auto} \Longrightarrow i_{\omega\, G \to G} : \text{auto}$.

Proof: $i_\omega : \text{bij}$;

$i_\omega : \text{inj}$; $i_\omega(g_0) = i_\omega(g_1) \Longrightarrow \omega g_0 \omega^{-1} = \omega g_1 \omega^{-1}$

$\Rightarrow g_0 = g_1$, $i_\omega : \text{surj}$; $g \in G \Longrightarrow \exists h^{\in G}_{(= \omega^{-1} g \omega)}$:

$i_\omega(h) = i_\omega(\omega^{-1} g \omega)$

$= \omega \omega^{-1} g \omega \omega^{-1} = e_G g e_G = g$

Proof cont'd : i_ω : homo ;

$$i_\omega(g_0 g_1) = \omega g_0 g_1 \omega^{-1} = \omega g_0 \omega^{-1} \omega g_1 \omega^{-1}$$
$$= i_\omega(g_0)\, i_\omega(g_1)$$

so $i_\omega : G \to G$: iso so i_ω : auto ∎

Def: $\mathrm{Inn}(G) := \{ i_\omega \mid \omega \in G \wedge i_\omega : \text{inner auto} \}$

Prop: $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Proof: $\mathrm{Inn}(G)$: closed under $\circ$:

$$(i_{\omega_0} \circ i_{\omega_1})(g) = i_{\omega_0}(i_{\omega_1}(g)) = i_{\omega_0}(\omega_1 g \omega_1^{-1})$$
$$= \omega_0 \omega_1 g \omega_1^{-1} \omega_0^{-1}$$
$$= (\omega_0 \omega_1) g (\omega_0 \omega_1)^{-1} = i_{\omega_0 \omega_1}(g)$$

$e_{\mathrm{Inn}(G)} := i_{e_G}$, $i_{e_G} = \varepsilon$; $i_{e_G}(g) = e_G g e_G^{-1}$
$$= e_G g e_G = g$$

$[i_\omega]^{-1} = i_{\omega^{-1}}$;

$$(i_\omega \circ i_{\omega^{-1}})(g) = i_\omega(i_{\omega^{-1}}(g)) = i_\omega(\omega^{-1} g \omega)$$
$$= \omega \omega^{-1} g \omega \omega^{-1} = e_G g e_G = g$$
$$= i_{e_G}(g) = g = e_G g e_G$$
$$= \omega^{-1} \omega g \omega^{-1} \omega = i_{\omega^{-1}}(\omega g \omega^{-1}) = (i_{\omega^{-1}} \circ i_\omega)(g)$$ ∎

Def: $\langle \emptyset \rangle := \{e_G\}$

$$\langle S \rangle := \{ \bullet_{\substack{i>0 \\ s_i \in S \\ \varepsilon_i \in \{-1,1\}}} s_i^{\varepsilon_i} \} .$$

Def: $G : \text{cyclic} := \exists x_{\in G} : G = \langle x \rangle$.

Prop: $G : \text{cyclic} \Longrightarrow G : \text{ab}$.

Proof: Let $G = \langle x \rangle$,

$$\omega_0 \cdot \omega_1 = x^{i_0} \cdot x^{i_1} = x^{i_0 + i_1}$$

$$= x^{i_1 + i_0} = x^{i_1} \cdot x^{i_0}$$

$$= \omega_1 \cdot \omega_0$$

■

Prop: $G : \text{cyclic} \wedge H \leq G$

$\Longrightarrow H : \text{cyclic}$

Proof: Let $G = \langle x \rangle$,

Case 1: $H = \{e_G\}$;

then $H = \langle e_G \rangle (= \{ e_G^n (= e_G) \mid n \geq 0 \})$

hence $H : \text{cyclic}$

Proof cont'd:

Case 2: $\mathcal{H} \neq \{e_G\}$;

note $e_G \in \mathcal{H}$ since $\mathcal{H} \leq G$,

so $\exists y_{\in \mathcal{H}}: y \neq e_G$, since $y \in G_{\geq \mathcal{H}}$

$\exists n: y = x^n$, note $n \neq 0$

as otherwise $(y_{\neq e_G}) = (x^0)_{(=e_G)}$,

since $\mathcal{H}$: group, $\exists y^{-1}_{\in \mathcal{H}}$ y^{-1}: inv of y

so $y^{-1} = (x^n)^{-1} = x^{-n}$, note $-n \neq 0$

since $n \neq 0$, define $\kappa_0 := \begin{cases} n, & n > 0 \\ -n, & n < 0 \end{cases}$

so $\exists \kappa^{>0}_{(=\kappa_0)}: x^\kappa \in \mathcal{H}$

hence $K \neq \emptyset$ where $K := \{\kappa_{>0}: x^\kappa \in \mathcal{H}\}$

define $\tilde{\kappa} := \min_{\kappa \in K} K$,

so $\langle x^{\tilde{\kappa}} \rangle \subseteq \mathcal{H}$, since $x^{\tilde{\kappa}} \in \mathcal{H}$ and $\mathcal{H}$: group

Proof cont'd: let $h \in H$,

so $\exists m : h = x^m$, as $H \leq G$

so $\exists q, r : m = \tilde{k}q + r$ where $0 \leq r < \tilde{k}$,

hence $h = x^m = x^{\tilde{k}q+r} = x^{\tilde{k}q} x^r = (x^{\tilde{k}})^q x^r$

so, as $h \in H$ and $(x^{\tilde{k}})^q \in H$,

$x^r_{(= (x^{\tilde{k}})^{-q} h)} \in H$,

if $r > 0$, then $r \in K$ but $r < \tilde{k}_{(= \min_{x \in K} x)}$

which is a contradiction,

so $r = 0$ so $x^r = e_G$

hence $h = (x^{\tilde{k}})^q$ so $H \subseteq \langle x^{\tilde{k}} \rangle$

so $H = \langle x^{\tilde{k}} \rangle$ so H: cyclic ■

Def: $C_n := \langle x \mid x^n = e \rangle$, $C_\infty := \langle x \mid \rangle$

Theorem: $C_\infty \cong \mathbb{Z}$.

Proof: $g \in C_\infty \Rightarrow \exists! n_g : g = x^{n_g}$,

define $\varphi_{C_\infty \to \mathbb{Z}} : g \mapsto n_g$,

φ : bij ;

φ : inj ; $\varphi(g_0) = \varphi(g_1) \Rightarrow n_{g_0} = n_{g_1}$

$\Rightarrow x^{n_{g_0}} = x^{n_{g_1}} \Rightarrow g_0 = g_1$

φ : surj ; $n \in \mathbb{Z} \Rightarrow \exists_{g \in C_\infty} n = n_g$

$\Rightarrow \varphi(g) = n$

φ : homo ;

$$\varphi(g_0 \cdot g_1) = \varphi(x^{n_{g_0}} \cdot x^{n_{g_1}}) = \varphi(x^{n_{g_0} + n_{g_1}})$$
$$= n_{g_0} + n_{g_1} = \varphi(x^{n_{g_0}}) + \varphi(x^{n_{g_1}})$$
$$= \varphi(g_0) + \varphi(g_1)$$

so $\varphi_{C_\infty \to \mathbb{Z}}$: iso , so $C_\infty \underset{\varphi}{\cong} \mathbb{Z}$ ■

Theorem: $C_n \cong \mathbb{Z}/n\mathbb{Z}$.

Proof: $g \in C_n \Longrightarrow \exists i_g : g = x^{i_g}$,

define $\varphi_{C_n \to \mathbb{Z}/n\mathbb{Z}} : g \mapsto [i_g]_n$

let $g_0, g_1 \in C_n$, $\exists q, r_{(0 \le r < n)} : i_{g_0} + i_{g_1} = qn + r$,

$$\begin{aligned}
\varphi(g_0 \cdot g_1) &= \varphi(x^{i_{g_0}} \cdot x^{i_{g_1}}) = \varphi(x^{i_{g_0} + i_{g_1}}) \\
&= \varphi(x^{qn+r}) = \varphi((x^n)^q \cdot x^r) \\
&= \varphi(e_{C_n}^q \cdot x^r) = \varphi(e_{C_n} \cdot x^r) \\
&= \varphi(x^r) = [r]_n = [qn + r]_n \\
&= [i_{g_0} + i_{g_1}]_n = [i_{g_0}]_n + [i_{g_1}]_n \\
&= \varphi(x^{i_{g_0}}) + \varphi(x^{i_{g_1}}) \\
&= \varphi(g_0) + \varphi(g_1)
\end{aligned}$$

so φ : homo ,

also φ : bij obviously ,

so φ : iso , hence $C_n \overset{\varphi}{\cong} \mathbb{Z}/n\mathbb{Z}$ ■

Prop: $C_n \cong C_m \iff n = m$.

