

# Basic properties of groups

generated by Lam Phong

# Contents

## Articles

Zassenhaus lemma	1
Center (group theory)	2
Centralizer and normalizer	4
Characteristic subgroup	6
Commutator	9
Composition series	11
Conjugacy class	14
Conjugate closure	17
Conjugation of isometries in Euclidean space	17
Core (group)	20
Coset	22
Commutator subgroup	24
Elementary group theory	27
Euler's theorem	33
Fitting subgroup	34
Hamiltonian group	36
Identity element	37
Lagrange's theorem (group theory)	38
Multiplicative inverse	40
Normal subgroup	43
Perfect group	47
Schreier refinement theorem	49
Subgroup	49
Transversal (combinatorics)	54
Torsion subgroup	56

## References

Article Sources and Contributors	58
Image Sources, Licenses and Contributors	60

## Article Licenses

License	61
---------	----

# Zassenhaus lemma

In mathematics, the **butterfly lemma** or **Zassenhaus lemma**, named after Hans Julius Zassenhaus, is a technical result on the lattice of subgroups of a group or the lattice of submodules of a module, or more generally for any modular lattice.<sup>[1]</sup>

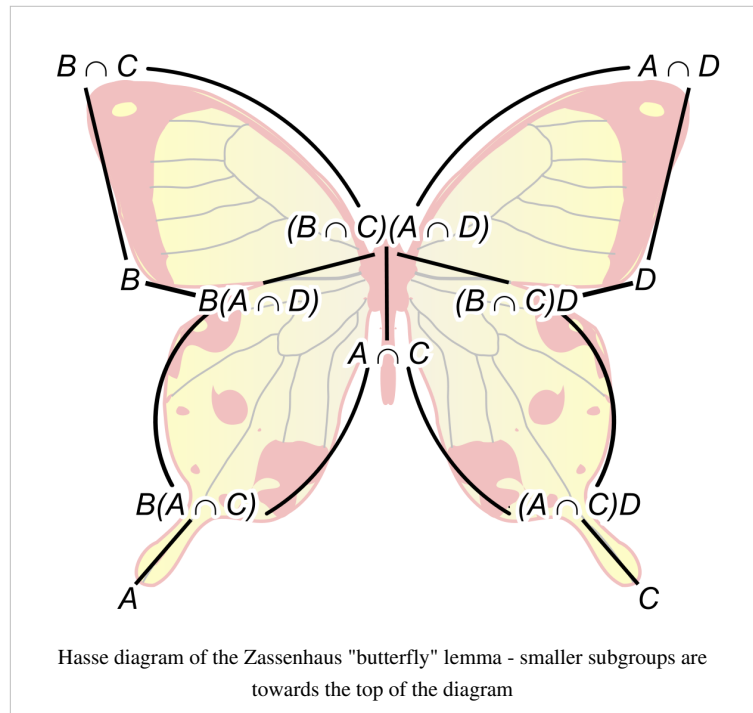
**Lemma:** Suppose  $(G, \Omega)$  is a group with operators and  $A$  and  $C$  are subgroups. Suppose

$$B \triangleleft A \text{ and } D \triangleleft C$$

are stable subgroups. Then,

$$(A \cap C)B / (A \cap D)B \text{ is isomorphic to } (A \cap C)D / (B \cap C)D.$$

Zassenhaus proved this lemma specifically to give the smoothest proof of the Schreier refinement theorem. The 'butterfly' becomes apparent when trying to draw the Hasse diagram of the various groups involved.



## Notes

[1] See Pierce, p. 27, exercise 1.

