Standard Proof Writing and Quotient Groups

Ryan Hausner
University of Southern California

March 2025
Mathematical Reasoning and Problem Solving

Contents

1 Problem 1

1.A

Among the numerous tips offered in formal proof writing, the three that stand out to me the most are "Separate mathematical symbols and expressions with words", "Use the first person plural", and "Explain each new symbol".[1]

1. **"Separate mathematical symbols and expressions with words".** Many of the proofs I write don't have enough text connecting the symbols with words, often leaving ambiguous terms for someone who isn't familiar with the problem. By adding words between mathematical symbols, it can clarify my intentions and separate ideas that aren't meant to appear concurrently.

2. **"Use the first person plural".** By using pronouns such as "we" and "us" it will help the reader feel as if I am guiding them through my work. Proofs tend to be very difficult to parse through and using these pronouns can help make them more clear and seem less daunting overall, as if I am trying to help the reader understand not make it more confusing.

3. **"Explain each new symbol".** In many of my proofs, I introduce new symbols or call the product of many variables a new variable, without saying what I am doing. Instead of saying: $n = 2k_1k_2$ followed directly by, $n = 2k_3, k_3 \in \mathbb{R}$, I can instead write: Since for a number to be even, it has to be a multiple of 2, we can write k_1k_2 as a new variable, k_3.

1.B Example Proof Without Standard Guidelines

Theorem 1. *If A is a non-empty set and R is an equivalence relation on A, then the set of equivalence classes of R partition A.*

Proof. In the set A, every element belongs to an equivalence class. Let $a \in A$, then $a \in [a]_R$ because R is reflexive. Consider the two equivalence classes: $[a], [b]$. For A to be written as the disjoint union of its equivalence classes, the classes have to be equal or disjoint. Consider the following cases:
Case 1)

$$[a] \cap [b] = \emptyset,$$

then we're done.
Case 2)

$$[a] \cap [b] \neq \emptyset$$

meaning there is an intersection. If there is an element $y \in [a]$, we can write aRy. Similarly, if there is an element $y \in [b]$, we can write bRy.By transitivity and symmetry of equivalence, aRb, which means a is related to b. By symmetry, b is also related to a. Since there is a relation between $[a]$ and $[b]$, if we pick an element $c \in [a]$, we can write cRa, since aRb, we can write bRa for every $c \in [a]$, this means that $[a] \subseteq [b]$. Similarly, we can pick any element $c \in [b]$. We can write cRb and cRa. This means that $[b] \subseteq [a]$. Since $[a] \subseteq [b]$ and $[b] \subseteq [a]$, $[a] = [b]$. Therefore A is the union of disjoint equivalence classes because the classes are either equal or do not intersect. □

1.C Improved Version with Standard Guidelines

Theorem 2. *If A is a non-empty set and R is an equivalence relation on A, then the set of equivalence classes of R partition A.*

[1] Richard Hammack. *Book of Proof.* 3rd. Virginia Commonwealth University, 2018.

Proof. Let $a \in A$ be an element in the set A. Since we defined an equivalence relation R on A, $\forall a \in A$, we know that aRa because R is reflexive, so we can can say every element $a \in A$ is related to itself. This implies $\forall a \in A$, by reflexivity, $a \in [a]_R$, meaning every element in the set A belongs to an equivalence class. Consider two equivalence classes of A: $[a], [b]$. For the set of equivalence classes of R to partition A, the classes must be either equal or disjoint. The trivial case, where $[a] \cap [b] = \emptyset$, requires no further evaluation. The non-trivial case, where $[a] \cap [b] \neq \emptyset$ implies $\exists$ common elements between the sets. Let $y \in [a]$ be an element in the equivalence class $[a]$. By the equivalence relation, we can write aRy, so there is a relation between a and y. Since we are assuming that the intersection between the two equivalence classes $[a]$ and $[b]$ we know that the element $y \in [a]$ is also in $[b]$. Similarly, we can define a relation between y and b as bRy. By definition of an equivalence relation, we can use symmetry to write yRb. By transitivity, since we know aRy and yRb, we also know that aRb. Let c be an element in $[a]$, the relation is cRa. By transitivity, since we have cRa and aRb, we know cRb. Since we know that $\forall c \in [a], cRb$, we can conclude that $[a] \subseteq [b]$. Similarly, let $d \in [b]$ be an element in the equivalence class $[b]$. Since cRb and aRb, we can write cRa. By this, $\forall d \in [b], cRa$, we can conclude that $[b] \subseteq [a]$. Since we know that $[a] \subseteq [b]$ and $[b] \subseteq [a]$, we can conclude that $[a] = [b]$. Therefore A is the disjoint union of equivalence classes of R partition A. $\square$

Improvements

In the improved version of the proof, I considered the standard guidelines for proof writing. I made sure not to start any sentence with a mathematical symbol and ended every sentence with a sentence with a period even if it had a mathematical symbol. I made sure to clarify any new symbols and be more explicit with the new letters I was introducing, for example "Let $y \in [a]$ be an element in the equivalence class $[a]$." I made sure to say what y actually was instead of just moving on.

