Part 1

Exercise 1. Show that every group of order ≤ 5 is abelian.

Proof. It is clear that a group of order 1 is abelian. Any group of prime order is cyclic, so we only need to check that all groups of order 4 are abelian.

Let G be a group of order 4, and $x \in G$ with $x \neq e$. So we have

$$\operatorname{ord}(x) = \begin{cases} 2 \\ 4 \end{cases}$$

Indeed since $1 \neq \operatorname{ord}(x) \mid 4$.

If $\operatorname{ord}(x) = 4$, then $\{e.x.x^2.x^3\} \leq G \Rightarrow G = \langle x \rangle$, so it is abelian.

If G has no elements of order 4, then for all $x \in G$ we have $x^2 = e \Rightarrow x = x^{-1}$, so for all $x, y \in G$ we have

$$\begin{aligned}(xy)(x^{-1}y^{-1}) &= (xy)(xy) \\ &= (xy)^2 \\ &= e\end{aligned}$$

Therefore $xy = yx$ for all $x, y \in G$. So G is abelian.

In all cases we have shown that if the order of $G \leq 5$, we have that G is abelian. $\square$

Exercise 2. Show that there are two-isomorphic groups of order 4, namely the cyclic one, and the product of two cyclic groups of order 2.

Proof. Let G be a group of order 4, assume that it is not cyclic. In this case, from last question we know that $x^2 = e$ for all $x \in G$, so $\{e, x\} = \langle x \rangle \leq G$ let $y \in G \setminus \langle x \rangle$.

So notice that $xy \notin \{e, x, y\}$ indeed since $x, y \neq e$ and $x \neq y$. So we see by comparing order $G = \{e, x, y, xy\}$.

Defining the homomorphism

$$\begin{aligned}\varphi \colon G &\to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ x &\to (1, 0) \\ y &\to (0, 1)\end{aligned}$$

Since $\varphi(xy) = \varphi(x) + \varphi(y) = (1, 1)$, by inspection we can see that $\ker \varphi = \{e\}$ and $\operatorname{im} \varphi = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so:

$$G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$\square$

Exercise 3. Let G be a group. A **commutator** in G is an element of the form $aba^{-1}b^{-1}$ with $a, b \in G$. Let G^c be the subgroup generated by the commutators. Then G^c is called the **commutator subgroup**. Show that G^c is normal. Show that any homomorphism of G into an abelian group factors through G/G^c.

Proof. Since $(aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$, the set of elements containing all finite products of commutators is a group. Since any subgroup containing all commutators contains this subgroup we see that

$$G^c = \{x_1 x_2 \cdots x_n \mid n \in \mathbb{N} \text{ and } x_i \text{ are commutators}\} \tag{1}$$

.

Now let $g \in G$ and $aba{-}1b^{-1}$ be a commutator we see that:

$$g(aba{-}1b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) = zwz^{-1}w^{-1}$$

Where $z = gag^{-1}$ and $w = gbg^{-1}$.

So we see that for any $g \in G$ and $a \in G^c$, we have:

$$\begin{aligned} gag^{-1} &= g(x_1 x_2 \cdots x_n)g^{-1} \text{ for commutators } x_i \\ &= (gx_1g^{-1})(gx_2g^{-1}) \cdots (gx_ng^{-1}) \\ &\in G^c \text{ since by above observation } gx_ig^{-1} \text{ is a commutator for all } x_i \end{aligned}$$

So $G^c \trianglelefteq G$.

Now let A be an abelian group and $\varphi\colon G \to A$ be a homomorphism. First of all we will show that φ contains G^c in it's kernel.

$$\begin{aligned} \varphi(aba^{-1}b^{-1}) &= \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} \\ &= e \text{ by commutating elements} \end{aligned}$$

Therefore we see that for all $x \in G^c$, let $x = x_1 \cdots x_n$ where x_i are commutators:

$$\varphi(x) = \varphi(x_1)\varphi(x_2) \cdots \varphi(x_n) = e \text{ since each } \varphi(x_i) = e \tag{2}$$

So we indeed see that $G^c \leq \ker \varphi$. So now let $\pi\colon G \to G/G^c$ be the canonical map and let $\tilde{\varphi}\colon G/G^c \to A$ be the homomorphism given by:

$$\tilde{\varphi}(xG^c) = \varphi(x)$$

Note we know that this is a homomorphism since φ is a homomorphism.

Since $G^c \leq \ker \varphi$ if $xG^c = yG^c$ we have $xy^{-1} \in G^c$ so we have $\varphi(xy^{=1}) = e \Rightarrow \varphi(x) = \varphi(y)$ so $\tilde{\varphi}(xG^c) = \tilde{\varphi}(yG^c)$, this homomorphism is indeed well-defined.

So we indeed see that there is a homomorphism $\tilde{\varphi}$ such that $\varphi = \tilde{\varphi} \circ \pi$. So φ factors through G^c. □

Exercise 4. Let H, K be subgroups of a finite group G with $K \subseteq N_H$. Show that:

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

Proof. Since K is contained in the normalizer of H. Recall by an isomorphism theorem:

$$K/(H \cap K) \simeq HK/H$$

So we have:

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

□

Exercise 5. Goursat's Lemma. Let G, G' be groups and let H be a subgroup of $G \times G'$ such that the projections $p_1\colon H \to G$ and $p_2\colon H \to G'$ are surjective. Let N be the kernel of p_2 and N' be the kernel of p_1. One can identify N as a normal subgroup of G, and N' as a normal subgroup of G'. Show that the image of H in $G/N \times G'/N'$ is the graph of an isomorphism

$$G/N \simeq G'/N'$$

Proof. First of all notice that

$$\ker p_1 = \{(e, b) \in H\} \simeq N' = \{b \in G' \mid (e, b) \in H\} \text{ and } \ker p_2 = \{(a, e') \in H\} \simeq N = \{a \in Ga \mid (a, e') \in H\}$$

Let

$$\varphi_1\colon G \to G/N \text{ and } \varphi_2\colon G' \to G'/N'$$

Be the canonical maps.