Proof: ($\Rightarrow$): $C_n \cong C_m \Rightarrow \exists \varphi_{C_n \to C_m}\ \varphi$: iso

$\Rightarrow \varphi_{C_n \to C_m}$: bij $\Rightarrow n = m$

($\Leftarrow$): $g \in C_n \wedge h \in C_m$

$\Rightarrow \exists i_g, i_h$: $g = x^{i_g} \wedge h = y^{i_h}$,

define $\varphi_{C_n \to C_m} : g \mapsto y^{i_g}$

$$\varphi(g_0 \bullet_1 g_1) = \varphi(x^{i_{g_0}} \bullet_1 x^{i_{g_1}}) = \varphi(x^{i_{g_0} + i_{g_1}})$$
$$= y^{i_{g_0} + i_{g_1}} = y^{i_{g_0}} \bullet_2 y^{i_{g_1}}$$
$$= \varphi(x^{i_{g_0}}) \bullet_2 \varphi(x^{i_{g_1}})$$
$$= \varphi(g_0) \bullet_2 \varphi(g_1)$$

so φ : homo , also φ : bij as $n = m$

so φ : iso , hence $C_n \cong_{\varphi} C_m$ ■

Lemma: $d \mid \omega \iff [\omega]_n \in \langle [d]_n \rangle$

Proof: $d \mid \omega \iff \exists K : \omega = dK$

$\iff [\omega]_n = [Kd]_n = K[d]_n = \sum_K [d]_n$

$\iff [\omega]_n \in \langle [d]_n \rangle$ ∎

Lemma: $\exists x_{\in \mathbb{Z}/n\mathbb{Z}} : \omega x = c \iff c \in \langle d \rangle$

$d := \gcd(\omega, n)$

Proof: $\exists x_{\in \mathbb{Z}/n\mathbb{Z}} : \omega x = c \iff \omega x \equiv_n c$

$\iff \exists y \ \ \omega x - c = ny \iff \omega x - ny = c$

$\underset{d \mid \omega \wedge d \mid n}{\iff} \exists q,p : dqx - dpy = c \iff d(qx - py) = c$

$\iff d \mid c \iff c \in \langle d \rangle$ ∎

Theorem: $\omega \in \mathbb{Z}/n\mathbb{Z}$ $\wedge$ $d = \gcd(\omega, n)$

$\Longrightarrow$ i. $\langle \omega \rangle = \langle d \rangle$ ii. $\langle \omega \rangle \cong C_{\frac{n}{d}}$

Proof: i. since $d \mid \omega$, by first lemma,

$\omega \in \langle d \rangle$, so $\langle \omega \rangle \subseteq \langle d \rangle$,

also since $d \in \langle d \rangle$, by second lemma,

$\exists x_{\in \mathbb{Z}/n\mathbb{Z}}$: $x\omega = d$ so $x \cdot (\omega) = d$

i.e. $\sum_x \omega = d$ so $d \in \langle \omega \rangle$ so $\langle d \rangle \subseteq \langle \omega \rangle$

hence $\langle \omega \rangle = \langle d \rangle$

ii. $\operatorname{ord}(d) \leq \frac{n}{d}$ as $\sum_{n/d} d = \frac{n}{d} d = n = 0$

suppose $\operatorname{ord}(d) = K$ where $0 < K < \frac{n}{d}$,

so $0 < Kd < n$ so $Kd \neq 0$ i.e. $\sum_x d \neq 0$

so $\operatorname{ord}(d) \neq K$, hence $\operatorname{ord}(d) = \frac{n}{d}$,

so $|\langle d \rangle| = \frac{n}{d}$, note $\langle d \rangle = \langle \omega \rangle$ by i.,

so $|\langle \omega \rangle| = \frac{n}{d}$ hence $\langle \omega \rangle \cong C_{\frac{n}{d}}$ ■

Theorem: $H \leq \mathbb{Z}/n\mathbb{Z} \implies |H| \mid n$.

Proof: $H \leq \mathbb{Z}/n\mathbb{Z} \implies \exists y \; H = \langle y \rangle$

$\implies H \cong C_{\frac{n}{d}}$: $d = \gcd(y, n)$

$\implies |H| = \frac{n}{d} \implies n = d\frac{n}{d} = d|H|$

$\implies |H| \mid n$ ∎

Theorem: $K \mid n \iff \exists! H_{\leq C_n} : |H| = K$

Proof: ($\implies$): $\exists \omega : n = K\omega$ since $K \mid n$

define $H := \langle \omega \rangle$,

so $H = \langle \omega \rangle \cong C_{\frac{n}{\gcd(\omega, n)}} = C_{\frac{n}{\omega}} = C_K$

hence $|H| = K$,

define $J = \langle u \rangle$ with $|J| = K$,

so $C_K \cong \langle \dot{u} \rangle \cong C_{\frac{n}{\gcd(\dot{u}, n)}} = C_{\frac{n}{\dot{u}}}$

where $\dot{u} = \gcd(u, n)$,

so $K = \frac{n}{\dot{u}}$ i.e. $\dot{u} = \frac{n}{K}$ so $\dot{u} = \omega$

so $J = \langle u \rangle = \langle \dot{u} \rangle = \langle \omega \rangle = H$

hence $\exists! H_{\leq \mathbb{Z}/n\mathbb{Z}}^{(= \langle \omega \rangle)} : |H| = K$

($\impliedby$): $H \leq C_n \implies K_{(=|H|)} \mid n$ ∎

Theorem: $C_n = \langle x \rangle$,

$\langle x^{i_0} \rangle = \langle x^{i_1} \rangle \iff \gcd(i_0, n) = \gcd(i_1, n)$

Proof: ($\Rightarrow$): $\langle x^{i_0} \rangle = \langle x^{i_1} \rangle$

$\Rightarrow C_{\frac{n}{\gcd(i_0,n)}} \cong \langle i_0 \rangle \cong \langle x^{i_0} \rangle$

$= \langle x^{i_1} \rangle \cong \langle i_1 \rangle \cong C_{\frac{n}{\gcd(i_1,n)}}$

$\Rightarrow \frac{n}{\gcd(i_0,n)} = \frac{n}{\gcd(i_1,n)}$

$\Rightarrow \gcd(i_0, n) = \gcd(i_1, n)$

($\Leftarrow$): $\gcd(i_0, n) = \gcd(i_1, n)$

$\Rightarrow \langle \gcd(i_0, n) \rangle = \langle \gcd(i_1, n) \rangle$

$\Rightarrow \langle i_0 \rangle = \langle i_1 \rangle \Rightarrow \langle x^{i_0} \rangle = \langle x^{i_1} \rangle$

$\therefore C_n = \langle x \rangle$ ■

Theorem: $C_n = \langle x \rangle$,

$\langle x \rangle = \langle x^k \rangle \iff k \perp n$.

Proof: $\langle x \rangle = \langle x^k \rangle \iff \langle x^1 \rangle = \langle x^k \rangle$

$\iff \gcd(1, n) = \gcd(k, n)$

$\iff 1 = \gcd(k, n) \iff k \perp n$ ■

Theorem: $\phi_{(G,\bullet)\to(H,\star)}$: homo

$\Longrightarrow \phi(\langle x\rangle) = \langle \phi(x)\rangle$.

Proof: $h \in \phi(\langle x\rangle)$

$\Longleftrightarrow \exists g_{\in\langle x\rangle} : h = \phi(g) : (\exists i_g : g = \bullet_{i_g} x)$

$\Longleftrightarrow h = \phi(g) = \phi(\bullet_{i_g} x) = \star_{i_g}[\phi(x)]$

$\Longleftrightarrow h \in \langle \phi(x)\rangle$ ■

Theorem: $\langle x\rangle = \langle x^{-1}\rangle$.

Proof: define $n := |\langle x\rangle|$,

note $x^{n-1} = x^{-1}$ as $x^{n-1} = x^n \cdot x^{-1} = e \cdot x^{-1} = x^{-1}$

$(n-1) \perp n \Longrightarrow \langle x\rangle = \langle x^{n-1}\rangle$

$\Longrightarrow \langle x\rangle = \langle x^{-1}\rangle$ ■

Def: $[x]_\sim :=$ left coset of $\mathcal{H} \leq G$ with rep $x \in G$:

$\sim \subseteq G \times G := x \sim y \iff x^{-1} \cdot y \in \mathcal{H}$.

Prop: $\sim$: eq rel .

