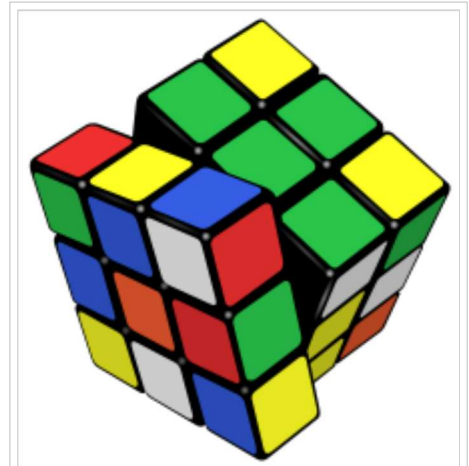


# Group (mathematics)

From Wikipedia, the free encyclopedia

In mathematics, a **group** is an algebraic structure consisting of a set together with an operation that combines any two of its elements to form a third element. To qualify as a group, the set and the operation must satisfy a few conditions called group axioms, namely closure, associativity, identity and invertibility. Many familiar mathematical structures such as number systems obey these axioms: for example, the integers endowed with the addition operation form a group. However, the abstract formalization of the group axioms, detached as it is from the concrete nature of any particular group and its operation, allows entities with highly diverse mathematical origins in abstract algebra and beyond to be handled in a flexible way, while retaining their essential structural aspects. The ubiquity of groups in numerous areas within and outside mathematics makes them a central organizing principle of contemporary mathematics.<sup>[1][2]</sup>



The possible manipulations of this Rubik's Cube form a group.

Groups share a fundamental kinship with the notion of symmetry. A symmetry group encodes symmetry features of a geometrical object: it consists of the set of transformations that leave the object unchanged, and the operation of combining two such transformations by performing one after the other. Such symmetry groups, particularly the continuous Lie groups, play an important role in many academic disciplines. Matrix groups, for example, can be used to understand fundamental physical laws underlying special relativity and symmetry phenomena in molecular chemistry.

The concept of a group arose from the study of polynomial equations, starting with Évariste Galois in the 1830s. After contributions from other fields such as number theory and geometry, the group notion was generalized and firmly established around 1870. Modern group theory—a very active mathematical discipline—studies groups in their own right.<sup>a[>]</sup> 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 (its group representations), both from a theoretical and a computational point of view. A particularly rich theory has been developed for finite groups, which culminated with the monumental classification of finite simple groups completed in 1983. Since the mid-1980s, geometric group theory, which studies finitely generated groups as geometric objects, has become a particularly active area in group theory.

## Contents

- 1 Definition and illustration
  - 1.1 First example: the integers
  - 1.2 Definition
  - 1.3 Second example: a symmetry group
- 2 History
- 3 Elementary consequences of the group axioms
  - 3.1 Uniqueness of identity element and inverses
  - 3.2 Division
- 4 Basic concepts
  - 4.1 Group homomorphisms

- 4.2 Subgroups
  - 4.3 Cosets
  - 4.4 Quotient groups
- 5 Examples and applications
  - 5.1 Numbers
  - 5.2 Cyclic groups
  - 5.3 Symmetry groups
  - 5.4 General linear group and representation theory
  - 5.5 Galois groups
- 6 Finite groups
  - 6.1 Classification of finite simple groups
- 7 Groups with additional structure
  - 7.1 Topological groups
  - 7.2 Lie groups
- 8 Generalizations
- 9 See also
- 10 Notes
  - 10.1 Citations
- 11 References
  - 11.1 General references
  - 11.2 Special references
  - 11.3 Historical references

## Definition and illustration

### First example: the integers

One of the most familiar groups is the set of integers **Z** which consists of the numbers

..., −4, −3, −2, −1, 0, 1, 2, 3, 4, ...<sup>[3]</sup>

The following properties of integer addition serve as a model for the abstract group axioms given in the definition below.

1. For any two integers  $a$  and  $b$ , the sum  $a + b$  is also an integer. In other words, the process of adding integers two at a time always yields an integer, not some other type of number such as a fraction. This property is known as *closure* under addition.
2. For all integers  $a$ ,  $b$  and  $c$ ,  $(a + b) + c = a + (b + c)$ . 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  $c$ , a property known as *associativity*.
3. If  $a$  is any integer, then  $0 + a = a + 0 = a$ . Zero is called the *identity element* of addition because adding it to any integer returns the same integer.
4. For every integer  $a$ , there is an integer  $b$  such that  $a + b = b + a = 0$ . 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 abstract definition is developed.

### Definition

A group is a set,  $G$ , together with an operation  $\bullet$  (called the **group law** of  $G$ ) that combines any two elements  $a$  and  $b$  to form another element, denoted  $a \bullet b$  or  $ab$ . To qualify as a group, the set and operation,  $(G, \bullet)$ , must satisfy four requirements known as the **group axioms**.<sup>[4]</sup>

#### Closure

For all  $a, b$  in  $G$ , the result of the operation,  $a \bullet b$ , is also in  $G$ .<sup>b[>]</sup>

#### Associativity

For all  $a, b$  and  $c$  in  $G$ ,  $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ .

#### Identity element

There exists an element  $e$  in  $G$ , such that for every element  $a$  in  $G$ , the equation  $e \bullet a = a \bullet e = a$  holds.

The identity element of a group  $G$  is often written as  $1$  or  $1_G$ ,<sup>[5]</sup> a notation inherited from the multiplicative identity.

#### Inverse element

For each  $a$  in  $G$ , there exists an element  $b$  in  $G$  such that  $a \bullet b = b \bullet a = 1_G$ .

The order in which the group operation is carried out can be significant. In other words, the result of combining element  $a$  with element  $b$  need not yield the same result as combining element  $b$  with element  $a$ ; the equation

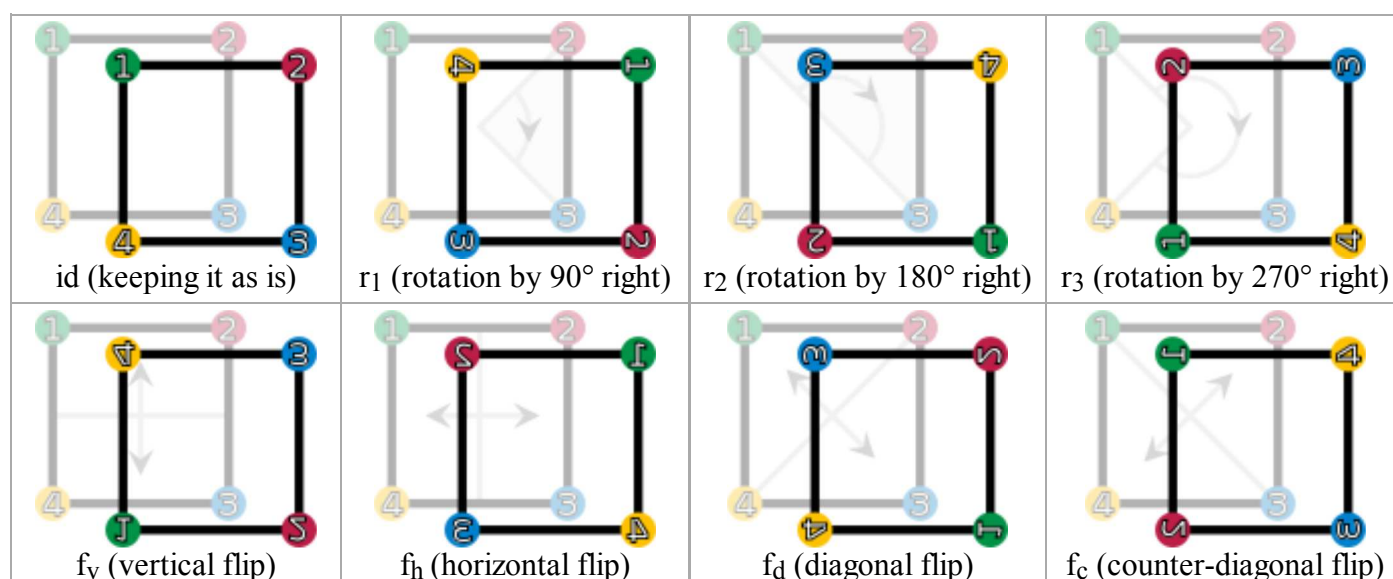
$$a \bullet b = b \bullet a$$

may not always be true. This equation does always hold in the group of integers under addition, because  $a + b = b + a$  for any two integers (commutativity of addition). However, it does not always hold in the symmetry group below. Groups for which the equation  $a \bullet b = b \bullet a$  always holds are called *abelian* (in honor of Niels Abel). Thus, the integer addition group is abelian, but the following symmetry group is not.

