1. A first glimpse at groups

1.1. **Motivation (can safely be skipped, start from 1.2 instead).** Typically we perceive symmetry as something beautiful, and we have an intuitive idea about one object being "more symmetric" than another (e.g. an irregular 4-gon is less symmetric than a rectangle which in turn is less symmetric than a square).

How can we capture this intuitive idea?

Suppose a solid object in the plane covers a certain subset, e.g. the interior (and the boundary) of a pentagon. Then we will allow "moves" of the object in the plane which keep the object itself undeformed. Sometimes we can find a move after which the object covers the *same* subset of the plane as before the move; let us call such a move "good". The symmetry of the object in question is now "measured" by the set of all such possible good moves.

Example: A regular pentagon, each side of the same length ℓ, say, allows the following "good" moves: clockwise rotations around its center of angle $\phi := 72°(= \left(\frac{360}{5}\right))$, 2ϕ, 3ϕ, 4ϕ, in fact any $n\phi$, $n \in \mathbb{Z}$ (where for $n < 0$ we rotate anticlockwise by $|n|\phi$).

But not all of these moves are visibly different: as we only compare starting and end positions of such a move, we cannot distinguish between a rotation by 360° or 720°, say; in fact they both have the same effect as if we didn't rotate at all; we "identify" all rotations by $n \cdot 360°$, $n \in \mathbb{Z}$, into a single class of rotations, similarly all rotations by $72° + n \cdot 360°$, $n \in \mathbb{Z}$, into a single class, etc.

This latter procedure results in 5 different classes, and this set of 5 elements (or rather its cardinality 5) is a kind of measure for the symmetry of regular pentagon. Even better: it is possible to *combine* any two good moves into yet another good move since rotating first by $n\phi$ followed by rotating by $m\phi$ has the same effect as to rotate in one stroke by $(n + m)\phi$. Also, we can "take back" a move ⟦press the rewind button⟧. And finally it is also a good move to do nothing (i.e. to leave the object in place)–this is typically an important (albeit somewhat exceptional) case that one tends to forget when one lists all moves.

The above properties actually are all what is needed to form a group (of symmetries). We want to make this more precise, where we try to extract the "bare essentials" of what we have used. ⟦This will make it very economical to focus the study on those "essentials", since all that we will find out about them will apply to any situation where those essentials occur—and there will be plenty.⟧

First we need to replace the set of "good moves" as well as the notion of "combining moves" by something more precise (and less concrete). In order to do this adequately, we replace the set of good moves by an arbitrary set, and we then need the notion of a *binary operation* on a set—this encodes simply that we can combine any two elements of the set and end up with another element in the set. We demand of our "moves"—or rather their more abstract replacement, the set G—that there is one element which plays the role of the "do-nothing" move; this element is denoted by e_G or simply e and is called the **identity element**.

Then we demand that each move can be taken back/reverted: for the set G this boils down to asking that to each element $g \in G$ we can find an element $h \in G$ which has the inverse effect in the following sense:

$$\forall g \in G \exists h \in G \text{ such that } g \circ h = e_G \quad \text{ and also } h \circ g = e_G\,.$$

This h is then called the **inverse** of g in G.

Finally, if we have a sequence of moves then we can successively combine two successive ones of them until we wind up with a single move, and the result should not depend on the order in which we combine. This requirement is captured in the **associativity condition** below.

1.2. **Sets.** By a **set** we mean a collection of *distinct* objects and this collection is considered as a whole. The essentially only property needed from a set is that it must clearly state whether an object is an **element (or member)** of that set or not. If an object a is considered to be an element of a set S, then we write $a \in S$, otherwise we write $a \notin S$. Typically one chooses the objects in a set of a similar kind (but that is not necessary).

A set is often described by a list of its elements, or else by a property which clearly distinguishes the elements in a set from the objects which are *not* in it. One uses braces $\{\dots\}$ to indicate a set, e.g. $\{3, 1, 4\}$ is the set consisting of the three numbers 3, 1 and 4; note that the elements need not be in their "natural" order (if there is one at all). It often happens that only a few elements of the set are written down, followed by $\dots$ which indicates that the remaining elements can be guessed by some obvious rule; for example, $\{2, 4, 6, \dots\}$ would suggest (to most people, presumably) that the positive even integers are meant.

