Dummit & Foote Ch. 1.6: Homomorphisms and Isomorphisms

Scott Donaldson

Mar. 2023

1. (3/25/23)

Let $\varphi : G \to H$ be a homomorphism.

(a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

Proof. By induction. When $n = 1, \varphi(x^1) = \varphi(x) = \varphi(x)^1$.

Suppose for some n, $\varphi(x^n) = \varphi(x)^n$. Then $\varphi(x^{n+1}) = \varphi(x^n x)$. By definition, because φ is a homomorphism from G to H, $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. So $\varphi(x^n x) = \varphi(x^n)\varphi(x)$. By the induction hypothesis, $\varphi(x^n) = \varphi(x)^n$, so this equals $\varphi(x)^{n+1}$.

Therefore $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$. $\square$

(b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

This proof diverges slightly from the directions but arrives at the same result.

Note that, for all $x \in G$, $\varphi(x) = \varphi(1 \cdot x) = \varphi(1)\varphi(x)$. Therefore $\varphi(1) = 1$ (in H). Now $1 = \varphi(1) = \varphi(x^n \cdot x^{-n}) = \varphi(x^n)\varphi(x^{-n})$. From part a), this equals $\varphi(x)^n\varphi(x^{-n})$. Left-multiplying both sides by $\varphi(x)^{-n}$, we obtain $\varphi(x^{-n}) = \varphi(x)^{-n}$, as desired.

2. (3/26/23)

If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$.

Proof. Let $\varphi : G \to H$ be an isomorphism and let $x \in G$. If $|x|$ is finite, then (from 1.a) $\varphi(x^n) = \varphi(x)^n$ and (from 1.b) $\varphi(1) = \varphi(x^n) = \varphi(x)^n = 1 \in H$. The order of the element $\varphi(x)^n \in H$ is therefore at most n. Because φ is an isomorphism, there is only one element whose image is 1, and that is $\varphi(1) = 1$. Therefore for no $m < n$ do we have $\varphi(x)^m = 1$, and so the $|\varphi(x) = n$.

Next, suppose that x has infinite order in G. Then $x^n \neq 1$ for all $n > 0$. Because φ is an isomorphism, we know that only $\varphi(1) = 1 \in H$. Therefore $\varphi(x^n) = \varphi(x)^n \neq 1$ for all $n > 0$. Therefore $|\varphi(x)| = \infty$.

This result is not necessarily true if φ is a homomorphism. For example, φ could send every element of G to the identity in H. (This is a homomorphism: $\varphi(x)\varphi(y) = 1 \cdot 1 = 1$ and $\varphi(x)\varphi(y) = \varphi(xy) = 1$.) Then for all $x \in G$, $|\varphi(x)| = 1$, regardless of the order of x. $\square$

3. (3/27/23)

If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If φ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

Proof. First, let G be an abelian group and $\varphi : G \to H$ be an isomorphism. Given arbitrary distinct elements of H, because φ is surjective, there are two distinct elements in G whose images are these elements in H. Let $\varphi(x), \varphi(y) \in H$ be distinct elements and $x, y \in G$. Then $\varphi(xy) = \varphi(x)\varphi(y)$. Also, because x and y commute, $\varphi(xy) = \varphi(yx) = \varphi(y)\varphi(x)$. Therefore $\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$, so H is an abelian group.

Next, let H be an abelian group. Again let $\varphi(x), \varphi(y) \in H$ and $x, y \in G$. Then $\varphi(x)\varphi(y) = \varphi(xy)$. Also, $\varphi(x)\varphi(y) = \varphi(y)\varphi(x) = \varphi(yx)$. So $\varphi(xy) = \varphi(yx)$. Because φ is one-to-one, this implies that $xy = yx$, and so G is an abelian group.

If φ is a homomorphism, then G being an abelian group does not imply that H is abelian. For example, H could be a non-abelian group and φ could send every element of G to the identity in H.

