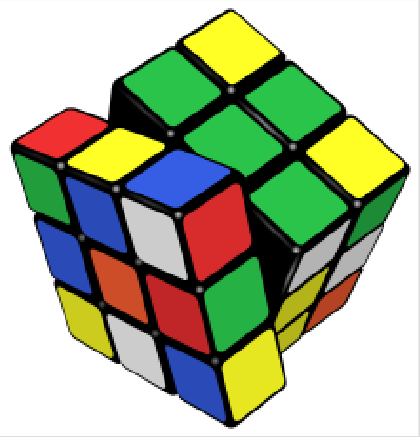
Wikipedia
The Free Encyclopedia

Group (mathematics)

In mathematics, a **group** is a set with an operation that satisfies the following constraints: the operation is associative and has an identity element, and every element of the set has an inverse element.



The manipulations of the Rubik's Cube form the Rubik's Cube group.

Many mathematical structures are groups endowed with other properties. For example, the integers with the addition operation form an infinite group, which is generated by a single element called 1 (these properties characterize the integers in a unique way).

The concept of a group was elaborated for handling, in a unified way, many mathematical structures such as numbers, geometric shapes and polynomial roots. Because the concept of groups is ubiquitous in numerous areas both within and outside mathematics, some authors consider it as a central organizing principle of contemporary mathematics.[1][2]

In geometry, groups arise naturally in the study of symmetries and geometric transformations: The symmetries of an object form a group, called the symmetry group of the object, and the transformations of a given type form a general group. Lie groups appear in symmetry groups in geometry, and also in the Standard Model of particle physics. The Poincaré group is a Lie group consisting of the symmetries of spacetime in special relativity. Point groups describe symmetry in molecular chemistry.

The concept of a group arose in the study of polynomial equations, starting with Évariste Galois in the 1830s, who introduced the term *group* (French: *groupe*) for the symmetry group of the roots of an equation, now called a Galois group. After contributions from other fields such as number theory and geometry, the group notion was generalized and firmly established around 1870. Modern group theory—an active mathematical discipline—studies groups in their own right. To explore groups, mathematicians have devised various notions to break groups into smaller, better-understandable pieces, such as subgroups, quotient groups and simple groups. In addition to their abstract properties, group theorists also study the different ways in which a group can be expressed concretely, both from a point of view of representation theory (that is, through the representations of the group) and of computational group theory. A theory has been developed for finite groups, which culminated with the classification of finite simple groups, completed in 2004. Since the mid-1980s, geometric group theory, which studies finitely generated groups as geometric objects, has become an active area in group theory.

Definition and illustration

First example: the integers

One of the more familiar groups is the set of integers

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

together with addition.[3] For any two integers a and b, the sum $a + b$ is also an integer; this *closure* property says that $+$ is a binary operation on $\mathbb{Z}$. The following properties of integer addition serve as a model for the group axioms in the definition below.

- For all integers a, b and c, one has $(a+b)+c=a+(b+c)$. Expressed in words, adding a to b first, and then adding the result to c gives the same final result as adding a to the sum of b and c. This property is known as *associativity*.
- If a is any integer, then $0+a=a$ and $a+0=a$. Zero is called the *identity element* of addition because adding it to any integer returns the same integer.
- For every integer a, there is an integer b such that $a+b=0$ and $b+a=0$. The integer b is called the *inverse element* of the integer a and is denoted $-a$.

The integers, together with the operation $+$, form a mathematical object belonging to a broad class sharing similar structural aspects. To appropriately understand these structures as a collective, the following definition is developed.

Definition

A group is a non-empty set G together with a binary operation on G, here denoted "$\cdot$", that combines any two elements a and b of G to form an element of G, denoted $a\cdot b$, such that the following three requirements, known as **group axioms**, are satisfied:[5][6][7][a]

Associativity

For all a, b, c in G, one has $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

Identity element

There exists an element e in G such that, for every a in G, one has $e\cdot a=a$ and $a\cdot e=a$.
Such an element is unique (see below). It is called the *identity element* (or sometimes *neutral element*) of the group.

Inverse element

For each a in G, there exists an element b in G such that $a\cdot b=e$ and $b\cdot a=e$, where e is the identity element.
For each a, the element b is unique (see below); it is called *the inverse* of a and is commonly denoted a^{-1}.

> The axioms for a group are short and natural... Yet somehow hidden behind these axioms is the monster simple group, a huge and extraordinary mathematical object, which appears to rely on numerous bizarre coincidences to exist. The axioms for groups give no obvious hint that anything like this exists.
>
> Richard Borcherds, *Mathematicians: An Outer View of the Inner World*[4]

Notation and terminology

Formally, the group is the ordered pair of a set and a binary operation on this set that satisfies the group axioms. The set is called the *underlying set* of the group, and the operation is called the *group operation* or the *group law*.

A group and its underlying set are thus two different mathematical objects. To avoid cumbersome notation, it is common to abuse notation by using the same symbol to denote both. This reflects also an informal way of thinking: that the group is the same as the set except that it has been enriched by additional structure provided by the operation.

For example, consider the set of real numbers $\mathbb{R}$, which has the operations of addition $a+b$ and multiplication ab. Formally, $\mathbb{R}$ is a set, $(\mathbb{R},+)$ is a group, and $(\mathbb{R},+,\cdot)$ is a field. But it is common to write $\mathbb{R}$ to denote any of these three objects.

The *additive group* of the field $\mathbb{R}$ is the group whose underlying set is $\mathbb{R}$ and whose operation is addition. The *multiplicative group* of the field $\mathbb{R}$ is the group $\mathbb{R}^{\times}$ whose underlying set is the set of nonzero real numbers $\mathbb{R}\smallsetminus\{0\}$ and whose operation is multiplication.

More generally, one speaks of an *additive group* whenever the group operation is notated as addition; in this case, the identity is typically denoted 0, and the inverse of an element x is denoted $-x$. Similarly, one speaks of a *multiplicative group* whenever the group operation is notated as multiplication; in this case, the identity is typically denoted 1, and the inverse of an element x is denoted x^{-1}. In a multiplicative group, the operation symbol is usually omitted entirely, so that the operation is denoted by juxtaposition, ab instead of $a \cdot b$.

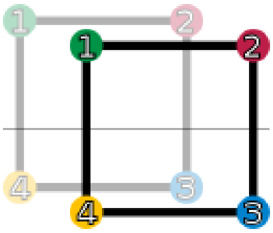
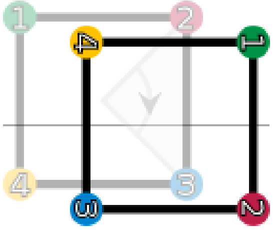
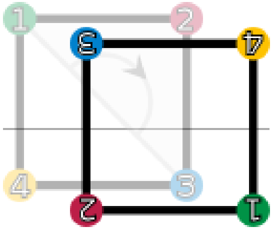
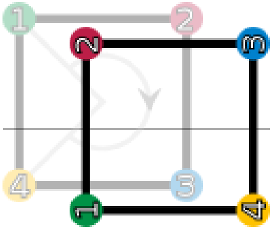
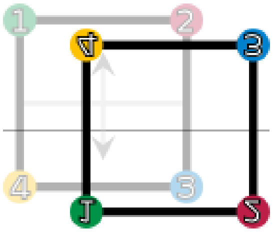
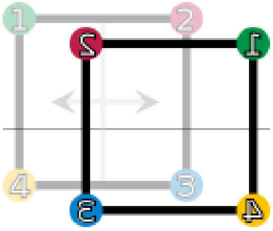
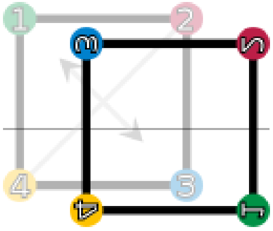
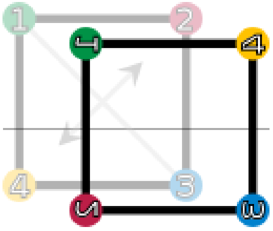
The definition of a group does not require that $a \cdot b = b \cdot a$ for all elements a and b in G. If this additional condition holds, then the operation is said to be commutative, and the group is called an abelian group. It is a common convention that for an abelian group either additive or multiplicative notation may be used, but for a nonabelian group only multiplicative notation is used.

Several other notations are commonly used for groups whose elements are not numbers. For a group whose elements are functions, the operation is often function composition $f \circ g$; then the identity may be denoted id. In the more specific cases of geometric transformation groups, symmetry groups, permutation groups, and automorphism groups, the symbol $\circ$ is often omitted, as for multiplicative groups. Many other variants of notation may be encountered.

Second example: a symmetry group

Two figures in the plane are congruent if one can be changed into the other using a combination of rotations, reflections, and translations. Any figure is congruent to itself. However, some figures are congruent to themselves in more than one way, and these extra congruences are called symmetries. A square has eight symmetries. These are:

The elements of the symmetry group of the square, D_4. Vertices are identified by color or number.

 id (keeping it as it is)	 r_1 (rotation by 90° clockwise)	 r_2 (rotation by 180°)	 r_3 (rotation by 270° clockwise)
 f_{v} (vertical reflection)	 f_{h} (horizontal reflection)	 f_{d} (diagonal reflection)	 f_{c} (counter-diagonal reflection)

- the identity operation leaving everything unchanged, denoted id;
- rotations of the square around its center by 90°, 180°, and 270° clockwise, denoted by r_1, r_2 and r_3, respectively;
- reflections about the horizontal and vertical middle line (f_{v} and f_{h}), or through the two diagonals (f_{d} and f_{c}).

These symmetries are functions. Each sends a point in the square to the corresponding point under the symmetry. For example, r_1 sends a point to its rotation 90° clockwise around the square's center, and f_{h} sends a point to its reflection across the square's vertical middle line. Composing two of these symmetries gives another symmetry. These symmetries determine a group called the dihedral group of degree four, denoted D_4. The underlying set of the group is the above set of symmetries, and the group operation is function composition.[8] Two symmetries are combined by composing them as functions, that is, applying the first one to the square, and the second one to the result of the first application. The result of performing first a and then b is written symbolically *from right to left* as $b \circ a$ ("apply the symmetry b after performing the symmetry a"). This is the usual notation for composition of functions.

