1. Groups — Definitions

A group is a set $\mathcal{S}$ of elements between which there is defined a binary operation, usually called *multiplication*. For the moment, the operation will be denoted × and the previous statement means that, if A and B are elements of the set, then $A \times B$ is defined. The first requirement for the set to constitute a group is that the result of the binary operation is itself a member of the set, $A \times B \in \mathcal{S}$, i.e. the set is *closed* under multiplication.

The next requirement is that the multiplication operation is *associative*, which means that $(A \times B) \times C = A \times (B \times C)$. In other words, the product of a number of elements of the set, $A \times B \times C \times D \times \ldots$, is well defined. In the interests of economy, the operator × will generally be omitted, so multiplication of elements is written AB or $ABCD$, etc. An immediate consequence of associativity is that powers of elements of the group are well defined — $A^n = \underbrace{A \times A \times \cdots \times A}_{n}$ — and satisfy the usual rule of powers, $A^m A^n = A^{m+n}$.

The third requirement of the set $\mathcal{S}$ is that it must contain an *identity* element, often denoted E or $\mathbf{1}$, with the property that $AE = A = EA$ for every element $A \in \mathcal{S}$. The identity is unique, since if E and F are both identities, then $E = EF = F$.

Finally, it is required that, for every element $A \in \mathcal{S}$, the set $\mathcal{S}$ must contain an element B such that $AB = E = BA$. The element B is called the *inverse* of A and is denoted A^{-1}. It is unique, since if B and C are both inverses of A, then $B = BE = BAC = EC = C$. (Note the central role played by associativity of multiplication.) Powers of A^{-1} are denoted $(A^{-1})^n = A^{-n}$ and satisfy $A^n A^{-n} = E = A^{-n} A^n$ and $A^n A^{-m} = A^{n-m}$. It also follows that $A^0 = E$ for any $A \in \mathcal{S}$. Note that $(AB)^{-1} = B^{-1} A^{-1}$ and that the inverse of A^{-1} is A, i.e. $(A^{-1})^{-1} = A$.

To summarize, **a group $\mathcal{G}$** is a set of elements with a binary operation of multiplication which satisfies the following conditions:

1. The set is *closed* under multiplication.
2. The multiplication is *associative*.
3. The set includes an *identity* element.
4. For every element in the set there is an *inverse* element in the set.

This basic definition can be modified in various ways. For example, it is sufficient to require a left (or right) identity and a left (or right) inverse — it can then be proved that the identity and inverse are two-sided.

Suppose $\mathcal{G}$ is a group and let A be any element of the group. Consider the set of elements $\mathcal{G}_A = \{AB \text{ for all } B \in \mathcal{G}\}$. They are all different, since the existence of the inverse A^{-1} means that $AB = AC \Longrightarrow B = C$. Since $\mathcal{G}$ is closed under multiplication, every element of $\mathcal{G}_A$ belongs to $\mathcal{G}$. But an arbitrary element $C \in \mathcal{G}$ can be written $C = AA^{-1}C$ and since $A^{-1}C \in \mathcal{G}$ it follows that every element of $\mathcal{G}$ belongs to $\mathcal{G}_A$. So the two sets $\mathcal{G}$ and $\mathcal{G}_A$ are in fact the same set — $\mathcal{G}_A$ is just the group $\mathcal{G}$, generally in some different order. This result is dignified with the title of *the rearrangement theorem*. It would clearly hold equally well if $\mathcal{G}_A$ were defined using right multiplication rather than left multiplication by the element A, i.e. $\mathcal{G}_A = \{BA \text{ for all } B \in \mathcal{G}\}$.

> **The rearrangement theorem:** The set of elements obtained by multiplying every element of a group $\mathcal{G}$ by a fixed element of $\mathcal{G}$ is just the set of elements of $\mathcal{G}$, generally in a different order.

From the existence of inverses and the identity, it follows that a group has the *cancellation property*: $XA = XB$ or $AX = BX$ implies $A = B$, for any elements $A, B, X \in \mathcal{G}$. (Just pre- or post-multiply by X^{-1}, as appropriate. Again, note the essential role of associativity.) For a group $\mathcal{G}$ with a finite number of elements, this property implies that $\mathcal{G}$ and $\mathcal{G}_A$ in the rearrangement theorem have the same number of elements.

If the set $\mathcal{G}$ has a finite number of elements and a binary operation of multiplication between them, then if (i) $\mathcal{G}$ is closed under multiplication, (ii) the multiplication is associative and (iii) the cancellation property holds, $\mathcal{G}$ is a group.

