1. Let $H = \langle 3 \rangle = \{ 1, 3, 9, 11 \}$ be subgroups of $\mathbb{Z}_{16}^\times$.

$K = \langle 5 \rangle = \{ 1, 5, 9, 13 \}$

$\mathbb{Z}_{16}^\times$ abelian $\rightarrow HK \leq \mathbb{Z}_{16}^\times$ is a subgroup.

$HK = \langle 1, 3, 5, 7, 9, 11, 13, 15 \rangle$. Note: $|\mathbb{Z}_{16}^\times| = \varphi(16) = 16(1 - \frac{1}{2}) = 8$.

But also, $|HK| = 8$ and $HK \leq \mathbb{Z}_{16}^\times$. Hence, $HK = \mathbb{Z}_{16}^\times$.

(Alternative: Problem #14 $\Rightarrow |HK| = \frac{|H| \cdot |K|}{|H \cap K|} = 4 \cdot 4 = 8$;

$HK = \mathbb{Z}_{16}^\times$, $|\mathbb{Z}_{16}^\times| = 8 \Rightarrow HK = \mathbb{Z}_{16}^\times$)

3. Find an example of two subgroups $H$ and $K$ of $S_3$ for which $HK$ is not a subgroup.

Solution: Let $H = \langle \sigma = (12) \rangle = \{ 1, \sigma \}$

$K = \langle \tau = (13) \rangle = \{ 1, \tau \}$.

Then $HK = \{ (1)(1) = (1), (1)\tau = \tau, \sigma(1) = \sigma, \sigma\tau \}$

$|HK| = 4 + 6 \Rightarrow HK$ is not a subgroup of $S_3$.

Lagrange's Thm.
4. Find \( \langle \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \rangle \leq GL_2(\mathbb{Z}_3) \)

**Solution:** \( M = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \). \( M^2 = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 4 \\ 0 & 4 \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod{3} \)

\( M^3 = M^2 \cdot M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 2 \end{pmatrix} \equiv \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \pmod{3} \)

\( M^4 = M^3 \cdot M = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 0 & 4 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \pmod{3} \)

\( M^5 = M^4 \cdot M = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 0 & 2 \end{pmatrix} \equiv \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} \pmod{3} \)

\( M^6 = M^5 \cdot M = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 6 \\ 0 & 4 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{3} \)

\[ \langle \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \rangle = \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \]

5. Prove: If \( G_1 \) and \( G_2 \) are abelian, then so is \( G_1 \times G_2 \).

**Proof:** Let \((a_1, a_2), (b_1, b_2) \in G_1 \times G_2 \).

\( G_1 \) abel. \( \implies a_1 b_1 = b_1 a_1 \)

\( G_2 \) abel. \( \implies a_2 b_2 = b_2 a_2 \). We have \[ (a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2) = (b_1 a_1, b_2 a_2) = (b_1, b_2)(a_1, a_2). \]

\[ G_1, G_2 \text{ abel} \]
6. Construct an abelian group of order 12 that is not cyclic. Let \( G = \mathbb{Z}_2 \times \mathbb{Z}_6 \). Claim: \( G \) is not cyclic. (Note \( 161 = \text{lcm}(12, 12) = 12 \))

Proof: Let \( (a, b) \in G \). Then \( o(a) \in \{1, 2, 3\} \)

\( o(b) \in \{1, 2, 3, 6\} \).

Since order of \( (a, b) \) is \( \text{lcm}(o(a), o(b)) \), no element \( (a, b) \in G \) has order 12. It follows that \( G \) is not cyclic.

7. Construct a group of order 12 that is not abelian. Let \( G = \mathbb{Z}_2 \times S_3 \). Note that \( 161 = |\mathbb{Z}_2| \times |S_3| = 2 \times 6 = 12 \).

Claim: \( G \) is not abelian.

Proof: \( S_3 \) is not abelian: \( (12)(13) = (132) \), but \( (13)(12) = (123) \).

Hence, \( (1, (12))(1, (13)) = (1, (132)) \)

but \( (1, (13))(1, (12)) = (1, (123)) \) in \( G \).
8. Let \( H_2 \leq G_2 \) \( \cap \) subgroups. Show that 
\( H_2 \leq G_2 \)
\( H_1 \times H_2 \leq G_1 \times G_2 \) is a subgroup.