2 Problem 2

2.A Symmetry and Multiplication Tables

Definition 1 (Symmetry)**.** *An undetectable motion - an object is symmetric if it has symmetries.* [2]

This definition of symmetry allows us to very concretely think about what symmetry really means. Goodman uses the image of a rectangular carpet to explain symmetry, where he says if you were to leave the room and the carpet were to be flipped by 180 degrees, it would look the same as before. Similarly, if nothing were to be done, the carpet would also look the same.

Multiplication tables allow us to understand how composition of symmetries affect the object that undergoes the symmetry. Goodman says that the result of two symmetries, one right after another, is alao a symmetry.[3] This becomes very apparent with a multiplication table. Consider the following table for the symmetries of the rectangle group, with the notation we used in class ($R = \{e, r, s, sr\}$).

*	**e**	**r**	**s**	**sr**
e	e	r	s	sr
r	r	e	sr	s
s	s	sr	e	r
sr	sr	s	r	e

Multiplication tables make symmetry clear by showing what happens when you compose symmetries together. Each entry in the table, represents the composition of the row symmetry and column symmetry. Consider the first row and first column, where the symmetry is e. When you compose two transformations that both don't change the object, the composition of them is as expected, the object remains unchanged. This seems very simple, but shows the power of the multiplication table to represent composition of symmetry, which is otherwise difficult to think about. This table itself even reflects symmetries, consider the diagonal. Every entry on the diagonal is e and the rest of the table are reflections across that diagonal. This is due to the fact that the symmetry of the rectangle group under this construction is abelian, and the diagonal is due the idea that every element in the group has order 2, namely $\forall a \in R, a^2 = e$, excluding the identity element e. Consider a less intuitive composition, s and sr. This is the same as reflecting the rectangle, reflecting it again, and then rotating it by π. This is equivalent to just rotating it by π, because reflecting it twice will result in no change, as seen by the table.

Remark 1. *Abstraction is used, applying the concept of a group to something very concrete, the rotating and reflecting of a rectangle.*

2.B How Groups Are Related

Goodman emphasizes that the importance of abstraction is being able to take very abstract phenomena and treat define ways to order them, with set rules that are proved and don't require subsequent proof. He stresses the idea that we can compare different groups. The three ways groups can be related are through isomorphisms, homomorphisms, and subgroups.

1. **Isomorphism** - Goodman describes the way groups can be essentially the same as an isomorphism. An isomorphism between two groups is when every element in one group is mapped to exactly one element in a different group. Namely, we can essentially write the multiplication of two groups the same with the switch of notation. Consider the two groups, G and M, these groups are isomorphic if there is a surjection and injection between them. For an injection to exist, the elements in G need to be mapped to exactly one element in M. For them to be surjective, every element in M must be mapped by an element in G. For there to be an isomorphism, these both need to be true.

[2] Frederick Goodman. *Algebra: Abstract and Concrete.* Prentice-Hall, 2003.
[3] Goodman, see n. 2.

Definition 2 (Isomorphic)**.** *Two groups G and H are said to be isomorphic if there is a bijective map $f : H \to G$ between them that makes the multiplication table of one group match up with the multiplication table of the other.*

Consider the multiplication tables for the integers modulus 4 and the symmetry of a square:

$\mathbb{Z}/4\mathbb{Z}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Symmetry of Square

$*$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

As seen from these tables, we can create a map from each unique element in $\mathbb{Z}_4$ to the symmetry of the square (bijective map), forming an isomorphism.

2. **Homomorphism** - Goodman describes another way that groups can be related, through homomorphisms.

   Definition 3 (Homomorphic)**.** *A map $f : H \to G$ between two groups is a homomorphism if f takes products to products, identity to identity, and inverses to inverses.*

   This means that two groups can be related if one group preserves the group operation, but isn't necessarily injecective or surjective. An isomorphism is a special case of a homomorphism that is bijective. To check for a homomorphism, it is sufficient to show that $f(ab) = f(a)f(b)$.

3. **Subgroups** - The third way groups can be related is if one is a subgroup of another, that is, it is contained in the original group, but also forms a group under the same binary operation. For example, the symmetry of the square card given by $G = \{e, r, r^2, r^3\}$ is a subgroup of the entire square group given by $H = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Each element of G is contained in H and H has the same operation and forms a group, therefore it is a subgroup under composition of symmetry.