Proof: i. $e_G \in \mathcal{H} \leq G \Rightarrow x^{-1} \cdot x \in \mathcal{H}$

$\Rightarrow x \sim x$

ii. $x \sim y \Rightarrow x^{-1} \cdot y \in \mathcal{H} \leq G$

$\Rightarrow (x^{-1} \cdot y)^{-1} \in \mathcal{H}$

$\Rightarrow y^{-1} \cdot x \in \mathcal{H} \Rightarrow y \sim x$

iii. $x \sim y \wedge y \sim z$

$\Rightarrow x^{-1} \cdot y \,,\, y^{-1} \cdot z \in \mathcal{H} \leq G$

$\Rightarrow x^{-1} \cdot z = x^{-1} \cdot e_G \cdot z$

$= x^{-1} \cdot y \cdot y^{-1} \cdot z \in \mathcal{H}$

$\Rightarrow x \sim z$ ■

Prop: $[x]_\sim = xH$.

Proof: $y \in [x]_\sim \iff x \sim y$

$\iff x^{-1} \cdot y \in H \iff \exists h_{\in H}\ h = x^{-1} \cdot y$

$\iff \exists h_{\in H}\ y = x \cdot h \iff y \in xH$ ∎

Prop: $e_G H = H$.

Proof: $\omega \in e_G H \iff \omega \in [e_G]_\sim$

$\iff e_G \sim \omega \iff e_G^{-1} \cdot \omega \in H$

$\iff \omega_{(= e_G \cdot \omega = e_G^{-1} \cdot \omega)} \in H$ ∎

Prop: i. $xH = yH \equiv$ ii. $x^{-1} \cdot y \in H$

$\equiv$ iii. $Hx^{-1} = Hy^{-1} \equiv x \in yH$ iv.

$\equiv$ v. $xH \subseteq yH$.

Proof: i $\Leftrightarrow$ ii : $xH = yH \iff [x]_\sim = [y]_\sim$

$\iff x \sim y \iff x^{-1} \cdot y \in H$

ii $\Leftrightarrow$ iii : $x^{-1} \cdot y \in H \iff x^{-1} \cdot (y^{-1})^{-1} \in H$

$\iff x^{-1} \sim_r y^{-1} \iff [x^{-1}]_{\sim_r} = [y^{-1}]_{\sim_r}$

$\iff Hx^{-1} = Hy^{-1}$

Proof cont'd: $i) \iff iv)$: $x^{-1} \cdot y \in H$

$\iff (x^{-1} \cdot y)^{-1} \in H \iff y^{-1} \cdot x \in H$

$\iff x \in yH$

$iv) \iff v)$:

$(\Rightarrow)$: $x \in yH \Rightarrow \exists h_{\in H}\ x = y \cdot h$

$\Rightarrow [\ \omega \in xH \Rightarrow \omega \in yhH$

$\Rightarrow \exists K^{(=xH)}_{\leq H}: \omega \in yK$

$\Rightarrow \omega \in yH\ ]$

$\Rightarrow xH \subseteq yH$

$(\Leftarrow)$: $xH_{(=[x]_\sim \ni x)} \subseteq yH$

$\Rightarrow x \in yH$ ■

Prop: $x \in H \iff xH = H$.

Proof: $x \in H \iff e_G \cdot x \in H$

$\iff e_G^{-1} \cdot x \in H \iff e_G H = xH$

$\iff H = xH$ ■

Prop: $G:ab \implies xH = Hx$.

Proof: $xH = \{x \cdot h : h \in H\}$

$= \{h \cdot x : h \in H\} = Hx$ ■

Prop: $\exists \varphi_{x \to xH}\ \varphi : bij$.

Proof: define $\varphi_{x \to xH} : h \mapsto x \cdot h$

$\varphi : inj$; $\varphi(h_0) = \varphi(h_1)$

$\implies x \cdot h_0 = x \cdot h_1 \implies h_0 = h_1$

$\varphi : surj$; $g \in xH \implies \exists h_{\in H} : g = x \cdot h$

$\implies \exists h_{\in H} : g = \varphi(h)$

hence $\varphi : bij$ ■

Prop: $|gH| = |H| = |Hg|$.

Proof: $\exists \varphi_l, \varphi_r : gH \xleftarrow[bij]{\varphi_l} H \xrightarrow[bij]{\varphi_r} Hg$

$\implies |gH| = |H| = |Hg|$ ■

Def: $[G:H] := |\mathcal{L}_H| = |\mathcal{R}_H|$:

$\mathcal{L}_H = \{gH : g \in G\}$, $\mathcal{R}_H = \{Hg : g \in G\}$

Prop: $|\mathcal{L}_H| = |\mathcal{R}_H|$.

Proof: define $f_{\mathcal{L}_H \to \mathcal{R}_H} : gH \mapsto Hg^{-1}$

f : inj ;

$f(g_0H) = f(g_1H) \implies Hg_0^{-1} = Hg_1^{-1}$

$\implies g_0H = g_1H$

f : surj ;

$Hg \in \mathcal{R}_H \implies \exists \omega H \in_{(= g^{-1}H)} \mathcal{L}_H$:

$f(\omega H) = H\omega^{-1} = H(g^{-1})^{-1} = Hg$;

so f : bij , hence $|\mathcal{L}_H| = |\mathcal{R}_H|$ ■

Prop: $\mathcal{L}_H$ partitions G .

Proof: i. let $gH \in \mathcal{L}_H$,

note $g \in gH_{(=[g]_\sim)}$ since $g \sim g$ as $\sim$: eq rel

so $gH \neq \emptyset$ so $\emptyset \notin \mathcal{L}_H$

ii. let $g_0H \neq g_1H$,

assume $g_0H \cap g_1H \neq \emptyset$, let $x \in g_0H \cap g_1H$

then $x \in g_0H, g_1H$ so $\exists h_0, h_1$:

$x = g_0 \cdot h_0$ and $x = g_1 \cdot h_1$

say $h_2 = h_1 \cdot h_0^{-1}$, $g_0 = g_1 \cdot h_1 \cdot h_0^{-1} = g_1 \cdot h_2$

so $g_0 \in g_1H$ hence $g_0H = g_1H$: contr

hence $g_0H \cap g_1H = \emptyset$ ¹

iii. $G = \bigcup_{g \in G} gH$ since $g \in gH$ ■

Theorem: $|G| = [G : H]\,|H|$.

Proof: $\mathcal{L}_H$ partitions G $\wedge$ $|gH_{\in \mathcal{L}_H}| = |H| : g \in G$

$\Longrightarrow |G| = |\mathcal{L}_H|\,|H|$

$= [G : H]\,|H|$ ■

Def: G : simple :=

$H \leq G \Longrightarrow H = \{e_G\} \vee H = G$.

Prop: $|G| = p$: p : prime

$\Longrightarrow G$: simple $\wedge$ G : cyclic .

Proof: p : prime $\Longrightarrow p \geq 2$

$\Longrightarrow \exists x_{\in G} : x \neq e_G$,

also $|\langle x \rangle| = 1$ or $|\langle x \rangle| = p$

since $|\langle x \rangle| \mid p_{(=|G|)}$,

note $|\langle x \rangle| = 1$ implies $x = e_G$

since $e_{G(=x')} \in \langle x \rangle : x \in G$

so $|\langle x \rangle| = p$ since $x \neq e_G$

so $\langle x \rangle = G$ hence G : cyclic

also $H \leq G$ implies $|H| \mid p$

hence obviously G : simple

since if $|H| = p$ then $H = G$;

and if $|H|_{(=\langle \omega \rangle)} = 1$ then $\omega = e_G$

so $H = \langle e_G \rangle = \{e_G\}$ ■

Prop: $|G| = p : p \text{ prime} \Longrightarrow G : ab$.

Proof: $p : \text{prime} \Longrightarrow G : \text{cyclic}$

$\Longrightarrow G : ab$ ∎

Prop: $I \leq_G \subseteq \mathcal{H} \leq_G \Longrightarrow [G : I] = [G : \mathcal{H}][\mathcal{H} : I]$

Proof: $[G : I] = \frac{|G|}{|I|} = \frac{|G|}{|\mathcal{H}|} \frac{|\mathcal{H}|}{|I|}$

$= [G : \mathcal{H}][\mathcal{H} : I]$ ∎

Def: $Z(G) := \{ c_{\in G} \mid c \cdot g = g \cdot c : g \in G \}$

Prop: $G : ab \iff G = Z(G)$.