**Proof:** It suffices to exhibit closure and inverses.

**Closure:** Let \((a_1, a_2), (b_1, b_2) \in H_1 \times H_2\).

\[ a_1, b_1 \in H_1 \Rightarrow a_1 b_1 \in H_1 \cap \text{subgroups, therefore closed} \]

\[ a_2, b_2 \in H_2 \Rightarrow a_2 b_2 \in H_2 \]

\[ \Rightarrow (a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2) \in H_1 \times H_2. \]

**Inverses:** Let \((a_1, a_2) \in H_1 \times H_2\).

\[ a_1 \in H_1 \Rightarrow a_1^{-1} \in H_1 \cap \text{subgroups, therefore inverses exist in each} \]

\[ a_2 \in H_2 \Rightarrow a_2^{-1} \in H_2 \]

\[ \Rightarrow (a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1}) \in H_1 \times H_2. \]
14. Let $G = G_1 \times G_2$.

Let $H = \{ (x_1, x_2) \in G_1 \times G_2 : x_2 = e \}$; $K = \{ (x_1, x_2) \in G_1 \times G_2 : x_1 = e \}$.

(2) Show that $H, K \leq G$ are subgroups.

Proof: It suffices to exhibit closure and inverses.

Closure: Let $(x_1, e), (y_1, e) \in H$.

$x_1, y_1 \in G_2 \Rightarrow x_1 y_1 \in G_2$ (since $G_2$ is a group) \[ \Rightarrow \]

$e = \text{id} \Rightarrow e \cdot e = e$ \[ \Rightarrow \]

$(x_1, e)(y_1, e) = (x_1 y_1, e \cdot e) = (x_1 y_1, e) \in H$.

Inverses: Let $(x_1, e) \in H$.

$x_1 \in G_1 \Rightarrow x_1^{-1} \in G_2$ (since $G_2$ is a group). \[ \Rightarrow \]

$e = \text{id} \Rightarrow e^{-1} = e$. \[ \Rightarrow \]

$(x_1, e)^{-1} = (x_1^{-1}, e^{-1}) = (x_1^{-1}, e) \in H$.

Hence, $H$ is a subgroup. A similar argument shows that $K$ is a subgroup.
(b) Show that $HK = KH = G$.

Proof: To show:

1. $HK = G$.
   
   $H, K \subseteq G \Rightarrow HK \subseteq G$. Take $(x_1, x_2) \in G$.
   
   We have $(x_1, x_2) = (x_1, e)(e, x_2) \in HK$, so $G \subseteq HK$.

   It follows that $HK = G$.

2. $KH = G$.
   
   $H, K \subseteq G \Rightarrow KH \subseteq G$. Take $(x_1, x_2) \in G$.
   
   We have $(x_1, x_2) = (e, x_2)(x_1, e) \in KH$, so $G \subseteq KH$.

   It follows that $KH = G$, and hence also that $HK = KH = G$.

(c) Show that $H \cap K = \{ (e, e) \}$.

Proof: Let $(x_1, x_2) \in H \cap K$.

$(x_1, x_2) \in H \Rightarrow x_2 = e \Rightarrow (x_1, x_2) = (e, e)$,

$(x_1, x_2) \in K \Rightarrow x_1 = e$
14. Let $G$ be finite and suppose that $H, K \trianglelefteq G$ are subgroups.

Show that $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

**Proof:** Fix $h, k \in HK$, and let

$S_{hk} = \{(h', k') : h' \in H, k' \in K, \text{ and } h'k = h'k'\}.$

It suffices to show that $|S_{hk}| = |H \cap K|$. Then we will have

$|HK| = \sum_{(h, k) \in S_{hk}} |H, k| = \frac{|H| \cdot |K|}{|H \cap K|}$.

**Claim:** $\varphi : H \cap K \rightarrow S_{hk}$ defined by

$x \mapsto (hx, x^{-1}k)$ is a bijection.

**Proof (of the claim):**

- **$\varphi$ is 1-1:** Let $x_1, x_2 \in H \cap K$, and suppose that

$\varphi(x_1) = (hx_1, x_1^{-1}k) = (hx_2, x_2^{-1}k) = \varphi(x_2)$.

Then $hx_1 = hx_2 \Rightarrow x_1 = x_2$, so $\varphi$ is 1-1.
\[ \psi \text{ is onto: } \] Let \( \gamma = (h', k') \in S_{hk} \).

