Question One

~ Given groups N and H, together with a group homomorphism $\varphi: H \to \mathrm{Aut}(N)$, we def
the semi-direct product $N \rtimes_\varphi H$ to be $N \times H$ with the group multiplication
by

$$(n_1,h_1)\cdot(n_2,h_2) \equiv (n_1\varphi(h_1)(n_2),\ h_1 h_2)$$

1) Show that this indeed defines a group
2) Show that $N \rtimes H$ contains N as a normal subgroup and H as a subgroup.
3) Give the formula for the adjoint action in terms of φ.

~1) Let $(n_1,h_1), (n_2,h_2), (n_3,h_3) \in N\times H$. Then

$$\begin{aligned}
[(n_1,h_1)\cdot(n_2,h_2)](n_3,h_3) &= (n_1\varphi(h_1)(n_2), h_1h_2)(n_3,h_3)\\
&= (n_1\varphi(h_1)(n_2)\varphi(h_1h_2)(n_3),\ h_1h_2h_3)\\
&= (n_1\varphi(h_1)(n_2)\varphi(h_1)(n_3)\varphi(h_2)(n_3),\ h_1h_2h_3)\\
&= (n_1\varphi(h_1)(n_2)\varphi(h_1)(\varphi(h_2)(n_3)),\ h_1h_2h_3)\\
&= (n_1\varphi(h_1)(n_2\varphi(h_2)(n_3)),\ h_1h_2h_3)\\
&= (n_1,h_1)(n_2\varphi(h_2)(n_3),\ h_2h_3)\\
&= (n_1,h_1)[(n_2,h_2)(n_3,h_3)]
\end{aligned}$$

(note that we've implicitly used the associativity of the underlying group operations for N
Therefore, the ~~group~~ binary operation is associative.

~ Denoting 1_N and 1_H as the identity elements of N, H respectively, we show that
$N\rtimes H$ is the identity element. For an arbitrary element (n,h) of $N\rtimes H$, we have t

$$\begin{aligned}
(1_N,1_H)(n,h) &= (1_N\varphi(1_H)(n),\ 1_H h)\\
&= (1_N\cdot n,\ 1_H h) = (n,h)
\end{aligned}$$

$\varphi(1_H) = I_N$ since homomorphisms preserve th

$$\begin{aligned}
&= (n1_N,\ h1_H)\\
&= (n\varphi(h)(1_N),\ h1_H) = (n,h)(1_N,1_H)
\end{aligned}$$

$\varphi(h)(1_N) = 1_N$

~ Lastly, we show that $(\varphi(h^{-1})(n^{-1}), h^{-1})$ is the inverse of any element $(n,h) \in N\rtimes H$
We have that

$$\begin{aligned}
(n,h)(\varphi(h^{-1})(n^{-1}),h^{-1}) &= (n\varphi(h)(\varphi(h^{-1})(n^{-1})),\ hh^{-1})\\
&= (n\varphi(h)(\varphi(h)^{-1}(n^{-1})),\ hh^{-1})\\
&= (nn^{-1},\ hh^{-1}) = (1_N,1_H)\\
&= (\varphi(h^{-1})(1_N),\ h^{-1}h)\\
&= (\varphi(h^{-1})(n^{-1}n),\ h^{-1}h)\\
&= (\varphi(h^{-1})(n^{-1})\varphi(h^{-1})(n),\ h^{-1}h)\\
&= (\varphi(h^{-1})(n^{-1}),\ h^{-1})(n,h)
\end{aligned}$$

(implicitly using the fact that inverses exist for N, H)

$\Rightarrow$ Hence, $N\rtimes_\varphi H$ is a group under the given binary operation.

