1) <u>$\mathrm{Aut}(\mathbb{Z})$</u>: Any automorphism $\varphi : \mathbb{Z} \to \mathbb{Z}$ is determined by $\varphi(1)$ since for n positive, $\varphi(n) = \varphi(\underbrace{1+\dots+1}_{n \text{ times}}) = \underbrace{\varphi(1)+\dots+\varphi(1)}_{n \text{ times}}$

for $-n$ $\quad \varphi(-n) = -\varphi(n)$

for $n=0$ $\quad \varphi(0) = 0$.

Any automorphism must be <u>surjective</u> $\Rightarrow \varphi(1) = \pm 1$

Otherwise 1 is not in the image of φ.

if $\varphi(1) = 1 \Rightarrow \varphi = id$, if $\varphi(1) = -1 \Rightarrow \varphi(n) = -n$

So $|\mathrm{Aut}(\mathbb{Z})| = 2$, & if $\varphi(n) = -n$ then $\varphi \circ \varphi = id$

$\Rightarrow \mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2$

<u>$\mathrm{Aut}(\mathbb{Z}/n)$</u>: As before any automorphism $\varphi : \mathbb{Z}/n \longrightarrow \mathbb{Z}/n$ is determined by $\varphi([1]_n) \in \mathbb{Z}/n$.

Claim: if $\varphi([1]_n) = [u]_n \in \mathbb{Z}/n$ (φ group hom) then φ is an automorphism $\Leftrightarrow (u,n) = 1$

($\Leftarrow$) $(u,n) = 1$ then $\exists$ integers $k, l \in \mathbb{Z}$ s.t. $ku + ln = 1$

to see that φ is surjective, let $[a]_n \in \mathbb{Z}/n$. We know

$aku + aln = a \Rightarrow [aku + aln]_n = [aku]_n = [a]_n$

but this means $\varphi([ak]_n) = [aku]_n = [a]_n$ so φ is surjective

By the pigeonhole principle φ is injective so φ is an automorphism.

($\Rightarrow$) if φ an automorphism ~~then φ is surjective~~.

where $\varphi([1]_n) = [u]_n$. φ is in particular surjective so

$\exists [k]_n \in \mathbb{Z}/n$ s.t. $\varphi([b]_n) = [ub]_n = [1]_n$

i.e. $uk \equiv 1 \mod n \Rightarrow \exists l \in \mathbb{Z}$ w/ $uk + ln = 1 \Rightarrow (u,n) = 1$.

So $Aut(\mathbb{Z}/n) = \{ [u]_n : (u,n) = 1 \}$ with the group operation multiplication (which corresponds to composition).

2a) Need to show that for any $\psi \in Aut(G)$ we have

$$\boxed{\psi \, Inn(G) \, \psi^{-1} \subseteq Inn(G)}$$

for $g \in G$, let $Inn_g \in Inn(G)$ denote the automorphism given by conjugation by g

i.e. $Inn_g(x) = gxg^{-1}$.
$(x \in G)$

need to show for any $g \in G$, that $\psi \circ Inn_g \circ \psi^{-1} \in Inn(G)$

for $x \in G$

$$\psi \circ Inn_g \circ \psi^{-1}(x) = \psi(g \psi^{-1}(x) g^{-1}) = \psi(g)\psi(\psi^{-1}(x))\psi(g^{-1})$$
$$= \psi(g) \, x \, \psi(g)^{-1}$$
$$= Inn_{\psi(g)}(x)$$

$$\Rightarrow \psi \circ Inn_g \circ \psi^{-1} = Inn_{\psi(g)} \in Inn(G)$$

$$\Rightarrow \boxed{\psi \, Inn(G) \, \psi^{-1} \subseteq Inn(G)}$$

so $Inn(G)$ is a normal subgroup of $Aut(G)$

2b) Recall that if $\varphi : G \to H$ a group homomorphism then $\mathrm{Im}(\varphi) \cong G/_{\mathrm{Ker}(\varphi)}$. In particular if φ is surjective

$\Rightarrow H \cong G/_{\mathrm{Ker}(\varphi)}$.