The group table lists the results of all such compositions possible. For example, rotating by 270° clockwise (r_3) and then reflecting horizontally (f_{h}) is the same as performing a reflection along the diagonal (f_{d}). Using the above symbols, highlighted in blue in the group table:

$$f_{\mathrm{h}} \circ r_3 = f_{\mathrm{d}}.$$

Group table of D_4

$\circ$	id	r_1	r_2	r_3	f_{v}	f_{h}	f_{d}	f_{c}
id	id	r_1	r_2	r_3	f_{v}	f_{h}	f_{d}	f_{c}
r_1	r_1	r_2	r_3	id	f_{c}	f_{d}	f_{v}	f_{h}
r_2	r_2	r_3	id	r_1	f_{h}	f_{v}	f_{c}	f_{d}
r_3	r_3	id	r_1	r_2	f_{d}	f_{c}	f_{h}	f_{v}
f_{v}	f_{v}	f_{d}	f_{h}	f_{c}	id	r_2	r_1	r_3
f_{h}	f_{h}	f_{c}	f_{v}	f_{d}	r_2	id	r_3	r_1
f_{d}	f_{d}	f_{h}	f_{c}	f_{v}	r_3	r_1	id	r_2
f_{c}	f_{c}	f_{v}	f_{d}	f_{h}	r_1	r_3	r_2	id

The elements id, r_1, r_2, and r_3 form a subgroup whose group table is highlighted in 🟥 red (upper left region). A left and right coset of this subgroup are highlighted in 🟩 green (in the last row) and 🟨 yellow (last column), respectively. The result of the composition $f_{\mathrm{h}} \circ r_3$, the symmetry f_{d}, is highlighted in 🟦 blue (below table center).

Given this set of symmetries and the described operation, the group axioms can be understood as follows.

Binary operation: Composition is a binary operation. That is, $a \circ b$ is a symmetry for any two symmetries a and b. For example,

$$r_3 \circ f_{\mathrm{h}} = f_{\mathrm{c}},$$

that is, rotating 270° clockwise after reflecting horizontally equals reflecting along the counter-diagonal (f_{c}). Indeed, every other combination of two symmetries still gives a symmetry, as can be checked using the group table.

Associativity: The associativity axiom deals with composing more than two symmetries: Starting with three elements a, b and c of D_4, there are two possible ways of using these three symmetries in this order to determine a symmetry of the square. One of these ways is to first compose a and b into a single symmetry, then to compose that symmetry with c. The other way is to first compose b and c, then to compose the resulting symmetry with a. These two ways must give always the same result, that is,

$$(a \circ b) \circ c = a \circ (b \circ c),$$

For example, $(f_{\mathrm{d}} \circ f_{\mathrm{v}}) \circ r_2 = f_{\mathrm{d}} \circ (f_{\mathrm{v}} \circ r_2)$ can be checked using the group table:

$$\begin{aligned} (f_{\mathrm{d}} \circ f_{\mathrm{v}}) \circ r_2 &= r_3 \circ r_2 = r_1 \\ f_{\mathrm{d}} \circ (f_{\mathrm{v}} \circ r_2) &= f_{\mathrm{d}} \circ f_{\mathrm{h}} = r_1. \end{aligned}$$

Identity element: The identity element is id, as it does not change any symmetry a when composed with it either on the left or on the right.

Inverse element: Each symmetry has an inverse: id, the reflections f_{h}, f_{v}, f_{d}, f_{c} and the 180° rotation r_2 are their own inverse, because performing them twice brings the square back to its original orientation. The rotations r_3 and r_1 are each other's inverses, because rotating 90° and then rotation 270° (or vice versa) yields a rotation over 360° which leaves the square unchanged. This is easily verified on the table.

In contrast to the group of integers above, where the order of the operation is immaterial, it does matter in D_4, as, for example, $f_{\mathrm{h}} \circ r_1 = f_{\mathrm{c}}$ but $r_1 \circ f_{\mathrm{h}} = f_{\mathrm{d}}$. In other words, D_4 is not abelian.

History

The modern concept of an abstract group developed out of several fields of mathematics.[9][10][11] The original motivation for group theory was the quest for solutions of polynomial equations of degree higher than 4. The 19th-century French mathematician Évariste Galois, extending prior work of Paolo Ruffini and Joseph-Louis Lagrange, gave a criterion for the solvability of a particular polynomial equation in terms of the symmetry group of its roots (solutions). The elements of such a Galois group correspond to certain permutations of the roots. At first, Galois's ideas were rejected by his contemporaries, and published only posthumously.[12][13] More general permutation groups were investigated in particular by Augustin Louis Cauchy. Arthur Cayley's *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$ (1854) gives the first abstract definition of a finite group.[14]

Geometry was a second field in which groups were used systematically, especially symmetry groups as part of Felix Klein's 1872 Erlangen program.[15] After novel geometries such as hyperbolic and projective geometry had emerged, Klein used group theory to organize them in a more coherent way. Further advancing these ideas, Sophus Lie founded the study of Lie groups in 1884.[16]

The third field contributing to group theory was number theory. Certain abelian group structures had been used implicitly in Carl Friedrich Gauss's number-theoretical work *Disquisitiones Arithmeticae* (1798), and more explicitly by Leopold Kronecker.[17] In 1847, Ernst Kummer made early attempts to prove Fermat's Last Theorem by developing groups describing factorization into prime numbers.[18]

The convergence of these various sources into a uniform theory of groups started with Camille Jordan's *Traité des substitutions et des équations algébriques* (1870).[19] Walther von Dyck (1882) introduced the idea of specifying a group by means of generators and relations, and was also the first to give an axiomatic definition of an "abstract group", in the terminology of the time.[20] As of the 20th century, groups gained wide recognition by the pioneering work of Ferdinand Georg Frobenius and William Burnside, who worked on representation theory of finite groups, Richard Brauer's modular representation theory and Issai Schur's papers.[21] The theory of Lie groups, and more generally locally compact groups was studied by Hermann Weyl, Élie Cartan and many others.[22] Its algebraic counterpart, the theory of algebraic groups, was first shaped by Claude Chevalley (from the late 1930s) and later by the work of Armand Borel and Jacques Tits.[23]

The University of Chicago's 1960–61 Group Theory Year brought together group theorists such as Daniel Gorenstein, John G. Thompson and Walter Feit, laying the foundation of a collaboration that, with input from numerous other mathematicians, led to the classification of finite simple groups, with the final step taken by Aschbacher and Smith in 2004. This project exceeded previous mathematical endeavours by its sheer size, in both length of proof and number of researchers. Research concerning this classification proof is ongoing.[24] Group theory remains a highly active mathematical branch,[b] impacting many other fields, as the examples below illustrate.

Elementary consequences of the group axioms

Basic facts about all groups that can be obtained directly from the group axioms are commonly subsumed under *elementary group theory*.[25] For example, repeated applications of the associativity axiom show that the unambiguity of

$$a \cdot b \cdot c = (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

generalizes to more than three factors. Because this implies that parentheses can be inserted anywhere within such a series of terms, parentheses are usually omitted.[26]

Uniqueness of identity element

The group axioms imply that the identity element is unique; that is, there exists only one identity element: any two identity elements e and f of a group are equal, because the group axioms imply $e = e \cdot f = f$. It is thus customary to speak of *the* identity element of the group.[27]

Uniqueness of inverses

The group axioms also imply that the inverse of each element is unique: Let a group element a have both b and c as inverses. (b and c are distinct.) Then

$$\begin{aligned} b &= b \cdot e && (e \text{ is the identity element}) \\ &= b \cdot (a \cdot c) && (c \text{ is an inverse}) \\ &= (b \cdot a) \cdot c && (\text{associativity}) \\ &= e \cdot c && (b \text{ is an inverse}) \\ &= c && (e \text{ is the identity element}) \end{aligned}$$

Therefore, it is customary to speak of *the* inverse of an element.[27]

Division

Given elements a and b of a group G, there is a unique solution x in G to the equation $a \cdot x = b$, namely $a^{-1} \cdot b$.[c][28] It follows that for each a in G, the function $G \to G$ that maps each x to $a \cdot x$ is a bijection; it is called *left multiplication* by a or *left translation* by a.

Similarly, given a and b, the unique solution to $x \cdot a = b$ is $b \cdot a^{-1}$. For each a, the function $G \to G$ that maps each x to $x \cdot a$ is a bijection called *right multiplication* by a or *right translation* by a.

Equivalent definition with relaxed axioms

The group axioms for identity and inverses may be "weakened" to assert only the existence of a left identity and left inverses. From these *one-sided axioms*, one can prove that the left identity is also a right identity and a left inverse is also a right inverse for the same element. Since they define exactly the same structures as groups, collectively the axioms are not weaker.[29]

In particular, assuming associativity and the existence of a left identity e (that is, $e \cdot f = f$) and a left inverse f^{-1} for each element f (that is, $f^{-1} \cdot f = e$), one can show that every left inverse is also a right inverse of the same element as follows.[29] Indeed, one has

$$\begin{aligned} f \cdot f^{-1} &= e \cdot (f \cdot f^{-1}) && (\text{left identity}) \\ &= ((f^{-1})^{-1} \cdot f^{-1}) \cdot (f \cdot f^{-1}) && (\text{left inverse}) \\ &= (f^{-1})^{-1} \cdot ((f^{-1} \cdot f) \cdot f^{-1}) && (\text{associativity}) \\ &= (f^{-1})^{-1} \cdot (e \cdot f^{-1}) && (\text{left inverse}) \\ &= (f^{-1})^{-1} \cdot f^{-1} && (\text{left identity}) \\ &= e && (\text{left inverse}) \end{aligned}$$

Similarly, the left identity is also a right identity:[29]

$$\begin{aligned} f \cdot e &= f \cdot (f^{-1} \cdot f) && \text{(left inverse)} \\ &= (f \cdot f^{-1}) \cdot f && \text{(associativity)} \\ &= e \cdot f && \text{(right inverse)} \\ &= f && \text{(left identity)} \end{aligned}$$

These proofs require all three axioms (associativity, existence of left identity and existence of left inverse). For a structure with a looser definition (like a semigroup) one may have, for example, that a left identity is not necessarily a right identity.

The same result can be obtained by only assuming the existence of a right identity and a right inverse.