2.C Euler's Theorem

Theorem 3. *Fix a natural number n. If $a \in \mathbb{Z}$ is relatively prime to n, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Abstraction is a very powerful technique. We have all of these properties and ideas formed around groups, which we can then apply to other problems. The example at the end of this section does that exactly.

Lemma 1 (Euler's Theorem)**.** *The set $\Phi(n)$ of elements in $\mathbb{Z}_n$ possessing a multiplicative inverse forms a group (of cardinality $\varphi(n)$) under multiplication, with identity element* [1].

Goodman notes that since this forms a group, we can use all of the properties of groups that we know (identity, inverse, closure, associativity). He then uses these to reprove Euler's Theorem (Theorem 3). When trying to show that elements $[a], [b] \in \Phi(n)$, the product $[ab]$ is also in $\Phi(n)$, he is able to show the formation of $\Phi(n)$ as a group. In his proof, he says "It is clear that $[1] \in \Phi(n)$. Now since multiplication is associative on $\mathbb{Z}_n$, it is also associative on $\Phi(n)$, and since [1] is a multiplicative identity for $\mathbb{Z}_n$, it is also a multiplicative identity for $\Phi(n)$. Finally, every element in $\Phi(n)$ has a multiplicative inverse, by definition of $\Phi(n)$. This proves that $\Phi(n)$ is a group." By understanding $\Phi(n)$ as a group, something like invertibility is trivial, which can make very complicated proofs much simpler. By understanding something as a group, a very abstract construct, we can use very handy properties of it.

2.D Application to Cryptography

We established in the previous section that abstraction allows us to use group theory in unexpected ways. One of those unexpected ways is in cryptography, which involves encrypting and decrypting messages. One of the most widely used cryptography methods is the RSA public key cryptography. The idea behind it is to use products of very large prime numbers and come up with four other numbers n, m, r, s where n and r are shared and the original two primes p, q and the other two numbers m, s are kept secret. Part of the encryption/decryption process is using number theory to pick numbers that are relatively prime and congruences, and when this is applied to very large numbers, it ensures the security of the system. Group theory is also used:

"Let p and q be distinct prime numbers. Let $n = pq$. Recall that $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$. The least common multiple m of $p-1$ and $q-1$ is $\varphi(n)/gcd(p-1, q-1)$. Group theory and Euler's Theorem are being used here, to pick meaningful encryption numbers. Algebra and group theory help keep the digital world safe through the many useful properties and applications.

3 Problem 3

Proposition 1. *If G is a group (not necessarily finite) and H is a normal subgroup of G, then $G/H = \{aH | a \in G\}$ the set of left cosets of H in G is a group under the operation $(aH)(bH) = (ab)H$. G/H (read as G mod H) is called a quotient group.*

3.A Equivalence Relation Proof

Let G be a group and H be a normal subgroup of G. Show that R is an equivalence relation on G where R is defined by

$$aRb \Leftrightarrow a^{-1}b \in H$$

Proof. To show that R is an equivalence relation, we need to show that it is reflexive, symmetric, and transitive.

1. **Reflexive** - for a relation to be reflexive, it needs to satisfy that $aRa \forall a \in S$ where S is the set of elements. $aRa \Leftrightarrow a^{-1}a \in H$. Since $a^{-1}a = e$ and $e \in H$, R is reflexive.

2. **Symmetric** - for a relation to be symmetric, it needs to satisfy the following: If $a, b \in S$ and aRb implies bRa. From aRb, we know that $a^{-1}b \in H$ by construction. We want to show that $b^{-1}a$ is also in H. Since we know that H is a normal subgroup and we know that $a^{-1}b \in H$, we can take the inverse of it: $(a^{-1}b)^{-1}$. This is equal to $b^{-1}a$, which is exactly what we wanted to show. Therefore R is symmetric.

3. **Transitive** - Finally, to show this is an equivalence relation, we need to show it is transitive. For it to be transitive, we need to show that if we have aRb, bRc, that implies aRc. If we have aRb and bRc, then we can know that $a^{-1}b$ and $b^{-1}c$ are both in H. Since H is closed under multiplication, the product of these becomes: $a^{-1}bb^{-1}c = a^{-1}c$. This must be in H since it is closed under multiplication. Therefore R is transitive and since it satisfies reflexivity, symmetry, and transitivity, it is an equivalence relation.