The set  $G$  is called the *underlying set* of the group  $(G, \bullet)$ . Often the group's underlying set  $G$  is used as a short name for the group  $(G, \bullet)$ . Along the same lines, sometimes a shorthand expression such as "a subset of the group  $G$ " is used when what is actually meant is "a subset of the underlying set  $G$  of the group  $(G, \bullet)$ ." Usually, it is clear from the context whether a symbol like  $G$  refers to a group or to an underlying set.

## Second example: a symmetry group

The symmetries (i.e., rotations and reflections) of a square form a group called a dihedral group, and denoted  $D_4$ .<sup>[6]</sup> The following symmetries occur:



The elements of the symmetry group of the square ( $D_4$ ). The vertices are colored and numbered only to visualize the operations.

- the identity operation leaving everything unchanged, denoted  $\text{id}$ ;
- rotations of the square by  $90^\circ$  right,  $180^\circ$  right, and  $270^\circ$  right, denoted by  $r_1$ ,  $r_2$  and  $r_3$ , respectively;
- reflections about the vertical and horizontal middle line ( $f_h$  and  $f_v$ ), or through the two diagonals ( $f_d$  and  $f_c$ ).

The defining operation of this group is function composition: The eight symmetries are functions from the square to the square, and 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

$b \cdot a$  ("apply the symmetry  $b$  after performing the symmetry  $a$ "). The right-to-left notation is the same notation that is used for composition of functions.

The group table on the right lists the results of all such compositions possible. For example, rotating by  $270^\circ$  right ( $r_3$ ) and then flipping 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:

$$f_h \cdot r_3 = f_d.$$

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

1. The closure axiom demands that the composition  $b \cdot a$  of any two symmetries  $a$  and  $b$  is also a symmetry. Another example for the group operation is

$$r_3 \cdot f_h = f_c,$$

i.e. rotating  $270^\circ$  right after flipping horizontally equals flipping 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.

2. The associativity constraint 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  $a$ . The associativity condition

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

means that these two ways are the same, i.e., a product of many group elements can be simplified in any order. For example,  $(f_d \cdot f_v) \cdot r_2 = f_d \cdot (f_v \cdot r_2)$  can be checked using the group table at the right

$$(f_d \cdot f_v) \cdot r_2 = r_3 \cdot r_2 = r_1, \text{ which equals}$$

$$f_d \cdot (f_v \cdot r_2) = f_d \cdot f_h = r_1.$$

While associativity is true for the symmetries of the square and addition of numbers, it is not true for all operations. For instance, subtraction of numbers is not associative:  $(7 - 3) - 2 = 2$  is not the same as  $7 - (3 - 2) = 6$ .

3. The identity element is the symmetry  $\text{id}$  leaving everything unchanged: for any symmetry  $a$ , performing  $\text{id}$  after  $a$  (or  $a$  after  $\text{id}$ ) equals  $a$ , in symbolic form,

$$\text{id} \cdot a = a,$$

$$a \cdot \text{id} = a.$$

**Group table of  $D_4$**

•	id	r <sub>1</sub>	r <sub>2</sub>	r <sub>3</sub>	f <sub>v</sub>	f <sub>h</sub>	f <sub>d</sub>	f <sub>c</sub>
id	id	r <sub>1</sub>	r <sub>2</sub>	r <sub>3</sub>	f <sub>v</sub>	f <sub>h</sub>	f <sub>d</sub>	f <sub>c</sub>
r <sub>1</sub>	r <sub>1</sub>	r <sub>2</sub>	r <sub>3</sub>	id	f <sub>c</sub>	f <sub>d</sub>	f <sub>v</sub>	f <sub>h</sub>
r <sub>2</sub>	r <sub>2</sub>	r <sub>3</sub>	id	r <sub>1</sub>	f <sub>h</sub>	f <sub>v</sub>	f <sub>c</sub>	f <sub>d</sub>
r <sub>3</sub>	r <sub>3</sub>	id	r <sub>1</sub>	r <sub>2</sub>	f <sub>d</sub>	f <sub>c</sub>	f <sub>h</sub>	f <sub>v</sub>
f <sub>v</sub>	f <sub>v</sub>	f <sub>d</sub>	f <sub>h</sub>	f <sub>c</sub>	id	r <sub>2</sub>	r <sub>1</sub>	r <sub>3</sub>
f <sub>h</sub>	f <sub>h</sub>	f <sub>c</sub>	f <sub>v</sub>	f <sub>d</sub>	r <sub>2</sub>	id	r <sub>3</sub>	r <sub>1</sub>
f <sub>d</sub>	f <sub>d</sub>	f <sub>h</sub>	f <sub>c</sub>	f <sub>v</sub>	r <sub>3</sub>	r <sub>1</sub>	id	r <sub>2</sub>
f <sub>c</sub>	f <sub>c</sub>	f <sub>v</sub>	f <sub>d</sub>	f <sub>h</sub>	r <sub>1</sub>	r <sub>3</sub>	r <sub>2</sub>	id

The elements  $\text{id}$ ,  $r_1$ ,  $r_2$ , and  $r_3$  form a subgroup, highlighted in red (upper left region). A left and right coset of this subgroup is highlighted in green (in the last row) and yellow (last column), respectively.

4. An inverse element undoes the transformation of some other element. Every symmetry can be undone: each of transformations—identity  $\text{id}$ , the flips  $f_h$ ,  $f_v$ ,  $f_d$ ,  $f_c$  and the  $180^\circ$  rotation  $r_2$ —is its own inverse, because performing each one twice brings the square back to its original orientation. The rotations  $r_3$  and  $r_1$  are each other's inverse, because rotating  $90^\circ$  and then rotation  $270^\circ$  (or vice versa) yields a rotation over  $360^\circ$  which leaves the square unchanged. In symbols,

$$f_h \cdot f_h = \text{id},$$

$$r_3 \cdot r_1 = r_1 \cdot r_3 = \text{id}.$$

In contrast to the group of integers above, where the order of the operation is irrelevant, it does matter in  $D_4$ :  $f_h \cdot r_1 = f_c$  but  $r_1 \cdot f_h = f_d$ . In other words,  $D_4$  is not abelian, which makes the group structure more difficult than the integers introduced first.

## History

*Main article: History of group theory*

The modern concept of an abstract group developed out of several fields of mathematics.<sup>[7][8][9]</sup> 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' ideas were rejected by his contemporaries, and published only posthumously.<sup>[10][11]</sup> 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.<sup>[12]</sup>

Geometry was a second field in which groups were used systematically, especially symmetry groups as part of Felix Klein's 1872 Erlangen program.<sup>[13]</sup> 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.<sup>[14]</sup>

The third field contributing to group theory was number theory. Certain abelian group structures had been used implicitly in Carl Friedrich Gauss' number-theoretical work *Disquisitiones Arithmeticae* (1798), and more explicitly by Leopold Kronecker.<sup>[15]</sup> In 1847, Ernst Kummer led early attempts to prove Fermat's Last Theorem to a climax by developing groups describing factorization into prime numbers.<sup>[16]</sup>

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).<sup>[17]</sup> Walther von Dyck (1882) gave the first statement of the modern definition of an abstract group.<sup>[18]</sup> 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.<sup>[19]</sup> The theory of Lie groups, and more generally locally compact groups was pushed by Hermann Weyl, Élie Cartan and many others.<sup>[20]</sup> Its algebraic counterpart, the theory of algebraic groups, was first shaped by Claude Chevalley (from the late 1930s) and later by pivotal work of Armand Borel and Jacques Tits.<sup>[21]</sup>