However, only assuming the existence of a *left* identity and a *right* inverse (or vice versa) is not sufficient to define a group. For example, consider the set $G = \{e, f\}$ with the operator $\cdot$ satisfying $e \cdot e = f \cdot e = e$ and $e \cdot f = f \cdot f = f$. This structure does have a left identity (namely, e), and each element has a right inverse (which is e for both elements). Furthermore, this operation is associative (since the product of any number of elements is always equal to the rightmost element in that product, regardless of the order in which these operations are done). However, $(G, \cdot)$ is not a group, since it lacks a right identity.

Basic concepts

When studying sets, one uses concepts such as subset, function, and quotient by an equivalence relation. When studying groups, one uses instead subgroups, homomorphisms, and quotient groups. These are the analogues that take the group structure into account.[d]

Group homomorphisms

Group homomorphisms[e] are functions that respect group structure; they may be used to relate two groups. A *homomorphism* from a group $(G, \cdot)$ to a group $(H, *)$ is a function $\varphi\colon G \to H$ such that

$\varphi(a \cdot b) = \varphi(a) * \varphi(b)$ for all elements a and b in G.

It would be natural to require also that φ respect identities, $\varphi(1_G) = 1_H$, and inverses, $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all a in G. However, these additional requirements need not be included in the definition of homomorphisms, because they are already implied by the requirement of respecting the group operation.[30]

The *identity homomorphism* of a group G is the homomorphism $\iota_G\colon G \to G$ that maps each element of G to itself. An *inverse homomorphism* of a homomorphism $\varphi\colon G \to H$ is a homomorphism $\psi\colon H \to G$ such that $\psi \circ \varphi = \iota_G$ and $\varphi \circ \psi = \iota_H$, that is, such that $\psi\bigl(\varphi(g)\bigr) = g$ for all g in G and such that $\varphi\bigl(\psi(h)\bigr) = h$ for all h in H. An *isomorphism* is a homomorphism that has an inverse homomorphism; equivalently, it is a bijective homomorphism. Groups G and H are called *isomorphic* if there exists an isomorphism $\varphi\colon G \to H$. In this case, H can be obtained from G simply by renaming its elements according to the function φ; then any statement true for G is true for H, provided that any specific elements mentioned in the statement are also renamed.

The collection of all groups, together with the homomorphisms between them, form a category, the category of groups.[31]

An injective homomorphism $\phi\colon G' \to G$ factors canonically as an isomorphism followed by an inclusion, $G' \overset{\sim}{\to} H \hookrightarrow G$ for some subgroup H of G. Injective homomorphisms are the monomorphisms in the category of groups.

Subgroups

Informally, a *subgroup* is a group H contained within a bigger one, G: it has a subset of the elements of G, with the same operation.[32] Concretely, this means that the identity element of G must be contained in H, and whenever h_1 and h_2 are both in H, then so are $h_1 \cdot h_2$ and h_1^{-1}, so the elements of H, equipped with the group operation on G restricted to H, indeed form a group. In this case, the inclusion map $H \to G$ is a homomorphism.

In the example of symmetries of a square, the identity and the rotations constitute a subgroup $R = \{\mathrm{id}, r_1, r_2, r_3\}$, highlighted in red in the group table of the example: any two rotations composed are still a rotation, and a rotation can be undone by (i.e., is inverse to) the complementary rotations 270° for 90°, 180° for 180°, and 90° for 270°. The subgroup test provides a necessary and sufficient condition for a nonempty subset *H* of a group *G* to be a subgroup: it is sufficient to check that $g^{-1} \cdot h \in H$ for all elements g and h in H. Knowing a group's subgroups is important in understanding the group as a whole.[f]

Given any subset S of a group G, the subgroup generated by S consists of all products of elements of S and their inverses. It is the smallest subgroup of G containing S.[33] In the example of symmetries of a square, the subgroup generated by r_2 and f_v consists of these two elements, the identity element id, and the element $f_\mathrm{h} = f_\mathrm{v} \cdot r_2$. Again, this is a subgroup, because combining any two of these four elements or their inverses (which are, in this particular case, these same elements) yields an element of this subgroup.

Cosets

In many situations it is desirable to consider two group elements the same if they differ by an element of a given subgroup. For example, in the symmetry group of a square, once any reflection is performed, rotations alone cannot return the square to its original position, so one can think of the reflected positions of the square as all being equivalent to each other, and as inequivalent to the unreflected positions; the rotation operations are irrelevant to the question whether a reflection has been performed. Cosets are used to formalize this insight: a subgroup H determines left and right cosets, which can be thought of as translations of H by an arbitrary group element g. In symbolic terms, the *left* and *right* cosets of H, containing an element g, are

$gH = \{g \cdot h \mid h \in H\}$ and $Hg = \{h \cdot g \mid h \in H\}$, respectively.[34]

The left cosets of any subgroup H form a partition of G; that is, the union of all left cosets is equal to G and two left cosets are either equal or have an empty intersection.[35] The first case $g_1 H = g_2 H$ happens precisely when $g_1^{-1} \cdot g_2 \in H$, i.e., when the two elements differ by an element of H. Similar considerations apply to the right cosets of H. The left cosets of H may or may not be the same as its right cosets. If they are (that is, if all g in G satisfy $gH = Hg$), then H is said to be a *normal subgroup*.

In D_4, the group of symmetries of a square, with its subgroup R of rotations, the left cosets gR are either equal to R, if g is an element of R itself, or otherwise equal to $U = f_\mathrm{c} R = \{f_\mathrm{c}, f_\mathrm{d}, f_\mathrm{v}, f_\mathrm{h}\}$ (highlighted in green in the group table of D_4). The subgroup R is normal, because $f_\mathrm{c} R = U = R f_\mathrm{c}$ and similarly for the other elements of the group. (In fact, in the case of D_4, the cosets generated by reflections are all equal: $f_\mathrm{h} R = f_\mathrm{v} R = f_\mathrm{d} R = f_\mathrm{c} R$.)

Quotient groups

Suppose that N is a normal subgroup of a group G, and

$$G/N = \{gN \mid g \in G\}$$

denotes its set of cosets. Then there is a unique group law on G/N for which the map $G \to G/N$ sending each element g to gN is a homomorphism. Explicitly, the product of two cosets gN and hN is $(gh)N$, the coset $eN = N$ serves as the identity of G/N, and the inverse of gN in the quotient group is $(gN)^{-1} = \left(g^{-1}\right)N$. The group G/N, read as "G modulo N",[36] is called a *quotient group* or *factor group*. The quotient group can alternatively be characterized by a universal property.

The elements of the quotient group D_4/R are R and $U = f_\mathrm{v}R$. The group operation on the quotient is shown in the table. For example, $U \cdot U = f_\mathrm{v}R \cdot f_\mathrm{v}R = (f_\mathrm{v} \cdot f_\mathrm{v})R = R$. Both the subgroup $R = \{\mathrm{id}, r_1, r_2, r_3\}$ and the quotient D_4/R are abelian, but D_4 is not. Sometimes a group can be reconstructed from a subgroup and quotient (plus some additional data), by the semidirect product construction; D_4 is an example.

Group table of the quotient group D_4/R

$\cdot$	R	U
R	R	U
U	U	R

The first isomorphism theorem implies that any surjective homomorphism $\phi\colon G \to H$ factors canonically as a quotient homomorphism followed by an isomorphism: $G \to G/\ker\phi \overset{\sim}{\to} H$. Surjective homomorphisms are the epimorphisms in the category of groups.

Presentations

Every group is isomorphic to a quotient of a free group, in many ways.

For example, the dihedral group D_4 is generated by the right rotation r_1 and the reflection f_v in a vertical line (every element of D_4 is a finite product of copies of these and their inverses). Hence there is a surjective homomorphism φ from the free group $\langle r, f\rangle$ on two generators to D_4 sending r to r_1 and f to f_1. Elements in $\ker\phi$ are called *relations*; examples include $r^4, f^2, (r \cdot f)^2$. In fact, it turns out that $\ker\phi$ is the smallest normal subgroup of $\langle r, f\rangle$ containing these three elements; in other words, all relations are consequences of these three. The quotient of the free group by this normal subgroup is denoted $\langle r, f \mid r^4 = f^2 = (r \cdot f)^2 = 1\rangle$. This is called a *presentation* of D_4 by generators and relations, because the first isomorphism theorem for φ yields an isomorphism $\langle r, f \mid r^4 = f^2 = (r \cdot f)^2 = 1\rangle \to \mathrm{D}_4$.[37]

A presentation of a group can be used to construct the Cayley graph, a graphical depiction of a discrete group.[38]

Examples and applications

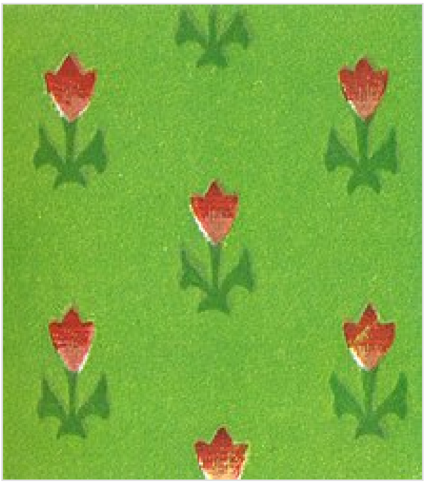
Examples and applications of groups abound. A starting point is the group $\mathbb{Z}$ of integers with addition as group operation, introduced above. If instead of addition multiplication is considered, one obtains multiplicative groups. These groups are predecessors of important constructions in abstract algebra.

Groups are also applied in many other mathematical areas. Mathematical objects are often examined by associating groups to them and studying the properties of the corresponding groups. For example, Henri Poincaré founded what is now called algebraic topology by introducing the fundamental group.[39] By means of this connection, topological properties such as proximity and continuity translate into properties of groups.[g]

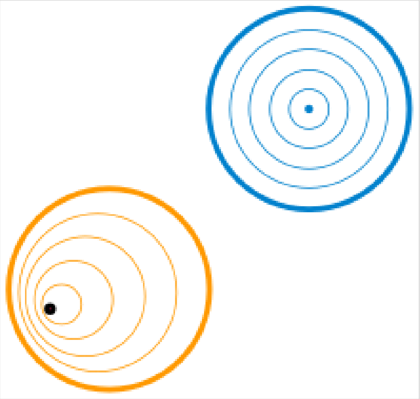
Elements of the fundamental group of a topological space are equivalence classes of loops, where loops are considered equivalent if one can be smoothly deformed into another, and the group operation is "concatenation" (tracing one loop then the other). For example, as shown in the figure, if the topological space is the plane with one point removed, then loops which do not wrap around the missing point (blue) can be smoothly contracted to a single point and are the identity element of the fundamental group. A loop which wraps around the missing point k times cannot be deformed into a loop which wraps m times (with $m \neq k$), because the loop cannot be smoothly deformed across the hole, so each class of loops is characterized by its winding number around the missing point. The resulting group is isomorphic to the integers under addition.