Let $\varphi\colon H \to G/N \times G'/N'$ be given by

$$\varphi((g_1, g_2)) = (\varphi_1(g_1), \varphi_2(g_2))$$

This is a homomorphism since φ_1 and φ_2 are homomorphisms.

Lemma 1. If $(xN, x'N'), (yN, y'N') \in \varphi(H)$ then $xN = yN \iff x'N = y'N$.

Proof. First assume that $xN = yN$:

We have: $(xy^{-1}N, x'y'^{-1}N') = (N, x'y'^{-1}N') \in \varphi(H)$. So let $(a, b) \in H$ such that:

$$(aN, bN') = \varphi(a, b) = (N, x'y'^{-1}N')$$

So we see that $aN = N \Rightarrow a \in N \simeq \ker p_2$. This means that $(a, e') \in H$, so we see that $(e, b) = (a, e')^{-1}(a, b) \in H$, so $b \in N'$. Therefore $N' = bN = x'y'^{-1}N'$ so $x'N' = y'N'$.

The other direction is similar. $\square$

Now we let

$$\psi\colon G/N \to G'/N' \text{ be such that } (aN, \psi(aN)) \in \varphi(H) \text{ for all } aN \in G/N$$

We will first show that this function makes sense, note that since the projection from H to G for all xN, we see that $(x, y) \in H$ for some y. So $\varphi(x, y) = (xN, yN') \in \varphi(H)$ so xN is in the projection off $\varphi(H)$ to G/N. So we see that the projection is surjective so: for all $aN \in G/N$ there exists a $bN' \in G'/N'$ such that $(aN, bN') \in \varphi(H)$. Furthermore by lemma 1 this bN' is unique. Since this bN' exists and is unique then we can let $\psi(aN) = bN'$ and this function is well-defined.

Now let $aN, cN \in G/N$ since $(aN, \psi(aN)), (cN, \psi(xN)) \in \varphi(H)$ so:

$$H \ni (aN, \psi(aN))(cN, \psi(xN)) = (acN, \psi(aN)\psi(cN)) \Rightarrow \psi(aNcN) = \psi(acN) = \psi(aN)\psi(cN)$$

So ψ is indeed a homomorphism. Finallly from lemma 1 we see that $\psi(aN) = \psi(bN)$ implies that $(aN, \psi(aN)), (bN, \psi(aN)) \in \varphi(H)$ so $aN = bN$. So this function is indeed an isomorphism. $\square$

Exercise 6. Prove that the group of inner automorphishms of a group G is normal in $\mathrm{Aut}(G)$.

Proof. For all $g \in G$ we let φ_g be the homomorphism such that

$$\varphi_g(x) = gxg^{-1}$$

Recall that an inner automorphishms is an automorphishms of the form φ_g for some $g \in G$. Now let: $I = \{\varphi_g \mid g \in G\}$.

Notice that

$$\forall x \in G,\ \varphi_a \circ \varphi_b(x) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x) \Rightarrow \varphi_a \circ \varphi_b = \varphi_{ab} \in I$$

Likewise

$$\forall x \in G,\ \varphi_{a^{-1}} \circ \varphi_a(x) = a^{-1}axa^{-1}a = x \Rightarrow {\varphi_a}^{-1} = \varphi_{a^{-1}} \in I$$

Let $f \in \mathrm{Aut}(G)$, let $\varphi_g \in I$, for all $x \in G$:

$$\begin{aligned} f \circ \varphi_g \circ f^{-1}(x) &= f(gf^{-1}(x)g^{-1}) \\ &= f(g)xf(g^{-1}) \text{ since } f \text{ is a homomorphism} \\ &= f(g)xf(g)^{-1} \\ &= \varphi_{f(g)}(x) \end{aligned}$$

Since this is true for all x then we have $f \circ \varphi_g \circ f^{-1} \in I$. Since this is true for all φ_g we have $fIf^{-1} \subseteq I$, for all $f \in \mathrm{Aut}(G)$. So $I \trianglelefteq \mathrm{Aut}(G)$.

$\square$

Exercise 7. Let G be a group such that $\mathrm{Aut}(G)$ is cyclic. Prove that G is abelian.

Proof. Let N be the inner automorphishms group, since it is a subgroup of $\mathrm{Aut}(G)$ it is cylic. Now we define:

$$\begin{aligned} \varphi\colon G &\to N \\ \varphi(g) &\to \varphi_g \end{aligned}$$

Where φ_g is defined as in exersise 6. Let $Z(G) = \{z \in G \mid zg = gz\ \forall g \in G\}$, it is clear that $Z(G) \subseteq \ker \varphi$. Furthermore

if $g \in \ker \varphi$ we have:
$$\forall x \in G \; x = \mathrm{id}(x) = \varphi_g(x) = gxg^{-1} \;\; \therefore gx = xg \Rightarrow g \in Z(G)$$

So we see that $\ker \varphi = Z(G)$, so we have
$$G/Z(G) \simeq N$$

Since N is cyclic so is $G/Z(G)$, so let $gZ(G)$ be a generator. Let $x.y \in G$ we have $x = g^m z$, $y = g^n z'$ for some $n, m \in \mathbb{Z}$ and $z, z' \in Z(G)$. We have:

$$\begin{aligned} xy &= g^m z g^n z' \\ &= g^m g^n z z' \\ &= g^n g^m z' z \\ &= g^n z' g^m z \\ &= yx \end{aligned}$$

Since x, y are arbitrary we see that G is indeed abelian. □

Exercise 8. Let G be a group and let H, H' be subgroups. By a **double coset** of H, H' one means a subset of G of the form HxH'.