## References

- Pierce, R. S., *Associative algebras*, Springer, pp. 27, ISBN 0387906932.
- Goodearl, K. R.; Warfield, Robert B. (1989), *An introduction to noncommutative noetherian rings*, Cambridge University Press, pp. 51, 62, ISBN 9780521369251.
- Lang, Serge, *Algebra*, Graduate Texts in Mathematics (Revised 3rd ed.), Springer-Verlag, pp. 20–21, ISBN 9780387953854.
- Carl Clifton Faith, Nguyen Viet Dung, Barbara Osofsky. *Rings, Modules and Representations*. p. 6. AMS Bookstore, 2009. ISBN 0821843702

## External links

- Zassenhaus Lemma and proof at [http://www.artofproblemsolving.com/Wiki/index.php/Zassenhaus%27s\\_Lemma](http://www.artofproblemsolving.com/Wiki/index.php/Zassenhaus%27s_Lemma)

# Center (group theory)

In abstract algebra, the **center** of a group  $G$ , denoted  $Z(G)$ ,<sup>[1]</sup> is the set of elements that commute with every element of  $G$ . In set-builder notation,

$$Z(G) = \{z \in G \mid \forall g \in G, zg = gz\}.$$

The center is a subgroup of  $G$ , which by definition is abelian (that is commutative). As a subgroup, it is always normal, and indeed characteristic, but it need not be fully characteristic. The quotient group  $G/Z(G)$  is isomorphic to the group of inner automorphisms of  $G$ .

A group  $G$  is abelian if and only if  $Z(G) = G$ . At the other extreme, a group is said to be **centerless** if  $Z(G)$  is trivial, i.e. consists only of the identity element.

The elements of the center are sometimes called **central**.

## As a subgroup

The center of  $G$  is always a subgroup of  $G$ . In particular:

1.  $Z(G)$  contains  $e$ , the identity element of  $G$ , because  $eg = g = ge$  for all  $g \in G$  by definition of  $e$ , so by definition of  $Z(G)$ ,  $e \in Z(G)$ ;
2. If  $x$  and  $y$  are in  $Z(G)$ , then  $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$  for each  $g \in G$ , and so  $xy$  is in  $Z(G)$  as well (i.e.,  $Z(G)$  exhibits closure);
3. If  $x$  is in  $Z(G)$ , then  $gx = xg$ , and multiplying twice, once on the left and once on the right, by  $x^{-1}$ , gives  $x^{-1}g = gx^{-1}$  — so  $x^{-1} \in Z(G)$ .

Furthermore the center of  $G$  is always a normal subgroup of  $G$ , as it is closed under conjugation.

## Conjugation

Consider the map  $f: G \rightarrow \text{Aut}(G)$  from  $G$  to the automorphism group of  $G$  defined by  $f(g) = \phi_g$ , where  $\phi_g$  is the automorphism of  $G$  defined by

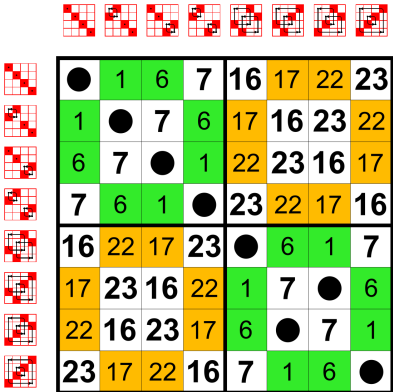
$$\phi_g(h) = ghg^{-1}.$$

The function  $f$  is a group homomorphism, and its kernel is precisely the center of  $G$ , and its image is called the inner automorphism group of  $G$ , denoted  $\text{Inn}(G)$ . By the first isomorphism theorem we get

$$G/Z(G) \cong \text{Inn}(G).$$

The cokernel of this map is the group  $\text{Out}(G)$  of outer automorphisms, and these form the exact sequence

$$1 \rightarrow Z(G) \rightarrow G \rightarrow \text{Aut}(G) \rightarrow \text{Out}(G) \rightarrow 1.$$



Cayley table of  $\text{Dih}_4$

The center is  $\{0,7\}$ : The row starting with 7 is the transpose of the column starting with 7. The entries 7 are symmetric to the main diagonal. (Only for the neutral element this is granted in all groups.)