In more recent applications, the influence has also been reversed to motivate geometric constructions by a group-theoretical background.[h] In a similar vein, geometric group theory employs geometric concepts, for example in the study of hyperbolic groups.[40] Further branches crucially applying groups include algebraic geometry and number theory.[41]

In addition to the above theoretical applications, many practical applications of groups exist. Cryptography relies on the combination of the abstract group theory approach together with algorithmical knowledge obtained in computational group theory, in particular when implemented for finite groups.[42] Applications of group theory are not restricted to mathematics; sciences such as physics, chemistry and computer science benefit from the concept.



A periodic wallpaper pattern gives rise to a wallpaper group.



The fundamental group of a plane minus a point (bold) consists of loops around the missing point. This group is isomorphic to the integers under addition.

Numbers

Many number systems, such as the integers and the rationals, enjoy a naturally given group structure. In some cases, such as with the rationals, both addition and multiplication operations give rise to group structures. Such number systems are predecessors to more general algebraic structures known as rings and fields. Further abstract algebraic concepts such as modules, vector spaces and algebras also form groups.

Integers

The group of integers $\mathbb{Z}$ under addition, denoted $(\mathbb{Z}, +)$, has been described above. The integers, with the operation of multiplication instead of addition, $(\mathbb{Z}, \cdot)$ do *not* form a group. The associativity and identity axioms are satisfied, but inverses do not exist: for example, $a = 2$ is an integer, but the only solution to the equation $a \cdot b = 1$ in this case is $b = \frac{1}{2}$, which is a rational number, but not an integer. Hence not every element of $\mathbb{Z}$ has a (multiplicative) inverse.[i]

Rationals

The desire for the existence of multiplicative inverses suggests considering fractions

$$\frac{a}{b}.$$

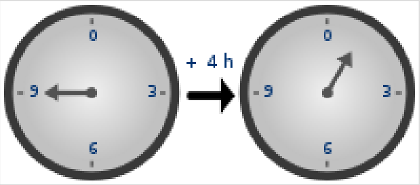
Fractions of integers (with b nonzero) are known as rational numbers.[j] The set of all such irreducible fractions is commonly denoted $\mathbb{Q}$. There is still a minor obstacle for $(\mathbb{Q}, \cdot)$, the rationals with multiplication, being a group: because zero does not have a multiplicative inverse (i.e., there is no x such that $x \cdot 0 = 1$), $(\mathbb{Q}, \cdot)$ is still not a group.

However, the set of all *nonzero* rational numbers $\mathbb{Q} \setminus \{0\} = \{q \in \mathbb{Q} \mid q \neq 0\}$ does form an abelian group under multiplication, also denoted $\mathbb{Q}^{\times}$.[k] Associativity and identity element axioms follow from the properties of integers. The closure requirement still holds true after removing zero, because the product of two nonzero rationals is never zero. Finally, the inverse of a/b is b/a, therefore the axiom of the inverse element is satisfied.

The rational numbers (including zero) also form a group under addition. Intertwining addition and multiplication operations yields more complicated structures called rings and – if division by other than zero is possible, such as in $\mathbb{Q}$ – fields, which occupy a central position in abstract algebra. Group theoretic arguments therefore underlie parts of the theory of those entities.[l]

Modular arithmetic

Modular arithmetic for a *modulus* n defines any two elements a and b that differ by a multiple of n to be equivalent, denoted by $a \equiv b \pmod{n}$. Every integer is equivalent to one of the integers from 0 to $n-1$, and the operations of modular arithmetic modify normal arithmetic by replacing the result of any operation by its equivalent representative. Modular addition, defined in this way for the integers from 0 to $n-1$, forms a group, denoted as Z_n or $(\mathbb{Z}/n\mathbb{Z}, +)$, with 0 as the identity element and $n-a$ as the inverse element of a.



The hours on a clock form a group that uses addition modulo 12. Here, 9 + 4 ≡ 1.

A familiar example is addition of hours on the face of a clock, where 12 rather than 0 is chosen as the representative of the identity. If the hour hand is on 9 and is advanced 4 hours, it ends up on 1, as shown in the illustration. This is expressed by saying that $9+4$ is congruent to 1 "modulo 12" or, in symbols,

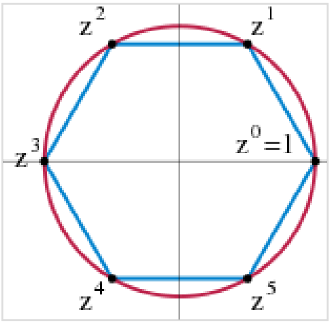
$$9 + 4 \equiv 1 \pmod{12}.$$

For any prime number p, there is also the multiplicative group of integers modulo p.[43] Its elements can be represented by 1 to $p-1$. The group operation, multiplication modulo p, replaces the usual product by its representative, the remainder of division by p. For example, for $p=5$, the four group elements can be represented by $1, 2, 3, 4$. In this group, $4 \cdot 4 \equiv 1 \bmod 5$, because the usual product 16 is equivalent to 1: when divided by 5 it yields a remainder of 1. The primality of p ensures that the usual product of two representatives is not divisible by p, and therefore that the modular product is nonzero.[m] The identity element is represented by 1, and associativity follows from the corresponding property of the integers. Finally, the inverse element axiom requires that given an integer a not divisible by p, there exists an integer b such that

$$a \cdot b \equiv 1 \pmod{p},$$

that is, such that p evenly divides $a \cdot b - 1$. The inverse b can be found by using Bézout's identity and the fact that the greatest common divisor $\gcd(a, p)$ equals 1.[44] In the case $p=5$ above, the inverse of the element represented by 4 is that represented by 4, and the inverse of the element represented by 3 is represented by 2, as $3 \cdot 2 = 6 \equiv 1 \bmod 5$. Hence all group axioms are fulfilled. This example is similar to $(\mathbb{Q} \setminus \{0\}, \cdot)$ above: it consists of exactly those elements in the ring $\mathbb{Z}/p\mathbb{Z}$ that have a multiplicative inverse.[45] These groups, denoted $\mathbb{F}_p^{\times}$, are crucial to public-key cryptography.[n]

Cyclic groups



The 6th complex roots of unity form a cyclic group. z is a primitive element, but z^2 is not, because the odd powers of z are not a power of z^2.

A *cyclic group* is a group all of whose elements are powers of a particular element a.[46] In multiplicative notation, the elements of the group are

$$\dots, a^{-3}, a^{-2}, a^{-1}, a^0, a, a^2, a^3, \dots,$$

where a^2 means $a \cdot a$, a^{-3} stands for $a^{-1} \cdot a^{-1} \cdot a^{-1} = (a \cdot a \cdot a)^{-1}$, etc.[o] Such an element a is called a generator or a primitive element of the group. In additive notation, the requirement for an element to be primitive is that each element of the group can be written as

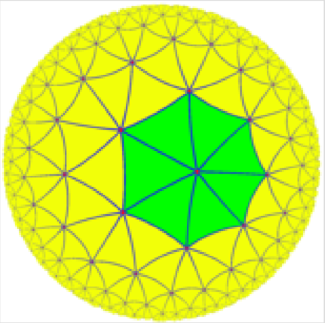
$$\dots, (-a) + (-a), -a, 0, a, a + a, \dots.$$

In the groups $(\mathbb{Z}/n\mathbb{Z}, +)$ introduced above, the element 1 is primitive, so these groups are cyclic. Indeed, each element is expressible as a sum all of whose terms are 1. Any cyclic group with n elements is isomorphic to this group. A second example for cyclic groups is the group of nth complex roots of unity, given by complex numbers z satisfying $z^n = 1$. These numbers can be visualized as the vertices on a regular n-gon, as shown in blue in the image for $n = 6$. The group operation is multiplication of complex numbers. In the picture, multiplying with z corresponds to a counter-clockwise rotation by 60°.[47] From field theory, the group $\mathbb{F}_p^\times$ is cyclic for prime p: for example, if $p = 5$, 3 is a generator since $3^1 = 3$, $3^2 = 9 \equiv 4$, $3^3 \equiv 2$, and $3^4 \equiv 1$.

Some cyclic groups have an infinite number of elements. In these groups, for every non-zero element a, all the powers of a are distinct; despite the name "cyclic group", the powers of the elements do not cycle. An infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$, the group of integers under addition introduced above.[48] As these two prototypes are both abelian, so are all cyclic groups.

The study of finitely generated abelian groups is quite mature, including the fundamental theorem of finitely generated abelian groups; and reflecting this state of affairs, many group-related notions, such as center and commutator, describe the extent to which a given group is not abelian.[49]

Symmetry groups



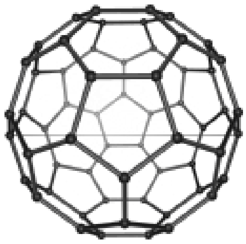
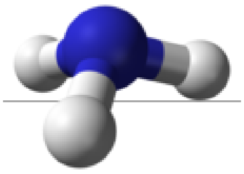
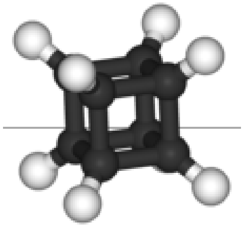
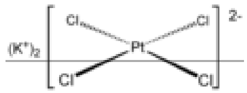
The (2,3,7) triangle group, a hyperbolic reflection group, acts on this tiling of the hyperbolic plane[50]

Symmetry groups are groups consisting of symmetries of given mathematical objects, principally geometric entities, such as the symmetry group of the square given as an introductory example above, although they also arise in algebra such as the symmetries among the roots of polynomial equations dealt with in Galois theory (see below).[51] Conceptually, group theory can be thought of as the study of symmetry.[p] Symmetries in mathematics greatly simplify the study of geometrical or analytical objects. A group is said to act on another mathematical object *X* if every group element can be associated to some operation on *X* and the composition of these operations follows the group law. For example, an element of the (2,3,7) triangle group acts on a triangular tiling of the hyperbolic plane by permuting the triangles.[50] By a group action, the group pattern is connected to the structure of the object being acted on.