A sufficient condition for a homomorphism $\varphi : G \to H$ to ensure that if G is abelian, then so is H, is that φ is surjective. Then for all $h \in H$, $h = \varphi(x)$ for some $x \in G$ (possibly more than one x). Let $h_1, h_2 \in H$ with $h_1 = \varphi(x_1) = \varphi(x_2) = ...$ and $h_2 = \varphi(y_1) = \varphi(y_2) = ...$ and with $x_i, y_j \in G$. φ is a homomorphism, so for any i, j, $\varphi(x_i y_j) = \varphi(x_i)\varphi(y_j) = h_1 h_2$. Also, because G is abelian, $\varphi(x_i y_j) = \varphi(y_j x_i) = \varphi(y_j)\varphi(x_i) = h_2 h_1$. Therefore $h_1 h_2 = h_2 h_1$, so H is abelian. $\square$

4. (3/27/23)

Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

Proof. For any $x \in \mathbb{R} - \{0\}$, $x \neq \pm 1$, x has infinite order. The proof of this is as follows: Let $x \in \mathbb{R} - \{0, \pm 1\}$. If the absolute value of x is greater than 1, then the absolute value of x^n is greater than 1 for all n, and by induction x has infinite order. If the absolute value of x is less than 1, then the absolute value of x^n is less than 1 for all n, and by induction x has infinite order. So 1 and -1 are the only elements of $\mathbb{R} - \{0\}$ with finite order.

In $\mathbb{C} - \{0\}$, i and $-i$ have order 4. From 2., isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. However, $\mathbb{R} - \{0\}$ has no elements of order 4, and $\mathbb{C} - \{0\}$ has at least 2. Therefore they are not isomorphic. □

5. (3/27/23)

Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Proof. Given that $\mathbb{R}$ and $\mathbb{Q}$ do not have the same cardinality ($\mathbb{R}$ is uncountable while $\mathbb{Q}$ is countably infinite), there is no map $\varphi : \mathbb{Q} \to \mathbb{R}$ that is surjective. An isomorphism is a bijection that is necessarily surjective, and so the two groups are not isomorphic.

Alternatively, consider the homomorphism $\varphi : \mathbb{Q} \to \mathbb{R}$ defined by $\varphi(q) = q$. Such a map is injective but not surjective: There is no $q \in \mathbb{Q}$ with $\varphi(q) = \sqrt{2} \in \mathbb{R}$. If we attempt to make φ surjective by assigning $\varphi(q_1) = \sqrt{2}$ for some q_1, then q_1 now has no preimage in $\mathbb{Q}$, and so we must find a q_2 and assign $\varphi(q_2) = q_1$. However, now q_2 has no preimage. This process continues *ad infinitum*, and φ is forever not surjective. Therefore $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic. □

6. (3/27/23)

Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Proof. Consider a homomorphism $\varphi : \mathbb{Z} \to \mathbb{Q}$. For all $n \in \mathbb{Z}$, $\varphi(0) = \varphi(n + (-n)) = \varphi(n) + \varphi(-n)$. From 1.b), $\varphi(0) = 0$, so φ preserves inverses: $\varphi(-n) = -\varphi(n)$. That is, $\varphi(n) = q$ implies that $\varphi(-n) = -q$.

We also claim that, if $\varphi(1) = k$, then φ assigns all integers to their product with k in $\mathbb{Q}$. Since φ preserves inverses, we only have to show this for $n \in \mathbb{Z}^+$, by induction (base case given): Suppose that $\varphi(n) = kn$ for some $n \in \mathbb{Q}^+$. Then $\varphi(n+1) = \varphi(n) + \varphi(1) = kn + k = k(n+1)$, as desired. Therefore φ assigns all integers to their product with k in $\mathbb{Q}$.

But now it is impossible for φ to be surjective, because only integer multiples of k have preimages in $\mathbb{Z}$. For example, $k/2 \in \mathbb{Q}$ has no preimage. Therefore $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic. □

7. (3/27/23)

Prove that D_8 and Q_8 are not isomorphic.

Proof. $s, sr, sr^2, sr^3 \in D_8$ all have order 2. However, in Q_8, only -1 has order 2. From 2., isomorphic groups must have the same number of elements of each order. Therefore D_8 and Q_8 are not isomorphic. □

8. (3/28/23)

Prove that if $n \neq m$, S_n and S_m are not isomorphic.