(a) Show that G is a disjoint union of double cosets.

(b) Let $\{c\}$ be a family of representatives for the double cosets. For each $a \in G$ denote by $[a]H'$ the conjugate $aH'a^{-1}$ of H'. For each c we have a decomposition into ordinary cosets

$$H = \bigcup_{x_c} x_c(H \cap [c]H')$$

where $\{x_c\}$ is a family of elements of H, depending on c. Show that the elements $\{x_c c\}$ form a family of left coset representatives for H' in G; that is,
$$G = \bigcup_c \bigcup_{x_c} x_c c H',$$

and the union is disjoint.

Proof. (a) First of all assume that $z \in HxH' \cap HyH'$ then let $h_1, h_2 \in H$ and $h_1', h_2' \in H'$ such that:

$$h_1 x h_1' = z = h_2 y h_2' \Rightarrow y = {h_2}^{-1} h_1 x h_1' {h_2'}^{-1} \Rightarrow HyH' = H{h_2}^{-1} h_1 x h_1' {h_2'}^{-1} H' = HxH'$$

For any $y, x \in G$ either HxH' and HyH' are disjoint or they are equal this fact combined with the fact that for all $x \in G$ we have $x \in HxH'$ tells us that we can write G as a disjoint union of double cosets.

(b) By our assumptions we have the disjoint unions:

$$\begin{aligned} G &= \bigcup_c HcH' \\ &= \bigcup_c \bigcup_{x_c} x_c(H \cap [c]H')cH' \end{aligned}$$

But notice that for $\alpha \in x_c(H \cap [c]H')cH'$ we have:

$$\alpha = x_c c h' c^{-1} c h'' = x_c c h' h'' \in x_c c H' \text{ for some } h', h'' \in H'$$

So we see that $x_c(H \cap [c]H')cH' \subseteq x_c c H'$, the other inclusion is clear since $e \in (H \cap [c]H')$. So we have:

$$G = \bigcup_c \bigcup_{x_c} x_c c H' \text{ and this union is disjoint}$$

□

Exercise 9. (a) Let G be a group and H a subroup of finite index. Show that there exists a normal subgroup N of G contained in H and also of finite index.

(b) Let G be a group and let H_1, H_2 be subgroups of finite index. Prove that $H_1 \cap H_2$ has finite index.

Proof. (a) Assume that $[G\colon H] = n$ and let $\{a_1H, a_2H, \dots, a_nH\}$ be the distinct cosets of H in G. Let $a \in G$ since we know that $aa_iH \in \{a_1H, a_2H, \dots, a_nH\}$, so let $\sigma_a \in S_n$ be such that $aa_iH = a_{\sigma_a(i)}H$ for all i. We define

$$\begin{aligned} \varphi\colon G &\to S_n \\ a &\to \sigma_a \end{aligned}$$

Let $x \in \ker\varphi$, this means that $xa_iH = a_{e(i)}H = a_iH$ for all i. In particular we know that for one i_0 we have $a_{i_0}H = H$, so we have

$$H = a_{i_0}H = xa_{i_0}H = xH$$

This means that $x \in H$. Therefore $\ker\varphi \subseteq H$. Letting $N = \ker\varphi$, we see that this is a normal subgroup conatined in H.

Now finally note that im $\varphi \leq S_n$, so we see by an isomorphism theorem:

$$[G\colon N] = |G/N| = |\text{im } \varphi| \leq |S_n| = n! < \infty$$

(b) First of all, let $x, y \in G$ be such that $xH_1 = yH_1$ and $xH_2 = yH_2$, then we have $y^{-1}x \in H_1$ and $y^{-1}x \in H_2$ so $y^{-1}x \in H_1 \cap H_2$ so $x(H_1 \cap H_2) = y(H_1 \cap H_2)$

Conversely assume that $x(H_1 \cap H_2) = y(H_1 \cap H_2)$, then we have that $y^{-1}x \in H_1 \cap H_2$ so $y^{-1}x \in H_1$ and $y^{-1}x \in H_2$.

So we have shown that $x(H_1 \cap H_2) = y(H_1 \cap H_2)$ if and only if $xH_1 = yH_1$ ans $xH_2 = yH_2$.

Now finally we let, C_i be the set of distinct reperesentatives of H_i and C be the set of distinct reperesentatives of $H_1 \cap H_2$

$$\begin{array}{rccc} f\colon & C & \to & C_1 \times C_2 \\ & c(H_1 \cap H_2) & \to & (cH_1, cH_2) \end{array}$$

Since we $x(H_1 \cap H_2) = y(H_1 \cap H_2)$ if and only if $(xH_1, xH_2) = (yH_1, yH_2)$ see that this function is well-defined and injective. Therefore from set theory:

$$[G\colon H_1 \cap H_2] = |C| \leq |C_1||C_2| = [G\colon H_1][G\colon H_2] < \infty$$

□

Exercise 10. Let G be a group and let H be a subgroup of finite index. Prove that there is only a finite number of right cosets of H, and that the number of right cosets is equal to the number of left cosets.