Proof: $(\Longrightarrow)$: $G : ab \wedge c \in G$

$\Longrightarrow c \cdot g = g \cdot c : g \in G \Longrightarrow c \in Z(G)$

$\Longrightarrow G_{\supseteq Z(G)} \subseteq Z(G) \Longrightarrow G = Z(G)$

$(\Longleftarrow)$: $G = Z(G) \wedge c \in G$

$\Longrightarrow c \in Z(G) \Longrightarrow c \cdot g = g \cdot c : g \in G$

$\Longrightarrow G : ab$ ■

Prop: $Z(G) \leq_{ab} G$.

Proof: Let $x, y \in Z(G)$ and $g \in G$;

$$(x \cdot y) \cdot g = x \cdot (y \cdot g) = x \cdot (g \cdot y)$$
$$= (x \cdot g) \cdot y = (g \cdot x) \cdot y$$
$$= g \cdot (x \cdot y)$$

so $x \cdot y \in Z(G)$ hence $Z(G)$ closed under $\cdot$

Proof cont'd:

$e_G \in Z(G)$ as $e_G \cdot g = g \cdot e_G \;:\; g \in G$

let $x \in Z(G)$, assume $x^{-1} \notin Z(G)$

so $\exists g_0 \in G : x^{-1} \cdot g_0 \neq g_0 \cdot x^{-1}$,

but $x^{-1} \cdot g_0 \neq g_0 \cdot x^{-1}$

$x \cdot x^{-1} \cdot g_0 \neq x \cdot g_0 \cdot x^{-1}$

$g_0 \neq g_0 \cdot x \cdot x^{-1}$

$g_0 \neq g_0$: contr

so $x^{-1} \in Z(G)$

let $c \in Z(G)$, so $c \cdot g = g \cdot c \;:\; g \in G$

so $c \cdot d = d \cdot c \;:\; d \in Z(G) \subseteq G$

hence $Z(G) \leq_{ab} G$ ■

Def: $C_G(\Omega) := \{ g \in G \mid g \cdot \omega = \omega \cdot g : \omega \in \Omega \}$

Prop: $Z(G) = \bigcap_{\omega \in G} C_G(\omega)$.

Proof: $g \in Z(G) \iff g \cdot \omega = \omega \cdot g : \omega \in G$

$\iff g \in C_G(\omega) : \omega \in G$

$\iff g \in \bigcap_{\omega \in G} C_G(\omega)$ ∎

Prop: $C_G(\Omega) \leq G$.

Proof: note $g \in C_G(\Omega)$ iff $g \cdot \omega \cdot g^{-1} = \omega : \omega \in \Omega$

since $g \cdot \omega = \omega \cdot g : \omega \in \Omega \wedge g \in C_G(\Omega)$

let $g_0, g_1 \in C_G(\Omega)$, $\omega \in \Omega$

then $(g_0 \cdot g_1) \cdot \omega \cdot (g_0 \cdot g_1)^{-1} = g_0 g_1 \cdot \omega \cdot g_1^{-1} \cdot g_0^{-1}$

$= g_0 \cdot \omega \cdot g_0^{-1} = \omega$

so $g_0 \cdot g_1 \in C_G(\Omega)$ so $C_G(\Omega)$: closed under $\cdot$

also $e_G \in C_G(\Omega)$ as $e_G \cdot \omega = \omega \cdot e_G : \omega \in \Omega$

let $g \in C_G(\Omega)$ so $g \cdot \omega \cdot g^{-1} = \omega : \omega \in \Omega$

so $\omega \cdot g^{-1} = g^{-1} \cdot \omega : \omega \in \Omega$ so $g^{-1} \in C_G(\Omega)$

hence $C_G(\Omega) \leq G$ ∎

Prop: $\mathcal{H}_{\leq G} \leq C_G(\mathcal{H}) \iff \mathcal{H} : ab$.

Proof: ($\Rightarrow$): $h_0, h_1 \in \mathcal{H} \leq C_G(\mathcal{H})$

$\Rightarrow h_0 \in C_G(\mathcal{H}) \Rightarrow h_0 \cdot h = h \cdot h_0 : h \in \mathcal{H}$

$\Rightarrow h_0 \cdot h_1 = h_1 \cdot h_0 \Rightarrow \mathcal{H} : ab$

($\Leftarrow$): $\mathcal{H}_{=\langle h_0 \rangle} : ab$

$\Rightarrow h_0 \cdot h = h \cdot h_0 : h \in \mathcal{H}$

$\Rightarrow h_0 \in C_G(\mathcal{H}) \Rightarrow \mathcal{H} \leq C_G(\mathcal{H})$ ■

Prop: i. $C_G(Z(G)) = G$

ii. $\Omega_0 \subseteq \Omega_1 \Rightarrow C_G(\Omega_1) \leq C_G(\Omega_0)$

iii. $Z(G) \leq C_G(\Omega) : \Omega \subseteq G$

Proof: i. $g \in C_G(Z(G))$

$\iff g \cdot \omega = \omega \cdot g : \omega \in Z(G)_{(= \{\omega \in G \mid \omega \cdot g = g \cdot \omega : g \in G\})}$

$\iff g \in G$

ii. $g \in C_G(\Omega_1 \supseteq \Omega_0) \Rightarrow g \cdot \omega = \omega \cdot g : \omega \in \Omega_1$

$\Rightarrow g \cdot \omega = \omega \cdot g : \omega \in \Omega_0 \subseteq \Omega_1$

$\Rightarrow g \in C_G(\Omega_0)$

iii. $Z(G)_{(= C_G(G))} \leq C_G(\Omega_{\subseteq G})$ ■

Def: $N_G(\Omega) := \{ g \in G \mid g\Omega g^{-1} = \Omega \}$

Prop: $N_G(\Omega) \leq G$.

Proof: let $g_0, g_1 \in N_G(\Omega)$,

$$(g_0 \cdot g_1)\,\Omega\,(g_0 \cdot g_1)^{-1} = g_0 g_1 \Omega g_1^{-1} g_0^{-1}$$

$$= g_0 \Omega g_0^{-1} = \Omega$$

so $g_0 \cdot g_1 \in N_G(\Omega)$

so $N_G(\Omega)$: closed under $\cdot$

also $e_G \in N_G(\Omega)$

since $e_G \Omega e_G^{-1} = \Omega e_G^{-1} = \Omega e_G = \Omega$

let $g \in N_G(\Omega)$, so $g\Omega g^{-1} = \Omega$

so $g\Omega = \Omega g$ so $\Omega = g^{-1}\Omega g$

so $g^{-1} \in N_G(\Omega)$

hence $N_G(\Omega) \leq G$ ■

Prop: $C_G(\Omega) \leq N_G(\Omega)$.

Proof: $g \in C_G(\Omega) \Longrightarrow g \cdot \omega \cdot g^{-1} = \omega \;:\; \omega \in \Omega$

$\Longrightarrow g\Omega g^{-1} = \Omega \Longrightarrow g \in N_G(\Omega)$ ■

Prop: $H \leq G \leq N_G(H)$.

Proof: let $h \in H$,

define $\varphi_h : H \to H : h_0 \mapsto h \cdot h_0 \cdot h^{-1}$,

φ_h: inj;

$$\varphi_h(h_0) = \varphi_h(h_1) \implies h \cdot h_0 \cdot h^{-1} = h \cdot h_1 \cdot h^{-1}$$

$$\implies h_0 \cdot h^{-1} = h_1 \cdot h^{-1} \implies h_0 = h_1$$

φ_h: surj;

$$h_0 \in H \implies \exists y \overset{\in H}{(= h^{-1} h_0 h)} :$$

$$\varphi_h(y) = \varphi_h(h^{-1} \cdot h_0 \cdot h) = h \cdot h^{-1} \cdot h_0 \cdot h \cdot h^{-1}$$

$$= e_G \cdot h_0 \cdot e_G = h_0$$

so φ_h: bij so $\varphi_h(H) = H$

also $\varphi_h(H) = \{ \varphi_h(h_0) : h_0 \in H \}$

$$= \{ h \cdot h_0 \cdot h^{-1} : h_0 \in H \} = hHh^{-1}$$

so $H = hHh^{-1}$

hence $h \in N_G(H)$ ∎

Prop: i. $N_G(\omega) = C_G(\omega) : \omega \in G$

ii. $N_G(Z(G)) = G$ iii. $Z(G) \leq N_G(\Omega)$

Proof: i. $N_G(\omega) = \{ g_{\in G} \mid g\{\omega\}g^{-1} = \{\omega\} \}$

$= \{ g_{\in G} \mid g \cdot \omega_0 \cdot g^{-1} = \omega_0 : \omega_0 \in \{\omega\} \}$

$= C_G(\omega)$

ii. note $C_G(\Omega) \leq N_G(\Omega)$,

so $G = C_G(Z(G)) \leq N_G(Z(G)) \leq G$

iii. $Z(G) \leq C_G(\Omega) \leq N_G(\Omega)$ ■

Prop: $H \leq G \Longrightarrow gHg^{-1} \leq G : g \in G$.