Standard examples of sets are

$\mathbb{Z}$, the set of all integers (also denoted by $\{\dots, -2, -1, 0, 1, 2, 3, \dots\}$);
$\mathbb{Q}$, the set of all rational numbers;
$\mathbb{R}$, the set of all real numbers;
$\mathbb{C}$, the set of all complex numbers.
$M(m, n, \mathbb{R})$, the set of all $m \times n$-matrices with real entries $(m, n \geqslant 1)$.

For example, one has $\frac{4}{7} \in \mathbb{Q}$ but $\frac{4}{7} \notin \mathbb{Z}$, and $\sqrt{5} \in \mathbb{R}$ but $\sqrt{5} \notin \mathbb{Q}$.

1.3. **The Cartesian product.** The **Cartesian product** of two sets A and B is defined as the set of pairs (a, b) with $a \in A$ and $b \in B$:

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

For example, for the sets $A = \{1, -3, \pi\}$ and $B = \{-11, \sqrt{5}\}$ we find

$$A \times B = \{(1, -11), (1, \sqrt{5}), (-3, -11), (-3, \sqrt{5}), (\pi, -11), (\pi, \sqrt{5})\},.$$

Note that the order of the elements in such a pair (a, b) is important: while $(1, -11)$ is in the set, the "swapped" version $(-11, 1)$ is not.

1.4. **Binary operations.** A **binary operation** "$\circ$" on a set A is a map which assigns to any $a \in A$ and $\alpha' \in A$ another element in A, denoted $a \circ a'$. More precisely, to any *pair* (a, a') in $A \times A$ (i.e. the Cartesian product of the set A with itself) the "$\circ$" assigns another element $a \circ a'$ in A.

For example, take $A = \mathbb{R}$ (the set of real numbers) and consider the binary operation "$+$" on it: to each pair (a, a') in $\mathbb{R} \times \mathbb{R}$ (you can think of (a, a') as a vector in $\mathbb{R}^2$ which is in fact a shorthand for $\mathbb{R} \times \mathbb{R}$). The binary operation "$+$" simply adds the two real numbers a and a' to the real number $a + a'$. As another example, take $A = \mathbb{R}$ (the set of real numbers), but this time consider the binary operation "$\cdot$" on it which to each pair (a, a') in $\mathbb{R} \times \mathbb{R}$ assigns the product $a\,a'$ which is again a real number.

1.5. **Groups.** With these preparations, we can state what a group is:

Definition: A **group** is a set G with a binary operation "$\circ$" satisfying the following four properties

Closure (C): to each $g_1 \in G$ and $g_2 \in G$ we have $g_1 \circ g_2 \in G$;

Identity (N): there is an **identity element** or **neutral element**, denoted e, in G, which is characterised by the following property; for every $g \in G$, we have

$$e \circ g = g \qquad \text{and} \qquad g \circ e = g\,.$$

Inverses (I): each element g in G has an inverse element (short "inverse") $h \in G$ which is characterised by the property

$$g \circ h = e \qquad \text{and} \qquad h \circ g = e\,.$$

The inverse of g is also denoted by g^{-1}.

Assoc. (A): for every $g_1, g_2, g_3 \in G$ the following equality must hold:

$$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)\,.$$

Examples: We will take for granted that both addition and multiplication on the integers, the rational numbers, real numbers and also on the complex numbers satisfy the associativity condition (A).

1) Put $G = \mathbb{Z}$ where "$\circ$" denotes the addition "$+$" in $\mathbb{Z}$. This forms a group. We check

Closure: two integers g_1 and g_2 always add to another integer (hence closure holds)

Identity: The identity is given by the integer 0: for any $g \in \mathbb{Z}$ we check $g+0 = g$ and $0 + g = g$.

Inverses: The inverse of the integer g is given by $-g$ (again an integer), since we check $g + (-g) = 0$ and $(-g) + g = 0$.

As to the associativity, we "know" from experience/school that this holds. (If you want to actually prove it, you will need to invoke the principle of induction.)

Similarly, we can replace $\mathbb{Z}$ in the above example by the rationals $\mathbb{Q}$, the reals $\mathbb{R}$ or the complex numbers $\mathbb{C}$, and still obtain a group.