Proof. Recall, that since H has finite index, There are only a finite number of left cosets of H in G.

$$ah = b \iff hb^{-1} = a^{-1}$$
$$\therefore\ b \in aH \iff a^{-1} \in Hb^{-1}$$

From this we see that $aH = bH \iff Ha^{-1} = Hb^{-1}$.
Let $H_L = \{aH \mid a \in G\}$ the set of left cosets, and let $H_R = \{Ha \mid a \in G\}$ the set of right cosets.
We define a set map:

$$f\colon H_L \to H_R$$

Given by $f(aH) = Ha^{-1}$. Now first we will show that this function is well-defined, let $aH = bH$ this implies from above that $Ha^{-1} = Hb^{-1}$:

$$f(aH) = Ha^{-1} = Hb^{-1} = f(bH)$$

So this function is indeed well-definied. Now this is also a bijection we notice that the inverse function is given by the map:

$$g\colon H_R \to H_L \text{ by } g(Ha) = a^{-1}H$$

This function is similarly seen to be well-defined since $aH = bH \iff Ha^{-1} = Hb^{-1}$.

So we see that $[G\colon H] = |H_L| = |H_R|$. Since $[G\colon H] < \infty$, there is only a finite number of right cosets and there as a many right as left cosets. $\square$

Exercise 11. Let G be a group, and A a normal abelian subgroup. Show that G/A operates on A by conjugation; and in this manner get a homomorphism of G/A into $\mathrm{Aut}(A)$.

Proof. We will first show that this action is well-defined: Assume that $xA = yA$ so let $a \in A$ such that $y = xa$ and let $s \in A$. So we have:

$$\begin{aligned}
xA \cdot s &= xsx^{-1} \\
&= xaa^{-1}sx^{-1} \\
&= (xa)s(a^{-1}x^{-1}) \text{ since } a, s \in A \text{ and } A \text{ is abelian.} \\
&= (xa)s(xa)^{-1} \\
&= ysy^{-1} \\
&= yA \cdot s
\end{aligned}$$

So this function is indeed well-defined. Now we will show that this function is a group action:

Let $xA, yA \in G/A$ and $s \in A$ we have

$$xA \cdot (yA \cdot s) = xA \cdot (ysy^{-1}) = xysy^{-1}x^{-1} = (xy)s(xy)^{-1} = (xyA) \cdot s$$

For all $s \in S$

$$eA \cdot s = ese^{-1} = s$$

So this indeed a group action.

Now let

$$\varphi\colon G/A \to \mathrm{Aut}(A)$$

Be such that for all $s \in A$:

$$\begin{aligned}
\varphi(xA)(s) &= xA \cdot s \\
&= xsx^{-1}
\end{aligned}$$

Note that it is clear that $\varphi(xA)$ is an automorphishms, since it is an inner-homomorphism.

Finallly it is clear that φ is a homomorphism, since the map $xA \cdot s = xsx^{-1}$ is a group action, so

$$\varphi(xyA)(s) = (xyA) \cdot s = xA \cdot (yA \cdot s) = \varphi(xA)\varphi(yA)(s) \Rightarrow \varphi(xy) = \varphi(x)\varphi(y)$$

And likewise from above we see that $\varphi(A) = \mathrm{id}$. $\square$

Part 2: Semidirect product We define G to be the **semidirect product** of H and N if $G = NH$ and $H \cap N = \{e\}$.

Exercise 12. Let G be a group and let H, N be subgroups with N normal. Let γ_x be conjugation by an element $x \in G$.

(a) Show that $x \to \gamma_x$ induces a homomorphism $f\colon H \to \mathrm{Aut}(N)$

(b) If $H \cap N = \{e\}$, show that the map $H \times N \to HN$ given by $(x, y) \to xy$ is a bijection, and that this map is an isomorphism if and only if f (from part (a)) is trivial.

(c) Conversely, let N, H be groups and let $\psi\colon H \to \mathrm{Aut}(N)$ be a given homomorphism. Let G be the set of pairs

(x, h) with $x \in N$ and $h \in H$ and define a composition law:

$$(x_1, h_1)(x_2, h_2) = (x_1\varphi(h_1)x_2, h_1h_2)$$

Show that this is a group law, and yields a semidirect product of N and H, identifying N with the set of elements $(x, 1)$ and H with the set of elements $(1, h)$.

Proof. (a) We will first show that for all $x \in G$ we have $\gamma_x|_N \in \operatorname{Aut}(N)$, first of all recall that $\gamma_x|_N : N \to G$ is indeed a homomorphism. Now let $y \in \ker(\gamma_x)$ then:

$$\gamma_x(y) = xyx^{-1} = e \Rightarrow xy = x \Rightarrow y = e$$

So this is injective, finally since N is a normal subgroup of G, we see that $\gamma_x(N) = xNx^{-1} = N$, so this function is indeed an automorphism.

So we define our function $f : H \to \operatorname{Aut}(N)$, by $f(x) = \gamma_x$ for all $x \in H$. Let $x, y \in H$, for all $n \in N$ we have

$$\begin{aligned} f(xy)(n) &= \gamma_{xy}(n) \\ &= xyny^{-1}x^{-1} \\ &= x(f(y)(n))x^{-1} \\ &= (f(x) \circ f(y))(n) \end{aligned}$$

This function is indeed a homomorphism.

