MAT 370: Proof Portfolio

77

[redacted]

May 2021

Theorem 1. The given map φ is an isomorphism of $\langle \mathbb{Z}, + \rangle$ with $\langle \mathbb{Z}, + \rangle$ where $\varphi(n) = -n$.

Proof: Let $\langle \mathbb{Z}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ be binary structures. Define $\varphi: \mathbb{Z} \to \mathbb{Z}$ by $\varphi(n) = -n$. To be isomorphic, the function has to satisfy the following three properties: one-to-one, onto, and possess the homomorphism property.

One-to one: Let $x, y \in \mathbb{Z}$. Assume $\varphi(x) = \varphi(y)$. This implies that $-x = -y$. When we divide both sides of the equation by -1, we conclude that $x = y$. Therefore, φ is one-to-one.

Onto: Let $y \in \mathbb{Z}$. Then set $x = -y \in \mathbb{Z}$ such that, $\varphi(x) = -(-y) = y$. Since y is an arbitrary element of the codomain and we have shown that it is in the range, φ is onto.

Homomorphism Property: Let $x, y \in \mathbb{Z}$. We'll prove that it satisfies the homomorphism property.

On one hand, $\varphi(x + y) = -(x + y) = -x - y$.

On the other hand, $\varphi(x) + \varphi(y) = -x - y$.

Notice $\varphi(x + y) = \varphi(x) + \varphi(y)$. Therefore, φ satisfies the homomorphism property.

Thus, since φ satisfies all three of the required properties to be an isomorphism, φ is an isomorphism.

9/9

■

Reflection on Theorem 1

A proof that I chose to be in my portfolio was: the given map φ is an isomorphism of the first binary structure with the second, $\langle \mathbb{Z}, + \rangle$ with $\langle \mathbb{Z}, + \rangle$ where $\varphi(n) = -n$. I chose to include this proof because I struggled with how to prove that the given map was onto. This proof was also confusing for myself to understand because the two binary structures compared are the same. This proof is beneficial to include within my proof portfolio since it satisfies the requirement for a proof that a function is an isomorphism.

When I first approached this proof, I knew that in order for the map φ to be isomorphic, it must satisfy three properties: one-to-one, onto, and possess the homomorphism property. I used my notes from class and started an outline for the proof on scratch paper, knowing I was not yet ready for a final copy. I knew how to prove that the map was one-to-one by showing that $\varphi(x) = \varphi(y)$ for any $x, y \in \mathbb{Z}$, but I ran into confusion when trying to show that the map was onto. I decided to go to office hours to receive help to better understanding the process. Within office hours, my professor showed me that in order to show that φ is onto we must introduce an arbitrary element in the codomain and show that it is also in the range. We went through a few examples and it helped me better understand the onto process. After I showed that φ is onto, I used the homomorphism property, $\varphi(x + y) = \varphi(x) + \varphi(y)$ to show that φ is indeed homomorphic. I could now conclude that φ is an isomorphism. To better the proof for my portfolio, I removed some unnecessary words and condensed my computations within the homomorphism property.

3/3

Theorem 2. Let n be a positive integer and let $n\mathbb{Z} = \{nm | m \in \mathbb{Z}\}$, then $\langle n\mathbb{Z}, + \rangle$ is a group.

Proof. Let n be a positive integer and let $n\mathbb{Z} = \{nm | m \in \mathbb{Z}\}$. We will show that $\langle n\mathbb{Z}, + \rangle$ is a group. To be so, it must satisfy the three group axioms.

$\mathcal{G}_1$: The operation is induced from addition on $\mathbb{Z}$, and addition is associative, thus the operation is associative on $n\mathbb{Z}$ and $\langle n\mathbb{Z}, + \rangle$ satisfies $\mathcal{G}_1$.

$\mathcal{G}_2$: Note that the identity element $0 \in n\mathbb{Z}$, since $n \cdot 0 = 0$ for any $n \in n\mathbb{Z}$. Thus, $0 + n = n + 0 = n$ and $\mathcal{G}_2$ is satisfied.

$\mathcal{G}_3$: Let $x \in n\mathbb{Z}$. This implies that $x = nm$ where m is some integer. Thus, $-x = -nm = n(-m) \in n\mathbb{Z}$. Notice, $x + (-x) = 0$ and $(-x) + x = 0$, where $-x$ is the inverse of x. As x was an arbitrary element of $\mathbb{Z}$, $\mathcal{G}_3$ is satisfied.