## Examples

- The center of an abelian group  $G$  is all of  $G$ .
- The center of the Heisenberg group  $G$  are all matrices of the form : 
$$\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
- The center of a nonabelian simple group is trivial.
- The center of the dihedral group  $D_n$  is trivial when  $n$  is odd. When  $n$  is even, the center consists of the identity element together with the  $180^\circ$  rotation of the polygon.
- The center of the quaternion group  $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$  is  $\{1, -1\}$ .
- The center of the symmetric group  $S_n$  is trivial for  $n \geq 3$ .
- The center of the alternating group  $A_n$  is trivial for  $n \geq 4$ .
- The center of the general linear group  $GL_n(F)$  is the collection of scalar matrices  $\{sI_n | s \in F \setminus \{0\}\}$ .
- The center of the orthogonal group  $O(n, F)$  is  $\{I_n, -I_n\}$ .
- The center of the multiplicative group of non-zero quaternions is the multiplicative group of non-zero real numbers.
- Using the class equation one can prove that the center of any non-trivial finite p-group is non-trivial.
- If the quotient group  $G/Z(G)$  is cyclic,  $G$  is abelian (and so  $G = Z(G)$ , and  $G/Z(G)$  is trivial).
- The quotient group  $G/Z(G)$  is not isomorphic to the quaternion group  $Q_8$ .

## Higher centers

Quotienting out by the center of a group yields a sequence of groups called the **upper central series**:

$$G_0 = G \rightarrow G_1 = G_0/Z(G_0) \rightarrow G_2 = G_1/Z(G_1) \rightarrow \dots$$

The kernel of the map  $G \rightarrow G_i$  is the  **$i$ th center** of  $G$  (**second center**, **third center**, etc.), and is denoted  $Z^i(G)$ .

Concretely, the  $(i + 1)$ -st center are the terms that commute with all elements up to an element of the  $i$ th center.

Following this definition, one can define the 0th center of a group to be the identity subgroup. This can be continued to transfinite ordinals by transfinite induction; the union of all the higher centers is called the **hypercenter**.<sup>[2]</sup>

The ascending chain of subgroups

$$1 \leq Z(G) \leq Z^2(G) \leq \dots$$

stabilizes at  $i$  (equivalently,  $Z^i(G) = Z^{i+1}(G)$ ) if and only if  $G_i$  is centerless.

## Examples

- For a centerless group, all higher centers are zero, which is the case  $Z^0(G) = Z^1(G)$  of stabilization.
- By Grün's lemma, the quotient of a perfect group by its center is centerless, hence all higher centers equal the center. This is a case of stabilization at  $Z^1(G) = Z^2(G)$ .

## Notes

[1] The notation  $Z$  is from German *Zentrum*, meaning "center".

[2] This union will include transfinite terms if the UCS does not stabilize at a finite stage.

# Centralizer and normalizer

---

In group theory, the **centralizer** of a subset  $S$  of a group  $G$  is the set of elements of  $G$  that commute with each element of  $S$ , and the **normalizer** of  $S$  is the set of elements of  $G$  that commute with  $S$  "as a whole". The centralizer and normalizer of  $S$  are subgroups of  $G$ , and can provide insight into the structure of  $G$ .

The definitions also apply to monoids and semigroups.

In ring theory, the **centralizer of a subset of a ring** is defined with respect to the semigroup (multiplication) operation of the ring. The centralizer of a subset of a ring  $R$  is a subring of  $R$ . This article also deals with centralizers and normalizers in Lie algebra.

The idealizer in a semigroup or ring is another construction that is in the same vein as the centralizer and normalizer.

## Definitions

Groups and semigroups

The **centralizer** of a subset  $S$  of group (or semigroup)  $G$  is defined to be<sup>[1]</sup>

$$C_G(S) = \{g \in G \mid sg = gs \text{ for all } s \in S\}$$

Sometimes if there is no ambiguity about the group in question, the  $G$  is suppressed from the notation entirely. When  $S = \{a\}$  is a singleton set, then  $C_G(\{a\})$  can be abbreviated to  $C_G(a)$ . Another less common notation for the centralizer is  $Z(a)$ , which parallels the notation for the center of a group. With this latter notation, one must be careful to avoid confusion between the center of a group  $G$ ,  $Z(G)$ , and the *centralizer* of an *element*  $g$  in  $G$ , given by  $Z(g)$ .