□

(b) Let

$$g : H \times N \to HN \text{ be given by } (x, y) \to xy$$

Since $HN = \{hn \mid h \in H \text{ and } n \in N\}$, this map is clearly surjective. Now assume that $g(x, y) = g(z, w)$, then we have:

$$xy = zw \Rightarrow \underbrace{z^{-1}x}_{\in H} = \underbrace{wy^{-1}}_{\in N} \in H \cap N = \{e\}$$

So $x = z$ and $y = w$, so $(x, y) = (z, w)$. So this function is injective, and so a bijection.

- ($\Rightarrow$) Assume that this map is also an isomorphism, then we have for all $x, z \in H$ and $y, w \in N$

  $$\begin{aligned} xzyw &= g(xz, yw) \\ &= g((x, y)(z, w)) \\ &= (xy)(zw) \end{aligned}$$

  Therefore, $zy = yz$ for all $z \in H$ and $y \in N$, which means that:

  $$f(z)(y) = zyz^{-1} = y \text{ for all } y \in N \text{ and } z \in H \Rightarrow f(z) = \mathrm{id} \text{ for all } z \in H$$

  So f is trivial.

- ($\Leftarrow$) Assume that f is trivial. Therefore we have for all $x, z \in H$ and $y, w \in N$:

  $$\begin{aligned} g((x, y)(z, w)) &= g(xz, yw) \\ &= xzyw \\ &= x(zyz^{-1})zw \\ &= x(f_z(y))zw \\ &= xyzw \\ &= g(x, y)g(z, w) \end{aligned}$$

  So this g is indeed a homomorphism, and so a isomorphism.

(c) First of all we will show that this composition law is associative:

$$\begin{aligned}((x_1,h_1)(x_2,h_2))(x_3,h_3) &= (x_1\psi(h_1)x_2, h_1h_2)(x_3,h_3)\\ &= ((x_1\psi(h_1)x_2)\psi(h_1h_2)x_3, (h_1h_2)h_3)\\ &= (x_1\psi(h_1)(x_2\psi(h_2)x_3), h_1(h_2h_3))\\ &= (x_1,h_1)(x_2\psi(h_2)x_3, h_2h_3)\\ &= (x_1,h_1)((x_2,h_2)(x_3,h_3))\end{aligned}$$

Now for all $(x,h) \in N \times H$ we have:

$$(e_N, e_H)(x,h) = (e_N\psi(e_H)x, e_Hh) = (x,h) = (x\psi(h)(e_N), he_H) = (x,h)(e_N,e_H)$$

and

$$(x,h)(\psi(h^{-1})x^{-1}, h^{-1}) = (x\psi(e_H)(x^{-1}), e_H) = (e_N, e_H)$$

So this is in deed a group law.

Now let $N = \{(x,1) \in G\}$ and $H = \{(1,x) \in G\}$, it is clear that these are subgroups of G by how we defined multiplication and inverses. We first need to show that $N \trianglelefteq G$: Let $(x,1) \in N$ and $(n,h) \in G$, then we have:

$$\begin{aligned}(\psi(h^{-1})n^{-1}, h^{-1})(x,1)(n,h) &= (\psi(h^{-1})n^{-1}\psi(1)x, h^{-1})(n,h)\\ &= (\psi(h^{-1})n^{-1}x\psi(h)n, 1) \in N\end{aligned}$$

So we indeed see that N is normal.

Also notice that $N \cap H = \{(1,1)\}$, by how they are defined. So we only need to show that $G = NH$.
Let $(n,h) \in G$:

$$(n,1)(1,h) = (n\psi(1)1, 1h) = (n,h)$$

So we indeed see $G \subseteq NH$, the other inclusion is trivial. So this group law indeed yields a semidirect product of N and H.

□

Exercise 13. (a) Let H, N be normal subgroups of a finite group G. Assume that the orders of H and G are relatively prime. Prove that $xy = yx$ for all $x \in H$ and $y \in G$ and that $H \times N \simeq HN$

(b) Let $H_1, \ldots, H_r$ be normal subgroups of G such that the order of H_i is relatively prime with the order of H_j for $i \neq j$. Prove that

$$H_1 \times \ldots \times H_r = H_1 \cdots H_r$$

Proof. (a) First of all recall that since $H \cap N \leq H$ and $H \cap N \leq N$, we see that $|H \cap N| \mid |H|$ ane $|H \cap N| \mid |N|$, so $|H \cap N| = 1$, since $\gcd(|H|, |N|) = 1$. So $|H| \cap N| = \{e\}$.
Now since H, N are normal subgroups of G, for $x \in N$ and $y \in H$:

$$xyx^{-1} \in H \Rightarrow (xyx^{-1})y^{-1} \in H$$

And

$$yx^{-1}y^{-1} \in N \Rightarrow x(yx^{-1}y^{-1}) \in N$$

so $xyx^{-1}y^{-1} \in H \cap N = \{e\} \Rightarrow xy = yx$.

Now let γ_x be conjugation by an element $x \in G$ and let $f\colon H \to \mathrm{Aut}(N)$ be the induced map. Then we have:

$$f(h)(n) = h^{-1}nh = hh^{-1}n = n \text{ for all } h \in H \text{ and } n \in N$$

So the map f is trivial, so by $12b$:

$$H \times N \simeq HN$$

(b) We will proceed by induction. The base case was shown in (a), so assume this is true for all integers less than r. We have

$$H_1 \times \ldots \times H_{r-1} \simeq H_1 \cdots H_{r-1}$$

So

$$H_1 \times \ldots \times H_{r-1} \times H_r \simeq H_1 \cdots H_{r-1} \times H_r$$

Since $|H_1 \cdots H_{r-1}| = |H_1 \times \ldots \times H_{r-1}| = |H_1| \cdots |H_{r-1}|$, which is coprime to $|H_r|$ since $|H_r|$ is coprime to all $|H_j|$, with $j < r$. So using (a) we get the desired result.

