Chapter 2 #8. Show that $G = \{5, 15, 25, 35\}$ is a group under $\times$ modulo 40. Relation between this group and U_8?

1. G is closed under $\cdot$:

$5\times5=25$, $5\times15=35$, $5\times25=5$, $5\times35=15$

$15\times15=25$, $15\times25=15$, $15\times35=5$

$25\times25=25$, $25\times35=35$, $35\times35=25$

(Since we know $\times$ modulo 40 is commutative these are enough to conclude closure)

2. Associativity is inherited from $(\mathbb{Z}_{40}, \times)$
3. From the calculations in 1, 25 is the identity
4. $5^{-1}=5$, $15^{-1}=15$, $25^{-1}=25$, $35^{-1}=35$

So, $(G, \times)$ is a group

In $U_8 = \{1,3,5,7\}$, $3^2=1$, $5^2=1$, and $7^2=1$

so $3^{-1}=3$, $5^{-1}=5$ and $7^{-1}=7$

This is similar to the group G above.
The identity 1 in U_8 corresponds to 25 in G.
They are essentially the same group.

#13 $G = \{1, 9, 16, 22, 53, 74, 79, 81\}$ modulo 91

What element needs to be added to G to get a group?

If you check possible products, you see that the only number missing is 29

For example $9\times74 = 29 \mod 91$.

#26 Prove that if $(ab)^2 = a^2b^2$ then $ab = ba$.

Proof $(ab)^2 = abab$

Assumption $abab = aabb$

Multiply by a^{-1} on the left & use associativity: $(a^{-1}a)bab = (a^{-1}a)abb$

$\Rightarrow ebab = eabb$

$\Rightarrow bab = abb$

Multiply by b^{-1} on the right and use associativity: $(bab)b^{-1} = (abb)b^{-1}$

$\Rightarrow ba(bb^{-1}) = ab(bb^{-1})$

$bae = abe$

$ba = ab$ ∎

#30.

#30 Give an example demonstrating $a\times b = c\times d$ but $ab \neq cd$.

$$a = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \quad b = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$c = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \quad d = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

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

Check that $a\times b = c\times d$ but $ab \neq cd$!

#33 prove: If $a^2 = e$ $\forall a \in G$ then $ab = ba$ $\forall a, b \in G$.

Proof. Since $a^2 = e$,

$*$ we have $a^{-1} = a$ $\forall a \in G$.

Let $a, b \in G$.

Then $ab \in G$ b/c G is closed under $\cdot$.

Then

$(ab)^{-1} = ab$ by $*$ above

$b^{-1}a^{-1} = ab$ (proved before that $(ab)^{-1} = b^{-1}a^{-1}$)

$ba = ab$ (b/c $b^{-1} = b$ and $a^{-1} = a$)

Therefore G is Abelian.

#34 $G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \ a, b, c \in \mathbb{R} \right\}$

1) closed: By definition of multiplication when you multiply two matrices in G you end up with a matrix in the same form, so it's in G.

2) associativity: Note that the multiplication is in fact the same as the regular matrix multiplication so associativity is inherited from $GL(2,\mathbb{R})$

3) identity $= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in G$

(check!) 4) $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$ (inverse is in G for any matrix in G)

Chapter 2 #37. $G=\left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid a\in\mathbb{R}, a\neq 0 \right\}$

1) $\begin{bmatrix} a & a \\ a & a \end{bmatrix} \cdot \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in G$

2) associativity is inherited from regular matrix multiplication

3) $\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$ is the identity (check!)

4) $\begin{bmatrix} a & a \\ a & a \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{bmatrix}$ is defined b/c $a\neq 0$ and is in G. 4

(check!)

The identity element for this set is not the usual identity for matrix multiplication, so even though the det is zero we get an inverse for a matrix. 1

Chapter 3 #1 a) $\mathbb{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

$|\mathbb{Z}_{12}| = 12$, $|0|=\infty$ $|3|=4$ $|6|=2$ $|9|=4$

$|1|=12$ $|4|=3$ $|7|=12$ $|10|=6$

$|2|=6$ $|5|=12$ $|8|=3$ $|11|=12$

b) $U_{10}=\{1,3,7,9\}$ $|1|=\infty$ $|7|=4$

$|U_{10}|=4$ $|3|=4$ $|9|=2$

c) $U_{12}=\{1,5,7,11\}$ $|1|=\infty$ $|7|=1$

$|U_{12}|=4$ $|5|=1$ $|11|=1$

d) $U_{20}=\{1,3,7,9,11,13,17,19\}$ $|1|=\infty$ $|11|=2$

$|U_{20}|=8$ $|3|=4$ $|13|=4$

$|7|=4$ $|17|=4$

$|9|=2$ $|19|=2$

e) $D_4=\{R_0, R_{90}, R_{180}, R_{270}, V, H, D, D'\}$

$|D_4|=8$ $|R_0|=\infty$ $|V|=2$

$|R_{90}|=4$ $|H|=2$

$|R_{180}|=2$ $|D|=2$

$|R_{270}|=4$ $|D'|=2$

11 pts

Chapter 3 #4

Let $(G,\cdot)$ be a group and $a\in G$. There are two possibilities for the order of a: ① $|a|=n<\infty$ and ② $|a|=\infty$.

Case ①. Consider $(a^{-1})^n = \underbrace{a^{-1}\cdots a^{-1}}_{n \text{ times}}$

$= (\underbrace{a\cdot a\cdots a}_{n\text{ times}})^{-1} = (a^n)^{-1} = e^{-1} = e$ since $|a|=n$.

We also need to show that n is the smallest such integer: Suppose $(a^{-1})^m = e$ for some $m<n$. Then $a^m = ((a^{-1})^{-1})^m = ((a^{-1})^m)^{-1} = e^{-1} = e$

So, we get $a^m=e$ but this is a contradiction because n is the order of a; we can't have $m<n$.

Case ② $|a|=\infty \Rightarrow a^m\neq e$ for any $m\in\mathbb{Z}$.

We need to prove $(a^{-1})^m\neq e$ for any $n\in\mathbb{Z}$ either.

Similar to above argument, suppose $(a^{-1})^m=e$ for some $m\in\mathbb{Z}$. Then $a^m=((a^{-1})^{-1})^m = ((a^{-1})^m)^{-1} = e^{-1} = e$

but this is a contradiction b/c a^m cannot equal e for any m. So $(a^{-1})^m\neq e$ for any m. Hence $|a^{-1}|=\infty$.

4