~~In case $\alpha \in \mathbb{R}$, we get a RHS as ...~~

2) In $N \rtimes_\varphi H$, the mappings $n \mapsto (n, 1_H)$ and $h \mapsto (1_N, h)$, where $1_N, 1_H$ are the identity elements of N, H respectively, are obviously injective from N, H into $N \rtimes_\varphi H$. Moreover, it is immediate that the mappings are non-empty, since $(1_N, 1_H)$ are elements of the mapping. These multiply together like elements of N and H do:

$$(n_1, 1_H)(n_2, 1_H) = (n_1 \varphi(1_H)(n_2), 1_H 1_H) = (n_1 n_2, 1_H) \quad \text{since } \varphi(1_H) = 1_N$$
$$(1_N, h_1)(1_N, h_2) = (1_N \varphi(h_1)(1_N), h_1 h_2) = (1_N, h_1 h_2) \quad \text{since } \varphi(h)(1_N) = 1_N$$

Therefore, we have copies of N and H inside $N \rtimes_\varphi H$ in a natural way. Furthermore,

$$(n, 1_H)^{-1} = (\varphi(1_H^{-1})(n^{-1}), 1_H^{-1}) = (\varphi(1_H)(n^{-1}), 1_H) = (n^{-1}, 1_H)$$
$$(1_N, h)^{-1} = (\varphi(h^{-1})(1_N^{-1}), h^{-1}) = (\varphi(h^{-1})(1_N), h^{-1}) = (1_N, h^{-1})$$

Thus, we can write both subgroups as $N \times 1$ and $1 \times H$, which is ok since elements of $N \times 1$ multiply just like a direct product of N with the trivial subgroup, similarly for $1 \times H$.

For a single pair (n, h) in $N \rtimes_\varphi H$,

$$(n, 1_H)(1_N, h) = (n\varphi(1_H)(1_N), 1_H h) = (n, h)$$
and
$$(1_N, h)(\varphi^{-1}(h)(n), 1_H) = (1_N \varphi(h)(\varphi^{-1}(h)(n)), h \cdot 1_H) = (n, h)$$

To show $N \times 1$ is a normal subgroup of $N \rtimes_\varphi H$, it suffices to show $1 \times H$ in $N \rtimes_\varphi H$ conjugates $N \times 1$ back to itself, since $N \times 1$ does and each element of $N \rtimes_\varphi H$ is built from $N \times 1$ and $H \times 1$ (that is $(n, h) = (n, 1_H)(1_N, h)$):

$$\begin{aligned}(1_N, h)(n, 1_H)(1_N, h)^{-1} &= (1_N, h)(n, 1_H)(1_N, h^{-1}) \\ &= (1_N \varphi(h)(n), h \cdot 1_H)(1_N, h^{-1}) \\ &= (\varphi(h)(n), h)(1_N, h^{-1}) \\ &= (\varphi(h)(n) \cdot \varphi(h)(1_N), hh^{-1}) \\ &= (\varphi(h)(n), 1).\end{aligned}$$

This shows that $N \times 1$ is normal in $N \rtimes_\varphi H$.

3) This also shows that the action $\varphi : H \to \mathrm{Aut}(N)$ of H on N looks like conjugation of $1 \times H$ on $N \times 1$ inside $N \rtimes_\varphi H$. Explicitly:

$$h \cdot n = hnh^{-1} = (\varphi(h)(n), 1)$$

Question Two

Let N, H be groups and let $\varphi_1, \varphi_2 : H \to \mathrm{Aut}(N)$ be two group homomorphisms. Suppose that

$$N \rtimes_{\varphi_1} H \cong N \rtimes_{\varphi_2} H.$$

Also, suppose that there does not exist any group homomorphism $\psi : N \to H$ except for the trivial one (ie: sending $N \ni n \mapsto e \in H$). Show that in this case there exists

$$F \in \mathrm{Aut}(N),\ G \in \mathrm{Aut}(H)$$

such that

$$\varphi_1(h) = F \circ \varphi_2(G(h)) \circ F^{-1}$$

~ Let $\Psi : N \rtimes_{\varphi_2} H \to N \rtimes_{\varphi_1} H$ be an isomorphism. Then, Ψ restricts to the automorphism $F : N \to N$ by the projection mapping ~~[illegible]~~ $\rightarrow$
$\rho_1 : N \to N \times H$, $\rho_1(n) = (n, 1)$ $\Rightarrow$ $n \to \Psi((n,1))$. Similarly, Ψ restricts to the automorphism $G : H \to H$ by the mapping $h \to G((1,h))$.

