1. (DF1.6.14) Let G and H be groups and let $\varphi\colon G \to H$ be a homomorphism. Prove that the kernel of φ is a subgroup of G (1). Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G (2).

   Proof. (1) To show that $\ker(\varphi) \leq G$, we can verify that $\ker(\varphi)$ is a nonempty subset of G which is closed under the group operation (of G) and is closed under taking inverses.

   Observe that $\ker(\varphi)$ is nonempty because $1 \in \ker(\varphi)$, as homomorphisms by definition map the identity of G to the identity of H. (To see this, let $a \in G$, and see that $\varphi(a) = \varphi(1_G a) = \varphi(1_G)\varphi(a)$, and by right cancellation, $1_H = \varphi(1_G)$.)

   Then let $a, b \in \ker(\varphi)$. Then $\varphi(ab) = \varphi(a)\varphi(b) = 1_H 1_H = 1_H$. Hence $ab \in \ker(\varphi)$. Hence $\ker(\varphi)$ is closed under the group operation.

   Then also see that for $a \in \ker(\varphi)$, $1_H = \varphi(1_G) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) = 1_H\varphi(a^{-1}) = \varphi(a^{-1})$. So a^{-1} is also mapped to the identity in H so it must be in $\ker(\varphi)$. Hence $\ker(\varphi)$ is closed under taking inverses, and we must have that $\ker(\varphi) \leq G$. □

   Proof. (2) Forwards direction. Suppose that $\ker(\varphi) = \{1_G\}$. Then for $a, b \in G$, see that if $\varphi(a) = \varphi(b)$, then $1_H = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$. Then since $\ker(\varphi) = \{1_G\}$, then $e = ab^{-1}$ implies $b = a$. (To see that φ maps inverses to inverses, take $c \in G$ and see that $1_H = \varphi(1_G)) = \varphi(cc^{-1}) = \varphi(c)\varphi(c^{-1})$, and so $\varphi(c)^{-1} = \varphi(c^{-1})$.) Hence φ is injective.

   Converse. Suppose that φ is injective. Then suppose by contradiction that there exists $a \in G$ where $a \neq 1_G$ such that $\varphi(a) = 1_H$. Then $\varphi(a) = \varphi(1_G) = 1_H$, but $a \neq 1_G$, which is in contradiction to φ being injective. Hence $\ker(\varphi)$ only contains the identity of G. (Automatically if we have injectivity, we should have that only the identity of G is sent to the identity of H.) □

2. (DF1.6.19) Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

   Proof. We should first check that G is a group under the standard multiplication in $\mathbb{C}$, which we know is already associative (and $G \subseteq \mathbb{C}$). It suffices to show that G is closed under the operation, contains an identity element, and has inverses for every element.

   The complex number $1 = 1 + 0i$ is the identity of G, as 1 raised to any positive integer will still be 1, and from $\mathbb{C}$ we know that $1z = z1 = z$ for any $z \in \mathbb{C}$ and hence is also true for any $z \in G$. Hence G is nonempty.

   Let $z, w \in G$. Then there exists $n, m \in \mathbb{Z}^+$ such that $z^n = w^m = 1$. Then observe that $\operatorname{lcm}(n,m) \in \mathbb{Z}^+$, and hence $(zw)^{\operatorname{lcm}(n,m)} = z^{\operatorname{lcm}(n,m)}w^{\operatorname{lcm}(n,m)} = z^{nk}w^{mj} = (z^n)^k(w^m)^j = 1^k 1^j = 1$, where since n and m divide $\operatorname{lcm}(n,m)$, there exist integers $k, j \in \mathbb{Z}^+$ where $\operatorname{lcm}(n,m) = nk = mj$. Hence $zw \in G$, so G is closed under the group operation.

   To find an inverse for some element w in G, observe that there exists a $j \in \mathbb{Z}^+$ such that $w^j = 1$. If $w = 1$, then automatically $w^{-1} = 1$. If w is not the identity, see that $w \cdot w^{j-1} = w^{j-1} \cdot w = 1$, where $j - 1 \in \mathbb{Z}^+$.

(Only 1 satisfies $z^1 = 1$ in $\mathbb{C}$.) Furthermore see that $(w^{j-1})^j = w^{j\cdot(j-1)} = (w^j)^{j-1} = 1^{j-1} = 1$. Then in this case $w^{-1} = w^{j-1}$, where j is a positive integer such that $w^j = 1$. Hence G is a group.