The **normalizer** of  $S$  in the group (or semigroup)  $G$  is defined to be

$$N_G(S) = \{g \in G \mid Sg = gS\}$$

The definitions are similar but not identical. If  $g$  is in the centralizer of  $S$  and  $s$  is in  $S$ , then it must be that  $gs = sg$ , however if  $g$  is in the normalizer,  $gs = tg$  for some  $t$  in  $S$ , potentially different from  $s$ . The same conventions mentioned previously about suppressing  $G$  and suppressing braces from singleton sets also apply to the normalizer notation. The normalizer should not be confused with the normal closure.

Rings, algebras, Lie rings and Lie algebras

If  $R$  is a ring or an algebra, and  $S$  is a subset of the ring, then the centralizer of  $S$  is exactly as defined for groups, with  $R$  in the place of  $G$ .

If  $\mathfrak{L}$  is a Lie algebra (or Lie ring) with Lie product  $[x,y]$ , then the centralizer of a subset  $S$  of  $\mathfrak{L}$  is defined to be<sup>[2]</sup>

$$C_{\mathfrak{L}}(S) = \{x \in \mathfrak{L} \mid [x, s] = 0 \text{ for all } s \in S\}$$

The definition of centralizers for Lie rings is linked to the definition for rings in the following way. If  $R$  is an associative ring, then  $R$  can be given the bracket product  $[x,y] = xy - yx$ . Of course then  $xy = yx$  if and only if  $[x,y] = 0$ . If we denote the set  $R$  with the bracket product as  $L_R$ , then clearly the *ring centralizer* of  $S$  in  $R$  is equal to the *Lie ring centralizer* of  $S$  in  $L_R$ .

The normalizer of a subset  $S$  of a Lie algebra (or Lie ring)  $\mathfrak{L}$  is given by<sup>[2]</sup>

$$N_{\mathfrak{L}}(S) = \{x \in \mathfrak{L} \mid [x, s] \in S \text{ for all } s \in S\}$$

While this is the standard usage of the term "normalizer" in Lie algebra, it should be noted that this construction is actually the idealizer of the set  $S$  in  $\mathfrak{L}$ . If  $S$  is an additive subgroup of  $\mathfrak{L}$ , then  $N_{\mathfrak{L}}(S)$  is the largest Lie subring (or Lie subalgebra, as the case may be) in which  $S$  is a Lie ideal<sup>[3]</sup>.

---

## Properties

### Groups<sup>[4]</sup>

- The centralizer and normalizer of  $S$  are both subgroups of  $G$ .
- Clearly,  $C_G(S) \subseteq N_G(S)$ . In fact,  $C_G(S)$  is always a normal subgroup of  $N_G(S)$ .
- $C_G(C_G(S))$  contains  $S$ , but  $C_G(S)$  need not contain  $S$ . Containment will occur if  $st=ts$  for every  $s$  and  $t$  in  $S$ . Naturally then if  $H$  is an abelian subgroup of  $G$ ,  $C_G(H)$  contains  $H$ .
- If  $S$  is a subsemigroup of  $G$ , then  $N_G(S)$  contains  $S$ .
- If  $H$  is a subgroup of  $G$ , then the largest subgroup in which  $H$  is normal is the subgroup  $N_G(H)$ .
- A subgroup  $H$  of a group  $G$  is called a **self-normalizing subgroup** of  $G$  if  $N_G(H) = H$ .
- The center of  $G$  is exactly  $C_G(G)$  and  $G$  is an abelian group if and only if  $C_G(G) = Z(G) = G$ .
- For singleton sets,  $C_G(a) = N_G(a)$ .
- By symmetry, if  $S$  and  $T$  are two subsets of  $G$ ,  $T \subseteq C_G(S)$  if and only if  $S \subseteq C_G(T)$ .
- For a subgroup  $H$  of group  $G$ , the **N/C theorem** states that the factor group  $N_G(H)/C_G(H)$  is isomorphic to a subgroup of  $\text{Aut}(H)$ , the automorphism group of  $H$ . Since  $N_G(G) = G$  and  $C_G(G) = Z(G)$ , the N/C theorem also implies that  $G/Z(G)$  is isomorphic to  $\text{Inn}(G)$ , the subgroup of  $\text{Aut}(G)$  consisting of all inner automorphisms of  $G$ .
- If we define a group homomorphism  $T : G \rightarrow \text{Inn}(G)$  by  $T(x)(g) = T_x(g) = xgx^{-1}$ , then we can describe  $N_G(S)$  and  $C_G(S)$  in terms of the group action of  $\text{Inn}(G)$  on  $G$ : the stabilizer of  $S$  in  $\text{Inn}(G)$  is  $T(N_G(S))$ , and the subgroup of  $\text{Inn}(G)$  fixing  $S$  is  $T(C_G(S))$ .