□

Exercise 14. Let G be a finite group and N a normal subgroup such that N and G/N have relatively prime orders.

(a) Let $H \leq G$, such that $|H| = |G/N|$. Prove that $G = HN$

(b) Let g be an automorphism of G. Prove that $g(N) = N$.

Proof. (a) Note since N is normal:

$$|HN| = \frac{|H||N|}{|H \cap N|}$$

By a previous question. But since the order of N and H are relatively prime, as we have seen this means $|H \cap N| = 1$. So we have

$$\begin{aligned} |HN| &= |H||N| \\ &= |G/N||N| \\ &= |G| \end{aligned}$$

So we see that $|HN| = |G|$, since G is finite and $HN \subseteq G$, this means that $HN = G$.

Lemma 2. If $H \leq G$ is such that $|H| = |N|$, then $H = N$

Proof. Let

$$\varphi \colon G \to G/N$$

be the canonical homomorphism.

We note that $\varphi(HN) = HN/N \leq G/N$, we have:

$$|H/(H \cap N)| = |HN/N| \mid |G/N| \tag{3}$$

So let $m \in \mathbb{N}$:

$$\frac{|H|}{|H \cap N|} m = |G/N| \Rightarrow |N|m = |H|m = |G/N||H \cap N|$$

Now let p be a prime divisor of $|N|$, then $p \mid |G/N||H \cap N|$, since $p \nmid |G/N|$ and p is prime we see that: $p \mid |H \cap N|$.

So all prime divisors of $|N|$ divide $|H \cap N|$, therefore $|N| \mid |H \cap N|$ but since $|H \cap N| \leq |N|$ this implies that $|H \cap N| = |N|$ so $H \subseteq N$. Likewise we can see that $N \subseteq H$. So $H = N$. □

Now let g be an automorphism of G. So we know that $g(N) \leq G$ and $|g(N)| = |N|$. So by the lemma $g(N) = N$.

□

Part 3: Some operations

Exercise 15. Let G be a finite group operating on a finite set S with $\#(S) \geq 2$. Assume that there is only one orbit. Prove that there exists an element $x \in G$ which has no fixed point, i.e.

$$xs \neq s \text{ for all } s \in S$$

Proof. Assume that for all $x \in G$, there is a $s \in S$ such that $xs = s$.

For each $x \in G$ we let $f(x) =$ number of elements $s \in S$ such that $xs = s$. We will use the formula that will be proved in question 19:

$$\begin{aligned} 1 = \text{ Orbits of } G \text{ in } S = \frac{1}{|G|}\sum_{x \in G} f(x) && (4) \\ \therefore |G| = |S| + \sum_{x \in G \setminus \{e\}} f(x) && (5) \\ \geq |S| + \sum +G \setminus \{e\} 1 \text{ since by assumption every element has a fixed point} && (6) \\ \geq 2 + |G| - 1 = |G| + 1. && (7) \end{aligned}$$

Which is a contradiction! Therefore there must be an element $x \in G$ which has no fixed point. $\square$

Exercise 16. Let H be a proper subgroup of a finite group G. Show that G is not the union of all the conjugates of H.

Proof. Let $|G| = m|H|$, where $m > 1$. Now let $S = \{x_1 H x_1^{-1}, \dots, x_r H x_r^{-1}\}$ be the set of conjugates of H. Recall that Since $e \in x_i H x_i^{-1}$, we see that: So we see that

$$|\bigcup_i x_i H x_i^{-1}| \leq \sum_i |x_i H x_i^{-1}| - r + 1 = \sum_i |H| - r + 1 = r|H| - r + 1.$$

Now by theorem we know that $r = |G\colon N_H| = \frac{|G|}{|N_H|}$, where N_H is the normalizer of H, since $H \leq G$ it is closed under multiplication so $hHh^{-1} = H$, for $h \in H$ so $H \subseteq N_H$. So we have

$$r = \frac{|G|}{|N_H|} \leq \frac{|G|}{|H|} = m..$$

Therefore we have

$$|\bigcup_i x_i H x_i^{-1}| \leq r|H| - r + 1 \leq m|H| - (m-1) < m|H| = |G| \text{ since } m > 1..$$

So G can't be the union of all the conjugates of H.

$\square$

Exercise 17. Let X, Y be finite sets and C be a subset of $X \times Y$. For $x \in X$ let

$$\varphi(x) = \text{ number of elements } y \in Y \text{ such that } (x, y) \in C$$

Verify that

$$|C| = \sum_{x \in X} \varphi(x)$$

Proof. Let $X = \{x_1, \dots, x_n\}$ and $Y = \{y_1, \dots, y_m\}$. Let $I = \{i \in \{1, \dots, n\} \mid \exists y \in Y \text{ such that } (x_i, y) \in C\}$. Now for each $i \in I$ we let $C_i = \{(x, y) \in C \mid x = x_i\}$. So note that the $C_i \cap C_j = \emptyset$ for all $j \neq i$ and that $\bigcup_{i \in I} C_i = C$. Finally we notice that $|C_i| =$ number of $y \in Y$ such that $(x_i, y) \in C = \varphi(x_i)$ Putting all of this together we have:

$$\sum_{x \in X} \varphi(x) = \sum_{i \in I} \varphi(x_i) = \sum_{i \in I} |C_i| = |\bigcup_{i \in I} C_i| = |C|$$

