Homework #1 Ch 2 (061)

6/54) Let $a = \begin{pmatrix} 2 & 3 \\ -1 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix} \in GL(2,\mathbb{R})$ ①

$$a^{-1} = \begin{pmatrix} 2 & 3 \\ -1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{5} & -\frac{3}{5} \\ +\frac{1}{5} & \frac{2}{5} \end{pmatrix}$$

$$a^{-1}ba = \begin{pmatrix} 2 & 3 \\ -1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{5} & -\frac{3}{5} \\ \frac{1}{5} & \frac{2}{5} \end{pmatrix} \begin{pmatrix} -1 & 6 \\ 3 & 2 \end{pmatrix} \quad ②$$

$$= \begin{pmatrix} -2 & 0 \\ 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix} = b.$$

8/54) $*$ is multip mod 40. Let $A = \{5, 15, 25, 35\}$

*	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

① A is closed under $*$. Cayley table

Let $a, b, c \in A$ we want to show $*$ assoc. i.e. $a*(b*c) = (a*b)*c$.
Now ~~$a*(bc)$~~ $a*(b*c) = a*(bc)$ since the difference between $a*(b*c)$ and $a*(bc)$ is a multiple of 40. Similarly, $(a*b)*c = (ab)*c$.
and since $(ab)*c = a*(bc)$ because $(ab)c = a(bc)$ ①
we are done and $*$ is associative on A.

$\exists$ an identity element namely $\underline{\underline{25}}$ from Cayley table. ①

$\therefore$ $a^{-1} = a \ \forall a \in A$, from Cayley table. $(A, *)$ is a gp. ①

U(8)	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

*	25	5	15	35
25	25	5	15	35
5	5	25	35	15
15	15	35	25	5
35	35	15	5	25

U(8) and (A,*) ① have the same structure which means they are basically the same gp with differen notation

$\frac{12}{54}$) $U(n) = \{1, \dots, n-1\}$ $n > 2$ $1 \neq n-1$

$1^2 = 1$, ~~$(n-1)^2 \bmod n = n^2 - 2n + 1 = 1 \bmod n$.~~

1 1

$n-1 \in U(n)$ since if $\gcd(n, n-1) = k > 1$

$\Rightarrow n = ka$, $n-1 = kb$ $a > b$

$\Rightarrow 1 = n - (n-1) = ka - kb = k(a-b) \geq k > 1$ Contradiction.
$\quad (a-b) > 0$

1

$\frac{20}{55}$) The inverse of $a_1 a_2 a_3 \cdots a_n = (a_1 a_2 a_3 \cdots a_n)^{-1}$

$= a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$. 1

To see why, we will prove it by induction:

$(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$; $a_1 a_2 \cdot a_2^{-1} a_1^{-1} = e = a_2^{-1} a_1^{-1} a_1 a_2$ 1

Suppose it is true for $n = k$ i.e. $(a_1 a_2 \cdots a_k)^{-1} = a_k^{-1} a_{k-1}^{-1} \cdots a_1^{-1}$

Now for $n = k+1$, $(a_1 a_2 \cdots a_k a_{k+1})^{-1} = ((a_1 a_2 \cdots a_k) a_{k+1})^{-1}$

$= a_{k+1}^{-1} (a_1 \cdots a_k)^{-1}$ 1 roughly speaking.

$= a_{k+1}^{-1} a_k^{-1} \cdots a_1^{-1}$.

$\Rightarrow (a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

$\frac{26}{55}$) Suppose that G is a grp and $a, b \in G$ s.t. ~~s.t. we have~~

$(ab)^2 = a^2 b^2$ ~~$\Rightarrow a^{-1}, b^{-1} \in G$~~

$\Rightarrow \cancel{a} b a \cancel{b} = \cancel{a} a b \cancel{b}$ by cancellation law 2 1

$\Rightarrow ba = ab$.