1. Prove that the kernel of a homomorphism is a subgroup of the domain of the homomorphism.

   Hints: Since the domain is a group, and since any subgroup shares the same operation as its parent there is no need to show that the operation is associative. Let $\varphi : G \to G'$ be a homomorphism, then you must show three things:

   1. **closure:** Pick two arbitrary elements say $a, b \in \ker(\varphi)$ and show that their product must necessarily also be an element of $\ker(\varphi)$, i.e. show $\varphi(ab) = 1$.
   2. **identity:** Show that $1 \in \ker(\varphi)$.
   3. **inverses:** Show that if $a \in \ker(\varphi)$, then $a^{-1} \in \ker(\varphi)$.

Solution: This is a "proof by definitions" where we combine applicable definitions to obtain the desired results.

closure: We must show that if φ is a homomorphism, and $a, b \in \ker(\varphi)$ then the product $ab \in \ker(\varphi)$.

φ a homomorphism $\iff$ for all $a, b \in G$, $\varphi(ab) = \varphi(a)\varphi(b)$.

Suppose $1'$ is the identity in G', then $a, b \in \ker(\varphi) \Leftrightarrow \varphi(a) = 1'$ and $\varphi(b) = 1'$.

$$\varphi(ab) = \varphi(a)\varphi(b) = 1'1' = 1'.$$

Which implies that the product $ab \in \ker(\varphi)$.

identity: We must show that if 1 is the identity of G, then $1 \in \ker(\varphi)$. By the definition of kernel, this is equivalent to showing $\varphi(1) = 1'$, if $1'$ is the identity of G'.

1 is the identity of G $\iff$ for all $a \in G, a1 = a = 1a$.

$$\varphi(a1) = \varphi(a) = \varphi(1a)$$

$$\varphi(a)\varphi(1) = \varphi(a) = \varphi(1)\varphi(a)$$

Notice that every factor on the bottom line is an element of G' and that the element $\varphi(1) \in G'$ satisfies the requirements for being the identity of G', therefore by the uniqueness of identities (see discussion after group definition), $\varphi(1) = 1'$.

inverses: We must show that if $a \in \ker(\varphi)$ then $a^{-1} \in \ker(\varphi)$. This is equivalent to showing $\varphi(a^{-1}) = 1'$.

a and a^{-1} are inverses in G $\iff$ $aa^{-1} = 1 = a^{-1}a$.

$a \in ker(\varphi)$ $\iff$ $\varphi(a) = 1'$.

Assume $a \in \ker(\varphi)$, but we can's assume this of a^{-1}. We can only assume that it exists because $a \in G$ and G is a group.

$$\varphi(aa^{-1}) = \varphi(1) = \varphi(a^{-1}a)$$

$$\varphi(a)\varphi(a^{-1}) = \varphi(1) = \varphi(a^{-1})\varphi(a)$$

By hypothesis, $\varphi(a) = 1'$ and by our previous result $\varphi(1) = 1'$ thus:

$$1'\varphi(a^{-1}) = 1' = \varphi(a^{-1})1'$$

The definition of what it means to be the identity of G' then implies that $\varphi(a^{-1}) = 1'$.

2. Let G be a group, the map $f : G \to G$ given by $f : g \mapsto g^{-1}$ is not always a homomorphism. Why not? What property must G have to make it a homomorphism?

   Hint: Consider the product of two elements in G say ab, then $f(ab) = [ab]^{-1}$, but you can actually figure out how to write $[ab]^{-1}$ in terms of a^{-1} and b^{-1} if you use the definition of inverses (found in the group definition).

> **Solution:** Suppose 1 is the identity of G, then $(ab)^{-1} = b^{-1}a^{-1}$ because:
>
> $$(ab)(ab)^{-1} = (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = a1a^{-1} = 1$$
>
> and
>
> $$(ab)^{-1}(ab) = (b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1b = 1,$$
>
> but
>
> $$f(ab) = (ab)^{-1} = b^{-1}a^{-1} = f(b)f(a) \neq f(a)f(b),$$
>
> unless G is abelian.

3. Let G be a group, prove that "the conjugation by g" map $\varphi_g : G \to G$ given by $\varphi_g : a \mapsto gag^{-1}$ is a homomorphism.

   Hint: You want to show that given $a, b \in G, \varphi_g(ab) = \varphi_g(a)\varphi_g(b)$. This can be done by inserting a special form of the identity element, namely, $g^{-1}g$, into the image of ab.

> **Solution:**
>
> $$\varphi_g(ab) = gabg^{-1} = ga1bg^{-1} = ga(g^{-1}g)bg^{-1} = \varphi_g(a)\varphi_g(b)$$