Groups 1

1 Introduction to Groups

Definition 1 *A **Group** G is a set with an operation $*$ which satisfies the following:*

1. *there is an identity element $e \in G$, such that for every $a \in G$*

$$e * a = a * e = e$$

2. *every element has an inverse, i.e. if $a \in G$ there exists an element $a^{-1} \in G$*

$$a * a^{-1} = a^{-1} * a = e$$

3. *the group is closed under the operation, i.e. if $a \in G$ and $b \in G$ then $a * b \in G$.*

4. *the associativity rule is satisfied: i.e. for all $a, b, c \in G$*

$$a * (b * c) = (a * b) * c$$

What does this mean?

- A group consists of two things:
  1. a set of elements
  2. an 'operation' which acts upon two elements in the set to return another element. This operation must satisfy the properties given above.
- the set can contain a finite or infinite number of elements
- the set **must** contain an identity. There can only be one identity. The identity depends on the operation.
  Example: For the real numbers, 0 is the identity for addition, but 1 is the identity for multiplication.
- Every element in the set must have an inverse in the set too (depending on the operation)
  Example: For the real numbers, taking the number 5, under addition its inverse is -5, but under multiplication it is $\frac{1}{5}$.

- The operator $*$ may **not** give you an element which is not in the set, so if $a, b \in G$ and

$$a * b = c \qquad\qquad c \notin G$$

then it is **not** a group.

- Associativity just checks that the order which you apply the operation does not matter.

- Note that we **do not** care about the following:

$$a * b = b * a$$

In many groups (especially those of matrices) this is not true, but that's okay. If this is true, then we say the operation is **commutative**. As long as

$$a * b \in G \qquad\qquad \text{and} \qquad\qquad b * a \in G$$

then the group is closed under the operation.

A group whose operation is commutative is called **Abelian**.

1.1 Examples

Examples are core to understanding the concept of groups. I shall take some set and operation pairings $(S, *)$ and see if they are groups by checking the required properties.

1.1.1 $G_1 = (\mathbb{Z}, +)$

Here the set is all the integers $\mathbb{Z}$, under the operation of addition "+". Taking each property in turn:

- **Identity:** What number can you add to 5 to get 5? More mathematically $x + 5 = 5$, solve for x. Ans: $x = 0$. So we can see that for addition the identity is zero, since for every $a \in \mathbb{Z}$

$$a + 0 = 0 + a = a$$

- **Inverse:** What number can you add to 5 to get the identity 0? That is we want to solve $x + 5 = 0$ for x. Ans: $x = -5$. So under addition, -5 is the inverse of 5. Extending this, you may say that for every $a \in \mathbb{Z}$ there is an inverse $-a \in \mathbb{Z}$ so that

$$a + (-a) = (-a) + a = 0$$

- **Closure:** If you add an integer to an integer, do you always get an integer? Yes! It is enough to state this fact, and conclude that when $a, b \in G_1$ then $a + b \in G_1$.

- **Associativity:** The operation of addition is associative since

$$a + (b + c) = a + b + c = (a + b) + c$$

i.e. the order you add integers is irrelevant.

Since all four properties are true, then G_1 a group.

1.2 $G_2 = (\mathbb{R}, \cdot)$

Here we take the set of all real numbers with the operation of multiplication " $\cdot$ ".

- **Identity:** What number can you multiply by 5 to get 5? Ans: 1. So for addition, the identity is one, since for every $a \in \mathbb{R}$
$$a \cdot 1 = 1 \cdot a = a$$

- **Inverse:** What number can you multiply by 5 to get the identity 1? Ans: $\frac{1}{5}$. So under multiplication, $\frac{1}{5}$ is the inverse of 5. Extending this, can we say that for every $a \in \mathbb{R}$ there is an inverse $\frac{1}{5} \in \mathbb{R}$ so that
$$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1 \qquad ?$$

  No! The element 0 does not have an inverse! The fraction $\frac{1}{0}$ is not defined.

Since this property is false, G_2 is **not** a group.
How can we make this a group? Since the only problem element is 0, try the following:

1.3 $G_3 = (\mathbb{R} \setminus \{0\}, \cdot)$

Here we take the set of all real numbers, but excluding the number 0, with the operation of multiplication " $\cdot$ ".

- **Identity:** As above, the identity is 1.

- **Inverse:** Is it true that for every $a \in \mathbb{R}$ there is an inverse $\frac{1}{a} \in \mathbb{R} \setminus 0$ so that
$$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1 \qquad ?$$

  Yes!

- **Closure:** If you multiply two (non-zero) real numbers, do you always get a (non-zero) real number? Yes! It is enough to state this fact, and conclude that when $a, b \in G_3$ then $a \cdot b \in G_3$.

- **Associativity:** The operation of addition is associative since
$$a \cdot (b \cdot c) = a \cdot b \cdot c = (a \cdot b) \cdot c$$

  since the order you multiply real numbers is irrelevant.

Since all four properties are true, G_3 is a group.