Proof. Without loss of generality, let $n > m$. From Chapter 1.3, the order of a symmetric group S_n is $n!$. Then S_n contains $n!$ elements, and S_m contains $m!$ elements. It is trivial to show that $n > m \Rightarrow n! > m!$. Since the two groups do not have the same cardinality, there is no bijection between them. Thus S_n and S_m are not isomorphic. □

9. (3/28/23)

Prove that D_{24} and S_4 are not isomorphic.

Proof. D_{24} has 24 elements, and S_4 has 24 elements. They are both non-abelian. In order to prove that they are not isomorphic, then, let us consider the orders of each group's respective elements.

D_{24} has 13 elements of order 2: $\{sr^i \mid i \in \{0, ..., 11\}\}$ and r^6.

The elements of order 2 in S_4 are those permutations with cycle decompositions that are disjoint 2-cycles:
$\{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. So there are 9 elements of order 2 in S_4.

Since D_{24} and S_4 do not have the same number of elements of order 2, they are not isomorphic. □

10. (3/31/23)

Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: Let $\theta : \Delta \to \Omega$ be a bijection. Define

$$\varphi : S_\Delta \to S_\Omega \text{ by } \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \text{ for all } \sigma \in S_\Delta$$

and prove the following:

(a) φ is well-defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.

To show that φ is well-defined, we need to show that it assigns a given permutation of Δ to a unique permutation of Ω.

An arbitrary permutation σ is a bijection from Δ to itself. It is represented with a cycle decomposition that shows how it assigns a given element of Δ to another element. For σ and a given element s_1, we can say that σ assigns s_1 to $s_2 \in \Delta$.

Since Δ and Ω have the same cardinality, there exists a bijection θ between them, and we can say that θ assigns distinct $s_1, s_2 \in \Delta$ to distinct $t_1, t_2 \in \Omega$, respectively.

Now let us consider what happens when we apply φ to σ. By definition, $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$. θ^{-1} is a bijection: $\Omega \to \Delta$, σ is a bijection: $\Delta \to \Delta$, and θ is a bijection: $\Delta \to \Omega$. Applying the compositions, we see that $\varphi(\sigma)$ is a map from $\Omega \to \Omega$ (not yet proven to be a bijection).

t_1 is an arbitrary element of Ω with preimage $s_1 \in \Delta$. Then:

$$\varphi(\sigma)(t_1) = \theta(\sigma(\theta^{-1}(t_1))) = \theta(\sigma(s_1)) = \theta(s_2) = t_2,$$

that is, $\varphi(\sigma)$ is a permutation of Ω that uniquely assigns t_1 to t_2. Therefore φ is well-defined.

(b) φ is a bijection from S_Δ onto S_Ω.

We have shown that φ is a well-defined map from S_Δ onto S_Ω. However, it remains to be shown that φ is a bijection.

To show that φ is invertible, define a map $\gamma : S_\Omega \to S_\Delta$, with $\gamma(\tau) = \theta^{-1} \circ \tau \circ \theta$ for $\tau \in \Omega$. The proof above suffices to show that γ is well-defined.

Consider what happens when we take $\gamma(\varphi(\sigma))$:

$$\gamma(\varphi(\sigma)) = \gamma(\theta \circ \sigma \circ \theta^{-1}) = \theta^{-1} \circ (\theta \circ \sigma \circ \theta^{-1}) \circ \theta = (\theta^{-1}\theta) \circ \sigma \circ (\theta^{-1}\theta) = \sigma.$$

That is, $\gamma(\varphi(\sigma)) = \sigma$ for all $\sigma \in S_\Delta$. Therefore $\gamma = \varphi^{-1}$. Since φ has a well-defined inverse, it is a bijection from S_Δ onto S_Ω.

(c) φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

We apply the function compositions:

$$\begin{aligned}\varphi(\sigma \circ \tau) &= \\ &(\theta \circ \sigma \circ \theta^{-1}) \circ (\theta \circ \tau \circ \theta^{-1}) = \theta \circ \sigma \circ (\theta^{-1} \circ \theta) \circ \tau \circ \theta^{-1} = \\ &\qquad \theta \circ \sigma \circ \tau \circ \theta^{-1} = \varphi(\sigma) \circ \varphi(\tau).\end{aligned}$$

Thus φ is a homomorphism, and since it is also a bijection, the groups S_Δ and S_Ω are isomorphic.