We therefore have that

$$\varphi_1(h) = F \circ \varphi_2(G^{-1}(h)) \circ F^{-1}$$

Question Two

Let N, H be groups and let $\varphi_1, \varphi_2 : H \to \mathrm{Aut}(N)$ be two group homomorphisms. Suppose that

$$N \rtimes_{\varphi_1} H \cong N \rtimes_{\varphi_2} H.$$

Also, suppose that there does not exist any group homomorphism $\psi : N \to H$ except for the trivial one (ie: sending $N \ni n \mapsto e \in H$). Show that in the case there exists

$$F \in \mathrm{Aut}(N), \ G \in \mathrm{Aut}(H)$$

such that

$$\varphi_1(h) = F \circ \varphi_2(G(h)) \circ F^{-1}$$

~~[illegible] consider the action of $N \rtimes_{\varphi} H$ under the isomorphism [illegible]~~

~ Let $\Psi : N \rtimes_{\varphi_2} H \to N \rtimes_{\varphi_1} H$ be an isomorphism. Then, Ψ restricts to the automorphism $F : N \to N$ by the projection mapping ~~[illegible]~~ $\Rightarrow$ $\rho_1 : N \to N \times H$, $\rho_1(n) = (n, 1)$ $\Rightarrow$ $n \to F((n,1))$. Similarly, Ψ restricts to the automorphism $G : H \to H$ by the mapping $h \to G((1,h))$.

We therefore have that

$$\varphi_1(h) = F \circ \varphi_2(G^{-1}(h)) \circ F^{-1}$$

Question Three

Any group G of order $|G| = 30$ is either abelian or isomorphic to

$$\mathbb{Z}/15\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$$

where $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/15\mathbb{Z})$ is inclusion of an element of order 2 of $\mathrm{Aut}(\mathbb{Z}/15\mathbb{Z})$. Use Problem 2) to show that different elements of order 2 give non-isomorphic groups.

~ We have that $\mathrm{Aut}(\mathbb{Z}/15\mathbb{Z}) \cong (\mathbb{Z}/15\mathbb{Z})^{\times} = \{1,2,4,7,8,11,13,14\}$. The only elements of $(\mathbb{Z}/15\mathbb{Z})^{\times}$ with order 2 are 4, 11 and 14.

Thus, we have three homomorphisms $\varphi_i : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/15\mathbb{Z})$ $i \in \{1,2,3\}$ defined by $\varphi_i(\bar{1}) = \psi_i$, where $\psi_i : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$ is one of the automorphisms defined by $\psi_1(1) = 4$, $\psi_2(1) = 11$, $\psi_3(1) = 14$.

Since no element of $\mathbb{Z}/15\mathbb{Z}$ has order 2, there is no non-trivial homomorphism $\psi : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. It follows from Problem 2 that if

$$\mathbb{Z}/15\mathbb{Z} \rtimes_{\varphi_i} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z} \rtimes_{\varphi_j} \mathbb{Z}/2\mathbb{Z} \text{ for some } i,j \in \{1,2,3\},\ i \neq j,$$

then there exists $F \in \mathrm{Aut}(\mathbb{Z}/15\mathbb{Z})$ and $G \in \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ such that

$\varphi_i(y) = F \circ \varphi_j(G(y)) \circ F^{-1}$ $\forall y \in \mathbb{Z}/2\mathbb{Z}$. In particular

$\varphi_i(1) = F \circ \varphi_j(G(1)) \circ F^{-1}$

hence $\psi_i = F \circ \varphi_j(G(1)) \circ F^{-1}$

But, there is only one ~~ident~~ $G \in \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$, namely the identity automorphism. Hence,

$$\psi_i = F \circ \varphi_j(G(1)) \circ F^{-1} = F \circ \varphi_j(1) \circ F^{-1} = F \circ \varphi_j \circ F^{-1}$$

Case 1 $i=1, j=2 \Rightarrow \psi_1 = F \circ \psi_2 \circ F^{-1}$. Hence

$$4 = \psi_1(1) = F(\psi_2(F^{-1}(1)))$$
$$\Rightarrow F^{-1}(4) = \psi_2(F^{-1}(1))$$
$$\Rightarrow 4F^{-1}(1) = \psi_2(F^{-1}(1))$$

If $F^{-1}(1) = n$, then $\psi_2(F^{-1}(1)) \equiv 11n \pmod{15}$ and we obtain $4n \equiv 11n \pmod{15}$, that is $15 \mid 7n$. But, this is not possible since $\gcd(n,15) = 1$ because F^{-1} is an automorphism (element order $k \to$ element order