1.4 $G_4 = (M_2(\mathbb{R}), +)$

Here the set is all the 2×2 matrices whose entries are real numbers, under the operation of addition "+". So every element $a \in M_2(\mathbb{R})$ is of the form:

$$a = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

where $a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2} \in \mathbb{R}$. Addition of two matrices is defined as:

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} + \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} \\ a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} \end{pmatrix} \tag{$\star$}$$

Taking each property in turn:

- **Identity:** $a \in M_2(\mathbb{R})$. Take

  $$e = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$$

  Then it is easy to see that

  $$a + e = e + a = a$$

- **Inverse:** For every $a \in M_2(\mathbb{R})$ there is an inverse "$-a$" $\in M_2(\mathbb{R})$ of the form

  $$-a = \begin{pmatrix} -a_{1,1} & -a_{1,2} \\ -a_{2,1} & -a_{2,2} \end{pmatrix}$$

  $$a + (-a) = (-a) + a = 0$$

- **Closure:** If you add two real numbers, you always get an real number (since $(\mathbb{R}, +)$ is a group). Adding two matrices is in effect, adding their components. The components are real, so their sum is real It is enough to state this, and conclude that when $a, b \in G_4$ then $a + b \in G_4$.

- **Associativity:** The operation of addition is associative since addition of real numbers is associative (as $(\mathbb{R}, +)$ is a group).

  $$a + (b + c) = a + b + c = (a + b) + c$$

  i.e. the order you add integers is irrelevant.

Since all four properties are true, then G_4 is a group.

1.5 $G_5 = (M_2(\mathbb{R}) \setminus \{0\}, \cdot)$

Here the set is all the 2×2 matrices whose entries are real numbers, excluding the all zero matrix, i.e.

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

under the operation of multiplication "$\cdot$". Multiplication of two matrices is defined as:

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \cdot \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} = \begin{pmatrix} a_{1,1}b_{1,1} + a_{1,2}b_{2,1} & a_{1,1}b_{2,1} + a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} + a_{2,2}b_{2,1} & a_{2,1}b_{2,1} + a_{2,2}b_{2,2} \end{pmatrix} \tag{$\star$}$$

Taking each property in turn:

- **Identity:** $a \in G_5$. Take

  $$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G_5$$

  Then it is easy to see that

  $$a + e = e + a = a$$

- **Inverse:** For every $a \in G_5$ is there an inverse $a^{-1} \in G_5$ of the form

  $$a^{-1} = \frac{1}{a_{1,1}a_{2,2} - a_{1,2}a_{2,1}} \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}$$

  such that

  $$a \cdot a^{-1} = a^{-1} \cdot a = 0 \qquad ?$$

  Warning! But what if $a_{1,1}a_{2,2} - a_{1,2}a_{2,1} = \det(a) = 0$? Then we have a divide-by-zero! Which means not every element in G_5 has an inverse, so G_5 is not a group!

1.6 $G_6 = (\{a \in M_2(\mathbb{R})$ where $\det(a) \neq 0\}, \cdot)$

Here the set is all the 2×2 matrices whose entries are real numbers with non-zero determinant, under the operation of multiplication "$\cdot$". Note that the zero matrix has zero determinant, so is excluded anyway.
Taking each property in turn:

- **Identity:** As above, the identity is

  $$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G_6$$

- **Inverse:** For every $a \in G_6$ there is an inverse $a^{-1} \in G_6$ of the form

  $$a^{-1} = \frac{1}{\det(a)} \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}$$

  so that

  $$a \cdot a^{-1} = a^{-1} \cdot a = 0$$

  Here it is impossible that $\det(a) = 0$, so we are safe.

- **Closure:** If you multiply two real numbers, you always get an real number (since $(\mathbb{R} \setminus \{0\}, \cdot)$ is a group). Adding two matrices is in effect, adding their components. The components are real, so their sum is real It is enough to state this, and conclude that when $a, b \in G_6$ then $a \cdot b \in G_6$.
- **Associativity:** The operation of addition is associative since addition of real numbers is associative (as $(\mathbb{R}, +)$ is a group).

  $$a + (b + c) = a + b + c = (a + b) + c$$

  i.e. the order you add integers is irrelevant.

Since all four properties are true, then G_6 a group.
More examples of groups use things other than numbers or matrices. However the rules to be checked are the exact same.

1.7 Permutations

1.8 Rotations

2 More Non-Groups

The following are **not** groups. Can you see why?

- $(\mathbb{Z}, \cdot)$ – the integers under multiplication
- $(\mathbb{Z}, -)$ – the integers under subtraction
- $(\mathbb{Z}, \div)$ – the integers under division
- $(\mathbb{R}, -)$ – the integers under subtraction
- $(\mathbb{R}, \div)$ – the integers under division

3 Answers to "More Non-Groups"

- $(\mathbb{Z}, \cdot)$ – no element has an inverse except the identity 1.
- $(\mathbb{Z}, -)$ – associativity rule broken
- $(\mathbb{Z}, \div)$ – not closed, associativity rule broken
- $(\mathbb{R}, -)$ – associativity rule broken
- $(\mathbb{R}, \div)$ – not closed ($\frac{1}{0} \notin \mathbb{R}$), associativity rule broken