2) Put $G = \mathbb{Q} \setminus \{0\}$ where "$\circ$" denotes the multiplication "$\cdot$" in $\mathbb{Q}$. This forms a group. We check

Closure: two non-zero rationals g_1 and g_2 always multiply to another non-zero rational (hence closure holds)

Identity: The identity is given by the rational number 1: for any $g \in \mathbb{Q} \setminus \{0\}$ we check $g \cdot 1 = g$ and $1 \cdot g = g$.

Inverses: The inverse of the non-zero rational g is given by $\frac{1}{g}$ (again a rational number), since we check $g \cdot (\frac{1}{g}) = 1$ and $(\frac{1}{g}) \cdot g = 1$.

As to the associativity, we again "know" from experience/school that this holds.

Similarly, we can replace $\mathbb{Q} \setminus \{0\}$ in the above eample by the non-zero reals $\mathbb{R} \setminus \{0\}$ or the non-zero complex numbers $\mathbb{C} \setminus \{0\}$, and still obtain a group.

3) Put $G = \mathbb{Z} \setminus \{0\}$ where "$\circ$" denotes the multiplication "$\cdot$" in $\mathbb{Z}$. This **does not** form a group. The identity element exists, as 1 lies in G, but not every element has an inverse: for example, 2 does not, since there is no $n \in \mathbb{Z}\setminus\{0\}$ such that $2 \cdot n = 1$.

4) Put $G = M(m, n, \mathbb{R})$, the matrices with m rows and n columns, with entries in $\mathbb{R}$, where "$\circ$" denotes matrix addition. Again, this forms a group: adding two such matrices gives again a matrix of the same kind, the identity element is the zero matrix O (which has all entries equal to zero), and

the inverse to a matrix A is the matrix $-A$ (which has each entry negative to the corresponding one in A).

Recall that matrix addition this works componentwise, e.g. for $m = 2$ and $n = 3$ an example would be

$$\begin{pmatrix} 1 & -3.2 & \pi \\ 0 & -14 & \sqrt{7} \end{pmatrix} + \begin{pmatrix} -2.11 & 0 & \frac{1}{\pi} \\ 3 & 1 & 5 \end{pmatrix} = \begin{pmatrix} -1.11 & -3.2 & \pi + \frac{1}{\pi} \\ 3 & -13 & \sqrt{7} + 5 \end{pmatrix}$$

Hence we "inherit" the associativity (componentwise) from the associativity in $\mathbb{R}$.

5) Put $G = \mathrm{GL}_2(\mathbb{R})$, which is defined as the 2×2-matrices with real entries and non-zero determinant, i.e.

$$\mathrm{GL}_2(\mathbb{R}) := \left\{ A \in M(2, 2, \mathbb{R}) \mid \det(A) \neq 0 \right\},$$

where "$\circ$" denotes matrix *multiplication*. This also forms a group, with identity being the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the inverse of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ being the "inverse matrix"

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

The associativity is not completely obvious, and to check it is a good exercise.

We find a new feature here: while for all the previous examples it did not matter in which order we take the corresponding binary operation, here we find that it does: multiply the matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ with $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. We get

$$A\,B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \qquad \text{but} \qquad B\,A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

and therefore $A\,B \neq B\,A$.

In the above example, the 2 (the size of the square matrices) can everywhere be replaced by an arbitrary positive integer n, and the corresponding group $GL_n(\mathbb{R})$ is still a group under matrix multiplication.

6) The **trivial group** is given by a set with one element $\{e\}$ and the only possible binary operation on that set (which assigns to the only pair (e, e) in $\{e\} \times \{e\}$ the only possible element e in $\{e\}$). An identity element is e itself, and e is also inverse to itself. For the associativity, there is nothing to check.

7) A vector space is in particular also a group, with vector addition. In fact, one can view that as a special case of 4), when $n = 1$ and matrices of size $m \times 1$ can be viewed as vectors of length m.

Definition:

(i) A group is called **finite** or **infinite**, according to whether its underlying set G is has finitely many or infinitely many elements, respectively.

(ii) A group G with binary operation $\circ$ is called **commutative** if for any $g, h \in G$ the following holds:

$$g \circ h = h \circ g\,.$$

Note that all the groups arising from the examples above are commutative, except for 5).