Thus, $\langle n\mathbb{Z}, + \rangle$ is a group.

■

Reflection on Theorem 2

A proof that I chose to include in my proof portfolio was: Let n be a positive integer and let n$\mathbb{Z} = \{nm | m \in \mathbb{Z}\}$, $\langle n\mathbb{Z}, + \rangle$ is a group. I chose to include this proof because when I initially approached it, I felt confident, but became quickly confused within the processes involved. This proof is beneficial to include within my portfolio because it satisfies the requirement for a proof about cyclic groups.

I started the proof on scratch paper, and I accidentally let n be an even integer and not a positive integer. This caused me to become stuck when I let $n = 2k$ where $k \in \mathbb{Z}$. I decided to go to office hours where I was made aware of my mistake for n. During office hours, another aspect of the proof became confusing. It was how we could conclude that the operation automatically satisfied $\mathcal{G}_1$. Through this confusion, my professor talked me through the definition of what it means to be under the induced operation. I now better understand this property. When I moved on to prove that $\langle n\mathbb{Z}, + \rangle$ satisfied $\mathcal{G}_2$, I noticed that $0 \in n\mathbb{Z}$, thus it became easy to show that $\mathcal{G}_2$ was satisfied. For the last group axiom, I began by letting $x \in n\mathbb{Z}$ and then used the given definition for n$\mathbb{Z}$ in order to show that for every $x \in n\mathbb{Z}$ there exists $x' \in \mathbb{Z}$ where x' is the inverse of x. In order to understand how to prove $\mathcal{G}_3$ I turned to my class notes. Exercise 16 in packet 4 was beneficial in aiding to this process. After demonstrating that $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$ were all satisfied I was able to conclude that $\langle n\mathbb{Z}, + \rangle$ is a group. When I submitted this proof, I did get it correct, but the mindful effort that went into solving it has helped me to better understand the processes behind proving that a given binary structure is a group. To improve the proof, I refrained from adding some of the unnecessary words from the original proof that made it lengthy.

Theorem 3. Given a partition on a Set S, the relation defined by "$x \sim y$ if and only if x and y are in the same cell" is an equivalence relation on S.

Proof. Let "$x \sim y$ if and only if x and y are in the same cell" be a partition on a set S. We will show that $x \sim y$ is an equivalence relation.

Reflexive: Let $x \in S$. Since x is in the same cell as x, $x \sim x$. Thus, as x is an arbitrary element in the set S, $\sim$ is reflexive.

Symmetric: Let $x, y \in S$. Suppose $x \sim y$. This means that x and y are within the same cell. Thus, as x and y are arbitrary elements of the set S, $y \sim x$, and $\sim$ is symmetric.

Transitive: Let $x, y, z \in S$. Suppose $x \sim y$ and $y \sim z$. This means that x and y are in the same cell and y and z are in the same cell. Thus, x and z must also be in the same cell. Therefore, $x \sim z$ and as x, y, and z are arbitrary elements of the set S, $\sim$ is transitive.

Therefore, the relation "$x \sim y$ if and only if x and y are in the same cell" is an equivalence relation on the set S given that it satisfies the three required properties.

■

Reflection on Theorem 3

A proof that I chose to include in my proof portfolio was: Given a partition on a Set S, the relation "$x \sim y$ if and only if x and y are in the same cell" is an equivalence relation on S. I chose to include this proof because it was a previous homework problem that I got incorrect and was initially very confused on. I am now proud of my ability to prove this theorem. This proof is also very beneficial to include within my portfolio because it satisfies the requirement for a proof that a relation is an equivalence relation.

This proof came from homework assignment number two. I was not sure how to prove theorems without using the actual definitions that I was trying to prove. In my initial proof for this theorem, I was trying to the jump to the conclusions of using the reflexive, symmetric, and transitive properties, instead of proving why they must be true. I did not understand why I could not do this. I then proceeded to go to office hours, where I was informed how to prove the properties of an equivalence relation without exclaiming that the properties must be true. In my new submission of the proof, I began by stating the obvious that since x and x are in the same cell, $x \sim x$. This proved that it is reflexive. I then let $x \sim y$. This step brought me some confusion during office hours because I knew what was to be said next, but I did not know exactly how to put it into words without making the explanation to lengthy. My professor helped me by explaining that since they are arbitrary elements of the set, $y \sim x$. I then felt confident with attempting the transitive property step. After that, I concluded that the relation was an equivalence relation. I now feel comfortable with this proof and more informed on what it means to be an arbitrary element of a set.