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, classified all finite simple groups in 1982. This project exceeded previous mathematical endeavours by its sheer size, in both length of proof and number of researchers. Research is ongoing to simplify the proof of this classification.<sup>[22]</sup> These days, group theory is still a highly

active mathematical branch crucially impacting many other fields.<sup>a[>]</sup>

## Elementary consequences of the group axioms

*Main article: Elementary group theory*

Basic facts about all groups that can be obtained directly from the group axioms are commonly subsumed under *elementary group theory*.<sup>[23]</sup> For example, repeated applications of the associativity axiom show that the unambiguity of

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

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.<sup>[24]</sup>

The axioms may be weakened to assert only the existence of a left identity and left inverses. Both can be shown to be actually two-sided, so the resulting definition is equivalent to the one given above.<sup>[25]</sup>

### Uniqueness of identity element and inverses

Two important consequences of the group axioms are the uniqueness of the identity element and the uniqueness of inverse elements. There can be only one identity element in a group, and each element in a group has exactly one inverse element. Thus, it is customary to speak of *the* identity, and *the* inverse of an element.<sup>[26]</sup>

To prove the uniqueness of an inverse element of  $a$ , suppose that  $a$  has two inverses, denoted  $l$  and  $r$ , in a group  $(G, \bullet)$ . Then

$$\begin{aligned} l &= l \bullet I_G && \text{as } I_G \text{ is the identity element} \\ &= l \bullet (a \bullet r) && \text{because } r \text{ is an inverse of } a, \text{ so } I_G = a \bullet r \\ &= (l \bullet a) \bullet r && \text{by associativity, which allows to rearrange the parentheses} \\ &= I_G \bullet r && \text{since } l \text{ is an inverse of } a, \text{ i.e. } l \bullet a = I_G \\ &= r && \text{for } I_G \text{ is the identity element} \end{aligned}$$

The two extremal terms  $l$  and  $r$  are equal, since they are connected by a chain of equalities. In other words there is only one inverse element of  $a$ . Similarly, to prove that the identity element of a group is unique, assume  $G$  is a group with two identity elements  $I_G$  and  $e$ . Then  $I_G = I_G \bullet e = e$ , hence  $I_G$  and  $e$  are equal.

### Division

In groups, it is possible to perform division: given elements  $a$  and  $b$  of the group  $G$ , there is exactly one solution  $x$  in  $G$  to the equation  $x \bullet a = b$ .<sup>[26]</sup> In fact, right multiplication of the equation by  $a^{-1}$  gives the solution  $x = x \bullet a \bullet a^{-1} = b \bullet a^{-1}$ . Similarly there is exactly one solution  $y$  in  $G$  to the equation  $a \bullet y = b$ , namely  $y = a^{-1} \bullet b$ . In general,  $x$  and  $y$  need not agree.

A consequence of this is that multiplying by a group element  $g$  is a bijection. Specifically, if  $g$  is an element of the group  $G$ , there is a bijection from  $G$  to itself called **left translation by  $g$**  sending  $h \in G$  to  $g \bullet h$ . Similarly, **right translation by  $g$**  is a bijection from  $G$  to itself sending  $h$  to  $h \bullet g$ . If  $G$  is abelian, left and right translation by a group element are the same.

## Basic concepts

*Further information: Glossary of group theory*

To understand groups beyond the level of mere symbolic manipulations as above, more structural concepts have to be employed.<sup>c[>]</sup> There is a conceptual principle underlying all of the following notions: to take advantage of the structure offered by groups (which sets, being "structureless", do not have), constructions related to groups have to be *compatible* with the group operation. This compatibility manifests itself in the following notions in various ways. For example, groups can be related to each other via functions called group homomorphisms. By the mentioned principle, they are required to respect the group structures in a precise sense. The structure of groups can also be understood by breaking them into pieces called subgroups and quotient groups. The principle of "preserving structures"—a recurring topic in mathematics throughout—is an instance of working in a category, in this case the category of groups.<sup>[27]</sup>

## Group homomorphisms

*Main article: Group homomorphism*

*Group homomorphisms*<sup>g[>]</sup> are functions that preserve group structure. A function  $a: G \rightarrow H$  between two groups  $(G, \bullet)$  and  $(H, *)$  is a homomorphism if the equation

$$a(g \bullet k) = a(g) * a(k)$$

holds for all elements  $g, k$  in  $G$ . In other words, the result is the same when performing the group operation after or before applying the map  $a$ . This requirement ensures that  $a(1_G) = 1_H$ , and also  $a(g)^{-1} = a(g^{-1})$  for all  $g$  in  $G$ . Thus a group homomorphism respects all the structure of  $G$  provided by the group axioms.<sup>[28]</sup>

Two groups  $G$  and  $H$  are called isomorphic if there exist group homomorphisms  $a: G \rightarrow H$  and  $b: H \rightarrow G$ , such that applying the two functions one after another (in each of the two possible orders) equal the identity function of  $G$  and  $H$ , respectively. That is,  $a(b(h)) = h$  and  $b(a(g)) = g$  for any  $g$  in  $G$  and  $h$  in  $H$ . From an abstract point of view, isomorphic groups carry the same information. For example, proving that  $g \bullet g = 1_G$  for some element  $g$  of  $G$  is equivalent to proving that  $a(g) \bullet a(g) = 1_H$ , because applying  $a$  to the first equality yields the second, and applying  $b$  to the second gives back the first.

## Subgroups

*Main article: Subgroup*

Informally, a *subgroup* is a group  $H$  contained within a bigger one,  $G$ .<sup>[29]</sup> Concretely, the identity element of  $G$  is contained in  $H$ , and whenever  $h_1$  and  $h_2$  are in  $H$ , then so are  $h_1 \bullet h_2$  and  $h_1^{-1}$ , so the elements of  $H$ , equipped with the group operation on  $G$  restricted to  $H$ , indeed form a group.

In the example above, the identity and the rotations constitute a subgroup  $R = \{\text{id}, r_1, r_2, r_3\}$ , highlighted in red in the group table above: any two rotations composed are still a rotation, and a rotation can be undone by (i.e. is inverse to) the complementary rotations  $270^\circ$  for  $90^\circ$ ,  $180^\circ$  for  $180^\circ$ , and  $90^\circ$  for  $270^\circ$  (note that rotation in the opposite direction is not defined). The subgroup test is a necessary and sufficient condition for a subset  $H$  of a group  $G$  to be a subgroup: it is sufficient to check that  $g^{-1}h \in H$  for all elements  $g, h \in H$ . Knowing the subgroups is important in understanding the group as a whole.<sup>d[>]</sup>

Given any subset  $S$  of a group  $G$ , the subgroup generated by  $S$  consists of products of elements of  $S$  and their inverses. It is the smallest subgroup of  $G$  containing  $S$ .<sup>[30]</sup> In the introductory example above, the subgroup generated by  $r_2$  and  $f_v$  consists of these two elements, the identity element  $\text{id}$  and  $f_h = f_v \bullet r_2$ . 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

*Main article: Coset*

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  $D_4$  above, once a flip is performed, the square never gets back to the  $r_2$  configuration by just applying the rotation operations (and no further flips), i.e. the rotation operations are irrelevant to the question whether a flip has been performed. Cosets are used to formalize this insight: a subgroup  $H$  defines left and right cosets, which can be thought of as translations of  $H$  by arbitrary group elements  $g$ . In symbolic terms, the *left* and *right coset* of  $H$  containing  $g$  are

$$gH = \{g \cdot h, h \in H\} \text{ and } Hg = \{h \cdot g, h \in H\}, \text{ respectively.}^{[31]}$$

The 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.<sup>[32]</sup> The first case  $g_1H = g_2H$  happens precisely when  $g_1^{-1} \cdot g_2 \in H$ , i.e. if the two elements differ by an element of  $H$ . Similar considerations apply to the right cosets of  $H$ . The left and right cosets of  $H$  may or may not be equal. If they are, i.e. for all  $g$  in  $G$ ,  $gH = Hg$ , then  $H$  is said to be a *normal subgroup*. One may then simply refer to  $N$  as the set of cosets.

In  $D_4$ , the introductory symmetry group, the left cosets  $gR$  of the subgroup  $R$  consisting of the rotations are either equal to  $R$ , if  $g$  is an element of  $R$  itself, or otherwise equal to  $U = f_cR = \{f_c, f_v, f_d, f_h\}$  (highlighted in green). The subgroup  $R$  is also normal, because  $f_cR = U = Rf_c$  and similarly for any element other than  $f_c$ .