> [**Proof:** Choose $A \in \mathcal{G}$ and form the set $\{AB, \text{ for all } B \in \mathcal{G}\}$. If $AB = AC$, then by the cancellation property $B = C$, so this set has distinct elements, all of which belong to $\mathcal{G}$, by closure, and it has as many elements as $\mathcal{G}$. It is thus just $\mathcal{G}$, in some order, i.e. the cancellation property is sufficient to establish the rearrangement theorem for a finite $\mathcal{G}$. It follows that one of the elements of this set is A itself, i.e. there is an element of $\mathcal{G}$, to be denoted E_A, such that $AE_A = A$. This element is a right identity for A. But then $AE_AA = AA$ and the cancellation property implies $E_AA = A$, so E_A is also a left identity for A. Since A was chosen at random, it follows that every element of $\mathcal{G}$ has a (two-sided) identity. Given two elements $A, B \in \mathcal{G}$, with their

> associated identities, $AE_AB = AB$ and the cancellation property implies $E_AB = B$. But $B = E_BB$, so $E_AB = E_BB$ and the cancellation property implies $E_A = E_B$. Hence, $\mathcal{G}$ contains a unique identity E. A similar argument, based on the fact that the set $\{AB$, for all $B \in \mathcal{G}\}$ must include the identity element $E \in \mathcal{G}$, shows that every element of $\mathcal{G}$ has a unique inverse in $\mathcal{G}$. So, finally, $\mathcal{G}$ is a group.]

As a rule, it is fairly straightforward to establish closure and the existence of the identity and inverse. However, there is no general way of confirming the associativity of the multiplication operation. In principle, it could be necessary to check every triplet ABC of group elements to confirm that, in fact, $A(BC) = (AB)C$ in every case. For large groups, this can be an immense task. (Of course, even a single triplet failing this test is enough to establish that the set and multiplication rule at issue do not constitute a group.) Fortunately, there are many cases in which associativity can be demonstrated quite directly. One very useful result is that mappings of a set of objects to itself are associative, where the multiplication rule is consecutive action of the mappings.

> [Let A,B and C be mappings of a set $\{x\}$ of elements, $A : x \rightarrow x^A$ for instance, with multiplication defined as consecutive action of mappings, $AB : x \rightarrow (x^B)^A$. (Note: the order of consecutive actions is always set by reading from right to left.) Then $A(BC) : x \rightarrow ((x^C)^B)^A$ and $(AB)C : x \rightarrow ((x^C)^B)^A)$.]

If it is possible to interpret the elements of a group as mappings of some set to itself, while preserving the multiplication rule, it follows immediately that the multiplication is associative.

The structure of a finite group is essentially determined by its *multiplication table*, a square array in which the rows and columns are labelled by the elements of the group and the product AB (an element of the group, by closure) is entered in the A row and B column. (It is important to stick to a fixed convention — entering the element AB in the A column and B row will very often produce a different multiplication table.)It is conventional to place the identity E first in the list of elements and to use the same ordering of the group elements in labelling the rows and the columns. Since $EA = A = AE$ for every element A of the group, the first row and first column of the multiplication table simply repeat the list of elements. It is therefore unnecessary to label the rows and columns explicitly.

Consider the X row of the multiplication table. If the elements of the group are $\{E, A, B, \ldots\}$, then this row is $\{X, XA, XB, \ldots\}$. By the rearrangement theorem, each row is therefore a permutation of the elements of the group. The same argument shows that each column of the table is a permutation of the elements of the group. This is a significant constraint on the form of the multiplication table. It implies that every element of the group appears exactly once in each row and column. In addition, since $AB = E \Longrightarrow A = B^{-1} \Longrightarrow B = A^{-1} \Longrightarrow BA = E$, the identity element can appear only on or symmetrically about the main diagonal of the table. To be acceptable as the multiplication table of a group, such an array must satisfy both of these constraints and, in addition, be compatible with associativity.

Note that multiplication is required to be associative, but need not be commutative. In general, $AB \neq BA$ for two elements of a group. If an element of the group appears symmetrically about the main diagonal of the group multiplication table, the elements labeling its row and column commute with one another. A group for which all pairs of elements commute is said to be commutative, or *Abelian*, and its multiplication table is symmetric about the main diagonal.

The multiplication table defines the group. It is obvious that changing the standard order of the elements in the first row and column of the table will change the appearance of the table without changing the group. Reshuffling the elements would restore the table to its original form. However, two apparently different groups may have the same multiplication table when their elements are appropriately ordered, differing from one another only in the labels on the elements. In some sense, they are the same group. Such groups are actually different realisations of the same abstract group structure. Two groups, having the same number of elements, which can be brought to have the same multiplication table by a suitable correspondence between their elements are said to be *isomorphic* to one another. More formally, an *isomorphism* of two groups is a one-to-one onto mapping between the groups which preserves the multiplication (i.e. the image of the product of two elements is the product of the images of the elements).

There is also a less restrictive relation between groups, called a *homomorphism.* This is a mapping from one group to another which preserves the multiplication, but need not be one to one. Two homomorphic groups need not have the same number of elements. In fact, all groups are homomorphic to the trivial single-element group consisting only of the identity (called the *unit group*). Because it preserves multiplication, any homomorphism maps the identity element to the identity element and inverses to inverses.

[Let h be a homomorphism of the group $\mathcal{G}$ to the group $\mathcal{G}'$. Write $h(R) = R'$ for $R \in \mathcal{G}$, where $R' \in \mathcal{G}'$. Then $h(ER) = h(E)h(R) \Longrightarrow R' = E'R'$ for any $R \in \mathcal{G}$, so E' is the identity in $\mathcal{G}'$. Similarly, $h(R)h(R^{-1}) = h(E) \Longrightarrow R'(R^{-1})' = E'$, so $(R^{-1})' = (R')^{-1}$.]