Claim: $\exists$ a surjective group homomorphism (for any group G)

$$\mathrm{Inn} : G \longrightarrow \mathrm{Inn}(G), \quad \mathrm{Inn}(g) = \mathrm{Inn}_g \quad (\text{where } \mathrm{Inn}_g(x) = gxg^{-1})$$

with kernel $Z(G)$ (the center of G)

Clearly Inn is surjective since every element of $\mathrm{Inn}(G)$ is of the form Inn_g for $g \in G$ & $\mathrm{Inn}(g) = \mathrm{Inn}_g$.

g is in the kernel of Inn $\Leftrightarrow$ $\mathrm{Inn}(g) = \mathrm{Inn}_g = \mathrm{id}$

this would mean that $\mathrm{Inn}_g(x) = x \ \forall x \in G$

i.e. $gxg^{-1} = x \ \forall x G \Rightarrow gx = xg \ \forall x \in G \Leftrightarrow g \in Z(G)$.

This means $\mathrm{Inn}(G) \cong G/_{Z(G)}$ so

- $\mathrm{Inn}(S_3) \cong S_3/Z(S_3)$
- $\mathrm{Inn}(S_4) \cong S_4/Z(S_4)$

Ex: $Z(S_n) = \{e\} \ \forall n$.

$\Rightarrow \mathrm{Inn}(S_3) \cong S_3, \ \mathrm{Inn}(S_4) \cong S_4$.

3a) Suppose $gH = Hg \ \forall g \in G$, ~~Claim~~ Want $gHg^{-1} \subseteq H$

~~Let $g \in G$, since $gH = Hg$~~

Let $g \in G$, $h \in H$, Claim: $ghg^{-1} \in H$.

Since $gH = Hg$ we have that $gh = h'g$ for some $h' \in H$

$\Rightarrow ghg^{-1} = h'gg^{-1} = h' \in H$

so H is normal

b) Suppose the index of H is 2.

Then the left cosets are $H = \{h \in H\}$, $gH = \{gh : h \in H\} = G \setminus H$

the right cosets are $H = \{h \in H\}$, $Hg = \{hg : h \in H\} = G \setminus H$

~~Since cosets~~ but this tells us that $gH = Hg \Rightarrow H$ is normal by a)

4) Claim: Let G be cyclic with $G = \langle g \rangle$ then any subgroup H is ~~also~~ cyclic, $H = \langle g^i \rangle$ for some i.

Let H be a non-trivial subgroup. Let i be the smallest positive ~~non-negative~~ integer with $g^i \in H$. Then I claim $H = \langle g^i \rangle$. (certainly $\langle g^i \rangle \subseteq H$)

~~Then~~ let $h \in H$, since $G = \langle g \rangle \Rightarrow h = g^j$ for some j w/ $i < j$.

(we can assume j is positive, otherwise take $-j$ & use that fact subgroups are closed under inverses).

Divison algorithm gives $j = ki + r$ for $0 \leq r < i$

$\Rightarrow h = g^j = (g^i)^k g^r \Rightarrow g^r = (g^j) \cdot (g^i)^{-k} \in H$ but i was smallest +ve integer

$\Rightarrow r = 0 \Rightarrow$ ~~g^j~~ $h = g^j = (g^i)^k$ ~~$\cdot$~~ $\Rightarrow H = \langle g^i \rangle$.

4 continued...

By the claim the subgroups of $\mathbb{Z}$ are $\langle n\mathbb{Z}\rangle$ for $n\in\mathbb{Z}$

By the claim the subgroups of $\underset{\langle g\rangle}{C_n} \cong$ are $\langle g^i\rangle$ for $i = 0,\dots,n-1$

In fact the subgroups of C_n are covered by the cases $i|n$ because g^i has order $n/\gcd(n,i)$ so we only need to consider divisors of n.

All of these subgroups are normal because cyclic groups are abelian & for any abelian group G, any subgroup H is normal since $gH = Hg$ (since the order ~~...~~ can be swapped)

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

taking the cyclic subgroups generated by each element gives 4 non-trivial subgroups: $\langle(123)\rangle = \langle(132)\rangle = A_3 = \{e,(123),(132)\} \cong C_3$.

as well as $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$ all isomorphic to C_2.

