(Q) Find the inverse of elts $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$ in $GL(2, Z_7)$

(Soln) $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \xrightarrow{\text{inverse}} \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

(as Back see $GL(2, Z_7)$ & operation here matrix multiplication so, inverse of 3 5 (as $3 \cdot 5 \equiv 1 \pmod 7$)

Here over Z_7 modulo

$\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$ determinant $4 \times 3 - 6 \times 5$ over Z_7

$= 12 - 30$

$= -18$ over Z_7

convert -18 to positive number

$-18 +$ (add multiple of 7 closet to 18 & greater than 18) $\Rightarrow -18 + 21$

$= 3$ over Z_7

Now inverse is

$\frac{1}{3}\begin{bmatrix} 3 & -5 \\ -6 & 4 \end{bmatrix}$ over modulo 7 i.e Z_7

~~(inverse of 3 is 5 in Z_7 $3 \times 7 \Rightarrow 7 - 3 = 5$)~~

$\Rightarrow 3^{-1}\begin{bmatrix} 3 & -5 \\ -6 & 4 \end{bmatrix}$ over Z_7

$\Rightarrow 5\begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix} \Rightarrow \begin{bmatrix} 5 \cdot 3 & 5 \cdot 2 \\ 1 \cdot 5 & 5 \cdot 4 \end{bmatrix} \Rightarrow \begin{bmatrix} 15 & 10 \\ 5 & 20 \end{bmatrix}$ over Z_7

$= \begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix}$

$-5 + 7 = 2$

$-6 + 7 = 1$

check $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} 4 \cdot 1 + 5 \cdot 5 & 4 \cdot 3 + 5 \cdot 6 \\ 6 \cdot 1 + 15 & 18 + 18 \end{bmatrix}$

$= \begin{bmatrix} 29 & 42 \\ 21 & 36 \end{bmatrix}$ over Z_7

$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in $GL(2, Z_7)$

Elementary Properties of Groups

Proposition ① If G be group, then identity element is unique.

(proof) Let e & e_1 be 2 identity elements of G

As e is identity element

$\therefore ae = ea = a \quad \forall a \in G$

In particular as $e_1 \in G$

$\therefore e_1 e = e e_1 = e_1 \quad -①$

As e_1 is identity elt (element)

$\therefore a e_1 = e_1 a = a \quad \forall a \in G$

In particular, as $e \in G$

$\Rightarrow e e_1 = e_1 e = e \quad -②$

From ① & ②

we get $e_1 = e$

(Prop. ②) If G be group, then each element has unique inverse.

(proof) Let $a \in G$, Let a' & a'' be 2 inverse of a.

As a' is inverse of a

$\therefore a a' = a' a = e \quad -①$

As a'' is inverse of a

$\therefore a a'' = a'' a = e \quad -②$

Consider, $a'' = a''e$ (by property of e)

$= a''(aa')$ (by ①)

$= (a''a)a'$ (by Associative law)

$= e a'$ (by ②)

$= a'$ (by property of e)

$\Rightarrow a'' = a'$

(Prop. ③) If G be group and $a, b, c \in G$

then (i) $ab = ac \Rightarrow b = c$ (left cancellation law)

(ii) $ac = bc \Rightarrow a = b$ (right cancellation law)

(proof) Consider $ab = ac$

Since $a \in G$, $a^{-1} \in G$ then

$a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)\cdot c$ (associative law)

$\Rightarrow e\cdot b = e\cdot c$

$\Rightarrow b = c$

(2) consider $ac = bc$

$\Rightarrow (ac)c^{-1} = (bc)c^{-1}$

$\Rightarrow a(cc^{-1}) = b(cc^{-1})$ (by Associative law)

$\Rightarrow a\cdot e = b\cdot e$

$\Rightarrow a = b$

(Proposition) (Associative law for 4 elements)

$(ab)(cd) = a(bc)d$ $\forall\ a, b, c, d \in G$, G is group

(proof) $(ab)(cd) = x(cd)$ where $x = ab$

$= (xc)d$ (by Associative law)

$= ((ab)c)d$

$= a(bc)d$ (by Associative law)

(Proposition) (Inverse law) $(ab)^{-1} = b^{-1}a^{-1}$ $\forall\ a, b \in G$ (Group)

(proof) Consider $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$ (by Ass. law of 4 elements)

$= a e a^{-1}$ (By inverse prop.)

$= a a^{-1}$ (By identity prop.)

$= e$ — (1) (By inverse prop.)

Similarly $(b^{-1}a^{-1})(ab) = e$ — (2)

$\therefore$ from (1) & (2), we get

$\Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

(Proposition) $(a^{-1})^{-1} = a$ where $a \in G$, G is group.

(proof) By group definition

$a^{-1}a = e$ & $(a^{-1}) \cdot (a^{-1})^{-1} = e$

$\therefore a^{-1}a = (a^{-1})(a^{-1})^{-1}$

$\Rightarrow a = (a^{-1})^{-1}$ (By left cancellation law)

Proposition: Prove that G is abelian iff $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$

(Soln) Let G be abelian

to show: $(ab)^{-1} = a^{-1}b^{-1}$

Consider, $(ab)^{-1} = b^{-1}a^{-1}$ (using $(ab)^{-1} = b^{-1}a^{-1}$)

$= a^{-1}b^{-1}$ ($\because$ G is abelian)

$\Rightarrow (ab)^{-1} = a^{-1}b^{-1}$

Conversely, Let $(ab)^{-1} = a^{-1}b^{-1}$

to show: G is abelian

Now, $(ab)^{-1} = a^{-1}b^{-1}$

$(ab)^{-1} = (ab)^{-1}$ (using $(ab)^{-1} = a^{-1}b^{-1}$)

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

$\Rightarrow ab = ba$

$\therefore$ G is abelian

(Q) Let G be group. If $a \in G$ and $g^2 = g$ then $g = e$

(Soln) Let $g^2 = g$ where $g \in G$

$\Rightarrow g \cdot g = g$

$\Rightarrow g \cdot g = g \cdot e$

$\Rightarrow g = e$ (by left cancellation law)