1 (5 pts). Define what it means for a set $G$ with a binary operation $*$ to be a group.

Solution. The set $G$ with binary operation $*$ is a group if (i) $*$ is associative, that is $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$; (ii) there exists an identity element $e \in G$ such that $(a * e) = a = (e * a)$ for all $a \in G$; and (iii) for all $a \in G$ there exists an element $b \in G$ (called the inverse of $a$) such that $a * b = e = b * a$.

2 (10 pts). Let $G$ be an Abelian group. Let $H = \{ a \in G \mid o(a) \text{ is a finite odd integer} \}$. Prove that $H$ is a subgroup of $G$.

Solution. To see that a nonempty set $H$ is a subgroup, it is enough to prove that for $a, b \in H$, we have $ab \in H$ and $a^{-1} \in H$. That is, we need to check that $H$ is closed under products and closed under inverses.

Note that $H \neq \emptyset$, because $o(e) = 1$ and hence $e \in H$.

First, if $a \in H$ then $m = o(a)$ is odd. Then $a^m = e$, so $(a^{-1})^m = (a^m)^{-1} = e$ as well. This implies that the order $o(a^{-1})$ must be a divisor of $m$. Since $m$ is odd, all of its divisors are also odd, so $o(a^{-1})$ is odd and thus $a^{-1} \in H$. (Actually it is easy to see that $o(a^{-1}) = o(a)$ but we don’t need this).

Next if $a, b \in H$ with $m = o(a)$ and $n = o(b)$, then since $ab = ba$, we get that $(ab)^{mn} = a^m b^m = (a^n)^m (a^n)^m = e$. Thus $o(ab)$ must be a divisor of $mn$. Since $m$ and $n$ are odd, $mn$ is odd, and so any divisor of $mn$ is odd. Thus $o(ab)$ is odd and so $ab \in H$ as well. This proves that $H$ is a subgroup using the two-step subgroup test.

3. Let $G$ be a group and consider the function $\phi : G \to G$ given by the formula $\phi(x) = x^{-1}$.

(a) (5 pts). Prove that $\phi$ is one-to-one and onto.

(b) (5 pts). Prove that $\phi$ is an isomorphism if and only if the group $G$ is Abelian.
Solution. (a). If \( \phi(x) = \phi(y) \), then \( x^{-1} = y^{-1} \). Then \( y = xx^{-1}y = xy^{-1}y = x \). Thus \( \phi \) is one-to-one.

Given \( x \in G \), we have \( xx^{-1} = e = x^{-1}x \) and thus by the definition of inverses we have \( (x^{-1})^{-1} = x \). Thus \( \phi(x^{-1}) = x \) and hence \( \phi \) is onto.

(b). Suppose that \( G \) is Abelian. Then for all \( x, y \in G \), \( \phi(xy) = (xy)^{-1} = (yx)^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y) \). Thus by definition \( \phi \) is a homomorphism of groups. Since \( \phi \) is one-to-one and onto by part (a), then \( \phi \) is an isomorphism by definition.

Conversely, if \( \phi \) is an isomorphism then we have \( y^{-1}x^{-1} = (xy)^{-1} = \phi(xy) = \phi(x)\phi(y) = x^{-1}y^{-1} \), for all \( x, y \in G \). Thus \( yx = yxy^{-1}x^{-1}xy = yxx^{-1}y^{-1}xy = xy \) for all \( x, y \in G \).

4 (10 pts). Let \( G = \mathbb{Z} \) be the group of integers under addition. Prove directly that every subgroup of \( G \) is of the form \( m\mathbb{Z} = \{mq | q \in \mathbb{Z} \} \) for some \( m \geq 0 \). (Do not quote the theorem that subgroups of cyclic groups are cyclic. Prove it directly, as you did when this was a homework exercise.)

Solution. If \( H = \{0\} \) is the trivial subgroup, then \( H = 0\mathbb{Z} \). So assume now that \( H \neq \{0\} \). Since \( H \) is closed under inverses, if \( a \in H \) then \( -a \in H \). Thus \( H \) contains some positive number, and we can define \( m \) to be the smallest positive number in \( H \). Now if \( a \in H \), then we can write \( a =qm + r \) in the division algorithm, with \( 0 \leq r < m \). Since \( m \in H \), we have \( qm \in H \) since \( H \) is a subgroup (recall that \(qm \) means \( \underbrace{m + m + \cdots + m}_q \) if \( q \) is positive, \( \underbrace{(-m) + (-m) + \cdots + (-m)}_q \) if \( q \) is negative, and \( 0m = 0 \)). Since \( a \in H \), we get \( r = a - qm \in H \). Thus contradicts the choice of \( m \) unless \( r = 0 \). Thus \( a = mq \) and so \( a \in m\mathbb{Z} \). So \( H \subseteq m\mathbb{Z} \). Conversely, since \( m \in H \) we get \( qm \in H \) for all \( q \in \mathbb{Z} \) as already noted and so \( m\mathbb{Z} \subseteq H \). Thus \( H = m\mathbb{Z} \).

5. For each of the following groups, decide if the group is cyclic or not and justify your answer.

(a) (5 pts). \( \mathbb{Z}_9^\times \).

(b) (5 pts). \( \mathbb{Z}_3 \times \mathbb{Z}_3 \).

Solution.
(a). $\mathbb{Z}_9^\times$ is cyclic. We have $\mathbb{Z}_9^\times = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$. Then considering the powers of $[2]$, we have $[2]^1 = [2] \neq [1], [2]^2 = [4] \neq [1], \text{ and } [2]^3 = [8] \neq [1]$. Since $o([2])$ must divide $|\mathbb{Z}_9^\times| = 6$, we have $o([2]) = 1, 2, 3, \text{ or } 6$. But $o([2])$ cannot be 1, 2, or 3 by the calculation above, so $o([2]) = 6$. This implies that $[2]^0 = [1], [2], [2]^2, [2]^3, [2]^4, [2]^5$ are all distinct and so give all 6 elements of the group. Thus $\mathbb{Z}_9^\times = \langle [2] \rangle$ is generated by a single element and so is cyclic.

(b). This group is not cyclic. For example, we can use the formula for the order of an element in a direct product. If $[a] \in \mathbb{Z}_3$, then we know that $o([a]) = 1 \text{ or } 3$, since $|\mathbb{Z}_3| = 3$. Then if $([a], [b]) \in \mathbb{Z}_3 \times \mathbb{Z}_3$, we have $o(([a], [b]) = \text{lcm}(o([a]), o([b]))$ as proved in class or in the textbook. But the least common multiple of two divisors of 3 is at most as large as 3, so all elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$ have order at most 3. On the other hand, $|\mathbb{Z}_3 \times \mathbb{Z}_3| = 9$, so if it were cyclic the group $\mathbb{Z}_3 \times \mathbb{Z}_3$ would have to have an element of order 9.