Zaki Glenroy Lindo Assignment 3 - Fall 2017

Assignment 3: Due Monday September 25, 2017, no later than 8pm.

$p.36-38$ # 18, 28, 33, 35, 37 (You will be writing three proofs this time so start early and be careful!)

#18. Find the 10 elements of the group $\mathbb{Z}_5 \times \mathbb{Z}_2$ and write out the Cayley table. Recall that its operation uses $+_5$ in the first coordinate and $+_2$ in the second coordinate. Identify the inverse of each element.

$\mathbb{Z}_5 x \mathbb{Z}_2$	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)	(4,0)	(4,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)	(4,0)	(4,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)	(3,1)	(3,0)	(4,1)	(4,0)
(1,0)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)	(4,0)	(4,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(2,1)	(2,0)	(3,1)	(3,0)	(4,1)	(4,0)	(0,1)	(0,0)
(2,0)	(2,0)	(2,1)	(3,0)	(3,1)	(4,0)	(4,1)	(0,0)	(0,1)	(1,0)	(1,1)
(2,1)	(2,1)	(2,0)	(3,1)	(3,0)	(4,1)	(4,0)	(0,1)	(0,0)	(1,1)	(1,0)
(3,0)	(3,0)	(3,1)	(4,0)	(4,1)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(3,1)	(3,1)	(3,0)	(4,1)	(4,0)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)
(4,0)	(4,0)	(4,1)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)
(4,1)	(4,1)	(4,0)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)	(3,1)	(3,0)

Inverses:

$(0,0)^{-1} = (0,0)$
$(0,1)^{-1} = (0,1)$
$(1,0)^{-1} = (4,0)$
$(1,1)^{-1} = (4,1)$
$(2,0)^{-1} = (3,0)$
$(2,1)^{-1} = (3,1)$
$(3,0)^{-1} = (2,0)$
$(3,1)^{-1} = (2,1)$
$(4,0)^{-1} = (1,0)$
$(4,1)^{-1} = (1,1)$

Nicely done, but don't put the name of the group in the table where the notation for the operation goes. Just put $*$ or leave it blank.

#28. Suppose G is a group and $a, b \in G$. **Prove**: If $a^3 = b$ then $b = aba^{-1}$.

Proof: Assume $a^3 = b$. Then we have $aaa = b$. Now, $aaaa^{-1} = ba^{-1}$. By definition of inverse, we have $aae_G = ba^{-1}$. By definition of identity, $aa = ba^{-1}$. We can now say that $aaa = aba^{-1}$. As $aaa = b$, we now have $b = aba^{-1}$. Therefore, if $a^3 = b$ then $b = aba^{-1}$.

Well done. Don't do too much at once, multiply on the left by a and on the right by a^{-1} in separate steps. Also don't skip mentioning where you used associativity, and instead of "definition of" each time be specific to this use such as saying $aa^{-1} = e_G$ or $aae_G = aa$.

#33. Find the order of each element in the group $A = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ under matrix multiplication. Show your work!
(Notice how I created the matrices in TeX to help you, feel free to copy and paste code as needed!)

ord($\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$):

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} X \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, ord($\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$) = 2.

ord($\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$) = 1 as $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity matrix.

ord($\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$):

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} X \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, ord($\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$) = 2.

ord($\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$):

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} X \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus, ord($\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$) = 2.

Nice Job. To put parentheses around the matrix that are also large such as $\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right)$, use the code \left({ }\right) around the code for the matrix instead of just ( ). Also do not use the letter X for multiplication, use the code \cdot for just a dot.

#35. Complete the Proof of Theorem 1.26 (p. 28 of the text).

Suppose G is a group and $a \in G$ with $ord(a) = n$. **Proof**: ($\leftarrow$) Assume n evenly divides t. That is, $t = nq$ for some integer q. We want to show that for any integer t(1) , $a^t = e_G$. As $ord(a) = n$, $a^n = e_G$. Now, $(a^n)^q = a^{nq}$. As $a^n = e_G$, $a^{nq} = (e_G)^q$. Now, by definition of identity and our power rules(2) , $(e_G)^q = e_G$. Thus, $a^{nq} = e_G$. As $t = nq$, $a^{nq} = a^t$. Therefore, $a^t = e_G$. Thus, for any integer t, if n evenly divides t, $a^t = e_G$.

With this, we can now conclude that for any integer t, $a^t = e_G$ if and only if n evenly divides t.

Well done, but you need to be careful in a couple of spots. (1) You have already assumed specific information about t so you no longer want to prove anything "for all t". But you should have said "Let $t \in \mathbb{Z}$" at the beginning of your proof. (2) You don't need the definition of identity and power rules here, we have repeatedly said $e_G^q = e_G$.

#37. Suppose G is a group and $a \in G$. Assume $a^{50} = e_G$ but $a^{75} \neq e_G$ and $a^{10} \neq e_G$. Find the order of a and prove that your answer is correct.

$ord(a) = 50$

Proof: Assume $a^{50} = e_G$ but $a^{75} \neq e_G$ and $a^{10} \neq e_G$. We want to show that $ord(a) = 50$. As we have already assumed that $a^{50} = e_G$, we only need to show that 50 is the least positive integer n such that $a^n = e_G$. By Theorem 1.26, we have to show that for each factor of 50, k, $a^k \neq e_G$.

The factors of 50 are: 1, 2, 5, 10, and 25.

Case 1: k = 1.
If $a^1 = e_G$, then $aaaaaaaaaa = a^{10} = e_G$. As $a^{10} \neq e_G$, $a^1 \neq e_G$.

Case 2: k = 2.
If $a^2 = e_G$, then $a^2a^2a^2a^2a^2 = a^{10} = e_G$. As $a^{10} \neq e_G$, $a^2 \neq e_G$.

Case 3: k = 5.
If $a^5 = e_G$, then $a^5a^5 = a^{10} = e_G$. As $a^{10} \neq e_G$, $a^5 \neq e_G$.

Case 4: k = 10.
As $a^{10} \neq e_G$, $a^10 \neq e_G$.

Case 5: k = 25.
If $a^25 = e_G$, then $a^25a^25a^25 = a^{75} = e_G$. As $a^{75} \neq e_G$, $a^25 \neq e_G$.

Thus, as we have showed that for each factor of 50, k, $a^k \neq e_G$, we know that 50 is the least positive integer n such that $a^n = e_G$. Thus, $ord(a) = 50$.

Nice Job.

Total Score: 34.5 out of 35