Proof: let $x, y \in gHg^{-1}$, so $\exists x_0, y_0 \in H$

$x = gx_0g^{-1}$, $y = gy_0g^{-1}$, so $g^{-1}xg, g^{-1}yg \in H$

so $g^{-1}xgg^{-1}yg \in H$ as $H \leq G$,

so $g^{-1}(xy)g \in H$ so $xy \in gHg^{-1}$

also $e_G \in gHg^{-1}$ as $e_G = gg^{-1} = ge_Gg^{-1}$

also, since $g^{-1}xg \in H$ and $H \leq G$

$(g^{-1}xg)^{-1} \in H$ i.e. $g^{-1}x^{-1}g \in H$

so $x^{-1} \in gHg^{-1}$ ■

Def: $N_{\leq G} \lhd G := gN = Ng : g \in G$.

Theorem: i. $\{e_G\} \lhd G$ ii. $G \lhd G$

iii. $G_{\geq H} : ab \Longrightarrow H \lhd G$.

Proof: i. $g\{e_G\} = \{g \cdot e_G\} = \{e_G \cdot g\}$

$= \{e_G\} g : g \in G$

ii. $gG = G = Gg : g \in G$

iii. $G_{\geq H} : ab \Longrightarrow gH = Hg : g \in G$ ∎

Theorem: $N \lhd G \iff \mathcal{L}_N = \mathcal{R}_N$.

Proof: $(\Longrightarrow)$: $l_N \in \mathcal{L}_N \iff \exists x_{\in G} : l_N = xN$

$\underset{N \lhd G}{\iff} \exists x_{\in G} : l_N = Nx \iff l_N \in \mathcal{R}_N$

$(\Longleftarrow)$: $g \in G \wedge \mathcal{L}_N = \mathcal{R}_N$

$\Longrightarrow Ng_{(\in \mathcal{R}_N)} \in \mathcal{L}_N \Longrightarrow \exists h_{\in G} : Ng = hN$

$\Longrightarrow g_{\in Ng} \in hN \Longrightarrow g^{-1} \cdot h \in N$

$\Longrightarrow Ng = hN = (e_G \cdot h)N = (g \cdot g^{-1} \cdot h)N$

$\Longrightarrow g(g^{-1} \cdot h)N = gN$ ∎

Theorem: $N \lhd G \iff gNg^{-1} \subseteq N : g \in G$.

Proof: $(\Longrightarrow)$: $N \lhd G \wedge g \in G$

$\Longrightarrow gN = Ng \Longrightarrow gN \subseteq Ng$

$\Longrightarrow gNg^{-1} \subseteq Ngg^{-1} \Longrightarrow gNg^{-1} \subseteq Ne_G$

$\Longrightarrow gNg^{-1} \subseteq N$

$(\Longleftarrow)$: $gNg^{-1} \subseteq N : g \in G$

$\Longrightarrow g^{-1}Ng \subseteq N : g \in G$

$\Longrightarrow gNg^{-1}g \subseteq Ng \wedge gg^{-1}Ng \subseteq gN$

$\Longrightarrow gNe_G \subseteq Ng \wedge e_GNg \subseteq gN$

$\Longrightarrow gN \subseteq Ng \wedge Ng \subseteq gN$

$\Longrightarrow gN = Ng : g \in G \Longrightarrow N \lhd G$ ∎

Theorem: $N \lhd G \iff gNg^{-1} \supseteq N : g \in G$.

Proof: $(\Longrightarrow)$: $N \lhd G \Longrightarrow gN = Ng$

$\Longrightarrow N = gNg^{-1} \Longrightarrow N \subseteq gNg^{-1} : g \in G$

$(\Longleftarrow)$: $g_{\in G}Ng^{-1} \supseteq N \Longrightarrow g^{-1}Ng \supseteq_{\in G} N : g \in G$

$\Longrightarrow Ng \subseteq gN \wedge gN \subseteq Ng$

$\Longrightarrow Ng = gN : g \in G \Longrightarrow N \lhd G$ ∎

Theorem: $N \triangleleft G \iff gNg^{-1} = N : g \in G$.

Proof: $N \triangleleft G \iff \forall g_{\in G} : gNg^{-1} \supseteq N \wedge gNg^{-1} \subseteq N$

$\iff gNg^{-1} = N : g \in G$ ∎

Theorem: $N \triangleleft G \iff (n \in N \iff gng^{-1} \in N) : g \in G$

Proof: $(\Longrightarrow)$: $N \triangleleft G \implies gN = Ng$

$\implies gn_{(\in gN)} \in Ng : n \in N$

$\iff \exists n_0 \in N : gn = n_0 g \iff gng^{-1} = n_0$

$\iff gng^{-1} \in N$

$(\Longleftarrow)$: $gng^{-1} \in N \implies \exists n_0 \in N : gng^{-1} = n_0$

$\overset{i}{\implies} gn = n_0 g_{(\in Ng)} \implies gN \subseteq Ng$

$\overset{ii}{\implies} ng^{-1} = g^{-1} n_{0\,(\in g^{-1}N)} \implies Ng^{-1} \subseteq g^{-1}N$

$\implies Ng \subseteq gN$

$\therefore Ng = gN \implies N \triangleleft G$ ∎

Theorem: $H \lhd G \iff [\, ab \in H \implies a^{-1}b^{-1} \in H \,] : a, b \in G$

Proof: ($\implies$): suppose $H \lhd G$, and $ab \in H$,

$$ab \in H \underset{\substack{H \lhd G \\ a \in G}}{\implies} a^{-1}(ab)a \in H \implies ba \in H$$

$$\underset{H \leq G}{\implies} (ba)^{-1} \in H \implies a^{-1}b^{-1} \in H$$

($\impliedby$): suppose $ab \in H \implies a^{-1}b^{-1} \in H$,

then $[\, ab \in H \implies ba \in H \,] : a, b \in G \quad (*)$

since $a^{-1}b^{-1} \in H \underset{H \leq G}{\implies} \underbrace{(a^{-1}b^{-1})^{-1}}_{(=ba)} \in H$

let $g \in G$ and $h \in H$, set $x := hg^{-1}$, so

$$h \in H \implies xg \in H \underset{*}{\implies} gx \in H$$

$$\implies ghg^{-1} \in H \implies gHg^{-1} \subseteq H$$

$$\implies H \lhd G \qquad \blacksquare$$

Theorem: $H \lhd G \wedge K_{\geq H} \lhd G \implies H \lhd K$

Proof: $H \lhd G \implies gH = Hg : g \in G_{\geq K}$

$\implies KH = HK : K \in K_{\leq G} \implies H \lhd K \qquad \blacksquare$

Theorem: $N_0 \trianglelefteq G \wedge N_1 \trianglelefteq G \implies N_0 \cap N_1 \trianglelefteq G$

Proof: $N_0 \trianglelefteq G \wedge N_1 \trianglelefteq G$

$\implies gN_0g^{-1} \subseteq N_0 \wedge gN_1g^{-1} \subseteq N_1 \quad : g \in G$

$\implies g(N_0 \cap N_1)g^{-1} \subseteq N_0 \wedge g(N_0 \cap N_1)g^{-1} \subseteq N_1$

$\implies g(N_0 \cap N_1)g^{-1} \subseteq N_0 \cap N_1$

$\implies N_0 \cap N_1 \trianglelefteq G$ ∎

Theorem: $H \leq G \wedge N \trianglelefteq G \implies H \cap N \trianglelefteq H$

Proof: note $H \cap N \leq H$,

let $x \in H \cap N$, $h \in H$;

then $hxh^{-1} \in H$ as $H \leq G$ and $h, x_{(\in x \cap N)} \in H$

also $hxh^{-1} \in N$ as $N \trianglelefteq G$, $x_{(\in x \cap N)} \in N$, $h_{\in H} \in G$

so $hxh^{-1} \in H \cap N$

hence $H \cap N \trianglelefteq H$ ∎

Theorem: $\exists! H_{\leq G} : |H| = n \implies H \lhd G$.

Proof: Let $g \in G$, note that $gHg^{-1} \leq G$,

and $|gHg^{-1}| = H$ i.e. $|gHg^{-1}| = n$

so $gHg^{-1} = H$ hence $H \lhd G$ ∎

Theorem: $[G : H] = 2 \implies H \lhd G$.