## Quotient groups

*Main article: Quotient group*

In addition to disregarding the internal structure of a subgroup by considering its cosets, it is desirable to endow this coarser entity with a group law called *quotient group* or *factor group*. For this to be possible, the subgroup has to be normal. Given any normal subgroup  $N$ , the quotient group is defined by

$$G / N = \{gN, g \in G\}, \text{ "G modulo N".}^{[33]}$$

This set inherits a group operation (sometimes called coset multiplication, or coset addition) from the original group  $G$ :  $(gN) \cdot (hN) = (gh)N$  for all  $g$  and  $h$  in  $G$ . This definition is motivated by the idea (itself an instance of general structural considerations outlined above) that the map  $G \rightarrow G / N$  that associates to any element  $g$  its coset  $gN$  be a group homomorphism, or by general abstract considerations called universal properties. The coset  $eN = N$  serves as the identity in this group, and the inverse of  $gN$  in the quotient group is

$$(gN)^{-1} = (g^{-1})N.^{e[3]}$$

The elements of the quotient group  $D_4 / R$  are  $R$  itself, which represents the identity, and  $U = f_vR$ . The group operation on the quotient is shown at the right. For example,  $U \cdot U = f_vR \cdot f_vR = (f_v \cdot f_v)R = R$ . Both the subgroup  $R = \{\text{id}, r_1, r_2, r_3\}$ , as well as the corresponding quotient are abelian, whereas  $D_4$  is not abelian. Building bigger groups by smaller ones, such as  $D_4$  from its subgroup  $R$  and the quotient  $D_4 / R$  is abstracted by a notion called semidirect product.

<b>•</b>	<b>R</b>	<b>U</b>
<b>R</b>	$R$	$U$
<b>U</b>	$U$	$R$
Group table of the quotient group $D_4 / R$ .		

Quotient and subgroups together form a way of describing every group by its *presentation*: any group is the quotient of the free group over the *generators* of the group, quotiented by the subgroup of *relations*. The dihedral group  $D_4$ , for example, can be generated by two elements  $r$  and  $f$  (for example,  $r = r_1$ , the right rotation and  $f = f_v$  the vertical (or any other) flip), which means that every symmetry of the square is a finite



composition of these two symmetries or their inverses. Together with the relations

$$r^4 = f^2 = (r \cdot f)^2 = 1,^{[34]}$$

the group is completely described. A presentation of a group can also be used to construct the Cayley graph, a device used to graphically capture discrete groups.

Sub- and quotient groups are related in the following way: a subset  $H$  of  $G$  can be seen as an injective map  $H \rightarrow G$ , i.e. any element of the target has at most one element that maps to it. The counterpart to injective maps are surjective maps (every element of the target is mapped onto), such as the canonical map  $G \rightarrow G/N.^{[35]}$  Interpreting subgroup and quotients in light of these homomorphisms emphasizes the structural concept inherent to these definitions alluded to in the introduction. In general, homomorphisms are neither injective nor surjective. Kernel and image of group homomorphisms and the first isomorphism theorem address this phenomenon.

## Examples and applications

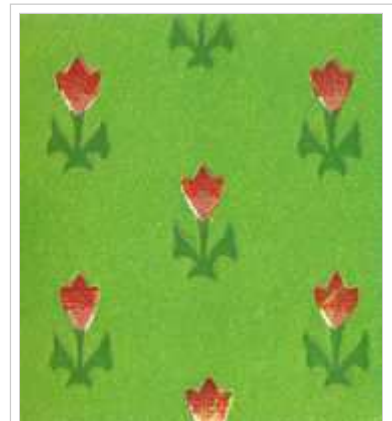
*Main articles: Examples of groups and Applications of group theory*

Examples and applications of groups abound. A starting point is the group  $\mathbf{Z}$  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.

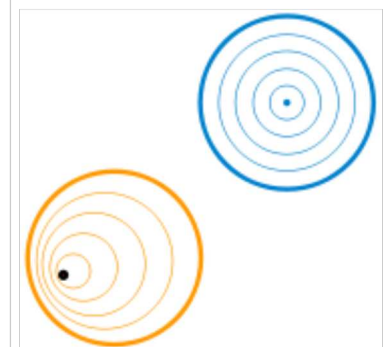
Groups are also applied in many other mathematical areas. Mathematical objects are often examined by associating groups to them and studying the properties of the corresponding groups. For example, Henri Poincaré founded what is now called algebraic topology by introducing the fundamental group.<sup>[35]</sup> By means of this connection, topological properties such as proximity and continuity translate into properties of groups.<sup>i[36]</sup> For example, elements of the fundamental group are represented by loops. The second image at the right shows some loops in a plane minus a point. The blue loop is considered null-homotopic (and thus irrelevant), because it can be continuously shrunk to a point. The presence of the hole prevents the orange loop from being shrunk to a point. The fundamental group of the plane with a point deleted turns out to be infinite cyclic, generated by the orange loop (or any other loop winding once around the hole). This way, the fundamental group detects the hole.

In more recent applications, the influence has also been reversed to motivate geometric constructions by a group-theoretical background.<sup>j[37]</sup> In a similar vein, geometric group theory employs geometric concepts, for example in the study of hyperbolic groups.<sup>[36]</sup> Further branches crucially applying groups include algebraic geometry and number theory.<sup>[37]</sup>

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.<sup>[38]</sup> 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.

## 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  $\mathbf{Z}$  under addition, denoted  $(\mathbf{Z}, +)$ , has been described above. The integers, with the operation of multiplication instead of addition,  $(\mathbf{Z}, \cdot)$  do *not* form a group. The closure, 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  $b = 1/2$ , which is a rational number, but not an integer. Hence not every element of  $\mathbf{Z}$  has a (multiplicative) inverse.<sup>k[>]</sup>

## 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.<sup>l[>]</sup> The set of all such fractions is commonly denoted  $\mathbf{Q}$ . There is still a minor obstacle for  $(\mathbf{Q}, \cdot)$ , the rationals with multiplication, being a group: because the rational number 0 does not have a multiplicative inverse (i.e., there is no  $x$  such that  $x \cdot 0 = 1$ ),  $(\mathbf{Q}, \cdot)$  is still not a group.

However, the set of all *nonzero* rational numbers  $\mathbf{Q} \setminus \{0\} = \{q \in \mathbf{Q}, q \neq 0\}$  does form an abelian group under multiplication, denoted  $(\mathbf{Q} \setminus \{0\}, \cdot)$ .<sup>m[>]</sup> 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 0) also form a group under addition. Intertwining addition and multiplication operations yields more complicated structures called rings and—if division is possible, such as in  $\mathbf{Q}$ —fields, which occupy a central position in abstract algebra. Group theoretic arguments therefore underlie parts of the theory of those entities.<sup>n[>]</sup>

## Nonzero integers modulo a prime

For any prime number  $p$ , modular arithmetic furnishes the multiplicative group of integers modulo  $p$ .<sup>[39]</sup> Its elements are integers not divisible by  $p$ , considered modulo  $p$ , i.e. two numbers are considered equivalent if their difference is divisible by  $p$ . For example, if  $p = 5$ , there are exactly four group elements 1, 2, 3, 4: multiples of 5 are excluded and 6 and  $-4$  are both equivalent to 1 etc. The group operation is given by multiplication. Therefore,  $4 \cdot 4 = 1$ , because the usual product 16 is equivalent to 1, for 5 divides  $16 - 1 = 15$ , denoted

$$16 \equiv 1 \pmod{5}.$$

The primality of  $p$  ensures that the product of two integers neither of which is divisible by  $p$  is not divisible by  $p$  either, hence the indicated set of classes is closed under multiplication.<sup>o[>]</sup> The identity element is 1, as usual for a multiplicative group, and the associativity follows from the corresponding property of integers.