### Rings and algebras<sup>[2]</sup>

- Centralizers in rings and algebras are subrings and subalgebras, respectively, and centralizers in Lie rings and Lie algebras are Lie subrings and Lie subalgebras, respectively.
- The normalizer of  $S$  in a Lie ring contains the centralizer of  $S$ .
- $C_R(C_R(S))$  contains  $S$  but is not necessarily equal. The double centralizer theorem deals with situations where equality occurs.
- If  $S$  is an additive subgroup of a Lie ring  $A$ , then  $N_A(S)$  is the largest Lie subring of  $A$  in which  $S$  is a Lie ideal.
- If  $S$  is a Lie subring of a Lie ring  $A$ , then  $S \subseteq N_A(S)$ .

## Notes

[1] Jacobson (2009), p. 41

[2] Jacobson 1979, p.28.

[3] Jacobson 1979, p.57.

[4] Isaacs 2009, Chapters 1–3.

## References

- Isaacs, I. Martin (2009), *Algebra: a graduate course*, Graduate Studies in Mathematics, **100**, Providence, RI: American Mathematical Society, pp. xii+516, ISBN 978-0-8218-4799-2, MR2472787
- Jacobson, Nathan (2009), *Basic algebra*, **1** (2 ed.), Dover, ISBN 978-0-486-47189-1.
- Jacobson, Nathan (1979), *Lie algebras*, New York: Dover Publications Inc., pp. ix+331, ISBN 0-486-63832-4, MR559927

# Characteristic subgroup

---

In mathematics, particularly in the area of abstract algebra known as group theory, a **characteristic subgroup** is a subgroup that is invariant under all automorphisms of the parent group.<sup>[1][2]</sup> Because conjugation is an automorphism, every characteristic subgroup is normal, though not every normal subgroup is characteristic. Examples of characteristic subgroups include the commutator subgroup and the center of a group.

## Definitions

A **characteristic subgroup** of a group  $G$  is a subgroup  $H$  that is invariant under each automorphism of  $G$ . That is,

$$\varphi(H) = H$$

for every automorphism  $\varphi$  of  $G$  (where  $\varphi(H)$  denotes the image of  $H$  under  $\varphi$ ).

The statement " $H$  is a characteristic subgroup of  $G$ " is written

$$H \text{ char } G.$$

## Characteristic vs. normal

If  $G$  is a group, and  $g$  is a fixed element of  $G$ , then the conjugation map

$$x \mapsto gxg^{-1}$$

is an automorphism of  $G$  (known as an inner automorphism). A subgroup of  $G$  that is invariant under all inner automorphisms is called normal. Since a characteristic subgroup is invariant under all automorphisms, every characteristic subgroup is normal.