Thus, we cannot have $i=1, j=2$

Case 2 $i=1, j=3$. $\psi_1 = F \circ \psi_3 \circ F^{-1}$, hence

$$F^{-1}(4) = \psi_3(F^{-1}(1))$$
$$4F^{-1}(4) = \psi_3(F^{-1}(1))$$

If $F^{-1}(4) = n$, then $\psi_3(F^{-1}(1)) = 14n \pmod{15} \Rightarrow 4n \equiv 14n \pmod{15}$, that is $15 \mid 10n$. But, this is not possible since $\gcd(n,15) = 1$. Thus, we cannot have $i=1, j=3$.

Case 3 $i=2, j=3$. $\psi_2 = F \circ \psi_3 \circ F^{-1}$, hence

$$11 = \psi_2(1) = F(\psi_3(F^{-1}(1))) \Rightarrow F^{-1}(11) = \psi_3(F^{-1}(1)) \Rightarrow 11F^{-1}(1) = \psi_3(F^{-1}(1))$$

If $F^{-1}(1) = n$, then $\psi_3(F^{-1}(1)) = 14n \pmod{15} \Rightarrow 11n \equiv 14n \pmod{15}$, that is $15 \mid 3n$. But, $\gcd(n,15) = 1 \Rightarrow i=2, j=3$ cannot occur.

~ $\psi_i = F \circ \psi_j \circ F^{-1} \Rightarrow \psi_j = F^{-1} \circ \psi_i \circ F$ so we've checked all possibilities

Problem 4

Prove that a group of order $351 = 3^3 \cdot 13$ has a normal Sylow p-subgroup for some prime p dividing its order.

~ A Sylow 3-subgroup would have order $3^3 = 27$ and a Sylow 13-subgroup would have order 13. Let's start at by finding what n_{13} could be. $n_{13} \mid 27$ and $n_{13} \equiv 1 \mod 13$. The only two possibilities are $n_{13} = 1$ or $n_{13} = 27$. If $n_{13} = 1$, then the Sylow 13-subgroup is normal and we've done.

If $n_{13} = 27$, then we're going to show that there can only be room for one Sylow 3-subgroup, and therefore the Sylow 3-subgroup is normal in G.

Recall that distinct subgroups of order p for p prime can only have the identity element in their intersection. [Suppose P_1 and P_2 are subgroups of order p. Then $P_1 \cap P_2 \leq P_1$ and $P_1 \cap P_2 \leq P_2$. So $|P_1 \cap P_2|$ must be either 1 or p and the only way it can be p is if $P_1 \cap P_2 = P_1$ and $P_1 \cap P_2 = P_2$, making $P_1 = P_2$. Therefore, if P_1 and P_2 are not the same subgroup, their intersection is order 1, which contains only the identity element.] warning: this only works when the order of subgroups is prime eg: doesn't work ~~for~~ Sylow 13-subgroups of order 13^2.

Since the Sylow 13-subgroups are of order 13, hence prime, they can only intersect each other at the identity element. Also, every element of order 13 forms a subgroup of order 13, which has to be one of the Sylow 13-subgroups.

Each Sylow 13-subgroup contains 12 elements of order 13 (each element except the identity). There are 27 Sylow 13-subgroups, so there are a total of $27 \times 12 = 324$ elements of order 13 in G.

This leaves $351 - 324 = 27$ elements of G that do not have order 13. Since a Sylow 3-subgroup would have to have exactly 27 elements in it, this means that all the 27 elements form a Sylow 3-subgroup, and it must be the only one (no extra ele[ments] of G to use). So, $n_3 = 1$ and thus this Sylow 3-subgroup must be normal in G.