□

3.B Equivalence Class - Coset Proof

Show that the equivalence classes of R are exactly the left cosets of H in G

Proof. Let L_a be an equivalence class of R, and $y \in L_a$. Since y is in an equivalence of R, we know that $aRy \Leftrightarrow a^{-}1y \in H$. We can write this as $y = ey = aa^{-}1y$. Let $h = a^{-1}y$, then we can write ah. Since we know that $a^{-1}y \in H$, we know that $h \in H$. Since we know that $y = ah$ and $h \in H$, we can conclude that the equivalence class $L_a \subseteq aH$. Similarly, let $y = ah \in aH$. Left multiplying by a^{-1} gives us $a^{-1}y = a^{-1}ah = h$. Since $h \in H$, then $a^{-1}y \in H$. This means that $L_a \subseteq aH$. Since we know $aH \subseteq L_a$ and $aH \subseteq L_a$, then we can conclude that $aH = L_a$, the equivalence classes of R are exactly the left cosets of H in G. □

3.C Group Construction Proof

Define G/H as the set of left cosets of H. Prove that G/H is a group under the operation $(aH)(bH) = (ab)H$

Proof. To show that G/H is a group under the operation $(aH)(bH) = (ab)H$, we need to show it is associative, closed under the operation, there exists an identity element, and each element has an inverse. Starting with associativity, let $aH, bH, cH \in G/H$. We want to show that $(aHbH)cH =$

$aH(bHcH)$. Using the group operation for the left side we get: $(ab)HcH = abcH$. For the right side we get: $aH(bc)H = abcH$. Since these sides are equal, G/H is associative. Next we have to check closure. Since G is closed, we know that $a, b, ab \in G$. Since $(aH)(bH) = (ab)H$ and $a, b, ab \in G$, we know that the left coset $abH \in G/H$, so this set is closed. Next we need to show $\exists\ e$ such that $ea = ae = a$. By the defined operation, we know that $(eH)(aH) = (eaH) = aH$. Similarly, we know that $(aH)(eH) = (ae)H = aH$, therefore there is an identity element, eH. Finally, we need to show that there is an inverse for each element in G/H such that $aa^{-1} = a^{-1}a = e$. By the defined operation, $(aH)(a^{-1}H) = aa^{-1}H = eH$. Similarly, $(a^{-1}H)(aH) = (a^{-1}aH) = eH$. Therefore each element has an inverse and G/H forms a group under the defined operation. □

3.D Normal Subgroup Proof

Let $G = \mathbb{Z}$ under addition and $H = 5\mathbb{Z}$. Show that H is a normal subgroup of G.

Proof. To show that H is a normal subgroup of G, we must show that it is a commutative group. First we check that $5\mathbb{Z}$ forms a group under addition. It is closed under addition because the sum of two integers is an integer. There is an identity element 0, where $a \in H$, $a + 0 = 0 + a = a$. It is associative because addition of integers is associative. Finally, there is an inverse for every element. Consider $a \in H$, $\exists - a$ such that $a + -a = 0$.

Lemma 2. *If G is commutative group, then every subgroup of G is normal. By definition $gHg^{-1} = \{ghg^{-1} | h \in H\}$. Since we know $g, g^{-1} \in G$ and G is commutative by assumption, we can write $ghg^{-1} = gg^{-1}h = eh = h$. Therefore we can say that $gHg^{-1} \subseteq H$. Similarly, we can say $\forall h \in H, h = eh = gg^{-1}h = ghg^{-1}$. This means that $H \subseteq gHg^{-1}$. Finally, we can conclude, $gHg^{-1} = H$. Therefore, if G is a commutative group, then every subgroup of G is normal.*

Since G is the set of integers, we know by the axioms that addition is commutative. From this we can conclude that G is a commutative group. By Lemma 2, since we know G is a commutative subgroup, we can conclude that H is a normal subgroup. □

3.E $\mathbb{Z}/5\mathbb{Z}$ Multiplication Table

Based on proposition 1, we can understand this quotient group as the left cosets of H (a normal subgroup) in G. In this case, the normal cosets are $0 + 5\mathbb{Z}$, $1 + 5\mathbb{Z}$, $2 + 5\mathbb{Z}$, $3 + 5\mathbb{Z}$, $4 + 5\mathbb{Z}$. The operation is addition, which gives us the following multiplication table.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Remark 2. *Quotient groups allow us to form new groups by taking the cosets of a normal subgroup and allows to understand groups through their cosets. By breaking a group down into its cosets, it allows us to understand the breakdown of the group, and the cosets allow us to see elements that are related in some way.*

3.F Connection between $\mathbb{Z}/5\mathbb{Z}$ to $\mathbb{Z}_5$

$\mathbb{Z}/5\mathbb{Z}$ is essentially $\mathbb{Z}_5$, the integers modulus 5, which we have dealt with many times. Since they have the same elements and operation, they behave the same way. $\mathbb{Z}/5\mathbb{Z}$ offers a new way of viewing $\mathbb{Z}_5$, through the cosets and normal groups.

References

Goodman, Frederick. *Algebra: Abstract and Concrete*. Prentice-Hall, 2003.
Hammack, Richard. *Book of Proof*. 3rd. Virginia Commonwealth University, 2018.