1.6. **Multiplication/Cayley/Group table.** To each finite group we assign its **multiplication table** (or **Cayley table**, **group table** or else *operation table* [non-medical]), which lists all elements of the group above the top row and left of the leftmost column, preferably in the same order; the most convenient convention is to list the identity element as the first one: so in a group with 4 elements, denoted by a, b, c and e (the latter being the identity element) we would write as follows:

$\circ$	e	a	b	c
e				
a				
b				
c				

now in each entry of that table we take the element which results when we apply the binary operation on the top left corner to the pair consisting of the number on the very left of that entry and the number on the very top of that entry; for example, the entry in the second row and third column would be $a \circ b$:

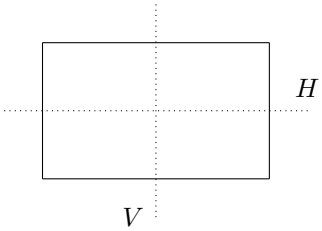
$\circ$	e	a	b	c
e				
a			$a \circ b$	
b				
c				

The whole group table looks as follows

$\circ$	e	a	b	c
e	$e \circ e$	$e \circ a$	$e \circ b$	$e \circ c$
a	$a \circ e$	$a \circ a$	$a \circ b$	$a \circ c$
b	$b \circ e$	$b \circ a$	$b \circ b$	$b \circ c$
c	$c \circ e$	$c \circ a$	$c \circ b$	$c \circ c$

where we finally need to replace each entry by the corresponding element that the binary operation gives.

For example, we can take the four symmetries of a non-square rectangle



It has the following four symmetries:

I : the idle move (this is the identity element in the group of symmetries);
H : the reflection about the horizontal axis of symmetry;
V : the reflection about the vertical axis of symmetry;
R : the rotation through 180°.

The Cayley table for these three symmetries is given as follows:

$\circ$	I	H	V	R
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

From the diagonal we can read off that each element is its own inverse.

Furthermore, from the Cayley table we can read off the closure of the set of four symmetries; and we can also read off the associativity (which is somewhat tedious): for example, we see that $H \circ (H \circ V)$ is equal to $H \circ R$, i.e. to V, while $(H \circ H) \circ V$ is equal to $I \circ V$ i.e., to V as well, so indeed $H \circ (H \circ V) = (H \circ H) \circ V$. Similarly one would need to check the corresponding equality for each possible choice of three of the four symmetries (the ones where at least one of the three is the identity being obvious). Finally, we can see that the resulting group is commutative: the Cayley table is symmetric with respect to the main diagonal (where the I's stand).

Proposition: Let G be a group.

(1) The identity element of G is unique.
(2) The inverse of an element $g \in G$ is unique.
(3) For any $g \in G$, we have $(g^{-1})^{-1} = g$.
(4) For any $g, h \in G$, we have $(gh)^{-1} = h^{-1}g^{-1}$ (note the order on the right).

Proof. (1) Suppose we have e and f, both acting as an identity element in G. Then consider the element $E := e \circ f$. On the one hand, since e satisfies the identity property, we get $E = e \circ f = f$, on the other hand, since f also satisfies the identity property, we find $E = e \circ f = e$. Putting both equalities together, we find $e = (E =) f$, which means that any two identity elements have to agree.

(2) Suppose both $h \in G$ and $k \in G$ are inverses to a given $g \in G$. Then we consider $h \circ g \circ k$; due to associativity, we have

$$(h \circ g) \circ k = h \circ (g \circ k)\,.$$

But since h is inverse to g, the left hand side is equal to $e \circ k$, i.e., to k, while the right hand side is, since k is also inverse to g, equal to $h \circ e$, i.e., to h. Putting both equalities together, we get $h = k$, which means that any two inverse elements of a given element g have to agree.

(3) The defining property of the inverse h of g^{-1} is that $h \circ g^{-1} = g^{-1} \circ h = e$. But certainly this equality is true if we replace h by g. By (2) we know that the inverse is unique, so h must actually coincide with g.

(4) Check that $(gh)(h^{-1}g^{-1}) = e$ and also $(h^{-1}g^{-1}(gh) = e$. Now proceed similarly to (3).