Theorem 4. Let G be a group and C be a subset of the group G where

$C = \{x \in G \mid xy = yx \text{ for every } y \in G\}$. C is a subgroup of G.

Proof. Let G be a group. The subset C of the group G can be defined by

$C = \{x \in G \mid xy = yx \text{ for every } y \in G\}$. We will prove that C is a subgroup of group G.

Closure: Let $x, y \in \mathbb{Z}$. Then $xb = bx$ for all $b \in G$ and $yb = by$ for all $y \in G$. Thus,

$$xyb = xby = bxy$$

Notice, $xy \in \mathbb{Z}$. Therefore, C is closed under the operation of G.

Identity: The identity element for G is e if $ey = ye = y$ for all $y \in G$. Thus, $ey = ye$

$\forall\ y \in G$ and e must be in C.

Inverse: Let $x \in C$. For any $x \in G$ there exists an $x^{-1} \in G$. Suppose that $xy = yx$ for any $y \in G$. So, we compute

$$xy = yx$$

$$x^{-1}xy = x^{-1}yx \qquad \text{(left multiplication)}$$

$$y = x^{-1}yx$$

$$yx^{-1} = x^{-1}yxx^{-1} \qquad \text{(right multiplication)}$$

$$yx^{-1} = x^{-1}y$$

Notice, $yx^{-1} = x^{-1}y$, thus $\forall\ x \in C, x^{-1} \in C$

Thus, C forms a subgroup under G since it satisfies the subgroup theorem.

■

9/9

Reflection on Theorem 4

A proof that I chose to be in my proof portfolio was: Let G be a group and C be a subset of the group G where $C = \{x \in G \mid xy = yx \text{ for every } y \in G\}$. C is a subgroup of G. I chose to include this proof because I did not complete it correctly on the second exam. After having a similar question on a homework assignment, I wanted to give the proof another try for mastery. This proof is beneficial to include in my portfolio because it satisfies the requirement to include a proof about subgroups.

On the exam, when I first attempted the proof, I received a comment stating "Major issues here". Immediately, this became an incentive to get help and to give it another try. When I first approached it, I thought I knew what I was doing. I started by applying the three properties of the subgroup theorem but became quickly confused with all of the notation within the proof, so I was not surprised that I completed it incorrectly. In order to get an idea of how to fix the proof, I went to office hours for a similar proof that was present on one of the homework assignments. We were able to go over each property of the subgroup theorem in a general application with the specific problem. One part of the proof that confused me was when to let an element exist in the subset C or the group G. When I handed in the similar proof on the homework, I made a few mistakes on letting elements exist in the subgroup/group, but I then felt confident enough to apply my new knowledge to the proof from the exam. Using my homework as a guide to help me along, I approached the proof with the same methods and was conscientious of the mistakes that I made on the homework. I now feel confident with this proof.

Theorem 5. Let G be a group and $a \in G$. Define the function $\varphi : G \to G$ by $\varphi(g) = a^{-1}ga$. φ is a permutation.

Proof. Let G be a group and $a \in G$. Define the function $\varphi : G \to G$ by $\varphi(g) = a^{-1}ga$. If φ is a permutation, it must be one-to-one and onto.

<u>One-to-one:</u> Let $x, y \in G$ and assume $\varphi(x) = \varphi(y)$. Thus,

$$a^{-1}xa = a^{-1}ya$$

$xa = ya$ (by left multiplication of a)

$x = y$ (by right multiplication of a^{-1})

Thus, φ is one-to-one.

<u>Onto:</u> Let $y \in G$. Then, $x = aya^{-1} \in G$. Thus,

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

Since y is an arbitrary element of the codomain and thus, we have shown it in the range,

φ is onto.

Therefore, φ is a permutation.

■

8/9

Reflection on Theorem 5

A proof that I chose to include within my proof portfolio was: Let G be a group and $a \in G$. Define the function $\varphi : G \to G$ by $\varphi(g) = a^{-1}ga$. φ is a permutation. I chose to include this proof because I did not complete it correctly on the third exam. After viewing my mistakes, I wanted to complete the proof again for mastery. This proof is beneficial to include in my portfolio because it satisfies the requirement to include a proof about permutation groups.

