1. Which of the following assertions is/are true? Give short justifications.
   a. The set of all complex numbers of the form x + iy with x, y integers and with x even is a group under addition of complex numbers.
   b. Let G be a multiplicative group in which $(ab)^{-1} = a^{-1} b^{-1}$ for all a, b € G. Then G is Abelian.
   c. Let f : G1 → G2 be a homomorphism of finite groups and a € G1. Then ord f(a) is an integral multiple of ord a.
   d. Let G be a group and m, n € N with gcd(m, n) = 1. Assume that G contains elements a, b with ord a = m and ord b = n. Then G is cyclic.

ANS:

a.

True: It suffices only to check closure and inverse. If x, y, x', y' are integers then $x + x'$ and $y + y'$ are also integers. Moreover, if x and x' are even, then so also is $x + x'$. Finally, the inverse of $x + iy$ is $-x - iy$. Here $-x, -y$ are also integers and $-x$ is also even (if x is so).

b.

True: Let $a, b \in G$. By the given property $(a^{-1}b^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1} = ab$. Moreover, in any group $(a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba$. Thus $ab = ba$.

c.

False: Take $G_1 = G_2$ to be any finite group and the trivial homomorphism $f : G_1 \to G_2$ that maps every $a \in G_1$ to the identity $e_2 \in G_2$. If $e_1 \neq a \in G_1$, then $\operatorname{ord} a > 1$, whereas $\operatorname{ord} f(a) = \operatorname{ord} e_2 = 1$.

d.

False: Take $m, n > 1$ and $G = C_{mn} \times C_{mn}$, where C_{mn} is a multiplicative cyclic group of order mn. Let g be a generator of C_{mn}. Take $a = (g^n, e)$ and $b = (g^m, e)$.

2. Prove that an infinite group has infinitely many subgroups.

Solution Let G be an infinite multiplicative group. If G has an element a of infinite order, then for every $n \in \mathbb{N}$, G has a subgroup generated by g^n. These subgroups are different for different values of n.

Finally assume that all elements of G have finite orders. Let $a_1, a_2, \ldots, a_n, \ldots$ be distinct elements of G. Consider the subgroups $H_n = \langle a_n \rangle$ for all $n \in \mathbb{N}$. Suppose that there are only finitely many different subgroups in the family $H_1, H_2, H_3, \ldots$ of subgroups. This means there exists an $n \in \mathbb{N}$ such that $H_n = H_{n+1} = H_{n+2} = \cdots$. But a_n is of finite order, i.e., H_n is a finite group and cannot contain all of the infinitely many elements $a_{n+1}, a_{n+2}, a_{n+3}, \ldots$. If $a_m \notin H_n$ for some $m > n$, then $H_m \neq H_n$, a contradiction.

3. Let G be a multiplicative group and H, K subgroups of G with H ∩ K = {e}. Assume that G = HK = {hk | h € H, k € K}. Prove that every element a € G can be written as a = hk for some *unique* elements h € H and k € K.

Solution Let $a \in G$ be written as $a = h_1k_1 = h_2k_2$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$. The element $h_1^{-1}h_2 = k_1k_2^{-1}$ belongs to $H \cap K$ and is the identity element by hypothesis. But then $h_1 = h_2$ and $k_1 = k_2$.

4. Let G be an Abelian group. An element a € G is called a *torsion element* of G if ord a is finite. Prove that the set of all torsion elements of G is a subgroup of G.

Solution Denote by H the set of all elements of G of finite orders.

[Closure] Let $a, b \in H$, $\operatorname{ord} a = m$ and $\operatorname{ord} b = n$. But then $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e$, i.e., $\operatorname{ord}(ab) \mid mn$. In particular, $\operatorname{ord}(ab)$ is finite, i.e., $ab \in H$.

[Inverse] Let $a \in H$. Since $a^k = e$ if and only if $(a^k)^{-1} = (a^{-1})^k = e$, we have $\operatorname{ord}(a^{-1}) = \operatorname{ord} a$.

5. Prove that for any integer n > 3 the multiplicative group $Z^*_{2^n}$ is *not* cyclic. (Hint: You may look at the elements $2^{n-1} \pm 1$.) [Here, $Z^*_{2^n} = (Z/2^nZ)$ i.e. group of all the integer remainder values if the integer is divided by 2^n. For example, Z_n is a group of {0, 1, 2, …, n-1}.]

Solution For $n \geqslant 3$ the elements $2^{n-1} \pm 1$ are distinct modulo 2^n and neither of them is the identity element. Also $(2^{n-1} \pm 1)^2 = 2^{2n-2} \pm 2^n + 1 = 1$ modulo 2^n, since $2n - 2 \geqslant n$ for $n \geqslant 3$. Thus $2^{n-1} - 1$ and $2^{n-1} + 1$ are distinct elements of $\mathbb{Z}^*_{2^n}$ of order 2, i.e., G has two distinct subgroups $\{1, 2^{n-1} - 1\}$ and $\{1, 2^{n-1} + 1\}$ of the same size 2. We know that a finite cyclic group of order r has a unique subgroup of order s for every divisor s of r. Therefore, $\mathbb{Z}^*_{2^n}$ cannot be cyclic.