Proof: note that $e_G H \in \mathcal{L}_H$ as $e_G \in G$,

so $\exists! x \neq e_G : xH \overset{(*)}{\in} \mathcal{L}_H$ as $|\mathcal{L}_H| = 2$

also note $G = \bigcup_{l \in \mathcal{L}_H} l$ and

$g_0 H \neq g_1 H$ implies that $g_0 H \cap g_1 H = \emptyset$

so $G \setminus H \cup H = G = H \cup xH$

i.e. $xH = G \setminus H$; similar for $\mathcal{R}_H$, say $Hy = G \setminus H$

Let $g \in G$; note $\omega \in S$ iff $\omega S = S = S\omega$

if $g \in H$, $gH = H = Hg$,

if $g \notin H$, $gH \neq H$ and $Hg \neq H$

i.e. $gH = xH$ and $Hg = Hy$

so $gH = G \setminus H = Hg$

hence $H \lhd G$ ∎

Theorem: $\phi_{G \to H}$: homo $\Longrightarrow \ker(\phi) \triangleleft G$.

Proof: note that $\ker(\phi) \leq G$, since ϕ: homo

Let $k \in \ker(\phi)$, $g \in G$;

$$\begin{aligned}
\phi(g \cdot k \cdot g^{-1}) &= \phi(g) \otimes \phi(k) \otimes \phi(g^{-1}) \\
&= \phi(g) \otimes e_H \otimes \phi(g^{-1}) \\
&= \phi(g) \otimes \phi(g^{-1}) \\
&= \phi(g) \otimes [\phi(g)]^{-1} \\
&= e_H
\end{aligned}$$

So $g \cdot k \cdot g^{-1} \in \ker(\phi)$

Hence, $\ker(\phi) \triangleleft G$ ∎

Theorem: $G \triangleright N \xrightarrow[\text{epi}]{\phi} H \implies \phi(N) \triangleleft H$.

Proof: note that $\phi(N) \leq H$, since ϕ: homo

let $\omega \in \phi(N)$, $h \in H$;

since ϕ: surj , $\exists \tilde{\omega}, \tilde{h} : \phi(\tilde{\omega}) = \omega \wedge \phi(\tilde{h}) = h$

note that $\tilde{h} \cdot \tilde{\omega} \cdot \tilde{h}^{-1} \in N$, as $N \ni \tilde{\omega} \triangleleft G$

so $\phi(\tilde{h} \cdot \tilde{\omega} \cdot \tilde{h}^{-1}) \in \phi(N)$

i.e. $\phi(\tilde{h}) \otimes \phi(\tilde{\omega}) \otimes \phi(\tilde{h}^{-1}) \in \phi(N)$

i.e. $\phi(\tilde{h}) \otimes \phi(\tilde{\omega}) \otimes [\phi(\tilde{h})]^{-1} \in \phi(N)$

i.e. $h \otimes \omega \otimes h^{-1} \in \phi(N)$

hence $\phi(N) \triangleleft H$ ∎

Theorem: $G \xrightarrow[\text{homo}]{\phi} H_{\triangleright N} \Longrightarrow \phi^{-1}(N) \triangleleft G$.

Proof: note that $\phi^{-1}(N) \leq G$, since ϕ: homo

let $\omega \in \phi^{-1}(N)$, $g \in G$;

note that $\phi(g \cdot \omega \cdot g^{-1}) = \phi(g) \circledast \phi(\omega) \bullet \phi(g^{-1})$

$= \phi(g) \circledast \phi(\omega) \circledast [\phi(g)]^{-1}$

also note that, since $N_{\ni \phi(\omega)} \triangleleft H$,

$\phi(g) \circledast \phi(\omega) \circledast [\phi(g)]^{-1} \in N$

i.e. $\phi(g \cdot \omega \cdot g^{-1}) \in N$

i.e. $\phi^{-1}(\phi(g \cdot \omega \cdot g^{-1})) \in \phi^{-1}(N)$

i.e. $g \cdot \omega \cdot g^{-1} \in \phi^{-1}(N)$

hence $\phi^{-1}(N) \triangleleft G$ ∎

Def: $HK = \{h \cdot k : h \in H \wedge k \in K\} : H \leq G \wedge K \leq G$

Theorem: let $H \leq G$, $K \leq G$;

$$HK \leq G \iff HK = KH$$

Proof: ($\Longrightarrow$): let $x \in HK$,

i.e. $\exists h_{\in H}, k_{\in K} : x = h \cdot k$,

note that $x^{-1} = (h \cdot k)^{-1} = k^{-1} \cdot h^{-1} \in KH$

so $\omega^{-1} \in KH : \omega \in HK$, fix $\omega = x^{-1}$;

$x_{(=(x^{-1})^{-1})} \in KH$ so $HK \subseteq KH$

let $y \in KH$, i.e $\exists k_{\in K}, h_{\in H} : y = k \cdot h$

note that $h_{(= h \cdot e_G)} \in HK$

and $k_{(= e_G \cdot k)} \in HK$, so $y_{(= k \cdot h)} \in HK$

as $HK \leq G$, so $KH \subseteq HK$

hence $HK = KH$

Proof cont'd:

($\Longleftarrow$): Let $x, y \in HK$,

so $\exists h, h' \in_H, k, k' \in_K : x = h \cdot k \wedge y = h' \cdot k'$

since $HK = KH$ and $k \cdot h' \in KH$,

$\exists \tilde{h} \cdot \tilde{k} \in_{HK} : k \cdot h' = \tilde{h} \cdot \tilde{k}$,

so $x \cdot y = h \cdot k \cdot h' \cdot k' = h \cdot \tilde{h} \cdot \tilde{k} \cdot k'$

as $H \leq G$ and $K \leq G$; $h \cdot \tilde{h} \in H$, $\tilde{k} \cdot k' \in K$

So $x \cdot y \in HK$

also $e_G \in HK$, as $e_G^{\in H \leq G} \cdot e_G^{\in K \leq G} = e_G$

also $x^{-1} = (h \cdot k)^{-1} = k^{-1} \cdot h^{-1} \in KH$

So $x^{-1} \in HK$, as $HK = KH$

hence $HK \leq G$ ∎

Def: $G/N := \{gN : g \in G\}$: $N \trianglelefteq G$.

Prop: G/N : group.

Proof:

i. let $x, y \in G/N$ i.e. $\exists x', y' \in G : x = x'N$ $\wedge$ $y = y'N$, note $x' \cdot y' \in G$, hence

$$xy = (x'N)(y'N) = (x' \cdot y')N \in G/N$$

ii. $$xN(yNzN) = xN(y \cdot z)N$$
$$= (x \cdot (y \cdot z))N = ((x \cdot y) \cdot z)N$$
$$= (x \cdot y)N\, zN = (xN\, yN)\, zN$$

iii. $e_{G/N} = e_G N$:

$$e_G N\, xN = (e_G \cdot x)N = xN$$
$$= (x \cdot e_G)N = xN\, e_G N$$

iv. $(xN)^{-1} = x^{-1}N$:

$$xN(xN)^{-1} = xN\, x^{-1}N = (x \cdot x^{-1})N$$
$$= e_G N = e_{G/N}$$ ∎

Prop: $G : ab \Longrightarrow G/N : ab$.

Proof: let $x, y \in G/N$;

$$xy = x'N\,y'N = (x' \cdot y')N$$
$$= (y' \cdot x')N = y'N\,x'N = yx$$ ■

Prop: $\langle x \rangle / H = \langle xH \rangle$.

Proof: let $\omega \in \langle x \rangle / H$

i.e. $\exists \tilde{x}_{\in \langle x \rangle} : \omega = \tilde{x}H$, but $\exists k : \tilde{x} = x^k$

so $\exists q_{(=k)} : \omega = x^q H = (xH)^q$

hence $\omega \in \langle xH \rangle$ ■

Prop: $G/Z(G) : \text{cyclic} \Longrightarrow G : ab$.

Proof: $\exists \sigma_{\in G/Z(G)} : G/Z(G) = \langle \sigma \rangle$,

but $\exists \omega_{\in G} : \sigma = \omega Z(G)$ i.e. $G/Z(G) = \langle \sigma \rangle$

$= \langle \omega Z(G) \rangle$

let $x, y \in G$, note $G = \bigcup_{C \in G/Z(G)} C$,

so $\exists C_0, C_1 \in G/Z(G) : x \in C_0$, $y \in C_1$

but $\exists i_j : C_j = (\omega Z(G))^{i_j} = \omega^{i_j} Z(G)$

Proof cont'd: so $\exists z_0, z_1 \in Z(G)$: $x = \omega^{i_0} z_0$, $y = \omega^{i_1} z_1$

hence $$\begin{aligned} xy &= \omega^{i_0} z_0 \omega^{i_1} z_1 = \omega^{i_0} \omega^{i_1} z_0 z_1 \\ &= \omega^{i_0+i_1} z_0 z_1 = \omega^{i_1+i_0} z_0 z_1 \\ &= \omega^{i_1} \omega^{i_0} z_0 z_1 = \omega^{i_1} \omega^{i_0} z_1 z_0 \\ &= \omega^{i_1} z_1 \omega^{i_0} z_0 = yx \end{aligned}$$ ∎

Def: $[x,y] := xyx^{-1}y^{-1}$.