On exam three, when I first completed the proof, I made some small mistakes, but nothing too major. I started the proof by restating the hypothesis and explaining the requirements for φ to be a permutation. I began the first part of the proof by showing that φ is one-to-one. I let $x, y \in G$ and assumed $\varphi(x) = \varphi(y)$ and then computed with left and right multiplication laws to show that $x = y$ and thus, φ is one-to-one. The mistakes that I made were in the onto portion of the proof. I stated to "Assume $\varphi(x) = y$. This implies that $x = aya^{-1}$.", but I should have stated $x = aya^{-1} \in G$ where $y \in G$. Once I fixed this mistake, I used the definition of the function, $(g) = a^{-1}ga$, in order to show that the arbitrary element of the codomain, y, was present within the range, proving that φ is onto. I now feel as if I am knowledgeable with these types of proofs after being examined on my ability to complete them. Proofs of group permutations are my favorite types of proofs within this course so far and I am pleased with my ability to complete them.

Resources? 11/3

Theorem 6. $\langle \mathbb{R}^*, \star \rangle$ is a group if $a \star b = 7ab$.

Proof. We will prove that $\langle \mathbb{R}^*, \star \rangle$ is a group if $a \star b = 7ab$.

$\mathcal{G}_1$: We will test the associativity of $\star$. Let $a, b, c \in \mathbb{R}^*$. We compute,

$$(a \star b) \star c = 7(7ab)c = 49abc$$
$$a \star (b \star c) = a \star (7bc) = 7a(7bc) = 49abc$$

Thus, $(a \star b) \star c$ agrees with $a \star (b \star c)$ and $\mathcal{G}_1$ is satisfied.

$\mathcal{G}_2$: We will test for an identity element in $\langle \mathbb{R}^*, \star \rangle$. For every $a \in \mathbb{R}^*$, $\exists e \in \mathbb{R}^*$ such that $a \star e = a$ and $e \star a = a$. Consider the element $e = \frac{1}{7} \in \mathbb{R}^*$. We compute,

$$a \star e = \frac{7a}{7} = a$$
$$e \star a = \frac{7a}{7} = a$$

Thus, $\frac{1}{7}$ is an identity element for $\star$ and $\mathcal{G}_2$ is satisfied.

$\mathcal{G}_3$: We will test for an inverse in $\langle \mathbb{R}^*, \star \rangle$. Let $a \in \mathbb{R}^*$. Then $\frac{1}{49a} \in \mathbb{R}^*$ where $a \neq 0$. We compute,

$$a \star a^{-1} = \frac{7a}{49a} = \frac{1}{7}$$
$$a^{-1} \star a = \frac{7a}{49a} = \frac{1}{7}$$

Thus, $a^{-1} = \frac{1}{49a}$ and $\mathcal{G}_3$ is satisfied.

Therefore, $\langle \mathbb{R}^*, \star \rangle$ is a group if $a \star b = 7ab$ given that it satisfies the three group axioms.

■

9/9

Reflection on Theorem 6

A proof that I chose to include within my proof portfolio was: $\langle \mathbb{R}^*, \star \rangle$ is a group if $a \star b = 7ab$. I chose to include this proof because I did not complete it correctly on the second exam. After viewing my initial response from the exam, I decided that I would try to complete the proof again for mastery. This proof is beneficial to include in my portfolio because it satisfies the requirement to include a proof that a set is a group.

On exam two, when I first completed the proof, I made a few conceptual errors that lead to my downfall. I knew that I was to show that the theorem satisfied the three group axioms. In group axiom one, where you show associativity, I correctly demonstrated that $\star$ satisfied the property. In group axiom two, where you demonstrate the identity property, I did not correctly show that $\star$ satisfied the requirements. I became quickly confused when I let 1, and not $1/7$, be the identity element of a. I became lost in the computations and was running out of time, so I moved on to group axiom three. Within the process of group axiom three, where you demonstrate the inverse property, I let $x = 7a$ and $x^{-1} = 1/7$ in efforts that this would lead me to my identity element of 1 from group axiom two. I made many conceptual and procedural errors that I now am aware of and able to correct. This type of proof can be a little confusing for myself to understand without deep thought, so I am proud of my ability to now complete it correctly. I believe that it is very important to look back at previous exams, determine your mistakes, and go through the process of completing them correctly.