Then \( h'k' = hk \implies h' = k(k')^{-1} \in K \land h \in H \).

Now, \( x = h'^{-1}h' \implies hx = h' \implies y = (h', k') = (hx, k^{-1}k) \)

\[ x = k(k')^{-1} \implies x^{-1}k = k' = \psi(x), \text{ so } \psi \text{ is onto.} \]

Hence, \( \psi \) is a 1-1 correspondence. It follows that \( |S_{hk}| = |H \land K| \).
15. Let \(|G| = 6\). Show:

\(\Box\)

a) \(G\) must contain an element of order 2.

b) \(G\) must contain an element \(g \neq e\) of order \(\neq 2\).

\textbf{Proof (of a):}

\(16| = 6\) is even \(\implies\) \(\exists b \neq e\) with \(b^2 = e\) \((\text{or} b = 2)\) by the result of §3.1, §24.

\textbf{Proof (of b): Argue by contradiction.}

Suppose that all elts. in \(G\) (not \(e\)) have order 2.

Then \(G\) is abelian by the result of §3.1, §23.

Let \(a, b \in G \setminus \{e\}\). Then we have:

\(G\) abelian \(\implies H = \{e, a, b, ab\} \subseteq G\) is a subgroup.

\(o(a) = o(b) = 2\)

But \(|H| = 4 + 1 = 6|\), which contradicts Lagrange's Thm.
16. Let $|G| = 6$ and suppose that $a, b \in G$ have $o(a) = 3$, $o(b) = 2$. Show: Either

(i) $G$ is cyclic

(ii) $ab \neq ba$ (non-abelian).

**Proof:** If $ab \neq ba$, we are done. Therefore, suppose that $ab = ba$. We will show that $G$ is cyclic.

$ab = ba \implies o(ab) = o(a) \cdot o(b) = 3 \cdot 2 = 6$

and $gcd(o(a) = 3, o(b) = 2) = 1$. By the result of §3.2, #26.

Since $|G| = 6$, we have $G = \langle ab \rangle$. I.e., $G$ is cyclic.

17. Let $|G| = 6$. Show: If $G$ is not cyclic, then it is isomorphic to $S_3$.

**Proof:** $15 \implies G$ must contain an element of order 2, say $b$.

$15b \implies G$ must contain an element $a$ with $o(a) \neq 1, 2, 3$.

Lagrange's Theorem $\implies o(a) | 6 \implies o(a) \in \{1, 2, 3\}$.

$G$ not cyclic $\implies o(a) \neq 6 \implies o(a) = 3$. 
Let \( H = \{ e, a, a^2, b, ab, a^2b \} \)

Claim: \( H \cong S_3 \)

Proof (if claim):

Since \( H \subseteq G \) and \( |H| = 6 \), it suffices to show that the elements of \( H \) are distinct.

1. \( e \notin \{a, a^2, b, ab, a^2b\} \).

Clearly, \( e \neq a, a^2, b \) since \( o(a) = 3, o(b) = 2 \).

\[
e = ab \iff a = b^{-1} = b \iff (a \neq b)
\]

\[
o(b) = 2
\]

\[
e = a^2b \iff b = a^{-2} = a \iff (a \neq b)
\]

\[
o(a) = 3
\]

2. \( a \notin \{a^2, b, ab, a^2b\} \).

\[
a \neq a^2 \text{ since } o(a) = 3; a \neq b; a = ab \iff b = e \iff \text{ same}
\]

\[
o(b) = 2
\]

\[
a = a^2b \iff ab = e \iff a = b^{-1} = b \iff (a \neq b)
\]

\[
o(b) = 2
\]

3. \( a^2 \notin \{b, ab, a^2b\} \).

\[
a^2 = ab \iff a = b = e \iff (a \neq b)
\]

\[
o(b) = 2
\]

\[
a^2 = b \iff a^3 = e = ab \iff a = b^{-1} = b \iff (a \neq b)
\]

\[
o(b) = 2
\]
\[ b \neq 1, a, a^2, b, a^2b. \]

\[ b = ab \implies a = e \implies (o(a) = 3) \]

\[ b = a^2b \implies a^2 = e \implies (o(a^2) = 3) \]

\[ a \neq a^2b (\text{If } ab = a^2b, \text{ then } a = e \implies (o(a) = 3)) \]

It follows that \( G = H \).

