This takehome exam is due 5:00 pm Friday, September 30. Your answers need to be typeset in LaTeX and uploaded on iLearn. Please also read and sign the following and return it with your answers.

While I may have consulted with Serkan regarding this exam, the solutions presented here are my own work. I have not consulted any books other than the textbook and notes, nor have I utilized the internet in any form in relation to the exam. I understand that to get full credit, I need to show all the steps necessary to arrive at the answer, and unless it is obvious, explain my reasoning with complete sentences.

Name: Christian Camano **Signature:**Chris Camano

1.a) Let $\mathbb{Q}^+$ be the set of all nonnegative rational numbers. Show that $\mathbb{Q}^+$ is a group under addition. **correction: Changing operator to multiplication, positive rationals 0 not included.**

Proof. (1) Validitiy of binary operator
for all $a, b \in \mathbb{Q}^+ > 0$ we have two positive rational numbers . The product of these two numbers will always be positive and is either another positive rational number or positive integer both of which are elements of $\mathbb{Q}^+$ so we have closure under multiplication and thus a functional binary operator for the given set.

(2) associativity
Let a,b,c$\in Q^+ > 0$ as follows

$$a = \frac{a_n}{a_m} \quad b = \frac{b_n}{b_m} \quad c = \frac{c_n}{c_m}$$

We wish to show that:

$$\frac{a_n}{a_m}\left(\frac{b_n}{b_m}\frac{c_n}{c_m}\right) = \left(\frac{a_n}{a_m}\frac{b_n}{b_m}\right)\frac{c_n}{c_m}$$

$$\frac{a_n}{a_m}\left(\frac{b_n c_n}{b_m c_m}\right) = \left(\frac{a_n b_n}{a_m b_m}\right)\frac{c_n}{c_m}$$

$$\left(\frac{a_n b_n c_n}{b_m c_m a_m}\right) = \left(\frac{a_n b_n c_n}{a_m b_m c_m}\right)$$

By commutativity of multiplication we have:

$$\left(\frac{a_n b_n c_n}{a_m b_m c_m}\right) = \left(\frac{a_n b_n c_n}{a_m b_m c_m}\right)$$

and have proven associativity

(3) Existence of identity element
For the identity consider the number 1 which $\forall a \in \mathbb{Q}^+ > 0$

$$a(1) = a$$

(4) Existence of inverse
For the inverse of this operation the luxury of working with rationals is that we can simply multiply by the reciprocal for any element in the set. so:

$$\forall a \in \mathbb{Q}^+ > 0 : a = \frac{a_n}{a_m} \quad a - 1 = \frac{a_m}{a_n}$$

□

1.b) Now let S be the set of positive irrational numbers. Decide whether S is a group under multiplication: either show that it is a group or provide a reason why it is not a group.

Proof. This set and operator do not form a group because the operation of mulitiplication is not closed to the set S. Consider the following counter example: Let a,b$\in S$ such that $a = \frac{\sqrt{5}}{3}, b = \frac{\sqrt{5}}{4}$ then we have through multiplication:

$$ab = \frac{\sqrt{5}}{3}\frac{\sqrt{5}}{4} = \frac{5}{12}$$

$\frac{5}{12}$ is clearly a rational number thus for two elements in S we have produced an element not in S so multiplication fails to be a binary operator and hence S, and multiplication do not form a group. □

---

2. Let G be a group and let a and b be two elements in G. Suppose n is a positive integer. Compute $(aba^{-1})^n$. [Induction !]

Proof. Intuitivley we would like this operation to abide to normal conventions of exponentation that we are familiar with if done so we would arrive at the following:

$$(aba^{-1})^n = (aba^{-1})(aba^{-1})\cdots(aba^{-1}) = (ab^n a^{-1})$$

We can intuitivley see that each a term would cancel with its inverse during composition leaving behind instances of k with the first a and last a inverse left behind. To prove this we will proceed with induction:
Base case: n=1

$$(aba^{-1})^1 = ab^1a^{-1}$$

Inductive hypothesis:

$$P(k) = (aba^{-1})^k = (ab^k a^{-1})$$

P(k+1)

$$\begin{aligned}
&(aba^{-1})^{k+1} = (ab^{k+1}a^{-1}) \\
&(aba^{-1})^k(aba^{-1}) = (ab^{k+1}a^{-1}) \\
&(ab^k a^{-1})(aba^{-1}) = (ab^{k+1}a^{-1}) \quad \text{by I.H} \\
&(ab^k eba^{-1}) = (ab^{k+1}a^{-1}) \\
&(ab^{k+1}a^{-1}) = (ab^{k+1}a^{-1})
\end{aligned}$$

by the principle of mathematical induction we have proven the implication for all k and k+1 and thus the statement is true. □

---

3. Let G be a group and let a and b be any two elements in G. Suppose n is a positive integer. Show that if G is an abelian group then $(ab)^n = a^n b^n$. Give an example of a non-abelian group in which this equation does not always hold.