Not every normal subgroup is characteristic. Here are several examples:

- Let  $H$  be a group, and let  $G$  be the direct product  $H \times H$ . Then the subgroups  $\{1\} \times H$  and  $H \times \{1\}$  are both normal, but neither is characteristic. In particular, neither of these subgroups is invariant under the automorphism  $(x, y) \rightarrow (y, x)$  that switches the two factors.
- For a concrete example of this, let  $V$  be the Klein four-group (which is isomorphic to the direct product  $\mathbf{Z}_2 \times \mathbf{Z}_2$ ). Since this group is abelian, every subgroup is normal; but every permutation of the three non-identity elements is an automorphism of  $V$ , so the three subgroups of order 2 are not characteristic. Here  $V = \{e, a, b, ab\}$ . Consider  $H = \{e, a\}$  and consider the automorphism  $T(e) = e, T(a) = b, T(b) = a, T(ab) = ab$ . Then  $T(H)$  is not contained in  $H$ .
- In the quaternion group of order 8, each of the cyclic subgroups of order 4 is normal, but none of these are characteristic. However, the subgroup  $\{1, -1\}$  is characteristic, since it is the only subgroup of order 2.

Note: If  $H$  is the unique subgroup of a group  $G$ , then  $H$  is characteristic in  $G$ .

- If  $n$  is even, the dihedral group of order  $2n$  has three subgroups of index two, all of which are normal. One of these is the cyclic subgroup, which is characteristic. The other two subgroups are dihedral; these are permuted by an outer automorphism of the parent group, and are therefore not characteristic.
- "Normality" is not transitive but Characteristic is transitive. If  $H \text{ Char } K$  and  $K$  normal in  $G$  then  $H$  normal in  $G$ .



## Comparison to other subgroup properties

### Distinguished subgroups

A related concept is that of a **distinguished subgroup**. In this case the subgroup  $H$  is invariant under the applications of surjective endomorphisms. For a finite group this is the same, because surjectivity implies injectivity, but not for an infinite group: a surjective endomorphism is not necessarily an automorphism.

### Fully invariant subgroups

For an even stronger constraint, a fully characteristic subgroup (also called a **fully invariant subgroup**)  $H$  of a group  $G$  is a group remaining invariant under every endomorphism of  $G$ ; in other words, if  $f : G \rightarrow G$  is any homomorphism, then  $f(H)$  is a subgroup of  $H$ .

### Verbal subgroups

An even stronger constraint is verbal subgroup, which is the image of a fully invariant subgroup of a free group under a homomorphism.

### Containments

Every subgroup that is fully characteristic is certainly distinguished and therefore characteristic; but a characteristic or even distinguished subgroup need not be fully characteristic.

The center of a group is easily seen to always be a distinguished subgroup, but it is not always fully characteristic. The finite group of order 12,  $\text{Sym}(3) \times \mathbf{Z}/2\mathbf{Z}$  has a homomorphism taking  $(\pi, y)$  to  $((1,2)^y, 0)$  which takes the center  $1 \times \mathbf{Z}/2\mathbf{Z}$  into a subgroup of  $\text{Sym}(3) \times 1$ , which meets the center only in the identity.

The relationship amongst these subgroup properties can be expressed as:

$$\begin{aligned} \text{subgroup} &\Leftarrow \text{normal subgroup} \Leftarrow \mathbf{\text{characteristic subgroup}} \Leftarrow \text{distinguished subgroup} \Leftarrow \text{fully characteristic} \\ &\text{subgroup} \Leftarrow \text{verbal subgroup} \end{aligned}$$

## Examples

### Finite example

Consider the group  $G = S_3 \times Z_2$  (the group of order 12 which is the direct product of the symmetric group of order 6 and a cyclic group of order 2). The center of  $G$  is its second factor  $Z_2$ . Note that the first factor  $S_3$  contains subgroups isomorphic to  $Z_2$ , for instance  $\{\text{identity}, (12)\}$ ; let  $f: Z_2 \rightarrow S_3$  be the morphism mapping  $Z_2$  onto the indicated subgroup. Then the composition of the projection of  $G$  onto its second factor  $Z_2$ , followed by  $f$ , followed by the inclusion of  $S_3$  into  $G$  as its first factor, provides an endomorphism of  $G$  under which the image of the center  $Z_2$  is not contained in the center, so here the center is not a fully characteristic subgroup of  $G$ .

