1. **(20 points)** *For each of the following sets and operations thereon, check whether they form a group; show your work, and for each that is not a group, say why not.*

   (a) *The set $\mathbb{R} \times \mathbb{R}$ under the multiplication operation $(a,b)(c,d) = (ad, bc)$.*

   This is not a group, and one easy way to observe it is to note that it has no identity: $(a,b)(1,1) = (a,b)$, but $(1,1)(a,b) = (b,a)$.

   (b) *The set $\{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\}$ under the operation of standard real-number multiplication.*

   This is an Abelian group; we could verify each individual property, or simply note an isomorphism to Z via mapping each x to $\log_2 x$.

   (c) *The set of all sets of positive rational numbers under the rule that $S \cdot T = \{st : s \in S, t \in T\}$. (For instance, $\{\frac{1}{2}, \frac{1}{3}\} \cdot \{\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \ldots\} = \{\frac{1}{15}, \frac{1}{10}, \frac{2}{15}, \frac{1}{5}, \frac{3}{10}, \frac{4}{15}, \frac{2}{10}, \ldots\}$.)*

   This is not a group. One easy way to show it is to note that the identity must be the set $\{1\}$ (since $\{a\} \cdot e$ must equal $\{1 \cdot a\}$), but then there are no inverses: $\{a, b\} \cdot S$ will never be a single-element set except when $S = \{0\}$, so there is no solution to $\{a, b\} \cdot S = \{1\}$.

2. **(30 points)** Prove or disprove *the following statements about subgroups.*

   (a) *For any finite group G, the set $\{g \in G : g^2 = e\}$ is a subgroup of G.*

   This is not actually a true statement! A simple example would be D_3, in which this set would be $\{e, f, fr, fr^2\}$, which is not closed under multiplication, since $f(fr) = r$.

   (b) *For any group G and element x thereof, the set $\{g \in G : gxg^{-1} = x\}$ is a subgroup of G.*

   Proof. Let $H = \{g \in G : gxg^{-1} = x\}$. Consider $h_1, h_2 \in H$: then it must be the case definitionally that $h_1 x h_1^{-1} = x$ and $h_2 x h_2^{-1} = x$. Then:

   $$(h_1 h_2) x (h_1 h_2)^{-1} = h_1 (h_2 x h_2^{-1}) h_1^{-1} = h_1 x h_1^{-1} = x$$

   so by the definition of H, $h_1 h_2 \in H$. Thus H is closed under multiplication.

   Now consider $h \in H$, so that $hxh^{-1} = x$. Let us note that

   $$x = (h^{-1}h)x(h^{-1}h) = h^{-1}(hxh^{-1})h = h^{-1}xh = (h^{-1})x(h^{-1})^{-1}$$

   so now, by definition, $h^{-1} \in H$, so H is closed under inversion. □

   (c) *For any integers m and n, D_{mn} has a $2m$-element subgroup.*

   Consider $\{e, r^n, r^{2n}, r^{3n}, \ldots, r^{(m-1)n}, f, fr^n, \ldots, fr^{(m-1)n}\}$; it is easy to show that this is a subgroup of D_{nm} with $2m$ elements.

3. **(20 points)** *Consider elements a and b ate elements of a group G such that the order of a is m and the order of b is n.*

   - *Prove that if $ab = ba$, then the order of ab is divisible by mn.*

   Proof. By the definition of order, we know it to be true that $a^m = e$ and $b^n = e$. Then

   $$(ab)^{mn} = (ab)(ab)(ab)\cdots(ab) = (aa\cdots a)(bb\cdots b) = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e;$$

   note that the rearrangement of terms in the middle required the given commutativity. Noting that $\langle ab \rangle$ is a cyclic group, whose order we might call k, and that $(ab)^{mn} = 1$, we know that mn is a multiple of k. □

- *Demonstrate that when $ab \neq ba$, then the order of ab might not be divisible by mn.*

  As was the answer to a previous question, D_5 is a prime example, where f and fr both have order 2, and $f^2r = r$ has order 5, which is not divisible by 4.