In chemistry, point groups describe molecular symmetries, while space groups describe crystal symmetries in crystallography. These symmetries underlie the chemical and physical behavior of these systems, and group theory enables simplification of quantum mechanical analysis of these properties.[52] For example, group theory is used to show that optical transitions between certain quantum levels cannot occur simply because of the symmetry of the states involved.[53]

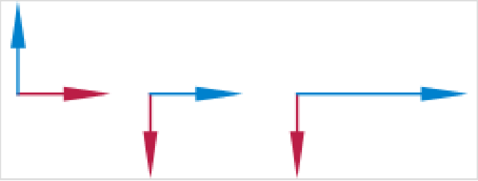
Group theory helps predict the changes in physical properties that occur when a material undergoes a phase transition, for example, from a cubic to a tetrahedral crystalline form. An example is ferroelectric materials, where the change from a paraelectric to a ferroelectric state occurs at the Curie temperature and is related to a change from the high-symmetry paraelectric state to the lower symmetry ferroelectric state, accompanied by a so-called soft phonon mode, a vibrational lattice mode that goes to zero frequency at the transition.[54]

Such spontaneous symmetry breaking has found further application in elementary particle physics, where its occurrence is related to the appearance of Goldstone bosons.[55]

			
Buckminsterfullerene displays icosahedral symmetry[56]	Ammonia, NH_3. Its symmetry group is of order 6, generated by a 120° rotation and a reflection.[57]	Cubane C_8H_8 features octahedral symmetry.[58]	The tetrachloroplatinate(II) ion, $[PtCl_4]^{2-}$ exhibits square-planar geometry

Finite symmetry groups such as the Mathieu groups are used in coding theory, which is in turn applied in error correction of transmitted data, and in CD players.[59] Another application is differential Galois theory, which characterizes functions having antiderivatives of a prescribed form, giving group-theoretic criteria for when solutions of certain differential equations are well-behaved.[q] Geometric properties that remain stable under group actions are investigated in (geometric) invariant theory.[60]

General linear group and representation theory



Two vectors (the left illustration) multiplied by matrices (the middle and right illustrations). The middle illustration represents a clockwise rotation by 90°, while the right-most one stretches the x-coordinate by factor 2.

Matrix groups consist of matrices together with matrix multiplication. The *general linear group* $\mathrm{GL}(n,\mathbb{R})$ consists of all invertible n-by-n matrices with real entries.[61] Its subgroups are referred to as *matrix groups* or *linear groups*. The dihedral group example mentioned above can be viewed as a (very small) matrix group. Another important matrix group is the special orthogonal group $\mathrm{SO}(n)$. It describes all possible rotations in n dimensions. Rotation matrices in this group are used in computer graphics.[62]

Representation theory is both an application of the group concept and important for a deeper understanding of groups.[63][64] It studies the group by its group actions on other spaces. A broad class of group representations are linear representations in which the group acts on a vector space, such as the three-dimensional Euclidean space $\mathbb{R}^3$. A representation of a group G on an n-dimensional real vector space is simply a group homomorphism $\rho : G \to \mathrm{GL}(n,\mathbb{R})$ from the group to the general linear group. This way, the group operation, which may be abstractly given, translates to the multiplication of matrices making it accessible to explicit computations.[r]

A group action gives further means to study the object being acted on.[s] On the other hand, it also yields information about the group. Group representations are an organizing principle in the theory of finite groups, Lie groups, algebraic groups and topological groups, especially (locally) compact groups.[63][65]

Galois groups

Galois groups were developed to help solve polynomial equations by capturing their symmetry features.[66][67] For example, the solutions of the quadratic equation $ax^2 + bx + c = 0$ are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Each solution can be obtained by replacing the $\pm$ sign by $+$ or $-$; analogous formulae are known for cubic and quartic equations, but do *not* exist in general for degree 5 and higher.[68] In the quadratic formula, changing the sign (permuting the resulting two solutions) can be viewed as a (very simple) group operation. Analogous Galois groups act on the solutions of higher-degree polynomial equations and are closely related to the existence of formulas for their solution. Abstract properties of these groups (in particular their solvability) give a criterion for the ability to express the solutions of these polynomials using solely addition, multiplication, and roots similar to the formula above.[69]

Modern Galois theory generalizes the above type of Galois groups by shifting to field theory and considering field extensions formed as the splitting field of a polynomial. This theory establishes—via the fundamental theorem of Galois theory—a precise relationship between fields and groups, underlining once again the ubiquity of groups in mathematics.[70]

Finite groups

A group is called *finite* if it has a finite number of elements. The number of elements is called the order of the group.[71] An important class is the *symmetric groups* S_N, the groups of permutations of N objects. For example, the symmetric group on 3 letters S_3 is the group of all possible reorderings of the objects. The three letters ABC can be reordered into ABC, ACB, BAC, BCA, CAB, CBA, forming in total 6 (factorial of 3) elements. The group operation is composition of these reorderings, and the identity element is the reordering operation that leaves the order unchanged. This class is fundamental insofar as any finite group can be expressed as a subgroup of a symmetric group S_N for a suitable integer N, according to Cayley's theorem. Parallel to the group of symmetries of the square above, S_3 can also be interpreted as the group of symmetries of an equilateral triangle.

The order of an element a in a group G is the least positive integer n such that $a^n = e$, where a^n represents

$$\underbrace{a \cdots a}_{n \text{ factors}},$$

that is, application of the operation "$\cdot$" to n copies of a. (If "$\cdot$" represents multiplication, then a^n corresponds to the nth power of a.) In infinite groups, such an n may not exist, in which case the order of a is said to be infinity. The order of an element equals the order of the cyclic subgroup generated by this element.

More sophisticated counting techniques, for example, counting cosets, yield more precise statements about finite groups: Lagrange's Theorem states that for a finite group G the order of any finite subgroup H divides the order of G. The Sylow theorems give a partial converse.

The dihedral group D_4 of symmetries of a square is a finite group of order 8. In this group, the order of r_1 is 4, as is the order of the subgroup R that this element generates. The order of the reflection elements f_v etc. is 2. Both orders divide 8, as predicted by Lagrange's theorem. The groups $\mathbb{F}_p^\times$ of multiplication modulo a prime p have order $p-1$.

Finite abelian groups

Any finite abelian group is isomorphic to a product of finite cyclic groups; this statement is part of the fundamental theorem of finitely generated abelian groups.

Any group of prime order p is isomorphic to the cyclic group Z_p (a consequence of Lagrange's theorem). Any group of order p^2 is abelian, isomorphic to Z_{p^2} or $\mathrm{Z}_p \times \mathrm{Z}_p$. But there exist nonabelian groups of order p^3; the dihedral group D_4 of order 2^3 above is an example.[72]

Simple groups

When a group G has a normal subgroup N other than $\{1\}$ and G itself, questions about G can sometimes be reduced to questions about N and G/N. A nontrivial group is called *simple* if it has no such normal subgroup. Finite simple groups are to finite groups as prime numbers are to positive integers: they serve as building blocks, in a sense made precise by the Jordan–Hölder theorem.

Classification of finite simple groups

Computer algebra systems have been used to list all groups of order up to 2000.[t] But classifying all finite groups is a problem considered too hard to be solved.

The classification of all finite *simple* groups was a major achievement in contemporary group theory. There are several infinite families of such groups, as well as 26 "sporadic groups" that do not belong to any of the families. The largest sporadic group is called the monster group. The monstrous moonshine conjectures, proved by Richard Borcherds, relate the monster group to certain modular functions.[73]

The gap between the classification of simple groups and the classification of all groups lies in the extension problem.[74]

Groups with additional structure

An equivalent definition of group consists of replacing the "there exist" part of the group axioms by operations whose result is the element that must exist. So, a group is a set G equipped with a binary operation $G \times G \rightarrow G$ (the group operation), a unary operation $G \rightarrow G$ (which provides the inverse) and a nullary operation, which has no operand and results in the identity element. Otherwise, the group axioms are exactly the same. This variant of the definition avoids existential quantifiers and is used in computing with groups and for computer-aided proofs.

This way of defining groups lends itself to generalizations such as the notion of group object in a category. Briefly, this is an object with morphisms that mimic the group axioms.[75]

Topological groups

Some topological spaces may be endowed with a group law. In order for the group law and the topology to interweave well, the group operations must be continuous functions; informally, $g \cdot h$ and g^{-1} must not vary wildly if g and h vary only a little. Such groups are called *topological groups,* and they are the group objects in the category of topological spaces.[76] The most basic examples are the group of real numbers under addition and the group of nonzero real numbers under multiplication. Similar examples can be formed from any other topological field, such as the field of complex numbers or the field of p-adic numbers. These examples are locally compact, so they have Haar measures and can be studied via harmonic analysis. Other locally compact topological groups include the group of points of an algebraic group over a local field or adele ring; these are basic to number theory[77] Galois groups of infinite algebraic field extensions are equipped with the Krull topology, which plays a role in infinite Galois theory.[78] A generalization used in algebraic geometry is the étale fundamental group.[79]

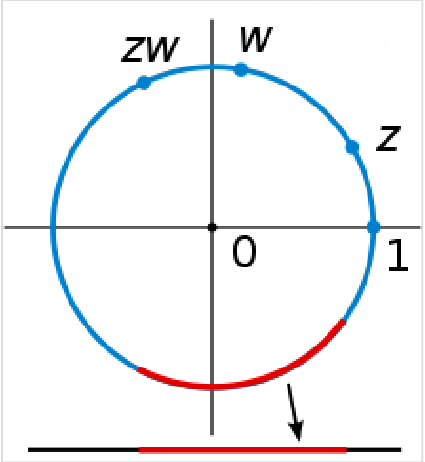
Lie groups

A *Lie group* is a group that also has the structure of a differentiable manifold; informally, this means that it looks locally like a Euclidean space of some fixed dimension.[80] Again, the definition requires the additional structure, here the manifold structure, to be compatible: the multiplication and inverse maps are required to be smooth.