Prop: $G/N : ab \iff [x,y] \in N : x,y \in G$.

Proof: $G/N : ab \iff xy = yx : x,y \in G/N$

$\iff xNyN = yNxN$

$\iff xNyNx^{-1}Ny^{-1}N = N \quad (= e_{G/N})$

$\iff xyx^{-1}y^{-1}N \quad (= [x,y]N) = N$

$\iff [x,y] \in N$ ∎

Prop: $G/N : ab \wedge G/K : ab \implies G/(N \cap K) : ab$.

Proof: note $N \cap K \trianglelefteq G$ since $N \trianglelefteq G$,

let $x,y \in G$; $[x,y] \in N$ and $[x,y] \in K$

so $[x,y] \in N \cap K$, hence $G/(N \cap K) : ab$ ∎

Def: $q_{N\, G \to G/N} : x \mapsto xN$.

Prop: q_N : epi .

Proof: i. $q_N(xy) = xyN = xN\,yN = q_N(x)\, q_N(y)$

ii. $\forall c_{\in G/N}\ \exists x_{\in G} : c = xN$ i.e. $q_N(x) = c$ ∎

Prop: $\ker(q_N) = N$.

Proof: $x \in \ker(q_N) \iff q_N(x) = e_{G/N} (= N)$

$\iff xN = N \iff x \in N$ ∎

Prop: $H/N \triangleleft G/N : H \triangleleft G$.

Proof: let $hN \in H/N$, $gN \in G/N$;

define $\tilde{h} := ghg^{-1}$, note that $\tilde{h} \in H$ as $H \triangleleft G$,

$(gN)\, hN\, (gN)^{-1} = gN\, hN\, g^{-1}N$

$= ghg^{-1}N = \tilde{h}N \in H/N$ ∎

Def: $G \times^{\theta} H := \{(g,h)_{\in G \times H} \mid \theta(gN) = hK \}$:

$\theta : G/N \xrightarrow{\cong} H/K$.

Prop: $G \times^{\theta} H \leq G \times H$.

Proof: i. since $e_{G/N} \xrightarrow{\theta} e_{H/K}$ as θ : homo ;

$\theta(e_G N) = \theta(e_{G/N}) = e_{H/K} = e_H K$,

so $(e_G, e_H) \in G \times^{\theta} H$ so $G \times^{\theta} H \neq \emptyset$

ii. let $(g,h), (g',h') \in G \times^{\theta} H$,

$\theta((gg')N) = \theta(gNg'N) = \theta(gN)\,\theta(g'N)$

$= hKh'K = (hh')K$

so $(g,h) \cdot (g',h')_{(:=(gg',hh'))} \in G \times^{\theta} H$

iii. let $(g,h) \in G \times^{\theta} H$,

$\theta(g^{-1}N) = \theta((gN)^{-1}) = [\theta(gN)]^{-1}$

$= [hK]^{-1} = h^{-1}K$

so $(g,h)^{-1}_{(:=(g^{-1},h^{-1}))} \in G \times^{\theta} H$ ∎

Prop: $NH \leq G : H \leq G \wedge N \lhd G$.

Proof: i. $e_G (= e_G e_G = e_N e_H) \in NH$, so $NH \neq \emptyset$

ii. let $n_0 h_0, n_1 h_1 \in NH$,

$$(n_0 h_0)(n_1 h_1) = n_0 (h_0 n_1 h_0^{-1} h_0) h_1$$

$$= n_0 (h_0 n_1 h_0^{-1}) (h_0 h_1)$$

say $n := h_0 n_1 h_0^{-1}$, note $n \in N$ as $N \lhd G$,

so $(n_0 h_0)(n_1 h_1) = (n_0 n)(h_0 h_1) \in NH$

iii. let $nh \in NH$, say $\tilde{n} := h^{-1} n^{-1} h$

note $\tilde{n} \in N$ as $N \lhd G$, so

$(nh)^{-1} = h^{-1} n^{-1} = h^{-1} n^{-1} h h^{-1} = \tilde{n} h^{-1} \in NH$

hence $NH \leq G$ ∎

Prop: $N \lhd NH : H \leq G \wedge N \lhd G$.

Proof: note that $NH \leq G$ as $N \lhd G$

so $NH = HN$; let $hn \in NH (= HN)$, $\bar{n} \in N$,

say $\tilde{n} := n \bar{n} n^{-1}$, note $\tilde{n} \in N$, and $g \tilde{n} g^{-1} \in N \lhd G$

$(hn) \bar{n} (hn)^{-1} = h n \bar{n} n^{-1} h^{-1}$

$= h \tilde{n} h^{-1} \in N$ ∎

Prop: $X(Y \cap Z) \subseteq XY \cap XZ$: $X, Y, Z \leq G$

Proof: let $\omega \in X(Y \cap Z)$,

then $\exists x_{\in X}, \sigma_{\in Y \cap Z} : \omega = x\sigma$;

note $x\sigma \in XY$ as $\sigma \in Y_{\geq Y \cap Z}$,

and $x\sigma \in XZ$ as $\sigma \in Z_{\geq Y \cap Z}$

hence $\omega_{(= x\sigma)} \in XY \cap XZ$ ∎

Prop: $X \cap YZ = Y(X \cap Z)$:

$X, Y_{\leq X}, Z \leq G$.

Proof: ($\subseteq$): let $s \in X \cap YZ$

so $\exists y_{\in Y}, z_{\in Z} : s = yz$ as $s \in YZ$

i.e. $z = y^{-1}s$, note $s \in X$ and $y^{-1} \in Y^{\leq G}_{\leq X}$

so $z \in X_{\leq G}$, hence $z \in X \cap Z$

so $s \in Y(X \cap Z)$

($\supseteq$): note $YX \subseteq XX$ as $Y \subseteq X$

so $YX \subseteq X_{(= xx)}$, also note that

$Y(X \cap Z) \subseteq YX \cap YZ$ and $YX \cap YZ \subseteq X \cap YZ$

hence $Y(X \cap Z) \subseteq X \cap YZ$ ∎

Prop: $N_1(H_1 \cap N_2) \lhd N_1(H_1 \cap H_2)$:

$H_1 \rhd N_1$, $H_2 \rhd N_2 \leq G$.

Proof: Let $\omega \in N_1(H_1 \cap N_2)$

and $\sigma \in N_1(H_1 \cap H_2)$, so

$\exists n_1 \in N_1, x \in H_1 \cap N_2 : \omega = n_1 x$, and

$\exists n_1' \in N_1, y \in H_1 \cap H_2 : \sigma = n_1' y$;

define $\overline{n}_1 := y n_1 y^{-1}$, note $\overline{n}_1 \in N_1$ as $y \in H_1$,

define $n_2 := y x y^{-1}$, note $n_2 \in N_2$

as $y \in H_2$ and $x \in N_2$, also note

$n_2 \in H_1$ as $y \in H_1$ so is $y^{-1} \in H_1^{\leq G}$ and $x \in H_1$,

define $\widehat{n}_1 := n_2 n_1'^{-1} n_2^{-1}$, note $\widehat{n}_1 \in N_1$

as $n_2 \in H_1$ and $n_1'^{-1} \in N_1^{\leq G}$,

define $\widetilde{n}_1 := n_1' \overline{n}_1 \widehat{n}_1$, note $\widetilde{n}_1 \in N_1$,

So; $\sigma \omega \sigma^{-1} = (n_1' y)\, n_1 x\, (n_1' y)^{-1}$

$= n_1' y\, n_1 x\, y^{-1} n_1'^{-1} = n_1' y\, n_1 y^{-1} y\, x\, y^{-1} n_1'^{-1}$

$= n_1' \overline{n}_1\, n_2\, n_1'^{-1} = n_1' \overline{n}_1\, n_2\, n_1'^{-1} n_2^{-1} n_2$

$= n_1' \overline{n}_1 \widehat{n}_1\, n_2 = \widetilde{n}_1\, n_2$ ∎

Prop: $(H_1 \cap N_2)(N_1 \cap H_2) \trianglelefteq H_1 \cap H_2$:

$H_1 \trianglelefteq N_1$, $H_2 \trianglelefteq N_2 \leq G$.