4. **(20 points)** *Answer the following questions.*

   (a) **(10 points)** *Identify a cyclic group Z_n which has exactly 6 subgroups, including Z_n itself and the trivial subgroup $\{e\}$.*

   Since a cyclic group has exactly one subgroup for each and every factor of its order, we with to find a cyclic group of order with exactly 6 divisors. Since $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_r^{\alpha_r}$ has exactly $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$ factors, we may choose a group of order p^5 for any prime p or order p^2q for any distinct primes p and q. The smallest such group would be Z_{12}, although many others are possible.

   (b) **(10 points)** *Suppose $H \leq G$ and $|H| = 10$. a is an element of G such that $a^6 \in H$. What are the possible values of $|a|$ and why?*

   We know by Lagrange's Theorem that for every $h \in H$, the order of h is a divisor of 10, so $h^{10} = e$. Then $a^{60} = e$, so a must have order dividing 60. In fact, *any* divisor of 60 is possible, which can easily be shown by considering the case where $G = Z_{60}$ and $H = \langle 6 \rangle$. Then Every $g \in G$ has $6g \in H$, and elements of G have every order dividing 60.

5. **(20 points)** *Let H and K be subgroups of G such that for some $a, b \in G$, it is the case that $aH \subseteq bK$. Prove that $H \subseteq K$.*

   Proof. Since $e \in H$, $a \in aH \subseteq bK$, so there is a $k_0 \in K$ such that $bk = a$. Specifically, we see thus that $k_0 = b^{-1}a$, so $b^{-1}a \in K$. Now, considering any h, we know that $ah \in aH \subseteq bK$, so there is a k such that $ah = bk$, so $h = a^{-1}bk = (b^{-1}a)^{-1}k = k_0k$. Since K is a group, the product $k_0k \in K$, so $h \in K$. Thus $H \subseteq K$. □

6. **(25 points)** *Let $N \leq H \leq G$, and furthermore $N \trianglelefteq G$. Prove that H/N is normal in G/N if and only if H is normal in G.*

   Proof. Suppose $H \trianglelefteq G$; we shall seek to prove that $H/N \trianglelefteq G/N$. By our premised normality, for any $h \in H$ and $g \in G$, we know that $ghg^{-1} \in H$. Then, considering conjugation of the coset hN by gN, we will find that:

   $$(gN)(hN)(gN)^{-1} = gNhNNg^{-1} = ghg^{-1}N = h'N \in (H/N)$$

   To migrate the Ns in this product to the end, we use normality of N in G; to assert that ghg^{-1} is equal to some element h' of h, we use the normality of H in G.

   Conversely, let us suppose that $H/N \trianglelefteq G/N$. Then for any $g \in G$, and $h \in H$, it is the case that $(gN)(hN)(gN)^{-1}$ is an element of H/N, or in other words that there is an $h' \in H$ such that $(gN)(hN)(gN)^{-1} = h'N$. As was seen above, we may rewrite the left side of this equation to determine that $(ghg^{-1})N = h'N$. Multiplying both sides on the left by $(h')^{-1}$, we find that $(h')^{-1}(ghg^{-1})N = N$, which is the case if and only if $(h')^{-1}(ghg^{-1}) \in N$; in other words, $ghg^{-1} = h'n$ for some $n \in N$. Since $N \leq H$, $h'n \in H$, so $ghg^{-1} \in H$; thus, H is normal in G. □

7. **(15 points)** *Prove that for any homomorphism $\varphi : G \to H$ and element a of G, the order of $\varphi(a)$ divides the order of a.*

Proof. Let $|a| = k$, so $a^k = e_G$. Then $\phi(a)^k = \phi(a^k) = \phi(e_G) = e_H$. Since $\phi(a)^k$ is the identity, we know that the order of $\phi(a)$ is divisible by k. □