# Abstract Problem Set 2

Andrew Rippy

February 2019

## 1 Problem Set

### 1.1 Problem 1

Let G be a group. Show that a nonempty subset H of G is a subgroup of G if and only if $gh^{-1} \in H$ for all $g, h \in H$.

*Proof.* $G$ is a group, and let $H \neq \varnothing$ be a subset of $G$. Based on Theorem 3.6, in order for $H \leq G, H$ must fulfill the Two (Three) Step Subgroup Test.
1.) $H$ is nonempty, verified in premise. ✓
2.) $H$ must have an inverse $h^{-1}$ for every $h \in H$.
3.) $H$ is closed under the binary operation of $G$.

If $H \leq G$, then $gh^{-1} \in H$
$H$ is a subgroup so the group is closed. Because it is a subgroup, there also exists an inverse for every element $\in H$. So, because we know $g, h \in H$, then $g^{-1}, h^{-1} \in H$ and because it is closed, we know that $gh^{-1} \in H$ ✓

If $gh^{-1} \in H$, then $H \leq G$
$g, h$ are arbitrary elements $\in H$, therefore, this allows for $g = e$, then if $g = e$, $gh^{-1}$ can be rewritten as $eh^{-1} = h^{-1}$, therefore $h^{-1} \in H$. We know $h^{-1}$ represents an arbitrary inverse. Because we know arbitrary elements $g, h \in H$, we then know there exists an arbitrary pair $h, h^{-1} \in H$. Because this pair is arbitrary, we know there exists an $h^{-1}$ for every $h \in H$, proving step 2 of the subgroup test. ✓

Knowing that $h^{-1} \in H$, and $gh^{-1}$ represents an arbitrary element and an arbitrary inverse, we can substitute $h^{-1}$ in for $h$, creating $g(h^{-1})^{-1}$ which is equivalent to $gh \in H$, proving that any combination of arbitrary elements $\in H$, Therefore, H is closed, satisfying step 3 of the subgroup test. ✓
Because all three steps of the subgroup test are satisfied, $H \leq G$✓

□

## 1.2 Problem 2

Show that any group with 3 elements must have the same group table

*Proof.* If $G$ is a group, then $G$ must have an inverse $g^{-1} \in G$ for every element $g \in G$ and must contain the identity element $e \in G$
Since the group may only contain 3 elements, one element must be the identity, leaving two elements left. One option is an element and the element's inverse, while the other option is two elements, who's inverses are their own. Any other combination would result in over 3 elements that must be present in the group $G$, which is not possible.

Say $e, a, a^{-1} \in G$, then the table would look like this

| $*$ | $e$ | $a$ | $a^{-1}$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $a^{-1}$ |
| $a$ | $a$ | $a^{-1}$ | $e$ |
| $a^{-1}$ | $a^{-1}$ | $e$ | $a$ |

This table would be valid under Theorem 2.63, which states if $G$ is a group, there can be no duplicate elements in the same row or column, which implies $a^2 = a^{-1}$ and $(a^{-1})^2 = a$.✓

Say $e, a, b \in G$, then the table would look like this

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $e$ | $ab$ |
| $b$ | $b$ | $ba$ | $e$ |

However, in order to remain a group of only 3 elements, $ab$ and $ba$ would have to result in $e, a$ or $b$. However, based on Theorem 2.63, ba cannot be $b$ or $e$ because those are already in the row, and it cannot be $a$ because it is already in the column. Therefore, this table cannot exist and is invalid, and consequently G is not a group, so by contradiction, this cannot be the table of G. ✓
Therefore, by proof by cases, the only table that is possible for a group of three elements is the table generated by $G = \{e, a, a^{-1}\}$ □

## 1.3 Problem 3

Determine whether the following subsets H are subgroups of the given group G:
(a) $G = (M_{n\times n}(\mathbb{R}), +)$, H = {upper triangular $n \times n$ matrices}
(b) $G = (M_{n\times n}(\mathbb{R}), +)$, H = {diagonal $n \times n$ matrices with nonzero diagonal entries}

By Theorem, 3.6, in order for $H \leq G$, $H$ must be closed, nonempty, contain inverses $h^{-1} \in H$ for every $h \in H$, and must contain the identity.