Claim: these are all subgroups of S_3.

any other non-trivial subgroup H would have to contain two elements from different cyclic subgroups above. If H contains a 2-cycle & a 3-cycle (e.g. (12) & (123)) then it automatically contains 4 elements (the cyclic subgroup generated by the 3-cycle & the 2-cycle) but $|H| \mid |S_3| = 6$ & $4 \nmid 6$ so $|H|$ must be 6 $\Rightarrow H = S_3$

if H contains 2 2-cycles (e.g. (12) & (13)) then it also contains a 3 cycle given by the product (e.g. $(12)(13) = (132)$) $\Rightarrow$ ~~...~~ ~~...~~

~~we have~~ $H = S_3$ again.

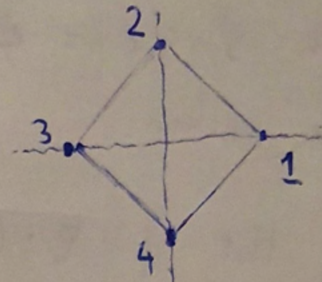
$C_{mn} \cong C_m \times C_n \iff (m,n)=1$

~~A4~~ A_3 is normal since its index is $|S_3|/|A_3| = 6/3 = 2$.

none of the others are normal since for example

$(13)(12)(13) = (23) \notin \langle(12)\rangle$ (& similarly for the others).

D_8: D_8 is the group of symmetries of



$D_8 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$

where r is rotation by $\pi/2$ & s is reflection in the x-axis.

equivalently D_8 is the subgroup of S_4 ~~gen~~ given by

$$D_8 = \{\overset{1}{e}, \overset{r}{(1234)}, \overset{r^2}{(13)(24)}, \overset{r^3}{(1432)}, \overset{s}{(24)}, \overset{rs}{(12)(34)}, \overset{r^2s}{(13)}, \overset{r^3s}{(14)(23)}\} \subseteq S_4$$

taking the cyclic subgroups generated by each element gives:

~~$\langle(1234)\rangle = \{1$~~

$\langle r\rangle$, $\langle r^2\rangle$, $\langle s\rangle$, $\langle rs\rangle$, $\langle r^2s\rangle$, $\langle r^3s\rangle$

where all but $\langle r\rangle$ have order 2, ~~which~~ $|\langle r\rangle| = 4$.

since D_8 is generated by r & s it is generated by r & any reflection.

The remaining subgroups are: $\langle r^2, s\rangle = \langle r^2, r^2s\rangle = \langle s, r^2s\rangle$

& $\langle r^2, rs\rangle = \langle r^2, r^3s\rangle = \langle rs, r^3s\rangle$.

all isomorphic to $C_2 \times C_2$.

all subgroups of order 4 are normal since they have index 2.

the only other subgroup which is normal is $\langle r^2\rangle$

since e.g. $\underset{r^2}{(13)(24)}$ commutes w/ (24), $(12)(34)$, (13) & $(14)(23)$

(& clearly other rotations

5) If $G/Z(G)$ is abelian there is some $g \in G$ w/ $G/Z(G) = \langle gZ(G) \rangle$

~~Let w,z∈~~

Let $h, k \in G$ $\quad h = g^i w$, $k = g^j z$ for $z, w \in Z(G)$.

But $hk = g^i w g^j z = \cancel{g^i w g^j} z\, g^{i+j} w = g^j z g^i w = kh$

so G is abelian.

