Name: ....

1] Let X and Y be sets, and let $f\colon X \to Y$ be a function. Please complete the following definitions:

A] We say that f is *injective* if

B] We say that f is *surjective* if

2] Let X, Y, and Z be sets, and let $f\colon X \to Y$ and $g\colon Y \to Z$ be functions.
Assume that the composition $g \circ f$ is injective.

A] Is it true or false that then f must be injective? Prove it or disprove it!

B] Is it true or false that then g must be injective? Prove it or disprove it!

3] Please complete the following definitions.

A] A *group* is a set G together with an operation $*$ satisfying the following axioms:

B] A group G is called *abelian* if

C] If G is a group and a is an element of G then the *cyclic subgroup generated by a* is the subgroup

$(a) =$

4] Consider a set S and let G be the set of all functions $f\colon S \to \mathbb{R}$ from S to the set $\mathbb{R}$ of all real numbers. We can define an operation $*$ on G as follows: given $f\colon S \to \mathbb{R}$ and $g\colon S \to \mathbb{R}$ we define $f * g\colon S \to \mathbb{R}$ to be the function $(f * g)(s) = f(s) \cdot g(s)$, where on the right-hand side $\cdot$ is multiplication of real numbers. Is it true or false that G with respect to this operation $*$ is a group? State explicitly which group axioms hold and which ones (if any) fail.

5] Prove by induction that if a and b are elements of an abelian group G then for every positive integer $n \geq 1$ we have $(ab)^n = a^n b^n$.

6] Consider a group G, a subgroup H of G, and an element $g \in G$. Define the subset H^g of G as follows:

$$H^g = \{ g^{-1}hg \mid h \in H \} .$$

Prove that H^g is a subgroup of G.

7] Consider the group U_{99}.

A] Find explicitly the number of elements in U_{99}.

B] Is [40] an element of U_{99}? Explain your answer, and if your answer is 'Yes' then compute the inverse of [40] in U_{99} and express it as $[a]$ with $0 < a < 99$.

C] Using your answer to the previous question, find explicitly the inverse of [59] in U_{99} **without** using the extended Euclidean algorithm.