*Proof.* (a)
Say $A, B \in H$
Say the entries of $A, B$ are $a_{ij}, b_{ij}$, respectively and the entries are given by

$$a_{ij}, b_{ij} = \begin{cases} a \in \mathbb{R} & if \text{ i} \leq j \\ 0 & if \text{ i} > \text{j} \end{cases}$$

The entries of $A + B$ sum together, $0 + 0 = 0$, therefore all 0 entries remain 0, and all entires of $a_{ij} + b_{ij} \in \mathbb{R}$ proving a triangular matrix + a triangular matrix = a triangular matrix, therefore, closed ✓

The inverse of $A$ is $-A$, as the entries behave as numbers $\in \mathbb{R}$, the inverse of the entry $a_{ij}$ would be $-a_{ij}$ since $a_{ij} + -a_{ij} = 0$, the identity is the matrix with all entries 0, thus the identity is the zero matrix, [0] ✓

Nonempty, contains all triangular matrices, ex. [0] matrix ✓

Therefore, $H \leq G$ □

*Proof.* (b)
Say $A, -A \in H$ such that the diagonal entries of $A$ are $a_{11}, a_{22}, \ \ldots\ , a_{nn}$ and 0 for $i \neq j$ and the diagonal entries of $-A$ are $-a_{11}, -a_{22}, \ \ldots\ , -a_{nn}$ and 0 for $i \neq j$
$A + (-A) = [0]$ however, the $[0] \notin H$ Therefore, H is not closed, and H is not a subgroup of G.

□

## 1.4 Problem 4

Given a subset S of a group G, prove that $\langle S \rangle$ is a group. (Yes, we did this in class, but I want you to write out the details nicely.)

*Proof.* In order to be a group on $*$, the group must be
1.) Associative
2.) Closed
3.) Contain an inverse for every element $s \in S$
4.) Contain the identity

Since $S$ is a subset, associativity is inherited, therefore $\langle S \rangle$ is associative. ✓

$\langle S \rangle$ is closed because $\langle S \rangle$ contains every possible word that can be created in $\langle S \rangle$. Every element of $\langle S \rangle$ is a composition of elements $s \in S$ and their inverses. For two arbitrary words $a \in \langle S \rangle = s_1...s_n$ and $b \in \langle S \rangle = t_1...t_m$, $a * b = s_1...s_n t_1...t_m \in \langle S \rangle$ therefore, because the arbitrary $a * b \in \langle S \rangle$, it is closed. ✓

Inverses for every element $s \in S$ exists in $\langle S \rangle$ by definition. Further, because every element in $\langle S \rangle$ is written as a combination of $s$ and $s^{-1}$, there exists an inverse for every element of $\langle S \rangle$. ✓

Because there exists an inverse $a^{-1} \in S$ for every element $a \in S$, $aa^{-1} = e$, $e$ being the identity, the identity exists. ✓

Therefore, $\langle S \rangle$ is a Group.

□

## 1.5 Problem 5

If G is a finite group of even order, then there must exist some $g \neq e$ such that $g^2 = e$.

*Proof.* Say the group G is an even order group. In order to be a group, the identity $e \in G$. Subtracting this element away would leave us with an odd number of elements. In order to be a group, every element $g \in G$ must have an inverse $g^{-1} \in G$. If each element has an inverse that is not itself, the elements would be added to the group in pairs of two, $g$ and $g^{-1}$. The other option is where the element is its own inverse, and would be added to the group by itself. Since pairs cannot add to an odd number of elements, there must exist some $g \in G$ such that $g^2 = e$.

□

## 1.6 Problem 6

Show that the group $(\mathbb{Q}, +)$ is not finitely generated. That is, there is no finite subset $S \subseteq \mathbb{Q}$ such that $\mathbb{Q} = \langle S \rangle$.

*Proof.* By definition of a generating set, only whole number multiples of elements from set S may be used to generate $\mathbb{Q}$, and all elements of $\mathbb{Q}$ have the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$

When adding fractions with different denominators, the resultant fraction's denominator can be broken up into factors of the denominators used to create it.
Exemplified by $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, when $b \neq d$, the resultant denominator's factors are the denominators used to create it.
A prime number's factors are only that prime number and 1.
Say the finite $\langle S \rangle$ contains $m$ elements with denominators 1 through $n$.
By Euclid's Theorem, we know there exists rational number $\in \mathbb{Q}$ with a prime denominator, $p$ such that $p > n$
In order for $\langle S \rangle$ to create this denominator, the fractions would have to follow the addition outlined above. However, since the prime's multiples are only 1 and itself, and $p \notin$ denominators of $\langle S \rangle$, the fraction can not be created using whole number multiples of $\langle S \rangle$.

Exemplified by $\frac{1}{p} = \frac{m}{ab}$ where $m \in \mathbb{Z}$ and is the multiple of $\frac{1}{ab}$ required to create $\frac{1}{p}$.
Solving the equation for $m$ gives, $m = \frac{ab}{p}$. However in order for $m \in \mathbb{Z}$, all factors of the denominator must cancel with factors of the numerator. But because $p$ can only be factored in $p$ and 1, and cannot create $ab$, as a result, the factors of the denominator cannot be canceled, meaning $m \notin Z$. This implies $p$ must be within n denominators of $\langle S \rangle$ in order to create $\frac{1}{p}$.

Therefore, because there are infinite primes, there will always be a rational number $\in \mathbb{Q}$ with a larger prime denominator $p \notin \langle S \rangle$. Therefore, $\langle S \rangle$ is infinite.

□