Problem 5

Show that

1) $Aut(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \cong Aut(\mathbb{Z}/n\mathbb{Z}) \times Aut(\mathbb{Z}/m\mathbb{Z})$ whenever $gcd(m,n)=1$

2) $|(\mathbb{Z}/p^\alpha\mathbb{Z})^\times| = p^{\alpha-1}(p-1)$, where p is a prime number and $\alpha \in \mathbb{N}$

3) Conclude that

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = p_1^{\alpha_1-1}(p_1-1) \cdots p_k^{\alpha_k-1}(p_k-1)$$

when $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of n

~1) Given any two groups G_1, G_2 we define the projection maps $\pi_i : G_1 \times G_2 \to G_i$ $i=1,2$ and the injection maps $\rho_i : G_i \to G_1 \times G_2$ $i=1,2$ as follows

$\rho_1(x_1) = (x_1, 1)$, $\rho_2(x_2) = (1, x_2)$ $\forall x_1 \in G_1, x_2 \in G_2$

$\pi_1(x_1,x_2) = x_1$, $\pi_2(x_1,x_2) = x_2$ $\forall x_1 \in G_1, x_2 \in G_2$

→ Lemma
i) $\alpha(x_1,x_2) = (\alpha_1(x_1), \alpha_2(x_2))$
ii) $\alpha_i\pi_1 = \pi_1\alpha$. $i=1,2$

ρ_i, π_i are clearly group homomorphisms and so if $\alpha : G_1 \times G_2 \to G_1 \times G_2$ is a group homomorphism, then $\pi_1 \cdot \alpha \cdot \rho_1 : G_1 \to G_1$ and $\pi_2 \cdot \alpha \cdot \rho_2 : G_2 \to G_2$ are group homomorphisms too.

Therefore, it makes sense to consider the following as a possible group isomorphism

$f: Aut(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \to Aut(\mathbb{Z}/n\mathbb{Z}) \times Aut(\mathbb{Z}/m\mathbb{Z})$, $f(\alpha) = (\pi_1\alpha\rho_1, \pi_2\alpha\rho_2)$ $\forall \alpha \in Aut(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$

~ f is well defined: let $\alpha \in Aut(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$ and put $\alpha_i := \pi_i\alpha\rho_i$ $i=1,2$. So $f(\alpha) = (\alpha_1,\alpha_2)$ and we need to show that $\alpha_i \in Aut(G_i)$, $i=1,2$. We show that $\alpha_1 \in Aut(\mathbb{Z}/n\mathbb{Z})$. We only need to show that $\ker \alpha_1$ is trivial as α_1 is a homomorphism and $\mathbb{Z}/n\mathbb{Z}$ is finite.

$\alpha(x_1, 1) = (\alpha_1(x_1), \alpha_2(1)) = (1,1) = \alpha(1,1)$ ~ ~~given~~ ~~...~~ Lemma

~ f is a group homomorphism: let $\alpha, \beta \in Aut(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$. Then, by definition of f

$$f(\alpha)f(\beta) = (\pi_1\alpha\rho_1, \pi_2\alpha\rho_2)(\pi_1\beta\rho_1, \pi_2\beta\rho_2) = (\pi_1\alpha\rho_1\pi_1\beta\rho_1, \pi_2\alpha\rho_2\pi_2\beta\rho_2)$$
$$= (\pi_1\alpha\beta\rho_1, \pi_2\alpha\beta\rho_2) = f(\alpha\beta)$$

~ f is injective: let $\alpha \in \ker f$ and $\alpha_i := \pi_i\alpha\rho_i$, $i=1,2$, so $(\alpha_1,\alpha_2) = f(\alpha) = id_{\mathbb{Z}/n\mathbb{Z}}$ and hence $\alpha_i = id_{\mathbb{Z}/n\mathbb{Z}}$ for $i=1,2$. Thus,

$\alpha(x_1,x_2) = (\alpha_1(x_1), \alpha_2(x_2)) = (x_1,x_2)$ $\forall x_i \in \{\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\}$ and therefore $\alpha = id_{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}}$

~ f is surjective: let $\alpha_1 \in Aut(\mathbb{Z}/n\mathbb{Z})$ and $\alpha_2 \in Aut(\mathbb{Z}/m\mathbb{Z})$. ~~It is clear~~ Define $\alpha : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ by

$\alpha(x_1,x_2) = (\alpha_1(x_1), \alpha_2(x_2))$ $\forall x_i \in G_i$ $i=1,2$.

It is clear that $\alpha \in Aut(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$. Also,

$\pi_1\alpha\rho_1(x_1) = \pi_1\alpha(x_1,1) = \pi_1(\alpha_1(x_1),1) = \alpha_1(x_1) \Rightarrow \pi_1\alpha\rho_1 = \alpha_1$.