## Cyclic groups

Every subgroup of a cyclic group is characteristic.

## Subgroup functors

The derived subgroup (or commutator subgroup) of a group is a verbal subgroup. The torsion subgroup of an abelian group is a fully invariant subgroup.

## Transitivity

The property of being characteristic or fully characteristic is transitive; if  $H$  is a (fully) characteristic subgroup of  $K$ , and  $K$  is a (fully) characteristic subgroup of  $G$ , then  $H$  is a (fully) characteristic subgroup of  $G$ .

Moreover, while it is not true that every normal subgroup of a normal subgroup is normal, it is true that every characteristic subgroup of a normal subgroup is normal. Similarly, while it is not true that every distinguished subgroup of a distinguished subgroup is distinguished, it is true that every fully characteristic subgroup of a distinguished subgroup is distinguished.

## Map on Aut and End

If  $H \text{ char } G$ , then every automorphism of  $G$  induces an automorphism of the quotient group  $G/H$ , which yields a map  $\text{Aut } G \rightarrow \text{Aut } G/H$ .

If  $H$  is fully characteristic in  $G$ , then analogously, every endomorphism of  $G$  induces an endomorphism of  $G/H$ , which yields a map  $\text{End } G \rightarrow \text{End } G/H$ .

## References

- [1] Dummit, David S.; Foote, Richard M. (2004). *Abstract Algebra* (3rd ed.). John Wiley & Sons. ISBN 0-471-43334-9.
- [2] Lang, Serge (2002). *Algebra*. Graduate Texts in Mathematics. Springer. ISBN 0-387-95385-X.

# Commutator

---

In mathematics, the **commutator** gives an indication of the extent to which a certain binary operation fails to be commutative. There are different definitions used in group theory and ring theory.

## Group theory

The **commutator** of two elements,  $g$  and  $h$ , of a group  $G$ , is the element

$$[g, h] = g^{-1}h^{-1}gh.$$

It is equal to the group's identity if and only if  $g$  and  $h$  commute (i.e., if and only if  $gh = hg$ ). The subgroup of  $G$  generated by all commutators is called the *derived group* or the *commutator subgroup* of  $G$ . Note that one must consider the subgroup generated by the set of commutators because in general the set of commutators is not closed under the group operation. Commutators are used to define nilpotent and solvable groups.

N.B. The above definition of the commutator is used by group theorists. Many other mathematicians define the commutator as

$$[g, h] = ghg^{-1}h^{-1}.$$

## Identities

Commutator identities are an important tool in group theory, (McKay 2000, p. 4). The expression  $a^x$  denotes the *conjugate* of  $a$  by  $x$ , defined as  $x^{-1}ax$ .

1.  $x^y = x[x, y]$ .
2.  $[y, x] = [x, y]^{-1}$ .
3.  $[x, zy] = [x, y] \cdot [x, z]^y$  and  $[xz, y] = [x, y]^z \cdot [z, y]$ .
4.  $[x, y^{-1}] = [y, x]^{y^{-1}}$  and  $[x^{-1}, y] = [y, x]^{x^{-1}}$ .
5.  $[[x, y^{-1}], z]^y \cdot [[y, z^{-1}], x]^z \cdot [[z, x^{-1}], y]^x = 1$  and  $[[x, y], z^x] \cdot [[z, x], y^z] \cdot [[y, z], x^y] = 1$ .

Identity 5 is also known as the *Hall-Witt identity*. It is a group-theoretic analogue of the Jacobi identity for the ring-theoretic commutator (see next section).

N.B. The above definition of the conjugate of  $a$  by  $x$  is used by group theorists. Many other mathematicians define the conjugate of  $a$  by  $x$  as  $xax^{-1}$ . This is often written  ${}^x a$ . Similar identities hold for these conventions.