Finally, the inverse element axiom requires that given an integer  $a$  not divisible by  $p$ , there exists an integer  $b$  such that

$$a \cdot b \equiv 1 \pmod{p}, \text{ i.e. } p \text{ divides the difference } a \cdot b - 1.$$

The inverse  $b$  can be found by using Bézout's identity and the fact that the greatest common divisor  $\gcd(a, p)$  equals 1.<sup>[40]</sup> In the case  $p = 5$  above, the inverse of 4 is 4, and the inverse of 3 is 2, as  $3 \cdot 2 = 6 \equiv 1 \pmod{5}$ . Hence all group axioms are fulfilled. Actually, this example is similar to  $(\mathbf{Q} \setminus \{0\}, \cdot)$  above, because it turns out to be the multiplicative group of nonzero elements in the finite field  $\mathbf{F}_p$ , denoted  $\mathbf{F}_p^\times$ .<sup>[41]</sup> These groups are crucial to public-key cryptography.<sup>p[✓]</sup>

## Cyclic groups

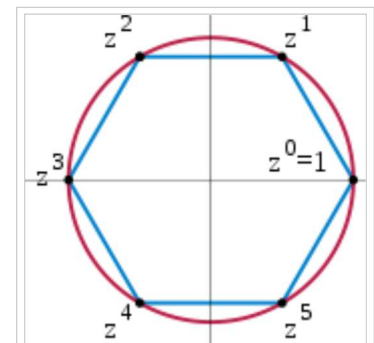
*Main articles: Cyclic group and Abelian group*

A *cyclic group* is a group all of whose elements are powers (when the group operation is written additively, the term 'multiple' can be used) of a particular element  $a$ .<sup>[42]</sup> In multiplicative notation, the elements of the group are:

$$..., a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, ...,$$

where  $a^2$  means  $a \cdot a$ , and  $a^{-3}$  stands for  $a^{-1} \cdot a^{-1} \cdot a^{-1} = (a \cdot a \cdot a)^{-1}$  etc.<sup>h[✓]</sup> Such an element  $a$  is called a generator or a primitive element of the group.

A typical example for this class of groups is the group of  $n$ -th complex roots of unity, given by complex numbers  $z$  satisfying  $z^n = 1$  (and whose operation is multiplication).<sup>[43]</sup> Any cyclic group with  $n$  elements is isomorphic to this group. Using some field theory, the group  $\mathbf{F}_p^\times$  can be shown to be cyclic: for example, if  $p = 5$ , 3 is a generator since  $3^1 = 3$ ,  $3^2 = 9 \equiv 4$ ,  $3^3 \equiv 2$ , and  $3^4 \equiv 1$ .



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  $z^2$ .

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  $(\mathbf{Z}, +)$ , the group of integers under addition introduced above.<sup>[44]</sup> As these two prototypes are both abelian, so is any cyclic group.

The study of 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.<sup>[45]</sup>

## Symmetry groups

*Main article: Symmetry group*

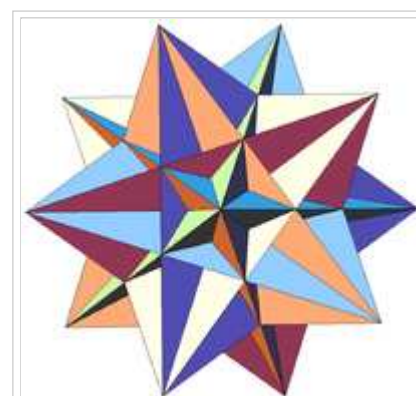
*See also: Molecular symmetry, Space group, and Symmetry in physics*

*Symmetry groups* are groups consisting of symmetries of given mathematical objects—be they of geometric nature, such as the introductory symmetry group of the square, or of algebraic nature, such as polynomial equations and their solutions.<sup>[46]</sup> Conceptually, group theory can be thought of as the study of symmetry.<sup>t[✓]</sup> 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 performs some operation on  $X$  compatibly to the group law. In the rightmost example below, an element of order 7 of the  $(2,3,7)$  triangle group acts on the tiling by permuting the highlighted warped triangles (and the other ones, too). By a group action, the group

pattern is connected to the structure of the object being acted on.

In chemical fields, such as crystallography, space groups and point groups describe molecular symmetries and crystal symmetries. These symmetries underlie the chemical and physical behavior of these systems, and group theory enables simplification of quantum mechanical analysis of these properties.<sup>[47]</sup> 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.

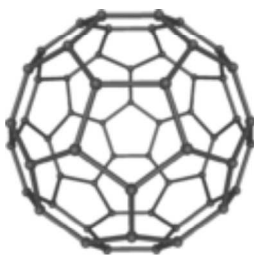
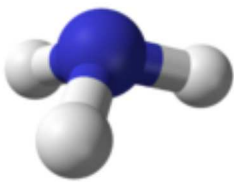

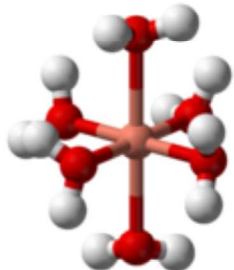
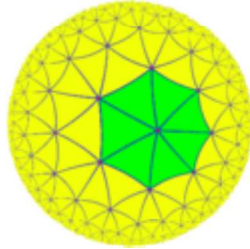
Not only are groups useful to assess the implications of symmetries in molecules, but surprisingly they also predict that molecules sometimes can change symmetry. The Jahn-Teller effect is a distortion of a molecule of high symmetry when it adopts a particular ground state of lower symmetry from a set of possible ground states that are related to each other by the symmetry operations of the molecule.<sup>[48][49]</sup>



Rotations and flips form the symmetry group of a great icosahedron.

Likewise, 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.<sup>[50]</sup>

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

				
Buckminsterfullerene displays icosahedral symmetry.	Ammonia, NH <sub>3</sub> . Its symmetry group is of order 6, generated by a 120° rotation and a reflection.	Cubane C <sub>8</sub> H <sub>8</sub> features octahedral symmetry.	Hexaaquacopper(II) complex ion, [Cu(OH <sub>2</sub> ) <sub>6</sub> ] <sup>2+</sup> . Compared to a perfectly symmetrical shape, the molecule is vertically dilated by about 22% (Jahn-Teller effect).	The (2,3,7) triangle group, a hyperbolic group, acts on this tiling of the hyperbolic plane.

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.<sup>[51]</sup> 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.<sup>[52]</sup> Geometric properties that remain stable under group actions are investigated in (geometric) invariant theory.<sup>[52]</sup>

## General linear group and representation theory

*Main articles: General linear group and Representation theory*

Matrix groups consist of matrices together with matrix multiplication. The *general linear group*  $GL(n, \mathbf{R})$  consists of all invertible  $n$ -by- $n$  matrices with real entries.<sup>[53]</sup> 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  $SO(n)$ . It describes all possible rotations in  $n$  dimensions. Via Euler angles, rotation matrices are used in computer graphics.<sup>[54]</sup>

*Representation theory* is both an application of the group concept and important for a deeper understanding of groups.

<sup>[55][56]</sup> It studies the group by its group actions on other spaces.

A broad class of group representations are linear representations, i.e. the group is acting on a vector space, such as the three-dimensional Euclidean space  $\mathbf{R}^3$ . A representation of  $G$  on an  $n$ -dimensional real vector space is simply a group homomorphism

$$\rho: G \rightarrow GL(n, \mathbf{R})$$

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.<sup>w[>]</sup>

Given a group action, this gives further means to study the object being acted on.<sup>x[>]</sup> 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.<sup>[55][57]</sup>

## Galois groups

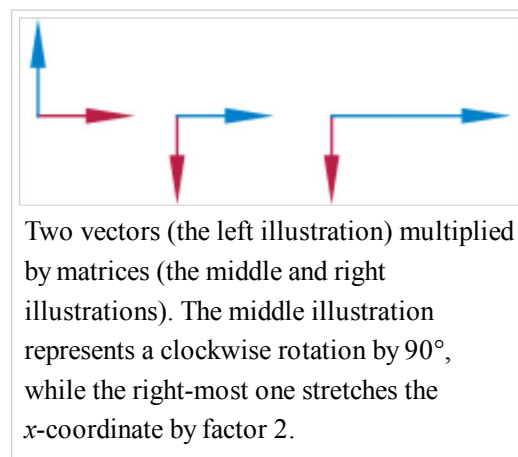
*Main article: Galois group*

*Galois groups* have been developed to help solve polynomial equations by capturing their symmetry features.<sup>[58][59]</sup> For example, the solutions of the quadratic equation  $ax^2 + bx + c = 0$  are given by

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

Exchanging "+" and "-" in the expression, i.e. permuting the two solutions of the equation can be viewed as a (very simple) group operation. Similar formulae are known for cubic and quartic equations, but do *not* exist in general for degree 5 and higher.<sup>[60]</sup> Abstract properties of Galois groups associated with polynomials (in particular their solvability) give a criterion for polynomials that have all their solutions expressible by radicals, i.e. solutions expressible using solely addition, multiplication, and roots similar to the formula above.<sup>[61]</sup>

The problem can be dealt with by shifting to field theory and considering the splitting field of a polynomial. Modern Galois theory generalizes the above type of Galois groups to field extensions and establishes—via the fundamental theorem of Galois theory—a precise relationship between fields and groups, underlining once again the ubiquity of groups in mathematics.