Proof. To approach this proof I think that it is important to explore the properties of exponentation and their relationship with commutativity. To begin:

$$(ab)^n = \prod_{i=1}^{n} ab = \prod_{i=1}^{n} a \prod_{i=1}^{n} b$$

Where here we abuse the notation of the product a little bit(I acknowledge its not necessarily multiplication) If G is abelian then under the operator we have commutativity which means that:

$$(ab)^n = \prod_{i=1}^{n} ab = ab \circ_1 ab \circ_2 \cdots \circ_n ab = abababababab \cdots ab$$

We have commutativity over the operator so we can move all of the first elements and second elements as follows:

$$abababababab \cdots ab = aaaa \cdots abbbb \cdots b = a^n b^n$$

So we have shown that if G is abelian then we can re express:

$$(ab)^n = a^n b^n$$

□

Give an example of a non-abelian group in which this equation does not always hold

Proof. The classic non abelian group we have been shown is the general linear group of n which is the set of nxn matricies equipped with matrix multiplication: consider two elements from GL_2 we have A and B.

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} B = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

let n =2

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$$

$$\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \right)^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$$

□

4.a) Let G be a group and $g \in G$. Prove that $g^2 = e$ if and only if $g = g^{-1}$.

Proof. This argument states that for any element of the group that the element composed with itself under the binary operation is equal to the identity if and only if it is true that for all elements each element's inverse is itself.
Taking a step back this makes sense if each element is in fact its own inverse then of course composition with its inverse would return the identity. To proceed with a proof we need to consider the following two conditional statements:

$$\text{If } g = g^{-1} \text{ then } g^2 = e$$
$$\text{If } g^2 = e \text{ then } g = g^{-1}$$

(1) If $g = g^{-1}$ then $g^2 = e$
If $g = g^{-1}$ then the statment g^2 is equivilant to:

$$gg^{-1} = e$$

By definition of inverse of an element in a group. Since $g = g^{-1}$ $gg^{-1} = g^2$ and we have shown $g^2 = e$

(2) If $g^2 = e$ then $g = g^{-1}$
Like wise we are going to have extremely similar reasoning here. If $g^2 = e$ Then this implies that g is its own inverse since the only way to return to the identity element in a group is through composition with its inverse.

□

4.b) Show that if $g^2 = e$ for all $g \in G$ then G is an abelian group.

Proof. This problem is quite interesting and calls upon a good inderstanding of the properties of inverses for groups. To show that G is abelian we must show that $\forall a, b \in Gab = ba$ This is actually quite straight foward though since we have the property that $(ab)^{-1} = ab$ by the sub proof of part a.

$$(ab)(ab)^{-1} = aa^{-1} = bb^{-1} = e$$
$$(ab)(ab) = aa = bb = e$$

$$(ab)(ab) = e = a(b)(b^{-1})a^{-1}$$
$$(ab)(ab) = e = a(b)(b)a$$
$$(ab)(ab) = (ab)(ba)$$

Left multiplying by ab gives:

$$(ab)(ab)(ab) = (ab)(ab)(ba)$$
$$e(ab) = e(ba)$$
$$(ab) = (ba)$$

So we have shown the operator is commutative and hence that G is abelian □

---

5. Let $n > 2$ be an integer. Show that there exist at least two elements $[x]$ and $[y]$ in $U(n)$ such that $[x]^2 = [y]^2 = [1]$.

Proof. Another way of understanding this problem is through the following phrasing: Prove that for any U(n) there exists two elements whose inverse is itself.This is to say:

$$\exists [x] \in U(n) : [x][x] = [1] \mod n$$

and

$$\exists [y] \in U(n) : [y][y] = [1] \mod n$$

The trivial case of this behavior is simply the equivilance class of 1 which is an element of all unit groups since 1 is realtively prime to all integers. This means that :

$$\forall n \in \exists [1] \in U(n) : [1][1] = [1] \mod n$$

So we have satisfied half of the proof.
We are now tasked with identifying a term that should exist in all unit groups such that its square mod n is equal to one. This implies we need a term with a general form that we can show is a multiple of n with a remainder of 1 through the division algorithm. Consider the term $n - 1$ this value when squared will always produce a multiple of n with remainder 1 by the following algebraic proof:

$$(n-1)^2 = n^2 - 2n + 1 = n(n-2) + 1$$

So we have shown that $\forall n \quad (n-1)^2 = n(k) + 1, k \in Z$ which is the exact desired behavior we want to see as this would leave a remainder of 1 and in the context of equivilances class an equivilance class of 1 so finally we arrive to our conclusion that :

$$\forall n \in \exists [n-1] \in U(n) : [n-1][n-1] = [1] \mod n$$

And the proof is complete □