**Math 307 – Problem Set 2** **Name: Alexander Powell**

Printed-copy Due: 5pm on 09/18/2014

(**1**) Let $G$ be a group and $g \in G$. For all positive integers $n$, show that $(g^{-1})^n = (g^n)^{-1}$.

*Proof.* We prove this by induction. Base step: when $n = 1$, it is clear that $(g^{-1})^1 = g^{-1} = (g^1)^{-1}$. Now assume this is true for $n = k, k \in \mathbb{Z}, k > 1$. Then let $n = k+1$, so we have that $(g^{-1})^{k+1} = (g^{-1})^k \cdot g^{-1} = (g^k)^{-1} \cdot g^{-1} = (g^{k+1})^{-1}$.

So, via the principle of mathematical induction, it is proven that for all positive integers $n$, $(g^{-1})^n = (g^n)^{-1}$.

$\square$

(**2**) For $n \in \mathbb{N}$, $n > 1$, let $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ and $\mathbb{Z}_n^\times := \{1, \ldots, n-1\}$.

(**a**) Show that $(\mathbb{Z}_n, +)$, where $a + b := (a + b) \bmod n$, is a group.

*Proof.* To prove something is a group, we must establish 4 things: closure, associativity, identity, and inverse relationships.

We can revert back to the division algorithm, which states that modular addition is a binary operation, to prove closure.

To prove associativity, let $a, b, c \in \mathbb{Z}_n$. It can be shown that: $((a+b)modn + c)modn = ((a+b)+c)modn = (a+(b+c))modn = (a+(b+c)modn)modn.$

To prove identity, it is clear that for any element $m \in \mathbb{Z}_n$, $(m+0)modn = (0+m)modn = m$. Therefore, an identity can be defined for every element in $\mathbb{Z}_n$.

Finally, to prove the inverse, we can show that if $m \in \mathbb{Z}_n$, then it is the case that $(m + (n-m))modn = nmodn = 0$

$\square$

(**b**) For positive integers $a$ and $n$, show that $ax \bmod n = 1$ has a solution if and only if $\gcd(a, n) = 1$.

*Proof.* First we prove that $ax \bmod n = 1$ has a solution if $\gcd(a, n) = 1$. Let $(ab)modn = 1, b \in \mathbb{Z}$. Now we know there exists $p \in \mathbb{Z}$ such that $ab = np + 1$ which can be rewritten as $ab - np = 1$ and $gcd(a, n) = 1$.

Next we need to prove that if $\gcd(a, n) = 1$, then $ax \bmod n = 1$ has a solution. Since $gcd(a, n) = 1$, we know that there exist $x, q \in \mathbb{Z}$ such that $ax + nq = 1$. Also, $(ax + nq)modn = 1modn = 1 = ((ax)modn + (nq)modn)modn = ((as)modn + 0)modn = (as)modn.$

$\square$

(**c**) Use part (b) to show that $(\mathbb{Z}_n^\times, \cdot)$, where $a \cdot b := (ab) \bmod n$, is a group if and only if $n$ is a prime.

*Proof.* To prove closure: Let $a, b \in \mathbb{Z}_n$, then $(ab)modn \in \mathbb{Z}$. Then we know that $ab \neq 0$. If $(ab)modn = 0$, then there exists $p \in \mathbb{Z}$ such that $ab = np$.

To prove associativity: Let $x, y, z \in \mathbb{Z}_n$, then

$$((ab)modn \cdot c)modn = ((ab) \cdot c)modn = (a \cdot (bc))modn) = (a \cdot (bc)modn)modn$$

.

To prove identity: Let $i \in \mathbb{Z}_n$, then $(i \cdot 1)modn = (1 \cdot i)modn = i$.

To prove inverse: From part b it is clear that $(ax)modn$ has an inverse for every $a \in \mathbb{Z}_n^\times$.

$\square$

(**3**) Let $\mathbb{Q}(\sqrt{2}) := \{a + \sqrt{2}b : a, b \in \mathbb{Q}\}$. Show that

**(a)** $\mathbb{Q}(\sqrt{2}) \leq \mathbb{R}$.

*Proof.* First it is necessary to prove that $\mathbb{Q}(\sqrt{2})$ is non-empty. This is clearly the case because if you plug any rational numbers, $a$ and $b$, into the expression $a + \sqrt{2}b$, it will return a result. Second, if we let $p, q \in \mathbb{Q}(\sqrt{2})$, then $p = a + \sqrt{2}b$ and $q = c + \sqrt{2}d$. Then $(a + \sqrt{2}b)/(c + \sqrt{2}d) \in \mathbb{Q}(\sqrt{2}) \leq \mathbb{R}$. □

**(b)** $\mathbb{Q}(\sqrt{2})^{\times} \leq \mathbb{R}^{\times}$.

*Proof.* Again, it can easily be determined that $\mathbb{Q}(\sqrt{2})^{\times}$ is non-empty by simply entering in rational numbers for $a$ and $b$. Also, we will again use $p, q \in \mathbb{Q}(\sqrt{2})^{\times}$, then $p = a + \sqrt{2}b$ and $q = c + \sqrt{2}d$. The inverse of $q$ can be defined as $\frac{1}{(c+\sqrt{2}d)} = \frac{1}{(c+\sqrt{2}d)} \cdot \frac{(c-\sqrt{2}d)}{(c-\sqrt{2}d)} = \frac{(c-\sqrt{2}d)}{(c^2-2d^2)}$. Then by taking the product of $x$ and $y^{-1}$, we get

$$\frac{ac - \sqrt{2}ad}{c^2 - 2d^2} + \sqrt{2} \times (\frac{bc - \sqrt{2}db}{c^2 - 2d^2})$$

which is clearly an element of $\mathbb{Q}(\sqrt{2})^{\times}$. □

**(4)** Recall that the transpose of an $m \times n$ matrix $A = [a_{ij}]$, denoted by $A^{\mathsf{T}}$, is the $n \times m$ matrix whose entries are $[a_{ji}]$. Show that

$$O_n(\mathbb{R}) := \{Q \in GL_n(\mathbb{R}) : Q^{\mathsf{T}}Q = QQ^{\mathsf{T}} = I_n\} \leq GL_n(\mathbb{R}),$$

where $I_n$ denotes the $n \times n$ identity matrix.

*Proof.* First we must show that $O_n(\mathbb{R})$ is non-empty. This is clearly the case because the identity matrix is an element of $O_n(\mathbb{R})$.

Next, because $Q^{\mathsf{T}}Q = QQ^{\mathsf{T}} = I$ we can determine that $Q$ is an orthogonal matrix. Therefore, $Q^{\mathsf{T}} = Q^{-1}$, so if we let $A$ and $B$ be matrices $\in O_n(\mathbb{R})$, then $AB^{-1} = AB^{\mathsf{T}}$. Now, we have that $(AB^{\mathsf{T}})^{\mathsf{T}}AB^{\mathsf{T}} = B(A^{\mathsf{T}}A)B^{\mathsf{T}} = BB^{\mathsf{T}} = I$.

This is an element of $O_n(\mathbb{R})$, thus $O_n(\mathbb{R}) \leq GL_n(\mathbb{R})$. □