## Finite groups

*Main article: Finite group*

A group is called *finite* if it has a finite number of elements. The number of elements is called the order of the group  $G$ .<sup>[62]</sup> An important class is the *symmetric groups*  $S_N$ , the groups of permutations of  $N$  letters. For example, the symmetric group on 3 letters  $S_3$  is the group consisting of all possible swaps of the three letters  $ABC$ , i.e. contains the elements  $ABC$ ,  $ACB$ , ..., up to  $CBA$ , in total 6 (or 3 factorial) elements. 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  $N$  (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

$$\underbrace{a \cdot \cdots \cdot a}_n,$$

$n$  factors

i.e. application of the operation  $\cdot$  to  $n$  copies of  $a$ . (If  $\cdot$  represents multiplication, then  $a^n$  corresponds to the  $n^{\text{th}}$  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 (discussed above) is a finite group of order 8. The order of  $r_1$  is 4, as is the order of the subgroup  $R$  it generates (see above). The order of the reflection elements  $f_v$  etc. is 2. Both orders divide 8, as predicted by Lagrange's Theorem. The groups  $\mathbf{F}_p^\times$  above have order  $p - 1$ .

## Classification of finite simple groups

*Main article: Classification of finite simple groups*

Mathematicians often strive for a complete classification (or list) of a mathematical notion. In the context of finite groups, this aim quickly leads to difficult and profound mathematics. According to Lagrange's theorem, finite groups of order  $p$ , a prime number, are necessarily cyclic (abelian) groups  $\mathbf{Z}_p$ . Groups of order  $p^2$  can also be shown to be abelian, a statement which does not generalize to order  $p^3$ , as the non-abelian group  $D_4$  of order  $8 = 2^3$  above shows.<sup>[63]</sup> Computer algebra systems can be used to list small groups, but there is no classification of all finite groups.<sup>[q]</sup> An intermediate step is the classification of finite simple groups.<sup>[r]</sup> A nontrivial group is called *simple* if its only normal subgroups are the trivial group and the group itself.<sup>[s]</sup> The Jordan–Hölder theorem exhibits finite simple groups as the building blocks for all finite groups.<sup>[64]</sup> Listing all finite simple groups was a major achievement in contemporary group theory. 1998 Fields Medal winner Richard Borcherds succeeded to prove the monstrous moonshine conjectures, a surprising and deep relation of the largest finite simple sporadic group—the "monster group"—with certain modular functions, a piece of classical complex analysis, and string theory, a theory supposed to unify the description of many physical phenomena.<sup>[65]</sup>

## Groups with additional structure

Many groups are simultaneously groups and examples of other mathematical structures. In the language of category theory, they are group objects in a category, meaning that they are objects (that is, examples of



another mathematical structure) which come with transformations (called morphisms) that mimic the group axioms. For example, every group (as defined above) is also a set, so a group is a group object in the category of sets.

## Topological groups

*Main article: Topological group*

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, that is,  $g \cdot h$ , and  $g^{-1}$  must not vary wildly if  $g$  and  $h$  vary only little. Such groups are called *topological groups*, and they are the group objects in the category of topological spaces.<sup>[66]</sup> The most basic examples are the reals **R** under addition,  $(\mathbf{R} \setminus \{0\}, \cdot)$ , and similarly with any other topological field such as the complex numbers or  $p$ -adic numbers. All of these groups are locally compact, so they have Haar measures and can be studied via harmonic analysis. The former offer an abstract formalism of invariant integrals. Invariance means, in the case of real numbers for example:

$$\int f(x) dx = \int f(x + c) dx$$

for any constant  $c$ . Matrix groups over these fields fall under this regime, as do adèle rings and adelic algebraic groups, which are basic to number theory.<sup>[67]</sup> Galois groups of infinite field extensions such as the absolute Galois group can also be equipped with a topology, the so-called Krull topology, which in turn is central to generalize the above sketched connection of fields and groups to infinite field extensions.<sup>[68]</sup> An advanced generalization of this idea, adapted to the needs of algebraic geometry, is the étale fundamental group.<sup>[69]</sup>

## Lie groups

*Main article: Lie group*

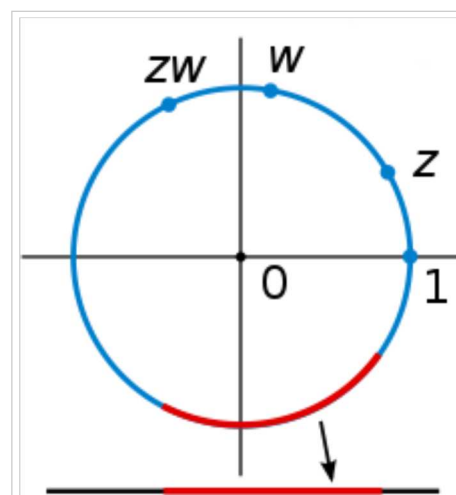
*Lie groups* (in honor of Sophus Lie) are groups which also have a manifold structure, i.e. they are spaces looking locally like some Euclidean space of the appropriate dimension.<sup>[70]</sup> Again, the additional structure, here the manifold structure, has to be compatible, i.e. the maps corresponding to multiplication and the inverse have 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.<sup>[71]</sup>

Lie groups are of fundamental importance in physics: Noether's theorem links continuous symmetries to conserved quantities.<sup>[72]</sup> 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



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).

physical description.<sup>v[t]</sup> Another example are the 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 space time in special relativity.<sup>[73]</sup> 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.<sup>[74]</sup> Symmetries that vary with location are central to the modern description of physical interactions with the help of gauge theory.<sup>[75]</sup>

## Generalizations

In abstract algebra, more general structures are defined by relaxing some of the axioms defining a group.

<sup>[27]</sup><sup>[76]</sup><sup>[77]</sup> For example, if the requirement that every element has an inverse is eliminated, the resulting algebraic structure is called a monoid. The natural numbers **N** (including 0) under addition form a monoid, as do the nonzero integers under multiplication (**Z** \ {0}, ·), see above. There is a general method to formally add inverses to elements to any (abelian) monoid, much the same way as (**Q** \ {0}, ·) is derived from (**Z** \ {0}, ·), known as the Grothendieck group. Groupoids are similar to groups except that the composition *a* • *b* need not be defined for all *a* and *b*. They arise in the study of more complicated forms of symmetry, often in topological and analytical structures, such as the fundamental groupoid or stacks. Finally, it is possible to generalize any of these concepts by replacing the binary operation with an arbitrary *n*-ary one (i.e. an operation taking *n* arguments). With the proper generalization of the group axioms this gives rise to an *n*-ary group.<sup>[78]</sup> The table gives a list of several structures generalizing groups.

Group-like structures				
	Totality	Associativity	Identity	Inverses
<b>Group</b>	Yes	Yes	Yes	Yes
<b>Monoid</b>	Yes	Yes	Yes	No
<b>Semigroup</b>	Yes	Yes	No	No
<b>Loop</b>	Yes	No	Yes	Yes
<b>Quasigroup</b>	Yes	No	No	No
<b>Magma</b>	Yes	No	No	No
<b>Groupoid</b>	No	Yes	Yes	Yes
<b>Category</b>	No	Yes	Yes	No

## See also

- Abelian group
- Group ring
- Group algebra
- Euclidean group
- Free group
- Finitely presented group
- Fundamental group
- Non-abelian group
- Grothendieck group
- Symmetry in physics

## Notes

**<sup>^</sup> a:** Mathematical Reviews lists 3,224 research papers on group theory and its generalizations written in 2005.

