1(a) continued.....

Identity: let e be the identity element
if it exists, Then

$a * e = e * a = a \quad \forall a \in \mathbb{Q}$

$\iff \frac{a+e}{2} = \frac{e+a}{2} = a \quad \forall a \in G$

$\iff a + e = 2a \quad \forall a \in G$

$\iff e = a \quad \forall a \in G$

So no unique identity element

Inverses: No identity = no inverses

(C) $(\mathbb{Z}, -)$ Not a group

$a - 0 = a$

$0 - a = -a \neq a$

Not associativity.

No Identity

No Identity => no inverses.

(d.) $S := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ under multiplication.

<u>Inverses</u>: 0 has no inverse. <u>Identity</u> $= 1$

So Not a group.

2.(a) $O(2,\mathbb{R}) := \{ U \in GL(2,\mathbb{R}) \mid U^{-1} = U^{T} \}$.

$GL(2,\mathbb{R}) = \{ M \in M_{2\times 2}(\mathbb{R}) \mid \mathrm{Det}\,(M) \neq 0 \}$

1. $(O(2,\mathbb{R}), \cdot)$

<u>Closure</u>: $A, B \in O$ $\quad A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \quad B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$

$$AB = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}$$

$A, B \in O(2, \mathbb{R})$

Is $AB \in O(2, \mathbb{R})$

Is $(AB)^{-1} = (AB)^T$

We know $A^{-1} = A^T$

$B^{-1} = B^T$

$(AB)^{-1} = B^{-1}A^{-1} = B^TA^T$

$(AB)^T = B^TA^T$

(yes. It is closed)

Associativity: ✓ because

For $A, B, C \in O \in M_{(2\times2)}$

because matrix multiplication is associative.

Identity: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Is $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in O$?

$I^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $I^{T} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ So $I^{-1} = I^{T}$

✓ yes Identity is in O

Inverses: let $U \in O(2,\mathbb{R})$ Is $U^{-1} \in O(2,\mathbb{R})$

Is $(U^{-1})^{-1} = (U^{-1})^T$

$(U^{-1})^{-1} = U$

$(U^{-1})^T = (U^T)^T = U$ as $U^{-1} = U^T$ as $U \in O(2,\mathbb{R})$

So $(U^{-1})^{-1} = (U^{-1})^T$

Therefore $U^{-1} \in O(2,\mathbb{R})$

Thus O is a group under multiplication

(a_2) is O a group under addition ?

① closure : let $U, V \in O(2, \mathbb{R})$

Is $U+V \in O(2, \mathbb{R})$

i.e. Is $(U+V)^{-1} = (U+V)^T$

<u>RHS</u> : $(U+V)^T = U^T + V^T$

$= U^{-1} + V^{-1}$ because $U, V \in O(2, \mathbb{R})$

So the question becomes

Is $(U+V)^{-1} = U^{-1} + V^{-1}$? No

If $U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $V = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$

Then $U + V = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$

$$(U+V)^{-1} = \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$$

but $U^{-1} + V^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$

$$= \begin{pmatrix} \frac{3}{2} & 0 \\ 0 & \frac{3}{2} \end{pmatrix}$$

So $(U+V)^{-1} \neq U^{-1} + V^{-1}$

Therefore not closed. So not a group.

5. $\rho = (1234)(234)$ in S_6 find ρ^{1001}

$= (1243)$

$|\rho| = 4$

$\rho^{1001} = (\rho^4)^{250} \cdot \rho$

$= (Id)^{250} \cdot \rho$

$= Id \cdot \rho = \rho$

Q6. $|G| = n = p$ a prime

$\gcd(n, s) = 1$

If g is cyclic then it has generator a with order s.

Let $a \in G$, $a \neq e$

Consider $\langle a \rangle$, Then by Lagrange's Theorem

$|\langle a \rangle|$ divides $|G| = p$ because $\langle a \rangle \leq G$

divides

So $|\langle a \rangle| \mid p$

Therefor $|\langle a \rangle| = 1$ or p

but $|\langle a \rangle| \neq 1$ as $a \neq e$

$\Rightarrow |\langle a \rangle| = p$

So $\langle a \rangle \leq G$

but $|\langle a \rangle| = p = |G|$

Therefore $\langle a \rangle = G \Rightarrow G$ is cyclic

⑧ let $G = \{Id, e, a, b, c\}$

① Assume G has an element of order 4

let's say $a^4 = e$

but closure $\Rightarrow a^2, a^3 \in G$ and $a^2, a^3 \neq e$

$\Rightarrow \{a^2, a^3\} = \{b, c\}$

because $a^2 = a$, $a^3 \neq a$

$\Rightarrow G = \{e, a, a^2, a^3\}$ $\quad a^4 = 1$

So G is cyclic and therefore abelian.

2nd Method : No element of order 4

So by Lagrange's theorem corollary the order of an element must divide the order of the group.

so $G = \{e, a, b, c\}$ with $a^2 = b^2 = c^2 = e$

Cayley Table

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

What is ab?

So in a cayley table of a group all elements appear once and only once in each row and coloumn.

So $ab \neq a$, $ab \neq b$, $ab = e$

$\Rightarrow ab = c$

The rest of the table follows by process of elimination

By inspection the group is abelian eg.

$ab = c$ $bc = a$. So abelian.

$a \cdot a = aa$

cyclic group generated by a $\langle a \rangle$

$= \{e, a, a^2, \cdots\cdots, a^{n-1}\}$ with $a^n = e$

Abelian ?

$a^s \cdot a^t = a^{s+t}$

$a^t \cdot a^s = a^{t+s}$

Q. 3(b) If $(ab)^2 = a^2 b^2$ Show G is abelian $\forall a,b \in G$

Abelian if $ab = ba \quad \forall\, a,b \in G$

We know $(ab)^2 = a^2 b^2$

$$
\left.
\begin{aligned}
&\Leftrightarrow && abab = aabb \\
&\Leftrightarrow && ababb^{-1} = aabbb^{-1} \\
&\Leftrightarrow && aba = aab \\
&\Leftrightarrow && a^{-1}aba = a^{-1}aab \\
&\Leftrightarrow && ba = ab
\end{aligned}
\right\} \forall\, a,b \in G
$$

Therefore Abelian

3. a WTS $(ab)^{-1} = b^{-1}a^{-1}$

$a, b \in G \Rightarrow ab \in G$

$\alpha \cdot \alpha^{-1} = \alpha^{-1}\alpha = Id$

WTS

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