Zaki Glenroy Lindo, Assignment 2

Assignment 2: Due Monday September 11, 2017, no later than 8pm.

$p.37 - 39$ # 16, 17, 21, 27 (Do not use part (iii) of Theorem 1.23 or any later theorems in your proof, since you are proving Theorem 1.23 part (iii)), 36

#16. Determine if the operation defined in Example 1.5 on the set $\{John, Sue, Henry, Pam\}$ is commutative, has an identity, and if each element has an inverse.
(I included the table below for an example on how to create a Cayley Table in TeX.)

$*$	John	Sue	Henry	Pam
John	John	John	John	John
Sue	John	Sue	Pam	Henry
Pam	John	Pam	Pam	Sue
Henry	John	Henry	Sue	Henry

To talk about the set above easier, let $NAMES = \{John, Sue, Henry, Pam\}$.

(Commutative) Observe $Pam * Henry$.

For this, $Pam * Henry = Pam$. However, $Henry * Pam = Henry$. As $Pam \neq Henry$, $NAMES$ is not commutative under the operation $*$.

(Identity) Observe $Sue \in NAMES$.

Looking at the Cayley Table, we can see that for any $name \in Names$, $Sue * name = name$. Also, $name * Sue = name$. With this, we know that Sue is the identity of this set on our operation $*$.

(Inverse) Observe $John \in NAMES$.

Looking at the Cayley Table, we can see that for all $name \in NAMES$, $John * name = John$. This tells us that there does not exist $name \in NAMES$ such that $John * name = Sue$(The identity element of the set). Therefore $John$ does not have an inverse.

For the inverse of each element aside from $John$, $name^{-1} = name$. That is, $Sue^{-1} = Sue$, $Pam^{-1} = Pam$, and $Henry^{-1} = Henry$.

#17. Write out the Cayley table for the group $(\mathbb{Z}_6, +_6)$ and identify the inverse of each element.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$0^{-1} = 0$
$1^{-1} = 5$
$2^{-1} = 4$
$3^{-1} = 3$
$4^{-1} = 2$
$5^{-1} = 1$

#21. We can even create groups with games! Consider four cups placed in a square pattern on a table. If we have a penny in one of the cups there are four ways we can move it to another cup: *Horizontally, Vertically, Diagonally,* or *Stay where it is.* We label them as H, V, D, S. To define the operation, consider two movements in a row, i.e. $x * y$ means first move the penny as x tells us to, then after that move the penny as y instructs. For example $H * V = D$ since if we first move it horizontally and then vertically altogether we have moved it diagonally. Create the Cayley table for this group, identify the identity, and the inverse of each element.

$*$	H	V	D	S
H	S	D	V	H
V	D	S	H	V
D	V	H	S	D
S	H	V	D	S

(Identity) The identity in this group is S.

(Inverse) The inverse for each element is itself.

$H^{-1} = H$
$V^{-1} = V$
$D^{-1} = D$
$S^{-1} = S$

#27. Assume G is a group and $a \in G$. Prove by PMI (Theorem 0.3) that for every $n \in \mathbb{N}$, $(a^n)^{-1} = a^{-n}$. (Do not use part *(iii)* of Theorem 1.23 or any later theorems in your proof, since you are proving Theorem 1.23 part (iii).)

Let G be a group and $a \in G$.

Proof: Let $n \in \mathbb{N}$. We want to show that $(a^n)^{-1} = a^{-n}$.

(Base Case): Let $n = 1$. As $n = 1$, $(a^n)^{-1} = (a^1)^{-1} = a^{1*(-1)} = a^{-1} = a^{-n}$. Thus, for $n = 1$, $(a^n)^{-1} = a^{-n}$.

(Inductive Hypothesis): Let $n \in \mathbb{N}$. Assume that for n, $(a^n)^{-1} = a^{-n}$.

(Inductive Step): Let $n+1 \in \mathbb{N}$. Now, we want to show that $(a^{n+1})^{-1} = a^{-(n+1)}$. By our exponent rules, $(a^{n+1})^{-1} = (a^n a^1)^{-1} = (a^n)^{-1}(a^1)^{-1}$. By our base case, we know that $(a^1)^{-1} = a^{-1}$. By our hypothesis, $(a^n)^{-1} = a^{-n}$. So now we have $(a^n)^{-1}(a^n)^{-1}(a^1)^{-1} = a^{-n}a^{-1}$. By our exponent rules, $a^{-n}a^{-1} = a^{-n+(-1)} = a^{-(n+1)}$. As we now have $(a^{n+1})^{-1} = a^{-(n+1)}$, by PMI, for every $n \in \mathbb{N}$, $(a^n)^{-1} = a^{-n}$.

#36. Suppose G is a group and $a \in G$. Prove: If $ord(a) = 6$ then $ord(a^5) = 6$. Do any other elements a^2, a^3, or a^4 have order 6? Explain.

Let G be a group and $a \in G$.

Proof: Assume $ord(a) = 6$. As $ord(a) = 6$, $a^6 = e_G$ and for $k \in \mathbb{Z}$, if $0 < k < 6$ then $a^k \neq e_G$. We want to show that $ord(a^5) = 6$. By our exponent rules, we know that $(a^6)^5 = a^6a^6a^6a^6a^6$. As $ord(a) = 6$, $a^6a^6a^6a^6a^6 = e_Ge_Ge_Ge_Ge_G = e_G$. We can rearrange the exponents of $(a^6)^5$ as multiplication is commutative. So now we have $(a^5)^6 = e_G$. Not only do we need to show this, we need to show that 6 is the smallest positive integer n for which $(a^5)^6 = e_G$. So, we need to show that $(a^5)^1 \neq e_G$, $(a^5)^2 \neq e_G$, $(a^5)^3 \neq e_G$, $(a^5)^4 \neq e_G$, $(a^5)^5 \neq e_G$.
$(a^5)^1 = a^5$. As $ord(a) = 6$, $(a^5)^1 \neq e_G$.
$(a^5)^2 = a^6a^4 = e_Ga^4 = a4$. As $ord(a) = 6$, $(a^4) \neq e_G$.
$(a^5)^3 = a^6a^6a^3 = e_Ge_Ga^3 = a^3$. As $ord(a) = 6$, $(a^3) \neq e_G$
$(a^5)^4 = a^6a^6a^6a^2 = e_Ge_Ge_Ga^2 = a^2$. As $ord(a) = 6$, $(a^2) \neq e_G$
$(a^5)^5 = a^6a^6a^6a^6a^5 = e_Ge_Ge_Ge_Ga^5 = a^5$. As $ord(a) = 6$, $(a^2) \neq e_G$. Thus, for $0 < k < 4$, $(a^5)^k \neq e_G$. Thus, with this and $(a^5)^6 = e_G$, $ord(a^5) = 6$.

a^2: no, because $(a^2)^3 = a^6 = e_G$.
a^3: no, because $(a^3)^2 = a^6 = e_G$.
a^4: no, because $(a^4)^3 = a^6a^6 = e_Ge_G = e_G$.