**<sup>^</sup> b:** The closure axiom is already implied by the condition that • be a binary operation. Some authors therefore omit this axiom. Lang 2002

**<sup>^</sup> c:** See, for example, the books of Lang (2002, 2005) and Herstein (1996, 1975).

**<sup>^</sup> d:** However, a group is not determined by its lattice of subgroups. See Suzuki 1951.

**<sup>^</sup> e:** The fact that the group operation extends this canonically is an instance of a universal property.

**<sup>^</sup> f:** For example, if *G* is finite, then the size of any subgroup and any quotient group divides the size of *G*, according to Lagrange's theorem.

**<sup>^</sup> g:** The word homomorphism derives from Greek ὁμός—the same and μορφή—structure.

**<sup>^</sup> h:** The additive notation for elements of a cyclic group would be *t* • *a*, *t* in **Z**.



- ^ **i**: See the Seifert–van Kampen theorem for an example.
- ^ **j**: An example is group cohomology of a group which equals the singular homology of its classifying space.
- ^ **k**: Elements which do have multiplicative inverses are called units, see Lang 2002, §II.1, p. 84.
- ^ **l**: The transition from the integers to the rationals by adding fractions is generalized by the quotient field.
- ^ **m**: The same is true for any field  $F$  instead of  $\mathbf{Q}$ . See Lang 2005, §III.1, p. 86.
- ^ **n**: 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.
- ^ **o**: The stated property is a possible definition of prime numbers. See prime element.
- ^ **p**: For example, the Diffie-Hellman protocol uses the discrete logarithm.
- ^ **q**: The groups of order at most 2000 are known. Up to isomorphism, there are about 49 billion. See Besche, Eick & O'Brien 2001.
- ^ **r**: The gap between the classification of simple groups and the one of all groups lies in the extension problem, a problem too hard to be solved in general. See Aschbacher 2004, p. 737.
- ^ **s**: Equivalently, a nontrivial group is simple if its only quotient groups are the trivial group and the group itself. See Michler 2006, Carter 1989.
- ^ **t**: More rigorously, every group is the symmetry group of some graph; see Frucht's theorem, Frucht 1939.
- ^ **u**: More precisely, the monodromy action on the vector space of solutions of the differential equations is considered. See Kuga 1993, pp. 105–113.
- ^ **v**: See Schwarzschild metric for an example where symmetry greatly reduces the complexity of physical systems.
- ^ **w**: This was crucial to the classification of finite simple groups, for example. See Aschbacher 2004.
- ^ **x**: 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.
- ^ **y**: Injective and surjective maps correspond to mono- and epimorphisms, respectively. They are interchanged when passing to the dual category.

## Citations

1. ^ Herstein 1975, §2, p. 26
2. ^ Hall 1967, §1.1, p. 1: "The idea of a group is one which pervades the whole of mathematics both pure and applied."
3. ^ Lang 2005, App. 2, p. 360
4. ^ Herstein 1975, §2.1, p. 27
5. ^ Weisstein, Eric W., "Identity Element (<http://mathworld.wolfram.com/IdentityElement.html>) " from MathWorld.
6. ^ Herstein 1975, §2.6, p. 54
7. ^ Wussing 2007
8. ^ Kleiner 1986
9. ^ Smith 1906
10. ^ Galois 1908
11. ^ Kleiner 1986, p. 202
12. ^ Cayley 1889
13. ^ Wussing 2007, §III.2
14. ^ Lie 1973
15. ^ Kleiner 1986, p. 204
16. ^ Wussing 2007, §I.3.4
17. ^ Jordan 1870
18. ^ von Dyck 1882
19. ^ Curtis 2003
20. ^ Mackey 1976
21. ^ Borel 2001
22. ^ Aschbacher 2004
23. ^ Ledermann 1953, §1.2, pp. 4–5
24. ^ Ledermann 1973, §I.1, p. 3

25. ^ Lang 2002, §I.2, p. 7
26. ^ <sup>a b</sup> Lang 2005, §II.1, p. 17
27. ^ <sup>a b</sup> Mac Lane 1998
28. ^ Lang 2005, §II.3, p. 34
29. ^ Lang 2005, §II.1, p. 19
30. ^ Ledermann 1973, §II.12, p. 39
31. ^ Lang 2005, §II.4, p. 41
32. ^ Lang 2002, §I.2, p. 12
33. ^ Lang 2005, §II.4, p. 45
34. ^ Lang 2002, §I.2, p. 9
35. ^ Hatcher 2002, Chapter I, p. 30
36. ^ Coornaert, Delzant & Papadopoulos 1990
37. ^ for example, class groups and Picard groups; see Neukirch 1999, in particular §§I.12 and I.13
38. ^ Seress 1997
39. ^ Lang 2005, Chapter VII
40. ^ Rosen 2000, p. 54 (Theorem 2.1)
41. ^ Lang 2005, §VIII.1, p. 292
42. ^ Lang 2005, §II.1, p. 22
43. ^ Lang 2005, §II.2, p. 26
44. ^ Lang 2005, §II.1, p. 22 (example 11)
45. ^ Lang 2002, §I.5, p. 26, 29
46. ^ Weyl 1952
47. ^ Conway, Delgado Friedrichs & Huson et al. 2001. See also Bishop 1993
48. ^ Bersuker, Isaac (2006), *The Jahn-Teller Effect*, Cambridge University Press, p. 2, ISBN 0-521-82212-2
49. ^ Jahn & Teller 1937
50. ^ Dove, Martin T (2003), *Structure and Dynamics: an atomic view of materials*, Oxford University Press, p. 265, ISBN 0-19-850678-3
51. ^ Welsh 1989
52. ^ Mumford, Fogarty & Kirwan 1994
53. ^ Lay 2003
54. ^ Kuipers 1999
55. ^ <sup>a b</sup> Fulton & Harris 1991
56. ^ Serre 1977
57. ^ Rudin 1990
58. ^ Robinson 1996, p. viii
59. ^ Artin 1998
60. ^ Lang 2002, Chapter VI (see in particular p. 273 for concrete examples)
61. ^ Lang 2002, p. 292 (Theorem VI.7.2)
62. ^ Kurzweil & Stellmacher 2004
63. ^ Artin 1991, Theorem 6.1.14. See also Lang 2002, p. 77 for similar results.
64. ^ Lang 2002, §I. 3, p. 22
65. ^ Ronan 2007
66. ^ Husain 1966
67. ^ Neukirch 1999
68. ^ Shatz 1972
69. ^ Milne 1980
70. ^ Warner 1983
71. ^ Borel 1991
72. ^ Goldstein 1980
73. ^ Weinberg 1972
74. ^ Naber 2003
75. ^ Becchi 1997
76. ^ Denecke & Wismath 2002
77. ^ Romanowska & Smith 2002
78. ^ Dudek 2001

## References

## General references

- Artin, Michael (1991), *Algebra*, Prentice Hall, ISBN 978-0-89871-510-1, Chapter 2 contains an undergraduate-level exposition of the notions covered in this article.
- Devlin, Keith (2000), *The Language of Mathematics: Making the Invisible Visible*, Owl Books, ISBN 978-0-8050-7254-9, Chapter 5 provides a layman-accessible explanation of groups.
- Fulton, William; Harris, Joe (1991), *Representation theory. A first course*, Graduate Texts in Mathematics, Readings in Mathematics, **129**, New York: Springer-Verlag, ISBN 978-0-387-97495-8, MR1153249 (<http://www.ams.org/mathscinet-getitem?mr=1153249>) , ISBN 978-0-387-97527-6.
- Hall, G. G. (1967), *Applied group theory*, American Elsevier Publishing Co., Inc., New York, MR0219593 (<http://www.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, MR1375019 (<http://www.ams.org/mathscinet-getitem?mr=1375019>) .
- Herstein, Israel Nathan (1975), *Topics in algebra* (2nd ed.), Lexington, Mass.: Xerox College Publishing, MR0356988 (<http://www.ams.org/mathscinet-getitem?mr=0356988>) .
- Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR1878556 (<http://www.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, MR0054593 (<http://www.ams.org/mathscinet-getitem?mr=0054593>) .
- Ledermann, Walter (1973), *Introduction to group theory*, New York: Barnes and Noble, OCLC 795613 (<http://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" (<http://www.ams.org/notices/200407/fea-aschbacher.pdf>) (PDF), *Notices of the American Mathematical Society* **51** (7): 736–740, <http://www.ams.org/notices/200407/fea-aschbacher.pdf>.
- Becchi, C. (1997), *Introduction to Gauge Theories*, arXiv:hep-ph/9705211 (<http://arxiv.org/abs/hep-ph/9705211>) .
- Besche, Hans Ulrich; Eick, Bettina; O'Brien, E. A. (2001), "The groups of order at most 2000" (<http://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 (<http://dx.doi.org/10.1090%2FS1079-6762-01-00087-7>) , MR1826989 (<http://www.ams.org/mathscinet-getitem?mr=1826989>) , <http://www.ams.org/era/2001-07-01/S1079-6762-01-00087-7/home.html>.
- 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, **126** (2nd ed.), Berlin, New York: Springer-Verlag, ISBN 978-0-387-97370-8, MR1102012 (<http://www.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.
- 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 (<http://arxiv.org/abs/math.MG/9911185>) , MR1865535 (<http://www.ams.org/mathscinet-getitem?mr=1865535>) .
- **(French)** Coornaert, M.; Delzant, T.; Papadopoulos, A. (1990), *Géométrie et théorie des groupes [Geometry and Group Theory]*, Lecture Notes in Mathematics, **1441**, Berlin, New York: Springer-