$\square$

Exercise 18. *Proof.* Let $S = \{s_1, \dots, s_n\}$ and $T = \{t_1, \dots, t_m\}$ Recall a map from S to T is defined by where the s_i maps to for each i. There are m possible values that each s_i can be mapped to. So there are $\underbrace{m \cdot m \cdots m}_{n \text{ times}} = m^n = |T|^{|S|}$ maps from S to T. ∎

Exercise 19. (a) *Proof.* Recall that since the orbits partition S we have $Gs = Gt$ for all $t \in Gs$. So we have:

$$\sum_{t \in Gs} \frac{1}{|Gt|} = \sum_{t \in Gs} \frac{1}{|Gs|} = \frac{|Gs|}{|Gs|} = 1.$$

∎

(b) *Proof.* Let $C = \{(x, s) \in G \times s \mid xs = s\}$, by question 17 we know that:

$$\sum_{x \in G} f(x) = |C|.$$

But furthermore if we let for all $s \in S$, $\varphi(s) = |\{x \in G \mid (x, s) \in C\}| = |\{x \in G \mid xs = s\}| = G_s$ then by question 17:

$$\sum_{s \in S} |G_s| = \sum_{s \in S} \varphi(s) = |C|.$$

We let $\{s_i\}_{i \in I}$ be the distinct represtatives for the orbits of G in S.

But we have:

$$\begin{aligned}
\sum_{s \in S} |G_s| &= \sum_{s \in S} \frac{|G|}{|Gs|} \\
&= |G| \sum_{s \in S} \frac{1}{|G_s|} \\
&= |G| \sum_{i \in I} \sum_{t \in Gs_i} \frac{1}{|Gt|} \\
&= |G| \sum_{i \in I} 1 = |G| \cdot \# \text{ of distinct orbits of } G \text{ in } S
\end{aligned}$$

Putting this all together we get:

$$\frac{1}{|G|} \sum_{x \in G} f(x) = \# \text{ of distinct orbits of } G \text{ in } S.$$

∎

Exercise 20. *Proof.* Let P act on A by conjugation. By the orbit-stabilizer theorem

$$|P| = |A \cap Z(P)| + \sum |P \colon P_x| \text{ where the sum is over all } x \text{ such that } |P \colon P_x| > 1.$$

This is indeed true since

$$x \in A \cap Z(P) \iff gx = xg \text{ for all } g \in P \text{ and } x \in A \iff P_x = P \iff |P \colon P_x| = 1.$$

But then we have since if $|P \colon P_x| > 1$ then it is divisible by p, then we have $|A \cap Z(P)| = 0 \pmod p$. So we have $|A \cap Z(P)| \neq 1$, but since $|A| = p$ this implies that $A \cap Z(P) = A$, so $A \subseteq Z(P)$. ∎

Exercise 21. *Proof.* Since P_H is a p-Sylow subgroup of H it is a p-subgroup of G. So there exists a p-Sylow subgroup, Q, of G such that $P_H \subseteq Q$.

Now since $Q \cap H \leq Q$, we see that $Q \cap H$ is a p-group contained in H, so $|Q \cap H| \leq |P_H|$ but since $P_H \subseteq Q \cap H$ we have $|Q \cap H| = |P_H|$.

So $|Q \cap H|$ is a p-Sylow subgroup of H, so there exists $g \in H$ such that $g(Q \cap H)g^{-1} = P_H$. But notice that since $g \in H$ we have $g(Q \cap H)g^{-1} = (gQg^{-1}) \cap H$. Let $P = gQg^{-1}$, it is a p-Sylow subgroup of G such that

$$P_H = P \cap H.$$

□

Exercise 22. *Proof.* Recall that since H is a p-subgroup of G, it is contained in a p-Sylow subgroup, say $P \subseteq G$. Now let Q be any other p-Sylow subgroup of G, then there exists g such that $gPg^{-1} = Q$. But since $H \trianglelefteq G$ we have

$$H = gHg^{-1} \subseteq gPg^{-1} = Q.$$

$\therefore$ H is contained in Q, since Q was an arbitrary p-Sylow subgroup of G, H is contained in all p-Sylow groups.

□

Exercise 23. Let $|G| = p^k m$, where $p \nmid m$.

(a) *Proof.* Assume that $P' \subseteq N(P)$. Note that $|N(P)| = p^k n$, where $p \nmid n$, so P' is a p-Sylow subgroup of $N(P)$. But we also know that P is a p-Sylow subgroup of $N(P)$, and since all p-Sylow groups are conjugate there is $g \in N(P)$ such that

$$gPg^{-1} = P'.$$

So since $g \in N(P)$, $P = gPg^{-1} = P'$. □

(b) *Proof.* $P' \subseteq N(P') = N(P)$, so by the previous question $P' = P$. □

(c) *Proof.* It is clear that $N(P) \subseteq N(N(P))$. So let $g \in N(N(P))$ and $n \in N(P)$. On the one hand since $gng^{-1} \in gN(P)g^{-1} = N(P)$ we know that

$$gng^{-1}Pgn^{-1}g^{-1} = P.$$

On the other hand by (a) we know that $g^{-1}Pg = P$ and since $n \in N(P)$ we have:

$$P = gn(g^{-1}Pg)n^{-1}g^{-1} = g(nPn^{-1})g^{-1} = gPg^{-1}.$$

Therefore $g \in N(P)$ so we have $N(N(P)) \subseteq N(P) \Rightarrow N(N(P)) = N(P)$ □

Part 4: Explicit determination of groups

Exercise 24. *Proof.* Assume that p is prime and let G be a group of order p^2.