A standard example is the general linear group introduced above: it is an open subset of the space of all n-by-n matrices, because it is given by the inequality

$$\det(A) \neq 0,$$

where A denotes an n-by-n matrix.[81]



The unit circle in the complex plane under complex multiplication is a Lie group and, therefore, a topological group. It is topological since complex multiplication and division are continuous. It is a manifold and thus a Lie group, because every small piece, such as the red arc in the figure, looks like a part of the real line (shown at the bottom).

Lie groups are of fundamental importance in modern physics: Noether's theorem links continuous symmetries to conserved quantities.[82] Rotation, as well as translations in space and time, are basic symmetries of the laws of mechanics. They can, for instance, be used to construct simple models—imposing, say, axial symmetry on a situation will typically lead to significant simplification in the equations one needs to solve to provide a physical description.[u] Another example is the group of Lorentz transformations, which relate measurements of time and velocity of two observers in motion relative to each other. They can be deduced in a purely group-theoretical way, by expressing the transformations as a rotational symmetry of Minkowski space. The latter serves—in the absence of significant gravitation—as a model of spacetime in special relativity.[83] The full symmetry group of Minkowski space, i.e., including translations, is known as the Poincaré group. By the above, it plays a pivotal role in special relativity and, by implication, for quantum field theories.[84] Symmetries that vary with location are central to the modern description of physical interactions with the help of gauge theory. An important example of a gauge theory is the Standard Model, which describes three of the four known fundamental forces and classifies all known elementary particles.[85]

Generalizations

Group-like structures

	Totality[α]	Associativity	Identity	Divisibility[β]	Commutativity
Partial magma	Unneeded	Unneeded	Unneeded	Unneeded	Unneeded
Semigroupoid	Unneeded	Required	Unneeded	Unneeded	Unneeded
Small category	Unneeded	Required	Required	Unneeded	Unneeded
Groupoid	Unneeded	Required	Required	Required	Unneeded
Magma	Required	Unneeded	Unneeded	Unneeded	Unneeded
Quasigroup	Required	Unneeded	Unneeded	Required	Unneeded
Unital magma	Required	Unneeded	Required	Unneeded	Unneeded
Loop	Required	Unneeded	Required	Required	Unneeded
Semigroup	Required	Required	Unneeded	Unneeded	Unneeded

Associative quasigroup	Required	Required	Unneeded	Required	Unneeded
Monoid	Required	Required	Required	Unneeded	Unneeded
Commutative monoid	Required	Required	Required	Unneeded	Required
Group	Required	Required	Required	Required	Unneeded
Abelian group	Required	Required	Required	Required	Required

^α The closure axiom, used by many sources and defined differently, is equivalent.

^β Here, divisibility refers specifically to the quasigroup axioms.

More general structures may be defined by relaxing some of the axioms defining a group.[31][86][87] The table gives a list of several structures generalizing groups.

For example, if the requirement that every element has an inverse is eliminated, the resulting algebraic structure is called a monoid. The natural numbers $\mathbb{N}$ (including zero) under addition form a monoid, as do the nonzero integers under multiplication $(\mathbb{Z}\smallsetminus\{0\},\cdot)$. Adjoining inverses of all elements of the monoid $(\mathbb{Z}\smallsetminus\{0\},\cdot)$ produces a group $(\mathbb{Q}\smallsetminus\{0\},\cdot)$, and likewise adjoining inverses to any (abelian) monoid M produces a group known as the Grothendieck group of M.

A group can be thought of as a small category with one object x in which every morphism is an isomorphism: given such a category, the set $\operatorname{Hom}(x,x)$ is a group; conversely, given a group G, one can build a small category with one object x in which $\operatorname{Hom}(x,x)\simeq G$. More generally, a groupoid is any small category in which every morphism is an isomorphism. In a groupoid, the set of all morphisms in the category is usually not a group, because the composition is only partially defined: fg is defined only when the source of f matches the target of g. Groupoids arise in topology (for instance, the fundamental groupoid) and in the theory of stacks.

Finally, it is possible to generalize any of these concepts by replacing the binary operation with an n-ary operation (i.e., an operation taking n arguments, for some nonnegative integer n). With the proper generalization of the group axioms, this gives a notion of n-ary group.[88]

Examples

Set	Natural numbers **N**		Integers **Z**		Rational numbers **Q** Real numbers **R** Complex numbers **C**				Integers modulo 3 **Z**/3**Z** = {0, 1, 2}	
Operation	+	×	+	×	+	−	×	÷	+	×
Closed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Identity	0	1	0	1	0	N/A	1	N/A	0	1
Inverse	N/A	N/A	−*a*	N/A	−*a*	N/A	1/*a* (*a* ≠ 0)	N/A	0, 2, 1, respectively	N/A, 1, 2, respectively
Associative	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes
Commutative	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes
Structure	monoid	monoid	abelian group	monoid	abelian group	quasi-group	monoid	quasi-group	abelian group	monoid

See also

Mathematics portal

- List of group theory topics

Notes

a. Some authors include an additional axiom referred to as the *closure* under the operation "·", which means that $a \cdot b$ is an element of G for every a and b in G. This condition is subsumed by requiring "$\cdot$" to be a binary operation on G. See Lang 2002.

b. The MathSciNet database of mathematics publications lists 1,779 research papers on group theory and its generalizations written in 2020 alone. See MathSciNet 2021.

c. One usually avoids using fraction notation $\frac{b}{a}$ unless G is abelian, because of the ambiguity of whether it means $a^{-1} \cdot b$ or $b \cdot a^{-1}$.)

d. See, for example, Lang 2002, Lang 2005, Herstein 1996 and Herstein 1975.

e. The word homomorphism derives from Greek ὁμός—the same and μορφή—structure. See Schwartzman 1994, p. 108.

f. However, a group is not determined by its lattice of subgroups. See Suzuki 1951.

g. See the Seifert–Van Kampen theorem for an example.

h. An example is group cohomology of a group which equals the singular cohomology of its classifying space, see Weibel 1994, §8.2.

i. Elements which do have multiplicative inverses are called units, see Lang 2002, p. 84, §II.1.

j. The transition from the integers to the rationals by including fractions is generalized by the field of fractions.

k. The same is true for any field *F* instead of $\mathbb{Q}$. See Lang 2005, p. 86, §III.1.

l. For example, a finite subgroup of the multiplicative group of a field is necessarily cyclic. See Lang 2002, Theorem IV.1.9. The notions of torsion of a module and simple algebras are other instances of this principle.

m. The stated property is a possible definition of prime numbers. See *Prime element*.

n. For example, the Diffie–Hellman protocol uses the discrete logarithm. See Gollmann 2011, §15.3.2.

o. The additive notation for elements of a cyclic group would be $t \cdot a$, where t is in $\mathbb{Z}$.

p. More rigorously, every group is the symmetry group of some graph; see Frucht's theorem, Frucht 1939.

q. More precisely, the monodromy action on the vector space of solutions of the differential equations is considered. See Kuga 1993, pp. 105–113.

r. This was crucial to the classification of finite simple groups, for example. See Aschbacher 2004.

s. See, for example, Schur's Lemma for the impact of a group action on simple modules. A more involved example is the action of an absolute Galois group on étale cohomology.

t. Up to isomorphism, there are about 49 billion groups of order up to 2000. See Besche, Eick & O'Brien 2001.

u. See Schwarzschild metric for an example where symmetry greatly reduces the complexity of physical systems.

Citations

1. Herstein 1975, p. 26, §2.
2. Hall 1967, p. 1, §1.1: "The idea of a group is one which pervades the whole of mathematics both pure and applied."
3. Lang 2005, p. 360, App. 2.
4. Cook 2009, p. 24.
5. Artin 2018, p. 40, §2.2.
6. Lang 2002, p. 3, I.§1 and p. 7, I.§2.
7. Lang 2005, p. 16, II.§1.
8. Herstein 1975, p. 54, §2.6.
9. Wussing 2007.
10. Kleiner 1986.

11. Smith 1906.
12. Galois 1908.
13. Kleiner 1986, p. 202.
14. Cayley 1889.
15. Wussing 2007, §III.2.
16. Lie 1973.
17. Kleiner 1986, p. 204.
18. Wussing 2007, §I.3.4.
19. Jordan 1870.
20. von Dyck 1882.
21. Curtis 2003.
22. Mackey 1976.
23. Borel 2001.
24. Solomon 2018.
25. Ledermann 1953, pp. 4–5, §1.2.
26. Ledermann 1973, p. 3, §I.1.
27. Lang 2005, p. 17, §II.1.
28. Artin 2018, p. 40.
29. Lang 2002, p. 7, §I.2.
30. Lang 2005, p. 34, §II.3.
31. Mac Lane 1998.
32. Lang 2005, p. 19, §II.1.
33. Ledermann 1973, p. 39, §II.12.
34. Lang 2005, p. 41, §II.4.
35. Lang 2002, p. 12, §I.2.
36. Lang 2005, p. 45, §II.4.
37. Lang 2002, p. 9, §I.2.
38. Magnus, Karrass & Solitar 2004, pp. 56–67, §1.6.
39. Hatcher 2002, p. 30, Chapter I.
40. Coornaert, Delzant & Papadopoulos 1990.
41. For example, class groups and Picard groups; see Neukirch 1999, in particular §§I.12 and I.13
42. Seress 1997.
43. Lang 2005, Chapter VII.
44. Rosen 2000, p. 54, (Theorem 2.1).
45. Lang 2005, p. 292, §VIII.1.
46. Lang 2005, p. 22, §II.1.
47. Lang 2005, p. 26, §II.2.
48. Lang 2005, p. 22, §II.1 (example 11).
49. Lang 2002, pp. 26, 29, §I.5.
50. Ellis 2019.
51. Weyl 1952.
52. Conway et al. 2001. See also Bishop 1993
53. Weyl 1950, pp. 197–202.
54. Dove 2003.
55. Zee 2010, p. 228.
56. Chancey & O'Brien 2021, pp. 15, 16.