6) a) Recall that if $\varphi : G \to H$ ~~is~~ a group homomorphism then $Im(\varphi) \cong G/Ker(\varphi)$, if φ is surjective $\Rightarrow H \cong G/Ker(\varphi)$

if A, B are groups there is a surjective group homomorphism

$$\begin{aligned} \pi_B : A \times B &\longrightarrow B \\ (a,b) &\longmapsto b \end{aligned}$$

so by the above result $B \cong A\times B/ker(\pi_B) = G/Ker(\pi_B)$

$Ker(\pi_A) = \{(a,b) : b = e_B\}$

but $Ker(\pi_B) \cong A$ via the isomorphism

$$\begin{aligned} Ker(\pi_B) &\longrightarrow A \\ (a, e_B) &\longmapsto a. \end{aligned} \quad \Rightarrow B \cong A\times B/Ker(\pi_B) \cong A\times B/A$$

The proof is similar for $G/B \cong A$.

b) $A_1 \subset A$, $B_1 \subset B$ are normal subgroups.

want to show that $(a,b) A_1 \times B_1 (a,b)^{-1} \subseteq A_1 \times B_1$ for any $(a,b) \in A \times B$.

Let $(a_1, b_1) \in A_1 \times B_1$

then $(a,b) \cdot (a_1, b_1) \cdot (a,b)^{-1} = (a a_1, b b_1) \cdot (a^{-1}, b^{-1})$

$= (a a_1 a^{-1}, b b_1 b^{-1}) \in A_1 \times B_1$ because $a a_1 a^{-1} \in A_1$, $b b_1 b^{-1} \in B_1$ since they are normal.

Next want to show that

$$A \times B / (A_1 \times B_1) \cong A/A_1 \times B/B_1$$

Consider the map $\varphi : A/A_1 \times B/B_1 \longrightarrow A \times B / (A_1 \times B_1)$

$$(aA_1, bB_1) \longmapsto (a,b) A_1 \times B_1$$

φ is a homomorphism: $a, a' \in A$, $b, b' \in B$

$$\varphi((aA_1, bB_1) \cdot (a'A_1, b'B_1))$$

$= \varphi(aa'A_1, bb'B_1) = (aa', bb') A_1 \times B_1$

$= (a,b) A_1 \times B_1 \cdot (a',b') A_1 \times B_1$

$= \varphi(aA_1, bB_1) \cdot \varphi(a'A_1, b'B_1)$.

6b continued...

Surjectivity: Let $(a,b)A_1 \times B_1 \in A\times B / A_1 \times B_1$

then $\varphi(aA_1, bB_1) = (a,b)A_1 \times B_1$ so φ is surjective.

Injectivity: Suppose $\varphi(aA_1, bB_1) = (e_A, e_B)A_1 \times B_1 = A_1 \times B_1$

$\Rightarrow (a,b)A_1 \times B_1 = (e_A, e_B)A_1 \times B_1 = A_1 \times B_1$

$\Rightarrow a \in A_1, b \in B_1 \Rightarrow \cancel{(a,b)A_1 \times B_1 = A}\ aA_1 = A_1, bB_1 = B_1$

so the kernel is just the identity element.

7) Let H be a subgroup of G containing $[G,G]$

need to show if $g \in G, h \in H \Rightarrow ghg^{-1} \in H$

we know $ghg^{-1}h^{-1} \in [G,G] \subseteq H$

so $ghg^{-1}h^{-1} \in H \Rightarrow ghg^{-1}h^{-1}h = ghg^{-1} \in H$

so H is normal.

8) Claim $C_{mn} \cong C_m \times C_n \iff (m,n) = 1$.

$(\Leftarrow)$ Let $C_m = \langle g \rangle$, $C_n = \langle h \rangle$ & Suppose $(m,n) = 1$

Claim that $(g,h) \in C_m \times C_n$ has order mn.

$(g,h)^a = (e_m, e_n) \iff g^a = e_m$, $h^a = e_n$

$\iff a|m$ & $a|n$

B_1 So the order of (g,h) is $\mathrm{lcm}(m,n) = \frac{m \cdot n}{(m,n)} = m \cdot n$.

Since $|C_m \times C_n| = m \cdot n$ & $\exists$ an element of order $m \cdot n$

$\Rightarrow C_m \times C_n$ is cyclic of order $m \cdot n$

$(\Rightarrow)$ if $(m,n) \neq 1 \Rightarrow (g,h)$ has order $\mathrm{lcm}(m,n) < m \cdot n$

$\Rightarrow$ there is no element of order $m \cdot n \Rightarrow C_m \times C_n$ not cyclic.