For any fixed integer $k > 1$, let $\varphi_k \colon G \to G$ be given by $\varphi_k(z) = z^k$. Then we must show that φ_k is surjective but not injective (but still preserves the group operation). Clearly for $z, w \in G$, $\varphi_k(zw) = (zw)^k = z^k w^k = \varphi_k(z)\varphi_k(w)$. Then for $z \in G$, observe that we may write $z = e^{2\pi i \frac{p}{q}}$, for some $p, q \in \mathbb{Z}^+$ (p, q are not unique for z), because there exists $n \in \mathbb{Z}^+$ such that $z^n = e^{2\pi i j} = 1$, where j is any positive integer (n will be any positive multiple of q). So then let $w = e^{2\pi i \frac{p}{qk}}$, so that there still exists a positive integer m such that $w^m = 1$ (here m will be a positive multiple of qk), and so $w \in G$. Observe that $\varphi_k(w) = w^k = \left(e^{2\pi i \frac{p}{qk}}\right)^k = e^{2\pi i \frac{p}{q}} = z$. Since z was an arbitrary element of G and we constructed another element w in G from z, we have that φ_k is surjective (for every $z \in G$ we can find $w \in G$ such that $\varphi_k(w) = z$).

We can show that φ_k is not injective by exhibiting an element (for each k) which is not 1 which maps to 1 under φ_k. So we try $z = e^{2\pi i \frac{1}{k}}$, and see that because $k > 1$, $z \neq 1$. $z \in G$ because raising z to some positive multiple of k, a positive integer, produces 1. Then see that $\varphi_k(z) = z^k = \left(e^{2\pi i \frac{1}{k}}\right)^k = e^{2\pi i} = 1 = 1^k = \varphi_k(1)$. Hence φ_k is not injective. □

3. (DF1.6.20) Let G be a group and let $\text{Aut}(G)$ be the set of all isomorphisms from G onto G. Prove that $\text{Aut}(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $\text{Aut}(G)$ are called *automorphisms* of G).

Proof. Let $\text{Aut}(G)$ be the set of isomorphisms from G onto G as given. Then because function composition is associative, we already have associativity in $\text{Aut}(G)$.

Naturally the identity map will be in $\text{Aut}(G)$ since it fixes every element and will preserve the group operation, so $\text{Aut}(G)$ is nonempty.

To show that the set is closed under function composition, recall that a composition of two bijections is a bijection also. What remains to show is that the group operation is still preserved. Let $f, g \in \text{Aut}(G)$. Then for $a, b \in G$, $(fg)(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b)) = (fg)(a)(fg)(b)$, so composition also preserves the group operation and so compositions of automorphisms are also automorphisms.

Then to show that the set contains inverses, see that if f is an automorphism, then the inverse mapping f^{-1} is bijective. We need to show that it preserves the group operation to be an automorphism. Let $a, b \in G$, and from $f^{-1}(ab)$ note that because f is a bijection, there exist $c, d \in G$ such that $f(c) = a$ and $f(d) = b$. So $f^{-1}(ab) = f^{-1}(f(c)f(d)) = f^{-1}(f(cd)) = cd = f^{-1}(a)f^{-1}(b)$. Hence f^{-1} is also an automorphism, and so $\text{Aut}(G)$ is a group under function composition. □

4. (DF1.6.23) Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called *fixed point free* of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]

Proof. Let G be a finite group as given, possessing a fixed point free automorphism σ of order 2.

First we show that every element $g \in G$ can be written in the form $x^{-1}\sigma(x)$, so that $g = x^{-1}\sigma(x)$ for some unique $x \in G$. Observe that for $y, z \in G$, then if $y^{-1}\sigma(y) = z^{-1}\sigma(z)$, then we can multiply on the left and right judiciously to find that $\sigma(y)\sigma(z)^{-1} = \sigma(y)\sigma(z^{-1}) = \sigma(yz^{-1}) = yz^{-1}$. But the *only* element which is fixed in G under σ is 1, so $yz^{-1} = 1 \implies y = z$ (so $y \neq z \implies y^{-1}\sigma(y) \neq z^{-1}\sigma(z)$). With this, if we consider the set given by $\{x^{-1}\sigma(x) \mid x \in G\}$, then it is clear that this set has the same cardinality as G, and since σ is an automorphism each element in the set is an element of G. Because each $x^{-1}\sigma(x)$ is a distinct element of G, each $x^{-1}\sigma(x)$ can be equated to a unique $g \in G$.

Then for some $g, x \in G$ where $g = x^{-1}\sigma(x)$, see that $\sigma(g) = \sigma(x^{-1}\sigma(x)) = \sigma(x^{-1})\sigma(\sigma(x)) = \sigma(x)^{-1}\sigma^2(x) = \sigma(x)^{-1}x$. But then also see that $g^{-1} = (x^{-1}\sigma(x))^{-1} = \sigma(x)^{-1}x = \sigma(g)$, so that really the action of σ on any element $g \in G$ is to map g to g^{-1}.

Then it suffices to show that if σ is an automorphism where for any $g \in G$, $\sigma(g) = g^{-1}$, G is abelian. Let $a, b \in G$ and see that $ab = \sigma(a^{-1})\sigma(b^{-1}) = \sigma(a^{-1}b^{-1}) = (a^{-1}b^{-1})^{-1} = ba$. So since a, b can be any element in G we have that G is abelian. $\square$