Similarly, $\pi_2\alpha\rho_2 = \alpha_2 \Rightarrow f(\alpha) = (\pi_1\alpha\rho_1, \pi_2\alpha\rho_2) = (\alpha_1,\alpha_2)$

2) $|\mathbb{Z}/p^\alpha\mathbb{Z}| = p^\alpha$

$\Rightarrow |(\mathbb{Z}/p^\alpha\mathbb{Z})^\times| = p^\alpha - |\{[n]\in \mathbb{Z}/p^\alpha\mathbb{Z} \mid (n,p^\alpha)\neq 1\}|$
$= p^\alpha - |\{[n]\in\mathbb{Z}/p^\alpha\mathbb{Z} \mid p \mid n\}|$
$= p^\alpha - p^\alpha/p = p^{\alpha-1}(p-1)$

3) $|(\mathbb{Z}/n\mathbb{Z})^\times| = |\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})|$

But, by the Chinese remainder theorem

$= |\mathrm{Aut}(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\times\dots\times\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})|$
$= |\mathrm{Aut}(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})|\times\dots\times|\mathrm{Aut}(\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})|$
$= |(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times|\times\dots\times|(\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times|$
$= p_1^{\alpha_1-1}(p_1-1)\times p_2^{\alpha_2-1}(p_2-1)\times\dots\times p_k^{\alpha_k-1}(p_k-1)$

Problem 6

1) Find all elements of order 2 in $\mathrm{Aut}(\mathbb{Z}/15\mathbb{Z})\cong\mathbb{Z}/15\mathbb{Z}^\times$ by checking all the elements.

2) Write down explicitly the group isomorphism $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\to\mathbb{Z}/15\mathbb{Z}$

3) Find all elements of order 2 in $\mathbb{Z}/3\mathbb{Z}^\times$ and $\mathbb{Z}/5\mathbb{Z}^\times$

4) Use 2) + 3) to check 1)

1) elements of $(\mathbb{Z}/15\mathbb{Z})^\times = \{[1],[2],[4],[7],[8],[11],[13],[14]\}$ ⇝ group of order 8, elements order must have power of 2

Taking each element and it's multiplicative powers mod 15:

$[1]=[1]$, $[2]^4=[1]$, $[4]^2=[1]$, $[7]^4$, $[8]^4=[1]$, $[11]^2=[1]$, $[13]^4=[1]$, $[14]^2=[1]$

$\Rightarrow$ elements of order 2 : $[4],[13],[14]$

2) $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\cong\mathbb{Z}/15\mathbb{Z} \Rightarrow \psi:\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\to\mathbb{Z}/15\mathbb{Z}$ group isomorphism.

Thus, for some $a\in\mathbb{Z}/3\mathbb{Z}$ and $b\in\mathbb{Z}/5\mathbb{Z}$

$\Rightarrow (a,b)\in\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$

$\Rightarrow \psi(a,b) = 5a+3b \pmod{15}$ ⇝ $\psi((a_1,b_1),(a_2,b_2))$
$=\psi(a_1+a_2, b_1+b)= 3(a_1+a_2)+5(b_1,b_2) \bmod 15$
$=(3a_1+5b_1)+(3a_2+5b_2) \bmod 15$
$=\psi(a_1,b_1)+\psi(a_2,b_2)$
⇝ injective, surjective.

3) Elements of $(\mathbb{Z}/3\mathbb{Z})^\times = \{[1],[2]\}$
$(\mathbb{Z}/5\mathbb{Z})^\times = \{[1],[2],[3],[4]\}$

$\Rightarrow$ Elements of order 2: $[2]$ for $(\mathbb{Z}/3\mathbb{Z})^\times$
: $[4]$ for $(\mathbb{Z}/5\mathbb{Z})^\times$

4) The order of (a,b) is the least common multiple of the order of a,b. Thus, elements of order 2 in $(\mathbb{Z}/3\mathbb{Z})^\times\times(\mathbb{Z}/5\mathbb{Z})^\times$ are $\{(2,4),(1,4),(2,1)\}$

Plugging into the isomorphism gives the elements of $(\mathbb{Z}/15\mathbb{Z})^\times$