Verlag, ISBN 978-3-540-52977-4, MR1075994 (<http://www.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.
- Dudek, W.A. (2001), "On some old problems in  $n$ -ary groups" (<http://www.quasigroups.eu/contents/contents8.php?m=trzeci>) , *Quasigroups and Related Systems* **8**: 15–36, <http://www.quasigroups.eu/contents/contents8.php?m=trzeci>.
- **(German)** Frucht, R. (1939), "Herstellung von Graphen mit vorgegebener abstrakter Gruppe [Construction of Graphs with Prescribed Group ([http://www.numdam.org/numdam-bin/fitem?id=CM\\_1939\\_\\_6\\_\\_239\\_0](http://www.numdam.org/numdam-bin/fitem?id=CM_1939__6__239_0))"] , *Compositio Mathematica* **6**: 239–50, [http://www.numdam.org/numdam-bin/fitem?id=CM\\_1939\\_\\_6\\_\\_239\\_0](http://www.numdam.org/numdam-bin/fitem?id=CM_1939__6__239_0).
- Goldstein, Herbert (1980), *Classical Mechanics* (2nd ed.), Reading, MA: Addison-Wesley Publishing, pp. 588–596, ISBN 0-201-02918-9.
- Hatcher, Allen (2002), *Algebraic topology* (<http://www.math.cornell.edu/~hatcher/AT/ATpage.html>) , Cambridge University Press, ISBN 978-0-521-79540-1, <http://www.math.cornell.edu/~hatcher/AT/ATpage.html>.
- 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 of London. Series A, Mathematical and Physical Sciences (1934–1990)* **161** (905): 220–235, doi:10.1098/rspa.1937.0142 (<http://dx.doi.org/10.1098/rspa.1937.0142>) .
- Kuipers, Jack B. (1999), *Quaternions and rotation sequences—A primer with applications to orbits, aerospace, and virtual reality*, Princeton University Press, ISBN 978-0-691-05872-6, MR1670862 (<http://www.ams.org/mathscinet-getitem?mr=1670862>) .
- Kuga, Michio (1993), *Galois' dream: group theory and differential equations*, Boston, MA: Birkhäuser Boston, ISBN 978-0-8176-3688-3, MR1199112 (<http://www.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, MR2014408 (<http://www.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.
- Michler, Gerhard (2006), *Theory of finite simple groups*, Cambridge University Press, ISBN 978-0-521-86625-5.
- Milne, James S. (1980), *Étale cohomology*, Princeton University Press, ISBN 978-0-691-08238-7
- Mumford, David; Fogarty, J.; Kirwan, F. (1994), *Geometric invariant theory*, **34** (3rd ed.), Berlin, New York: Springer-Verlag, ISBN 978-3-540-56963-3, MR1304906 (<http://www.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, MR2044239 (<http://www.ams.org/mathscinet-getitem?mr=2044239>) .
- Neukirch, Jürgen (1999), *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, **322**, Berlin: Springer-Verlag, ISBN 978-3-540-65399-8, MR1697859 (<http://www.ams.org/mathscinet-getitem?mr=1697859>) .
- 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, MR1739433 (<http://www.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" (<http://www.math.ohio->

state.edu/~akos/notices.ps) , *Notices of the American Mathematical Society* **44** (6): 671–679, MR1452069 (<http://www.ams.org/mathscinet-getitem?mr=1452069>) , <http://www.math.ohio-state.edu/~akos/notices.ps>.

- Serre, Jean-Pierre (1977), *Linear representations of finite groups*, Berlin, New York: Springer-Verlag, ISBN 978-0-387-90190-9, MR0450380 (<http://www.ams.org/mathscinet-getitem?mr=0450380>) .
- Shatz, Stephen S. (1972), *Profinite groups, arithmetic, and geometry*, Princeton University Press, ISBN 978-0-691-08017-8, MR0347778 (<http://www.ams.org/mathscinet-getitem?mr=0347778>)
- Suzuki, Michio (1951), "On the lattice of subgroups of finite groups" (<http://jstor.org/stable/1990375>) , *Transactions of the American Mathematical Society* **70** (2): 345–371, doi:10.2307/1990375 (<http://dx.doi.org/10.2307/1990375>) , JSTOR 1990375 (<http://www.jstor.org/stable/1990375>) , <http://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.
- Weinberg, Steven (1972), *Gravitation and Cosmology*, 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.

## Historical references

*See also: Historically important publications in group theory*

- 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>) , **II (1851–1860)**, Cambridge University Press, <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>.
- O'Connor, J.J; Robertson, E.F. (1996), *The development of group theory* ([http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Development\\_group\\_theory.html](http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Development_group_theory.html)) , [http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Development\\_group\\_theory.html](http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Development_group_theory.html).
- 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.
- **(German)** von Dyck, Walther (1882), "Gruppentheoretische Studien (Group-theoretical Studies)", *Mathematische Annalen* **20** (1): 1–44, doi:10.1007/BF01443322 (<http://dx.doi.org/10.1007/BF01443322>) .
- **(French)** Galois, Évariste (1908), Tannery, Jules, ed., *Manuscripts de Évariste Galois [Évariste Galois' Manuscripts]* (<http://quod.lib.umich.edu/cgi/t/text/text-idx?c=umhistmath;idno=AAN9280>) , Paris: Gauthier-Villars, <http://quod.lib.umich.edu/cgi/t/text/text-idx?c=umhistmath;idno=AAN9280> (Galois work was first published by Joseph Liouville in 1843).
- **(French)** Jordan, Camille (1870), *Traité des substitutions et des équations algébriques [Study of Substitutions and Algebraic Equations]* (<http://gallica.bnf.fr/notice?N=FRBNF35001297>) , Paris: Gauthier-Villars, <http://gallica.bnf.fr/notice?N=FRBNF35001297>.
- Kleiner, Israel (1986), "The evolution of group theory: a brief survey", *Mathematics Magazine* **59** (4): 195–215, doi:10.2307/2690312 (<http://dx.doi.org/10.2307/2690312>) , MR863090 (<http://www.ams.org/mathscinet-getitem?mr=863090>) .
- **(German)** Lie, Sophus (1973), *Gesammelte Abhandlungen. Band 1 [Collected papers. Volume 1]*, New York: Johnson Reprint Corp., MR0392459 (<http://www.ams.org/mathscinet-getitem?mr=0392459>) .
- Mackey, George Whitelaw (1976), *The theory of unitary group representations*, University of

Chicago Press, MR0396826 (<http://www.ams.org/mathscinet-getitem?mr=0396826>)

- Smith, David Eugene (1906), *History of Modern Mathematics* (<http://www.gutenberg.org/etext/8746>) , Mathematical Monographs, No. 1, <http://www.gutenberg.org/etext/8746>.
- 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.

Retrieved from "[http://en.wikipedia.org/wiki/Group\\_\(mathematics\)](http://en.wikipedia.org/wiki/Group_(mathematics))"

Categories: Abstract algebra | Algebraic structures | Group theory | Mathematical structures | Symmetry

---

- This page was last modified on 18 March 2011 at 19:54.
  - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of Use for details.
- Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.