57. Simons 2003, §4.2.1.
58. Eliel, Wilen & Mander 1994, p. 82.
59. Welsh 1989.
60. Mumford, Fogarty & Kirwan 1994.
61. Lay 2003.
62. Kuipers 1999.
63. Fulton & Harris 1991.
64. Serre 1977.
65. Rudin 1990.
66. Robinson 1996, p. viii.
67. Artin 1998.
68. Lang 2002, Chapter VI (see in particular p. 273 for concrete examples).
69. Lang 2002, p. 292, (Theorem VI.7.2).
70. Stewart 2015, §12.1.
71. Kurzweil & Stellmacher 2004, p. 3.
72. Artin 2018, Proposition 6.4.3. See also Lang 2002, p. 77 for similar results.
73. Ronan 2007.
74. Aschbacher 2004, p. 737.
75. Awodey 2010, §4.1.
76. Husain 1966.
77. Neukirch 1999.
78. Shatz 1972.
79. Milne 1980.
80. Warner 1983.
81. Borel 1991.
82. Goldstein 1980.
83. Weinberg 1972.
84. Naber 2003.
85. Zee 2010.
86. Denecke & Wismath 2002.
87. Romanowska & Smith 2002.
88. Dudek 2001.

References

General references

- Artin, Michael (2018), *Algebra*, Prentice Hall, ISBN 978-0-13-468960-9, Chapter 2 contains an undergraduate-level exposition of the notions covered in this article.
- Cook, Mariana R. (2009), *Mathematicians: An Outer View of the Inner World* (https://books.google.com/books?id=06h8NT77OgMC&q=Richard+Ewen+Borcherds&pg=PA24), Princeton, N.J.: Princeton University Press, ISBN 978-0-691-13951-7
- Hall, G. G. (1967), *Applied Group Theory*, American Elsevier Publishing Co., Inc., New York, MR 0219593 (https://mathscinet.ams.org/mathscinet-getitem?mr=0219593), an elementary introduction.
- Herstein, Israel Nathan (1996), *Abstract Algebra* (3rd ed.), Upper Saddle River, NJ: Prentice Hall Inc., ISBN 978-0-13-374562-7, MR 1375019 (https://mathscinet.ams.org/mathscinet-getitem?mr=1

375019).

- Herstein, Israel Nathan (1975), *Topics in Algebra* (2nd ed.), Lexington, Mass.: Xerox College Publishing, MR 0356988 (https://mathscinet.ams.org/mathscinet-getitem?mr=0356988).
- Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, vol. 211 (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR 1878556 (https://mathscinet.ams.org/mathscinet-getitem?mr=1878556)
- Lang, Serge (2005), *Undergraduate Algebra* (3rd ed.), Berlin, New York: Springer-Verlag, ISBN 978-0-387-22025-3.
- Ledermann, Walter (1953), *Introduction to the Theory of Finite Groups*, Oliver and Boyd, Edinburgh and London, MR 0054593 (https://mathscinet.ams.org/mathscinet-getitem?mr=0054593).
- Ledermann, Walter (1973), *Introduction to Group Theory*, New York: Barnes and Noble, OCLC 795613 (https://www.worldcat.org/oclc/795613).
- Robinson, Derek John Scott (1996), *A Course in the Theory of Groups*, Berlin, New York: Springer-Verlag, ISBN 978-0-387-94461-6.

Special references

- Artin, Emil (1998), *Galois Theory*, New York: Dover Publications, ISBN 978-0-486-62342-9.
- Aschbacher, Michael (2004), "The status of the classification of the finite simple groups" (https://www.ams.org/notices/200407/fea-aschbacher.pdf) (PDF), *Notices of the American Mathematical Society*, **51** (7): 736–740.
- Awodey, Steve (2010), *Category Theory*, Oxford University Press, ISBN 978-0-19-958736-0
- Behler, Florian; Wickleder, Mathias S.; Christoffers, Jens (2014), "Biphenyl and bimesityl tetrasulfonic acid – new linker molecules for coordination polymers", *Arkivoc*, **2015** (2): 64–75, doi:10.3998/ark.5550190.p008.911 (https://doi.org/10.3998%2Fark.5550190.p008.911), hdl:2027/spo.5550190.p008.911 (https://hdl.handle.net/2027%2Fspo.5550190.p008.911)
- Bersuker, Isaac (2006), *The Jahn–Teller Effect* (https://archive.org/details/jahntellereffect0000bers/page/2), Cambridge University Press, ISBN 0-521-82212-2.
- Besche, Hans Ulrich; Eick, Bettina; O'Brien, E. A. (2001), "The groups of order at most 2000" (https://www.ams.org/era/2001-07-01/S1079-6762-01-00087-7/home.html), *Electronic Research Announcements of the American Mathematical Society*, **7**: 1–4, doi:10.1090/S1079-6762-01-00087-7 (https://doi.org/10.1090%2FS1079-6762-01-00087-7), MR 1826989 (https://mathscinet.ams.org/mathscinet-getitem?mr=1826989).
- Bishop, David H. L. (1993), *Group Theory and Chemistry*, New York: Dover Publications, ISBN 978-0-486-67355-4.
- Borel, Armand (1991), *Linear Algebraic Groups*, Graduate Texts in Mathematics, vol. 126 (2nd ed.), Berlin, New York: Springer-Verlag, ISBN 978-0-387-97370-8, MR 1102012 (https://mathscinet.ams.org/mathscinet-getitem?mr=1102012).
- Carter, Roger W. (1989), *Simple Groups of Lie Type*, New York: John Wiley & Sons, ISBN 978-0-471-50683-6.
- Chancey, C. C.; O'Brien, M. C. M. (2021), *The Jahn–Teller Effect in C60 and Other Icosahedral Complexes*, Princeton University Press, ISBN 978-0-691-22534-0
- Conway, John Horton; Delgado Friedrichs, Olaf; Huson, Daniel H.; Thurston, William P. (2001), "On three-dimensional space groups", *Beiträge zur Algebra und Geometrie*, **42** (2): 475–507, arXiv:math.MG/9911185 (https://arxiv.org/abs/math.MG/9911185), MR 1865535 (https://mathscinet.ams.org/mathscinet-getitem?mr=1865535).
- Coornaert, M.; Delzant, T.; Papadopoulos, A. (1990), *Géométrie et théorie des groupes [Geometry and Group Theory]*, Lecture Notes in Mathematics (in French), vol. 1441, Berlin, New York: Springer-Verlag, ISBN 978-3-540-52977-4, MR 1075994 (https://mathscinet.ams.org/mathscinet-getitem?mr=1075994).
- Denecke, Klaus; Wismath, Shelly L. (2002), *Universal Algebra and Applications in Theoretical Computer Science*, London: CRC Press, ISBN 978-1-58488-254-1.

- Dove, Martin T (2003), *Structure and Dynamics: An Atomic View of Materials*, Oxford University Press, p. 265, ISBN 0-19-850678-3.
- Dudek, Wiesław A. (2001), "On some old and new problems in n-ary groups" (https://ibn.idsi.md/sites/default/files/imag_file/15-36_On%20some%20old%20and%20new%20problems%20in%20n-ary%20groups.pdf) (PDF), *Quasigroups and Related Systems*, **8**: 15–36, MR 1876783 (https://mathscinet.ams.org/mathscinet-getitem?mr=1876783).
- Eliel, Ernest; Wilen, Samuel; Mander, Lewis (1994), *Stereochemistry of Organic Compounds*, Wiley, ISBN 978-0-471-01670-0
- Ellis, Graham (2019), "6.4 Triangle groups", *An Invitation to Computational Homotopy*, Oxford University Press, pp. 441–444, doi:10.1093/oso/9780198832973.001.0001 (https://doi.org/10.1093%2Foso%2F9780198832973.001.0001), ISBN 978-0-19-883298-0, MR 3971587 (https://mathscinet.ams.org/mathscinet-getitem?mr=3971587).
- Frucht, R. (1939), "Herstellung von Graphen mit vorgegebener abstrakter Gruppe [Construction of graphs with prescribed group]" (https://web.archive.org/web/20081201083831/http://www.numdam.org/numdam-bin/fitem?id=CM_1939__6__239_0), *Compositio Mathematica* (in German), **6**: 239–50, archived from the original (http://www.numdam.org/numdam-bin/fitem?id=CM_1939__6__239_0) on 2008-12-01.
- Fulton, William; Harris, Joe (1991), *Representation Theory: A First Course*, Graduate Texts in Mathematics, Readings in Mathematics, vol. 129, New York: Springer-Verlag, ISBN 978-0-387-97495-8, MR 1153249 (https://mathscinet.ams.org/mathscinet-getitem?mr=1153249)
- Goldstein, Herbert (1980), *Classical Mechanics* (2nd ed.), Reading, MA: Addison-Wesley Publishing, pp. 588–596, ISBN 0-201-02918-9.
- Gollmann, Dieter (2011), *Computer Security* (2nd ed.), West Sussex, England: John Wiley & Sons, Ltd., ISBN 978-0-470-74115-3
- Hatcher, Allen (2002), *Algebraic Topology* (http://www.math.cornell.edu/~hatcher/AT/ATpage.html), Cambridge University Press, ISBN 978-0-521-79540-1.
- Husain, Taqdir (1966), *Introduction to Topological Groups*, Philadelphia: W.B. Saunders Company, ISBN 978-0-89874-193-3
- Jahn, H.; Teller, E. (1937), "Stability of polyatomic molecules in degenerate electronic states. I. Orbital degeneracy", *Proceedings of the Royal Society A*, **161** (905): 220–235, Bibcode:1937RSPSA.161..220J (https://ui.adsabs.harvard.edu/abs/1937RSPSA.161..220J), doi:10.1098/rspa.1937.0142 (https://doi.org/10.1098%2Frspa.1937.0142).
- Kuipers, Jack B. (1999), *Quaternions and Rotation Sequences: A Primer with Applications to Orbits, Aerospace, and Virtual Reality*, Princeton University Press, Bibcode:1999qrsp.book.....K (https://ui.adsabs.harvard.edu/abs/1999qrsp.book.....K), ISBN 978-0-691-05872-6, MR 1670862 (https://mathscinet.ams.org/mathscinet-getitem?mr=1670862).
- Kuga, Michio (1993), *Galois' Dream: Group Theory and Differential Equations* (https://archive.org/details/galoisdreamgroup0000kuga), Boston, MA: Birkhäuser Boston, ISBN 978-0-8176-3688-3, MR 1199112 (https://mathscinet.ams.org/mathscinet-getitem?mr=1199112).
- Kurzweil, Hans; Stellmacher, Bernd (2004), *The Theory of Finite Groups*, Universitext, Berlin, New York: Springer-Verlag, ISBN 978-0-387-40510-0, MR 2014408 (https://mathscinet.ams.org/mathscinet-getitem?mr=2014408).
- Lay, David (2003), *Linear Algebra and Its Applications*, Addison-Wesley, ISBN 978-0-201-70970-4.
- Mac Lane, Saunders (1998), *Categories for the Working Mathematician* (2nd ed.), Berlin, New York: Springer-Verlag, ISBN 978-0-387-98403-2.
- Magnus, Wilhelm; Karrass, Abraham; Solitar, Donald (2004) [1966], *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations* (https://books.google.com/books?id=1LW4s1RDRHQC&pg=PR2), Courier, ISBN 978-0-486-43830-6
- MathSciNet (2021), *List of papers reviewed on MathSciNet on "Group theory and its generalizations" (MSC code 20), published in 2020* (https://mathscinet.ams.org/mathscinet/search/publications.html?pg4=AUCN&s4=&co4=AND&pg5=TI&s5=&co5=AND&pg6=PC&s6=20&co6=AND&pg7=ALLF&s7=&co7=AND&dr=pubyear&yrop=eq&arg3=2020&yearRangeFirst=&yearRangeSecond=&pg8=ET&s8=All&review_format=html&Submit=Suche), retrieved 14 May 2021

