1. (10 points) Compute the following arithmetic expression and given the answer in the form $a + bi$ for $a, b \in \mathbb{R}$.

   (1). $(1 + i)^4$

   $$
   = 1 + 4i + 6i^2 + 4i^3 + i^4
   = 1 + 4i - 6 - 4i + 1 = -4
   $$

   (2). $|12 + 5i|$

   $$
   = \sqrt{12^2 + 5^2} = 13
   $$

   (3). $(2 + 3i)(4 - i)$.

   $$
   = 8 + 12i - 2i + 3
   = 11 + 10i
   $$

2. (10 points) Find all solutions $x$ of the given equation.

   (1). $x +_{12} x = 6$ in $\mathbb{Z}_{12}$.

   $$
   2x = 6 \Leftrightarrow 18
   $$

   $$
   \Leftrightarrow x = 3 \Leftrightarrow 9.
   $$

   (2). $x +_{7} x +_{7} x = 5$ in $\mathbb{Z}_7$.

   $$
   3x = 5 \Leftrightarrow 12 = 19
   $$

   only solution in $\mathbb{Z}_7$ is $x = 4$.  


3. (10 points) Write two non-abelian groups. For each of them, explain why it is non-abelian.

Hint: $M_n^+$ for $n \geq 2$, or its subgroups or bijective maps from a set to itself under composition.

4. (20 points) Mark each of the following true or false.

(a) $\underline{\text{F}}$ The cardinality of $\mathbb{Z}^+$ is strictly less than the cardinality of $\mathbb{Z}$ since $\mathbb{Z}^+$ is a proper subset of $\mathbb{Z}$.

(b) $\underline{T}$ For any set $S$, the cardinality of $S$ is strictly less than the cardinality of the power set of $S$.

(c) $\underline{\text{F}}$ There is a set which contains everything.

(d) $\underline{\text{F}}$ A relation on $S$ is an equivalence relation if it is symmetric and transitive.

(e) $\underline{\text{F}}$ Any commutative binary operation is also associative.

(f) $\underline{\text{F}}$ Let $(S, \ast)$ and $(S', \ast')$ be two algebras. A function $\phi : S \rightarrow S'$ is an isomorphism if and only if $\phi(a \ast b) = \phi(a) \ast' \phi(b)$.

(g) $\underline{T}$ Every finite group of at most three elements is abelian.

(h) $\underline{\text{F}}$ Every group has at least two subgroups.

(i) $\underline{T}$ In any group the quadratic equation $x^2 = x$ has a unique solution.

(j) $\underline{T}$ There exists a cyclic group which has only one generator.
5. (10 points) Let \( L \) be the set of lattice points in the Euclidean space \( \mathbb{Z}^3 \), i.e., \( L = \{(x, y, z) : x, y, z \in \mathbb{Z}\} \). Decide the cardinality of \( L \), and state your reasoning. (You can simply cite some theorems without proof.)

\[
L = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}
\]

Since \( \text{card}(\mathbb{Z}) = \aleph_0 \),
\[
\text{card}(A \times B) = \text{card}(A) \cdot \text{card}(B)
\]
and \( \aleph_0 \cdot \aleph_0 = \aleph_0 \)

we have \( \text{card}(L) = \aleph_0 \).

6. (10 points) Let \( G \) be a group and let \( a, b \in G \). Show that \((a \ast b)^{-1} = a^{-1} \ast b^{-1}\) if and only if \( a \ast b = b \ast a \).

\[
(a \ast b)^{-1} = a^{-1} \ast b^{-1}
\]

\(\iff\)

\[
b^{-1} \ast a^{-1} = a^{-1} \ast b^{-1}
\]

\(\iff\)

\[
(b^{-1} \ast a^{-1})^{-1} = (a^{-1} \ast b^{-1})^{-1}
\]

\(\iff\)

\[
a \ast b = b \ast a
\]

7. (10 points) Prove that a cyclic group with only one generator can have at most 2 elements.

Let \( G = \langle a \rangle \)

If \( a = e \), then \( |G| = 1 \)

If \( a \neq e \), then \( a^{-1} \) is also a generator.

By uniqueness, \( a = a^{-1} \Rightarrow G = \langle e, a \rangle \cong \mathbb{Z}_2 \)

\(\Rightarrow\) \( |G| = 2 \)
8. (10 points) For sets $H$ and $K$, we define the intersection $H \cap K$ by

$$H \cap K = \{ x \mid x \in H \text{ and } x \in K \}.$$ 

Show that if $H \leq G$ and $K \leq G$, then $H \cap K \leq G$. (If you use a theorem other than the definition, please cite it first. You don’t need to prove the theorem.)

**Proof.** It is sufficient to show that $H \cap K \neq \emptyset$ 
and $\forall a, b \in H \cap K$, $a b^{-1} \in H \cap K$.

Since $H \leq G$, $k \leq G$, $e \in H \cap k \Rightarrow H \cap k \neq \emptyset$.

$\forall a, b \in H \cap k$.

$a, b \in H$, $H \leq G \Rightarrow a b^{-1} \in H$

$a, b \in K$, $K \leq G \Rightarrow a b^{-1} \in K$ \{ \Rightarrow a b^{-1} \in H \cap k \}.

9. (10 points) Let $a$ and $b$ be elements of a group $G$. Show that if $ab$ has finite order $n$, then $ba$ also has order $n$.

$$(ab)^n = e$$

$$(ba)^{n+1} = b \cdot (ab)^n \cdot a = ba \Rightarrow (ba)^n = e$$

Hence order $(ba) \leq n$.

On the other hand, if the order of $ba$ is $m < n$, the above argument applied to $ba$ will give order$(ab) \leq m$. Contradicting order$(ab) = n$.

Hence order$(ba) = n$. 

4