Lec. 1

Group Theory is central to not only many areas of Mathematics but also has applications in Physics, Chemistry, Biology etc.

A group is, very loosely speaking a set in which you can "multiply" and "divide". But instead of dwelling right into the definition, let's see some familiar examples:—

Examples I

Ex. 1 The set of integers $\mathbb{Z}$ with the operation addition '+'.

1) If we take any two integers, say a and b (e.g. take 2 and 3), we know that $a+b \in \mathbb{Z}$ ($2+3=5 \in \mathbb{Z}$). [Closure]

2) We also have $0 \in \mathbb{Z}$ and the property 0 has is that $a+0 = 0+a = a$ ($2+0=2$, $3+0=3$). [identity]

3) For a, we have an element in $\mathbb{Z}$ itself, $-a$ such that $a+(-a) = (-a)+a = 0$ ($2+(-2)=0$, $3+(-3)=0$) [inverse]

4) If we have three elements from $\mathbb{Z}$ say a, b, c (e.g. 2, 3, 5) then $a+(b+c) = (a+b)+c$ ($(2+3)+5 = 5+5 = 10$ and $2+(3+5) = 2+8 = 10$) [associativity]

5) Finally we have $a+b = b+a$ ($2+3=5=3+2$) [commutative]

Let's see some more examples and see if all of them have similar properties.

Ex.2 Let's take the set of rational numbers $\mathbb{Q}$ under addition, '+' [you can see that I am emphasizing the operation]

1) If $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q} \Rightarrow \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in \mathbb{Q}$ [closure]

2) We have $0 \in \mathbb{Q}$ such that for any $\frac{a}{b} \in \mathbb{Q}$, $\frac{a}{b} + 0 = 0 + \frac{a}{b} = \frac{a}{b}$.
[identity]

3) For any $\frac{a}{b} \in \mathbb{Q}$, $\exists$ $-\frac{a}{b} \in \mathbb{Q}$ such that $\frac{a}{b} + \left(-\frac{a}{b}\right) = \left(-\frac{a}{b}\right) + \left(\frac{a}{b}\right)$
$= 0$. [inverse]

4) For $\frac{a}{b}, \frac{c}{d}$ and $\frac{e}{f} \in \mathbb{Q}$, we see $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f}$

$$= \frac{adf + bcf + bde}{bdf}$$

[associative]

same

and $\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf+ed}{df} = \frac{adf + cfb + bde}{bdf}$

5) Finally, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{c}{d} + \frac{a}{b}$. [commutative]

Ex.3 Consider $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ with the operation multiplication '$\cdot$'.

1) If $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}^*$ then $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \neq 0 \in \mathbb{Q}^*$.

[closure]

2) We have $1 \in \mathbb{Q}^*$ and for any $\frac{a}{b} \in \mathbb{Q}^*$, $1 \cdot \frac{a}{b} = \frac{a}{b} \cdot 1 = \frac{a}{b}$

[identity]

3) For any $\frac{a}{b}$, we have $\frac{b}{a} \in \mathbb{Q}^*$ such that

$$\frac{a}{b} \cdot \frac{b}{a} = 1 = \frac{b}{a} \cdot \frac{a}{b} \qquad [\text{inverse}]$$

4) For $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}^*$, $\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$

[associativity]

5) Finally, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{c}{d} \cdot \frac{a}{b}$ [commutative]

Ex. 4 Check that the set of complex numbers $\mathbb{C}$ with the operation addition '+' satisfies all of above properties.

Question:- What should be the identity element?

Ex. 5 Check that the set of non-zero complex numbers $\mathbb{C}^*$ under the operation multiplication '$\cdot$' satisfies all of above properties.

Question:- What is the inverse of $a + ib \in \mathbb{C}^*$?

Ex. 6 Let's do a different type of example.

Let us define $GL(n, \mathbb{R})$ to be the set of $n \times n$ matrices which are invertible.

<u>Aside</u> :- GL stands for General Linear, n denotes the order of the matrices and $\mathbb{R}$ is telling us that the entries of the matrices are real numbers.

i.e, $$GL(n,\mathbb{R}) = \left\{ A \in M_n(\mathbb{R}) \;\middle|\; \det(A) \neq 0 \right\}$$

and consider the operation '$\cdot$' on $GL(n,\mathbb{R})$ which is matrix multiplication. For simplicity, let's take $n=2$ and try to see if $GL(2,\mathbb{R})$ has all the properties which are satisfied by other examples.

1) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in GL(2,\mathbb{R})$

Then $$A \cdot B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

now if we want to see if $A \cdot B \in GL(2,\mathbb{R})$, then we must have that $$\det \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} \neq 0$$

One can check that this is indeed the case and we have to use the fact that $\det(A) \neq 0$, $\det(B) \neq 0$. Hence closure.

2) We have the element $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R})$ as its det $= 1$.

for any $A \in \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{R})$, we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Hence $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity.

3) We have learned that the inverse of a 2×2 matrix

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is given by $\dfrac{1}{\det A} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

Let's check that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \frac{1}{\det A} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{\det A} \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix}$$

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

Hence for any $A \in GL(2,\mathbb{R})$ we have the existence of inverse.

4) We have learned in previous courses that matrix multiplication is associative and so for any $A, B, C \in GL(2,\mathbb{R})$, we have $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ and hence associative.

However, consider the following two matrices

5) $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $\det A = 4 - 6 = -2 \neq 0$

$B = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$, $\det B = -1 - 1 = -2 \neq 0$

One can check that $A \cdot B = \begin{bmatrix} -1 & -3 \\ -1 & -7 \end{bmatrix}$ and

$BA = \begin{bmatrix} -2 & -2 \\ -4 & -6 \end{bmatrix}$ and hence $A \cdot B \neq B \cdot A$

So this is non-commutative.

In particular, this example suggests that there might be sets whose operation is not commutative and hence must be treated separately.

<u>Exercise</u> :- Try to understand above examples and come up with your own definition of group. Don't look in any book or on internet. This is how new definitions come into existence by understanding many important examples and observing common unifying themes!!

A group G is a set with a binary operation '·'
[for example, addition, multiplication, matrix multiplication etc.] which satisfies Properties 1) to 4) in above examples.

If it satisfies property 5) too, it is called a commutative or an abelian group. Otherwise called a non-commutative or anabelian group.

—— x —— x ——