- Michler, Gerhard (2006), *Theory of Finite Simple Groups*, Cambridge University Press, ISBN 978-0-521-86625-5.
- Milne, James S. (1980), *Étale Cohomology* (https://archive.org/details/etalecohomology00miln), Princeton University Press, ISBN 978-0-691-08238-7
- Mumford, David; Fogarty, J.; Kirwan, F. (1994), *Geometric Invariant Theory*, vol. 34 (3rd ed.), Berlin, New York: Springer-Verlag, ISBN 978-3-540-56963-3, MR 1304906 (https://mathscinet.ams.org/mathscinet-getitem?mr=1304906).
- Naber, Gregory L. (2003), *The Geometry of Minkowski Spacetime*, New York: Dover Publications, ISBN 978-0-486-43235-9, MR 2044239 (https://mathscinet.ams.org/mathscinet-getitem?mr=2044239).
- Neukirch, Jürgen (1999), *Algebraic Number Theory*, *Grundlehren der mathematischen Wissenschaften*, vol. 322, Berlin: Springer-Verlag, ISBN 978-3-540-65399-8, MR 1697859 (https://mathscinet.ams.org/mathscinet-getitem?mr=1697859), Zbl 0956.11021 (https://zbmath.org/?format=complete&q=an:0956.11021)
- Romanowska, A. B.; Smith, J. D. H. (2002), *Modes*, World Scientific, ISBN 978-981-02-4942-7.
- Ronan, Mark (2007), *Symmetry and the Monster: The Story of One of the Greatest Quests of Mathematics*, Oxford University Press, ISBN 978-0-19-280723-6.
- Rosen, Kenneth H. (2000), *Elementary Number Theory and its Applications* (4th ed.), Addison-Wesley, ISBN 978-0-201-87073-2, MR 1739433 (https://mathscinet.ams.org/mathscinet-getitem?mr=1739433).
- Rudin, Walter (1990), *Fourier Analysis on Groups*, Wiley Classics, Wiley-Blackwell, ISBN 0-471-52364-X.
- Seress, Ákos (1997), "An Introduction to Computational Group Theory" (https://www.ams.org/notices/199706/seress.pdf) (PDF), *Notices of the American Mathematical Society*, **44** (6): 671–679, MR 1452069 (https://mathscinet.ams.org/mathscinet-getitem?mr=1452069).
- Serre, Jean-Pierre (1977), *Linear Representations of Finite Groups* (https://archive.org/details/linearrepresenta1977serr), Berlin, New York: Springer-Verlag, ISBN 978-0-387-90190-9, MR 0450380 (https://mathscinet.ams.org/mathscinet-getitem?mr=0450380).
- Schwartzman, Steven (1994), *The Words of Mathematics: An Etymological Dictionary of Mathematical Terms Used in English*, Mathematical Association of America, ISBN 978-0-88385-511-9.
- Shatz, Stephen S. (1972), *Profinite Groups, Arithmetic, and Geometry*, Princeton University Press, ISBN 978-0-691-08017-8, MR 0347778 (https://mathscinet.ams.org/mathscinet-getitem?mr=0347778)
- Simons, Jack (2003), *An Introduction to Theoretical Chemistry*, Cambridge University Press, ISBN 978-0-521-53047-7
- Solomon, Ronald (2018), "The classification of finite simple groups: A progress report", *Notices of the AMS*, **65** (6): 1, doi:10.1090/noti1689 (https://doi.org/10.1090%2Fnoti1689)
- Stewart, Ian (2015), *Galois Theory* (4th ed.), CRC Press, ISBN 978-1-4822-4582-0
- Suzuki, Michio (1951), "On the lattice of subgroups of finite groups", *Transactions of the American Mathematical Society*, **70** (2): 345–371, doi:10.2307/1990375 (https://doi.org/10.2307%2F1990375), JSTOR 1990375 (https://www.jstor.org/stable/1990375).
- Warner, Frank (1983), *Foundations of Differentiable Manifolds and Lie Groups*, Berlin, New York: Springer-Verlag, ISBN 978-0-387-90894-6.
- Weibel, Charles A. (1994), *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, ISBN 978-0-521-55987-4, MR 1269324 (https://mathscinet.ams.org/mathscinet-getitem?mr=1269324), OCLC 36131259 (https://www.worldcat.org/oclc/36131259)
- Weinberg, Steven (1972), *Gravitation and Cosmology* (https://archive.org/details/gravitationcosmo00stev_0), New York: John Wiley & Sons, ISBN 0-471-92567-5.
- Welsh, Dominic (1989), *Codes and Cryptography*, Oxford: Clarendon Press, ISBN 978-0-19-853287-3.
- Weyl, Hermann (1952), *Symmetry*, Princeton University Press, ISBN 978-0-691-02374-8.

- Zee, A. (2010), *Quantum Field Theory in a Nutshell* (second ed.), Princeton, N.J.: Princeton University Press, ISBN 978-0-691-14034-6, OCLC 768477138 (https://www.worldcat.org/oclc/768477138)

Historical references

- Borel, Armand (2001), *Essays in the History of Lie Groups and Algebraic Groups*, Providence, R.I.: American Mathematical Society, ISBN 978-0-8218-0288-5
- Cayley, Arthur (1889), *The Collected Mathematical Papers of Arthur Cayley* (http://www.hti.umich.edu/cgi/t/text/pageviewer-idx?c=umhistmath;cc=umhistmath;rgn=full%20text;idno=ABS3153.0001.001;didno=ABS3153.0001.001;view=image;seq=00000140), vol. II (1851–1860), Cambridge University Press.
- O'Connor, John J.; Robertson, Edmund F., "The development of group theory" (https://mathshistory.st-andrews.ac.uk/HistTopics/Development_group_theory.html), *MacTutor History of Mathematics Archive*, University of St Andrews
- Curtis, Charles W. (2003), *Pioneers of Representation Theory: Frobenius, Burnside, Schur, and Brauer*, History of Mathematics, Providence, R.I.: American Mathematical Society, ISBN 978-0-8218-2677-5.
- von Dyck, Walther (1882), "Gruppentheoretische Studien (Group-theoretical studies)" (https://web.archive.org/web/20140222213905/http://gdz.sub.uni-goettingen.de/index.php?id=11&PPN=PPN235181684_0020&DMDID=DMDLOG_0007&L=1), *Mathematische Annalen* (in German), **20** (1): 1–44, doi:10.1007/BF01443322 (https://doi.org/10.1007%2FBF01443322), S2CID 179178038 (https://api.semanticscholar.org/CorpusID:179178038), archived from the original (http://gdz.sub.uni-goettingen.de/index.php?id=11&PPN=PPN235181684_0020&DMDID=DMDLOG_0007&L=1) on 2014-02-22.
- Galois, Évariste (1908), Tannery, Jules (ed.), *Manuscrits de Évariste Galois [Évariste Galois' Manuscripts]* (http://quod.lib.umich.edu/cgi/t/text/text-idx?c=umhistmath;idno=AAN9280) (in French), Paris: Gauthier-Villars (Galois work was first published by Joseph Liouville in 1843).
- Jordan, Camille (1870), *Traité des substitutions et des équations algébriques [Study of Substitutions and Algebraic Equations]* (https://archive.org/details/traitdessubstit00jordgoog) (in French), Paris: Gauthier-Villars.
- Kleiner, Israel (1986), "The evolution of group theory: A brief survey", *Mathematics Magazine*, **59** (4): 195–215, doi:10.2307/2690312 (https://doi.org/10.2307%2F2690312), JSTOR 2690312 (https://www.jstor.org/stable/2690312), MR 0863090 (https://mathscinet.ams.org/mathscinet-getitem?mr=0863090).
- Lie, Sophus (1973), *Gesammelte Abhandlungen. Band 1 [Collected papers. Volume 1]* (in German), New York: Johnson Reprint Corp., MR 0392459 (https://mathscinet.ams.org/mathscinet-getitem?mr=0392459).
- Mackey, George Whitelaw (1976), *The Theory of Unitary Group Representations*, University of Chicago Press, MR 0396826 (https://mathscinet.ams.org/mathscinet-getitem?mr=0396826)
- Smith, David Eugene (1906), *History of Modern Mathematics* (https://www.gutenberg.org/ebooks/8746), Mathematical Monographs, No. 1.
- Weyl, Hermann (1950) [1931], *The Theory of Groups and Quantum Mechanics*, translated by Robertson, H. P., Dover, ISBN 978-0-486-60269-1.
- Wussing, Hans (2007), *The Genesis of the Abstract Group Concept: A Contribution to the History of the Origin of Abstract Group Theory*, New York: Dover Publications, ISBN 978-0-486-45868-7.

External links

- Weisstein, Eric W., "Group" (https://mathworld.wolfram.com/Group.html), *MathWorld*

Retrieved from "https://en.wikipedia.org/w/index.php?title=Group_(mathematics)&oldid=1197404287"