Problem Set 1 Solutions

1. Show that $GL(2,R)$ is non-abelian.

Solution:

Let $A=\begin{bmatrix}1 & 3\\ -1 & 1\end{bmatrix}, B=\begin{bmatrix}-2 & 5\\ -3 & 0\end{bmatrix}$. Clearly $A,B\in GL(2,R)$ since they have determinants that are non-zero. $AB=\begin{bmatrix}-11 & 5\\ -1 & -5\end{bmatrix}$ and $BA=\begin{bmatrix}-7 & *\\ * & *\end{bmatrix}$. Clearly $AB\neq BA\ \forall G\in GL(2,R)$. Thus, $GL(2,R)$ is a non-abelian group.

* Note: Answers may vary for this problem

QED

2. Find the inverse of $A=\begin{bmatrix}2 & 6\\ 3 & 5\end{bmatrix}$ in $GL(2,Z_{11})$.

Solution:

$If\ A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$, then $A^{-1}=(Det\ A)^{-1}\begin{bmatrix}d & -b\\ -c & a\end{bmatrix}$. Note that $(Det\ (A))^{-1}$ plays the role of $\frac{1}{\det(A)}$, in the "Usual formula," that is easily verified. So, $Det\ (A)=-8\equiv 3\ (\text{mod}11)$.

So, $(Det(A))^{-1}=3^{-1}\ (\text{mod}11)=4$. So,

$A^{-1}=4\begin{bmatrix}5 & -6\\ -3 & 2\end{bmatrix}=4\begin{bmatrix}5 & 5\\ 8 & 2\end{bmatrix}\ (\text{mod}\ 11)=\begin{bmatrix}20 & 20\\ 32 & 8\end{bmatrix}=\begin{bmatrix}9 & 9\\ 10 & 8\end{bmatrix}$. One can easily verify that $AA^{-1}=A^{-1}A=e=I_2=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ (using arithmetic modulo 11)

QED

3. Show that there exists at least two elements in the group $G = U(n)$ that satisfy $x^2 = 1$.

Solution:

This is equivalent to proving that there exists two elements that are their own inverses (Note: for $x \in G = U(n)$ $x^2 = 1$ means $x \cdot x = 1$, which means x is its own inverse!). Clearly the identity element, 1, works (as it is always its own inverse). We now need to find one more. Note that in mod n (don't forget the group operation is defined to be multiplication modulo n, $(n-1)^2 \equiv (-1)^2 = 1$. So, since $11^2 = (n-1)^2 = 1$, we have established that the group elements **1 and** $(n-1)$ **satisfy the desired property.** [Note: there could be more, but we do not need to search because the problem was stated as find "At least two..."].

<u>*Motivation*</u>: We choose $1, (n-1) \in U(n)$ because if $x^2 = 1 \pmod{n}$, then $x = \pm 1 \pmod{n}$

and $-1 \equiv n-1 \pmod{n}$.

QED

4. Let G be group such that $b = c$ whenever $ab = ca$ for all $a, b, c \in G$. Show G abelian.

Proof:

Suppose G a group with $a, b, c \in G$ and $ab = ca$ implies $b = c$. Now, $aba = aba$. By associativity, $a(ba) = (ab)a$. Using the above hypothesis , we can conclude $ba = ab$. So, G is abelian.

QED

5. Prove: If in a group G, $\forall\ a, b \in G,\ (ab)^2 = a^2b^2$, then G is abelian.

Proof: Consider arbitrary $a, b \in G$. Then,

$(ab)^2 = a^2b^2$	Given
$(ab)(ab) = a^2b^2$	Definition of exponentiation
$a(ba)b = a^2b^2$	Associativity
$(ba)b = ab^2$	Left multiplication by a^{-1}
$ba = ab$	Right multiplication by b^{-1}

Thus, since $ab = ba\ \forall\ a, b \in G$, G is abelian. QED

6. Consider $G = \left(Z_{10}, +_{10}\right)$. What is the order of G? What are the orders of the elements 3 and 4 in G? That is, Find $|3|$ and $|4|$

Solution:

Consider the group $G = \left(Z_{10}, +_{10}\right)$. The order of G is 10 since $G = \{0, 1,\ \ldots,\ n\text{-}1\}$.

$|3| = 10$, since $3^{10} = 3 + 3 + 3 .... + 3 = 3(10) = 30 \equiv 0 \ \left(\text{mod}10\right) = e \in G$ *(but* $\exists$ *no* $n < 10$ *such that* $3^n = e$).

[Note: the part in parentheses is important to note since it is part of the definition of the order of an element $g \in G$.]

Similarly, $|4| = 5$ since :
$4^5 = 4(5) = 20 \equiv 0 = e \ \left(\text{mod}10\right)$, but $\exists$ no $n < 5$ such that $4^n = e$ ($n \in \aleph$).

Thus, $|G| = 10$, $|3| = 10$, $|4| = 5$, where $4, 5 \in G$.

QED