Since each element in the center of G forms a conjugacy class containing just itslef, if $x_1, \ldots, x_r$ are the conjugacy representatives not in the center

$$|G| = |Z(G)| + \sum_i |G \colon G_{x_i}|$$

Therefore we know that $p \mid |Z(G)|$. So we have $|Z(G)| = \begin{cases} p^2 \\ p \end{cases}$ Assume that $|Z(G)| = p$, $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic say $G/Z(G) = \langle gZ(G) \rangle$. Now let $x, y \in G$ then we have $x = g^n a$ and $y = g^m b$, where $n, m \in \mathbb{Z}$ and $a, b \in Z(G)$:

$$\begin{aligned} xy &= (g^n a)(g^m b) \\ &= g^n g^m ab \text{ since } a \in Z(G) \\ &= g^{n+m} ba \text{ since } b \in Z(G) \\ &= g^m b g^n a \\ &= yx \end{aligned}$$

Since x, y were arbitrary elements in G, then G is abelian which contradicts the fact that $Z(G) \neq G$. $\therefore$ $|Z(G)| = p^2$, so $Z(G) = G$ and G is abelian.

Assume that G is not isomorphic to the cyclic group $\mathbb{Z}/p^2\mathbb{Z}$. This means that $\mathrm{ord}(x) = p$ for all $x \in G \setminus \{e\}$.

Let $x \in G \setminus \{e\}$, we define H to be the subgroup of G generated by x and let $y \in G \setminus H$, and K be the subgroup generated by y. Since $K \cap H = \{e\}$, and since G is abelian then from question 12 we conclude that $|HK| = |H| \cdot |K| = p^2$. Therefore $HK = G$ and

$$G = HK \simeq H \times K \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

.

□

Exercise 25. (a) *Proof.* By the class equation $p \mid |Z|$, therefore since G is not abelian

$$|Z| = \begin{cases} p \\ p^2 \end{cases} .$$

Assume that $|Z| = p^2$, then $|G/Z| = p$, which would mean that G/Z is cyclic so G is abelian which is a contradiction. So $|Z| = p$. Therefore $Z \simeq C$. Now notice that $|G/Z| = p^2$, but it is not cyclic since G is not abelian, so by last question $G/Z \simeq C \times C$. □

(b) *Proof.* Since the index of H is p it is normal. Assume for a contradiction that Z is not contained in H. Then notice that $Z \cap H = \{e\}$, since $Z = \langle g \rangle$ for some $g \in G$ and $g \notin H$. Therefore since $gh = hg$ for all $h \in H$ and $g \in Z$, by question 12 we see that $|ZH| = |Z| \cdot |H| = p^3$. So we have that $ZH = G$.

The last thing we need to recall is that from question 24, H is an abelian group.

Let $x, y \in G$ there exists $g_1, g_2 \in Z$ and $h_1, h_2 \in H$ such that $x = g_1h_1$ and $y = g_2h_2$.

$$\begin{aligned} xy &= (g_1h_1)(g_2h_2) \\ &= g_2g_1h_1h_2 \text{ since } g_2 \in Z \\ &= g_2g_1h_2h_1 \text{ since } H \text{ is abelian we have } h_2h_1 = h_1h_2 \\ &= (g_2h_2)(g_1h_1) \text{ since } g_1 \in Z \\ &= yx \end{aligned}$$

Which implies that G is abelian, which is a contradiction. Therefore, $Z \subseteq H$. □

(c) *Proof.* Let $x \in G \setminus Z$ and let $K = \langle x \rangle$. We notice that since K and Z are both cyclic groups of prime order and $x \notin Z$ we have $K \cap Z = \{e\}$

Since $Z \trianglelefteq G$ we see that $H = KZ \leq G$. Furthermore from question 12:

$$|H| = |K||Z| = p^2.$$

From the previous question this subgroup is normal and since $|H| = p^2$ and $x^p = e$ for all $x \in H$ by question 24, $H \simeq C \times C$. □

Exercise 26. (a) *Proof.* Let P be a Sylow p-subgroup of G and Q be a Sylow q-subgroup of G. Since Q has index p, we know that it is a normal subgroup of G. From 14(a), since P has the same order as G/Q and p, q are distinct primes we know that $G = PQ$.

Now we let P acts on Q by conjugation. This gives us a homomorphism

$$\varphi \colon P \to Aut(Q).$$

Now since $\ker \varphi \leq P$ and P is a simple group we know by the isomorphism theorem that

$$|\varphi(P)| = |P|/|\ker \varphi| = \begin{cases} p \\ 1 \end{cases}$$

But furthermore we know that $|\varphi(P)| \mid |Aut(Q)| = q-1$, so if $|\varphi(P)| = p$ we would have $q-1 = 0 \pmod p$, which contradicts our assumption. So we must have that φ is trivial. Since $P \cap Q = \{e\}$, from question 12 we know that $P \times Q \simeq PQ$. Finally from proposition 4.3(v), we know that $P \times Q$ is cyclic so $G = PQ \simeq P \times Q$ is also cyclic. □

(b) Since $15 = 3 \cdot 5$ and $5 = 2 \pmod 3$. The result is immidiate from last question.

Exercise 27.

Exercise 28.

Exercise 29.

Exercise 30. (a) *Proof.* Since $40 = 5 \cdot 2^3$. We have $n_5|8$ and $n_5 = 1 \pmod 5$ which forces $n_5 = 1$. □

(b) *Proof.* Since $12 = 3 \cdot 2^2$. This is true from Exercise 28. □

Exercise 31.