1. *Identify each of the following algebraic structures as either a group or not a group, and justify your answer. For each structure which is a group explain if it is Abelian.*

   - *The real numbers* $\mathbb{R}$ *under the operation* $a \odot b = a + b + 1$.

     This structure is an Abelian group: for any two real numbers a and b, $a \odot b$ is real, so we have closure; $a \odot b \odot c = a + b + c + 2$ regardless of the grouping, so we have associativity; $a \odot (-1) = (-1) \odot a = a$, so we have an identity element (specifically -1); finally, $a \odot (-2-a) = (-2-a) \odot a = -1$, so every element a has an inverse. Finally, note that $a \odot b = b \odot a$, so this group is commutative.

   - *The integers* $\mathbb{Z}$ *under the operation* a *max* b, *which returns the larger of* a *and* b *(e.g.* 7 *max* $-3 = 7$.

     This is not a group, because it has no identity — there is no number e whose maximum with any number a is equal to a.

     A variation on this algebraic structure, the maximum operation on $\mathbb{Z} \cup \{-\infty\}$, *does* have an identity element, since the artificial element $-\infty$ is defined to be less than every integer so $-\infty$ max $a = a$ for all a. However, even this algebra lacks an inverse.

     The above operation is in fact closed, associative, and commutative.

   - *The set of subsets of* $\{1, 2, 3, 4, 5\}$ *under the union operation* $S \cup T$.

     This operation lacks an inverse. The identity element is the set $\emptyset$, since $S \cup \emptyset = S$ for all S, but for any nonempty set, e.g. $S = \{1, 2\}$, $S \cup T$ will be at least as large as S and thus $S \cup T \neq \emptyset$. This operation actually has all properties of an Abelian group except for the inverse.

   - *The set of strings of the symbols* a, b, *and* b^{-1} *under the operation of concatenation with the rule that two adjacent as or bs cancel, e.g.* $(ababa)(ab) = abab\not{a}\not{a}b = aba\not{b}\not{b} = aba$.

     This is a group: concatenating and canceling two strings results in a string, so this structure is closed; concatenating three strings does not depend on the order in which they are "glued together", so the operation is associative; the empty string is an identity; and the reversal of a string is its inverse.

     Note that this operation is not commutative, so the group is non-Abelian: $(ab)b = a$, while $b(ab) = bab$.

2. *Let* D_6 *be the group of symmetries of a hexagon. Identify a subgroup of* D_6 *with each of the following orders:* 1, 2, 3, 6.

   Let r be a 60-degree rotation and f an (arbitrary) flip. We may denote the elements of D_6 canonically as such: $\{e, r, r^2, r^3, r^4, r^5, f, fr, fr^2, fr^2, fr^3, fr^4, fr^5\}$, and then identify the given subgroups.

   There is only one subgroup of order 1; unsurprisingly, it's the trivial group $\{e\}$.

   There are seven different subgroups of order 2. Generally, a group of order 2 is always $\{e, x\}$ with $x^2 = e$, and the possible stand-in values for x are r^3 or any of the six flips.

   A group of order three basically has to be $\{e, x, x^2\}$ where $x^3 = e$; you might think $\{e, x, y\}$ in general should work, but then x^2, xy, and y^2 all need to be in the group, and that gets messy. The only possible subgroup matching this template is $\{e, r^2, r^4\}$.

   Groups of order 6 are much more versatile in their form, but finding a few in D_6 isn't hard; there are at least three possibilities: $\{e, r, r^2, r^3, r^4, r^5\}$, $\{e, r^2, r^4, f, fr^2, fr^4\}$, and $\{e, r^2, r^4, fr, fr^3, fr^5\}$.

3. *Prove that if* G *is a finite group with order 7, then* G *is cyclic.*

   We wish to show that G contains an element of order 7; this element would then generate the whole group. We shall show specifically that G *cannot* contain elements of orders from 2 to 6 (G does, of course, contain an element of order 1, namely, the identity). We shall address each case individually:

Proposition 1. *If $|G| = 7$, then G contains no element of order 2.*

Proof. Suppose counterfactually that G contains an element a of order 2; we may call the elements of G by the names e, a, b, c, d, f, and g. Since $a \neq e$, we can be certain that $ba \neq b$, $ca \neq c$, etc. Without loss of generality we can assert that $ba = c$, and then $ca = ba^2 = b$. Likewise, if we assert $da = f$, then $fa = d$ as well. However, now there is no possible value for ga: ga cannot equal xa for $x \neq g$, and we have already assigned the values of a, b, c, d, e, and f to ea, ca, ba, fa, aa, and da respectively, so that ga must equal g, but this cannot be the case because a is not the identity. □

Proposition 2. *If $|G| = 7$, then G contains no element of order 3.*

Proof. Suppose counterfactually that G contains an element a of order 3; we may call the elements of G by the names e, a, a^2, b, c, d, and f. Since $a \neq a^2 \neq e$, we can be certain that b, ba, and ba^2 are distinct. Without loss of generality we can assert that $ba = c$ and $ba^2 = d$. Then $ca = d$ and $da = b$. However, at this point since we know: $ea = a$, $aa = a^2$, $(a^2)a = e$, $ba = c$, $ca = d$, and $da = b$. It must be the case that fa is distinct from all of these, so $fa = f$, which is impossible since $a \neq e$. □

Proposition 3. *If $|G| = 7$, then G contains no element of order 4.*

Proof. If a was an element of G of order 4, then a^2 would have order 2; we saw above that that is impossible. □

Proposition 4. *If $|G| = 7$, then G contains no element of order 5.*

Proof. If a was an element of G of order 5, we could build a near-complete Cayley table for G, positing the existence of sixth and seventh elements of G called b and c:

	e	a	a^2	a^3	a^4	b	c
e	e	a	a^2	a^3	a^4	b	c
a	a	a^2	a^3	a^4	e	?	?
a^2	a^2	a^3	a^4	a	e	?	?
a^3	a^3	a^4	a	a^2	e	?	?
a^4	a^4	a	a^2	a^3	e	?	?
b	b	?	?	?	?	?	?
c	c	?	?	?	?	?	?

However, to complete this table following the group laws, ab and ac must be b and c in some order; to not conflict with the identity, $ab = c$ and $ac = b$. But then a^2b and a^2c must *also* be b and c in some order, and since $eb = b$ and $ab = c$, a^2b can be neither b nor c, leading to a contradiction. □

Proposition 5. *If $|G| = 7$, then G contains no element of order 6.*

Proof. If a was an element of G of order 6, then a^3 would have order 2; we saw above that that is impossible. □

4. *Let G be a group such that for any $a, b, c, d, x \in G$, if $axb = cxd$, then $ab = cd$. Prove that G is Abelian.*

For any a and b, consider $x = a^{-1}b^{-1}$, $c = ba$, and $d = e$. Note that $axb = e = cxd$, so $ab = cd$. Thus $ab = ba$.

Other choices also work, like letting $x = a^{-1}$, $c = b$, and $d = a$.

5. *Which elements of Z_{200} have order 5? Explain how you know.*

   By the Fundamental Theorem of Cyclic Groups, the unique subgroup of Z_{200} of order 5 is $\langle \frac{200}{5} \rangle = \{0, 40, 80, 120, 160\}$, Each of the elements of this group except 0 generates this subgroup, and since the order of an element of G is equal to the order of the subgroup it generates, these four numbers (40, 80, 120, and 160) are the only elements of Z_{200} with order 5.