Observe : \( a, b \in G \implies ba \in G = \{ e, a, a^2, b, ab, a^2b \} \).

Claim : \( ba = a^2b \)

\(\text{Proof of claim} \) : Process of elimination.

\[ e = ba \iff a = b^{-2} = b \implies (o(b) = 2) \]

\[ a = ba \implies ba = e \implies (o(b) = 2) \]

\[ a^2 = ba \implies a = b \implies (o(a^2) = 3) \]

\[ b = ba \implies a = e \implies (o(a^2) = 3) \]

\( ab = ba \) : cannot happen by the result of Problem 16 since \( G \) is not cyclic.

Hence, we must have \( ba = a^2b \).
It remains to compare mult. tables for $G, S_3$.

For $G$: key fact is that $b a = a^2 b$. Then also:

1. $b a^2 = (b a) a = a^2 (b a) = a^2 a^2 b = a b$
2. $(b a) b = a^2 b b = a^2$
3. $b a^2 b = (b a) a b = a^2 (b a b) = a^4 = a$
4. $a (b a) = a a^2 b = b$
5. $a b a^2 = a (a b) = a^3 b$
6. $a b a b = a (b a b) = a^3 = e$
7. $a b a^2 b = a (b a^2 b) = a^2$
8. $a^2 b a = a (a b a) = a b$
9. $a^2 b a^2 = a (a b a^2) = a^3 b = b$
10. $a^2 b a b = a (ab a^2) = a$
11. $a^2 b a^2 b = a (a b a^2 b) = a^3 = e$

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>$a^2$</th>
<th>b</th>
<th>$ab$</th>
<th>$a^2 b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>$a^2$</td>
<td>b</td>
<td>$ab$</td>
<td>$a^2 b$</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>$a^2$</td>
<td>e</td>
<td>a b</td>
<td>$a^2 b$</td>
<td>b</td>
</tr>
<tr>
<td>$a^2$</td>
<td>$a^2$</td>
<td>e</td>
<td>a</td>
<td>$a^2 b$</td>
<td>b</td>
<td>a b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>$a^2 b$</td>
<td>a b</td>
<td>e</td>
<td>$a^2$</td>
<td>$a$</td>
</tr>
<tr>
<td>$ab$</td>
<td>$ab$</td>
<td>b</td>
<td>$a^2 b$</td>
<td>a</td>
<td>e</td>
<td>$a^2$</td>
</tr>
<tr>
<td>$a^2 b$</td>
<td>$a^2 b$</td>
<td>b</td>
<td>$a^2$</td>
<td>a</td>
<td>e</td>
<td>$a$</td>
</tr>
</tbody>
</table>

One can verify that this is the same as that for $S_3$. 
Problem: Let $p$ be prime. Show that $|GL_2(\mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$

Proof: Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_p)$

- # choices for $(a)$: $p^2 - 1$ since $(c) \neq (0)$.

- Now, compute # choices for $(d)$.

① case 1: Suppose that $c \neq 0$.

Let $a, c, d \in \mathbb{Z}_p$ with $c \neq 0$ (and $p$). Then $\exists$ unique $b \in \mathbb{Z}_p$

with $ad - bc \equiv 0 \pmod{p}$ since we have:

$ad - bc \equiv 0 \pmod{p} \iff ad \equiv bc \pmod{p}$

$c \neq 0 \pmod{p} \iff adc^{-1} \equiv b \pmod{p}$.

Here, # choices for $d$: $p$ (can be arbitrary)

# choices for $b$: $p - 1$ (throw out the choice (unique)

\[ \text{giving } ad - bc \equiv 0 \pmod{p} \]

$\Rightarrow$ # choices for $(d)$: $p(p - 1) = p^2 - p$. 


(2) case 2: Suppose that $c = 0$.

If $c \equiv 0 \pmod{p}$, then we must have $a \not\equiv 0 \pmod{p}$. (otherwise, $\begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} c \end{pmatrix}$)

Now, $c \equiv 0 \pmod{p} \Rightarrow ad - bc \equiv ad \pmod{p}$.

Hence, *choose for* $b : \rho$ (*$b$ can be arbitrary*).

Also, $ad \equiv 0 \pmod{p} \iff d \equiv 0 \pmod{p}$ (since $a \not\equiv 0 \pmod{p}$)

$\Rightarrow$ *choose for* $d : \rho - 1$ (throw out $d \equiv 0 \pmod{p}$).