Proof: let $\omega \in (H_1 \cap N_2)(N_1 \cap H_2)$

and $\sigma \in H_1 \cap H_2$, so $\exists x_{\in H_1 \cap N_2}, y_{\in N_1 \cap H_2}$:

$\omega = xy$; define $g := \sigma x \sigma^{-1}$,

note $g \in N_2$ as $\sigma \in H_2$ and $x \in N_2$, and

$g \in H_1$ as $x \in H_1$ and $\sigma \in H_1$ so is

$\sigma^{-1} \in H_1 \leq G$

define $h := \sigma y \sigma^{-1}$,

note $h \in N_1$ as $\sigma \in H_1$ and $y \in N_1$, and

$h \in H_2$ as $y \in H_2$ and $\sigma \in H_2$

so is $\sigma^{-1} \in H_2 \leq G$

so; $\sigma \omega \sigma^{-1} = \sigma x y \sigma^{-1}$

$= \sigma x \sigma^{-1} \sigma y \sigma^{-1}$

$= gh$ ∎

Theorem: $\phi(G) \cong G/\ker(\phi)$: $G \xrightarrow[\text{homo}]{\phi} H$.

Proof: note that $G/\ker(\phi)$ exists as $\ker(\phi) \triangleleft G$

define $\psi_{G/\ker(\phi) \to H} : x\ker(\phi) \mapsto \phi(x)$

let $x, y \in G$;

$$x\ker(\phi) = y\ker(\phi) \iff x^{-1} \cdot y \in \ker(\phi)$$

$$\iff \phi(x^{-1} \cdot y) = e_H \iff \phi(x^{-1}) \otimes \phi(y) = e_H$$

$$\iff [\phi(x)]^{-1} \otimes \phi(y) = e_H \iff \phi(x) = \phi(y)$$

$$\iff \psi(x\ker(\phi)) = \psi(y\ker(\phi))$$

so ψ : well-defined by [$\Longrightarrow$],

and ψ : inj by [$\Longleftarrow$],

also ψ : surj as $\forall (\phi(x))_{\in \phi(G)} \exists y^{(=x\ker(\phi))}_{\in G/\ker(\phi)} : \psi(y) = \phi(x)$

hence ψ : bij

also ψ : homo as : let $x, y \in G$;

$$\psi(x\ker(\phi)\, y\ker(\phi)) = \psi((x \cdot y)\ker(\phi))$$

$$= \phi(x \cdot y) = \phi(x) \otimes \phi(y) = \psi(x\ker(\phi)) \otimes \psi(y\ker(\phi))$$

so ψ : iso ,

hence $\phi(G) \underset{\psi}{\cong} G/\ker(\phi)$ ∎

Theorem: $\mathcal{H}/\mathcal{H}\cap\mathcal{N} \cong \mathcal{H}\mathcal{N}/\mathcal{N}$:

$\mathcal{H} \leq G \;\wedge\; \mathcal{N} \trianglelefteq G$.

Proof: note that $\mathcal{H}/\mathcal{H}\cap\mathcal{N}$ exists

since $\mathcal{H}\cap\mathcal{N} \trianglelefteq \mathcal{H}$ as $\mathcal{N} \trianglelefteq G$

also, note that $\mathcal{H}\mathcal{N}/\mathcal{N}$ exists

since $\mathcal{N} \trianglelefteq \mathcal{H}\mathcal{N}$ as $\mathcal{N} \trianglelefteq G$

define $\phi_{\mathcal{H}\to\mathcal{H}\mathcal{N}/\mathcal{N}} : h \mapsto h\mathcal{N}$

note that $h\mathcal{N} \in \mathcal{H}\mathcal{N}/\mathcal{N}$ since $h\,(=h\cdot e_G) \in \mathcal{H}\mathcal{N}$

Let $x,y \in \mathcal{H}$; $\phi(x\cdot y) = (x\cdot y)\mathcal{N} = x\mathcal{N}\,y\mathcal{N} = \phi(x)\phi(y)$

so ϕ : homo , note that $e_{\mathcal{H}\mathcal{N}} = e_G$

since $\mathcal{H}\mathcal{N} \leq G$ as $\mathcal{N} \trianglelefteq G$

so $e_{\mathcal{H}\mathcal{N}/\mathcal{N}} = e_{\mathcal{H}\mathcal{N}}\mathcal{N} = e_G\mathcal{N} = \mathcal{N}$,

$\ker(\phi) = \{h_{\in\mathcal{H}} : \phi(h) = e_{\mathcal{H}\mathcal{N}/\mathcal{N}}\} = \{h_{\in\mathcal{H}} : \phi(h) = \mathcal{N}\}$

$= \{h_{\in\mathcal{H}} : h\mathcal{N} = \mathcal{N}\} = \{h_{\in\mathcal{H}} : h \in \mathcal{N}\} = \mathcal{H}\cap\mathcal{N}$

$\phi(\mathcal{H}) = \mathcal{H}\mathcal{N}/\mathcal{N}$ as $x \in \mathcal{H}\mathcal{N}/\mathcal{N} \iff \exists h_{\in\mathcal{H}}, n_{\in\mathcal{N}}$:

$x = hn\mathcal{N} \iff x = h\mathcal{N} \iff x\,(=\phi(h)) \in \phi(\mathcal{H})$

$\mathcal{H}/\mathcal{H}\cap\mathcal{N} = \mathcal{H}/\ker(\phi) \cong \phi(\mathcal{H}) = \mathcal{H}\mathcal{N}/\mathcal{N}$ ■

Theorem: $\frac{G/N}{H/N} \cong \frac{G}{H}$: $H, N_{\leq H} \triangleleft G$.

Proof: note that H/N exists as $N \triangleleft H$,

and also note that $\frac{G/N}{H/N}$ exists as $H/N \triangleleft G/N$,

define $\phi_{G/N \to G/H} : gN \mapsto gH$;

ϕ: well-defined ;

$$xN = yN \implies y^{-1} \cdot x \in N_{\leq H}$$

$$\implies y^{-1} \cdot x \in H \implies xH = yH$$

$$\implies \phi(xN) = \phi(yN)$$

ϕ: homo ;

$$\phi(xN\ yN) = \phi((x \cdot y)N) = (x \cdot y)H$$

$$= xH\ yH = \phi(xN)\ \phi(yN)$$

$\phi(G/N) = G/H$;

$$x \in G/H \iff \exists_{g \in G} : x = gH$$

$$\iff \exists_{g \in G} : x = \phi(gN) \iff x \in \phi(G/N)$$

$$\ker(\phi) = \{ gN_{\in G/N} : \phi(gN) = e_{G/H\ (= e_G H = H)} \}$$

$$= \{ gN_{\in G/N} : \phi(gN) = H \} = \{ gN_{\in G/N} : gH = H \}$$

$$= \{ gN_{\in G/N} : g \in H \} = H/N$$

$$(G/N)/(H/N) = (G/N)/\ker(\phi) \cong \phi(G/N) = G/H$$

Theorem: $H_1 \triangleright N_1, H_2 \triangleright N_2 \leq G$

$$\Longrightarrow \frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \cong \frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)} .$$

Proof: note that $\dfrac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)}$ exists

as $N_1(H_1 \cap N_2) \triangleleft N_1(H_1 \cap H_2)$

and also note that $\dfrac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)}$ exists

as $(H_1 \cap N_2)(N_1 \cap H_2) \triangleleft H_1 \cap H_2$;

$(H_1 \cap N_2)H_2 = H_2$ since $H_1 \cap N_2 \leq H_2$

as $H_1 \cap N_2 \leq G$ and $H_1 \cap N_2 \subseteq N_2 \subseteq H_2$

$H_1 \cap ([H_1 \cap N_2]H_2) = [H_1 \cap N_2](H_1 \cap H_2)$

as $H_1 \cap N_2 \subseteq H_1$

$N_1(H_1 \cap H_2) = N_1(H_1 \cap ([H_1 \cap N_2]H_2))$

$= N_1(H_1 \cap N_2)(H_1 \cap H_2)$;

$(H_1 \cap H_2) \cap N_1(H_1 \cap N_2)$

$= (H_1 \cap H_2) \cap (H_1 \cap N_2)N_1$

$= (H_1 \cap N_2)[(H_1 \cap H_2) \cap N_1^{\subseteq H_1}]$

$= (H_1 \cap N_2)(N_1 \cap H_2)$;

Proof cont'd :

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} = \frac{[N_1(H_1 \cap N_2)](H_1 \cap H_2)}{N_1(H_1 \cap N_2)}$$

$$\cong \frac{H_1 \cap H_2}{(H_1 \cap H_2) \cap N_1(H_1 \cap N_2)}$$

$$= \frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)}$$