Examples of finite groups

1. Addition of integers modulo 6 defines a group of six elements, the numbers $\{0, 1, 2, 3, 4, 5\}$, where the "multiplication" is addition (mod 6) and the identity is 0. The multiplication table is

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

and is symmetric, since addition is commutative. (Note that the elements of the group can be interpreted as mappings of a set of six points arranged in a circle, with element n representing a clockwise shift by n dots. The multiplication is thus associative.)

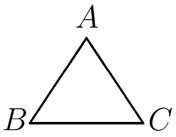
2. The $\frac{1}{6}$ roots of unity form a group under multiplication. Denoting $\omega = e^{2\pi i/6}$, the six elements of the group are $\{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$ and the identity is 1. The multiplication table is

1	ω	ω^2	ω^3	ω^4	ω^5
ω	ω^2	ω^3	ω^4	ω^5	1
ω^2	ω^3	ω^4	ω^5	1	ω
ω^3	ω^4	ω^5	1	ω	ω^2
ω^4	ω^5	1	ω	ω^2	ω^3
ω^5	1	ω	ω^2	ω^3	ω^4

and is again symmetric, since complex multiplication is commutative (and also associative). (It would also be possible to interpret the elements of the group as mappings of a set of six unit vectors in the plane at angles of $2\pi/n$ to the x axis, with element ω^n representing a clockwise rotation through $360°/n$ about the origin.)

3. The symmetries of an equilateral triangle form a group, where multiplication is the consecutive application of the transformations leaving the

triangle invariant. Suppose the triangle has its base along the x axis and its vertex on the positive y axis and that its vertices are labelled A, B, C from the top counterclockwise.



The triangle will remain invariant, though the labelling of the vertices will change, under the following operations:

- (i) no transformation at all, the identity, denoted 1 $[1 : ABC \to ABC]$;
- (ii) a counterclockwise rotation through 120° about an axis perpendicular to the $x - y$ plane through the centre of gravity of the triangle, denoted r_1 $[r_1 : ABC \to CAB]$;
- (iii) a counterclockwise rotation through 240° about the same axis, denoted r_2 $[r_2 : ABC \to BCA]$;
- (iv) - (vi) rotations through 180° about axes through the vertices of the triangle and perpendicular to the opposite sides, denoted m_1, m_2 and m_3 $[m_1 : ABC \to ACB$, $m_2 : ABC \to CBA$, $m_3 : ABC \to BAC]$.

The group has six elements and its multiplication table is

1	r_1	r_2	m_1	m_2	m_3
r_1	r_2	1	m_3	m_1	m_2
r_2	1	r_1	m_2	m_3	m_1
m_1	m_2	m_3	1	r_1	r_2
m_2	m_3	m_1	r_2	1	r_1
m_3	m_1	m_2	r_1	r_2	1

which is not symmetric — this group is not Abelian. (Note again the convention that the product of transformations T_1T_2 implies that T_2 acts first and is followed by T_1. The order of action of a product of transformations is from right to left.) The six symmetry operations map the set of six triplets ABC, ACB, BAC, BCA, CAB, CBA into itself and reflect the multiplication table, so the multiplication is associative.

4. The set of permutations of three objects form a group, where multiplication is again the consecutive action of two permutations. The six elements of the group are

- (i) the identity permutation 1 $[1 : uvw \to uvw]$,

- (ii) the three transpositions P_{ij}, $[P_{12} : uvw \to vuw$, $P_{13} : uvw \to wvu$, $P_{23} : uvw \to uwv]$,
- (iii) the cyclic permutation C $[C : uvw \to wuv]$ and
- (iv) the anticyclic permutation A $[A : uvw \to vwu]$,

and its multiplication table is

1	P_{12}	P_{13}	P_{23}	C	A
P_{12}	1	A	C	P_{23}	P_{13}
P_{13}	C	1	A	P_{12}	P_{23}
P_{23}	A	C	1	P_{13}	P_{12}
C	P_{13}	P_{23}	P_{12}	A	1
A	P_{23}	P_{12}	P_{13}	1	C

which is again not symmetric — this group, too, is non-Abelian. The elements of the group are mappings to itself of the set of six ordered triplets uvw, uwv, vuw, vwu, wuv, wvu, so the multiplication is associative.

The above are examples of four different groups of six elements each. They are certainly not all realisations of the same abstract group, since two of them are Abelian and two are non-Abelian, so the multiplication tables cannot be made to coincide. However, the first two are isomorphic to one another and so are the last two. The mapping $n \rightleftharpoons \omega^n$ maps the first and second groups into each other while preserving the multiplication table, and the same is true of the mapping $1 \rightleftharpoons 1, r_1 \rightleftharpoons C, r_2 \rightleftharpoons A, m_1 \rightleftharpoons P_{23}, m_2 \rightleftharpoons P_{13}, m_3 \rightleftharpoons P_{12}$ of the third and fourth groups into each other. So there are, in fact, only two different groups of six elements among the four examples.