A wide range of identities are used that are true modulo certain subgroups. These can be particularly useful in the study of solvable groups and nilpotent groups. For instance, in any group second powers behave well

$$(xy)^2 = x^2y^2[y, x][[y, x], y].$$

If the derived subgroup is central, then

$$(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}.$$

## Ring theory

The **commutator** of two elements  $a$  and  $b$  of a ring or an associative algebra is defined by

$$[a, b] = ab - ba.$$

It is zero if and only if  $a$  and  $b$  commute. In linear algebra, if two endomorphisms of a space are represented by commuting matrices with respect to one basis, then they are so represented with respect to every basis. By using the commutator as a Lie bracket, every associative algebra can be turned into a Lie algebra. The commutator of two operators defined on a Hilbert space is an important concept in quantum mechanics since it measures how well the two observables described by the operators can be measured simultaneously. The uncertainty principle is ultimately

---

a theorem about these commutators via the Robertson-Schrödinger relation.

## Identities

The commutator has the following properties:

*Lie-algebra relations:*

- $[A, A] = 0$
- $[A, B] = -[B, A]$
- $[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$

The second relation is called anticommutativity, while the third is the Jacobi identity.

*Additional relations:*

- $[A, BC] = [A, B]C + B[A, C]$
- $[AB, C] = A[B, C] + [A, C]B$
- $[ABC, D] = AB[C, D] + A[B, D]C + [A, D]BC$
- $[AB, CD] = A[B, CD] + [A, CD]B = A[B, C]D + AC[B, D] + [A, C]DB + C[A, D]B$
- $[[[A, B], C], D] + [[[B, C], D], A] + [[[C, D], A], B] + [[[D, A], B], C] = [[A, C], [B, D]]$
- $[AB, C] = A\{B, C\} - \{A, C\}B$ , where  $\{A, B\} = AB + BA$  is the anticommutator defined below

If  $A$  is a fixed element of a ring  $\mathfrak{A}$ , the first additional relation can also be interpreted as a Leibniz rule for the map  $D_A: R \rightarrow R$  given by  $B \mapsto [A, B]$ . In other words: the map  $D_A$  defines a derivation on the ring  $\mathfrak{A}$ .

The following identity involving nested commutators, underlying the Campbell-Baker-Hausdorff expansion, is also useful:

- $e^A B e^{-A} = B + [A, B] + \frac{1}{2!}[A, [A, B]] + \frac{1}{3!}[A, [A, [A, B]]] + \dots \equiv e^{ad(A)} B.$

## Graded rings and algebras

When dealing with graded algebras, the commutator is usually replaced by the **graded commutator**, defined in homogeneous components as  $[\omega, \eta]_{gr} := \omega\eta - (-1)^{\deg \omega \deg \eta} \eta\omega$ .

## Derivations

Especially if one deals with multiple commutators, another notation turns out to be useful involving the adjoint representation:

$$\text{ad}(x)(y) = [x, y].$$

Then  $\text{ad}(x)$  is a derivation and  $\text{ad}$  is linear, *i.e.*,  $\text{ad}(x + y) = \text{ad}(x) + \text{ad}(y)$  and  $\text{ad}(\lambda x) = \lambda \text{ad}(x)$ , and a Lie algebra homomorphism, *i.e.*,  $\text{ad}([x, y]) = [\text{ad}(x), \text{ad}(y)]$ , but it is **not** always an algebra homomorphism, *i.e.* the identity  $\text{ad}(xy) = \text{ad}(x)\text{ad}(y)$  **does not hold in general**.

Examples:

- $\text{ad}(x)\text{ad}(x)(y) = [x, [x, y]]$
- $\text{ad}(x)\text{ad}(a + b)(y) = [x, [a + b, y]].$

## Anticommutator

The **anticommutator** of two elements  $a$  and  $b$  of a ring or an associative algebra is defined by

$$\{a, b\} = ab + ba.$$

Sometimes the brackets  $[ ]_+$  are also used.<sup>[1]</sup> The anticommutator is used less often than the commutator, but can be used for example to define Clifford algebras and Jordan algebras.

## References

[1] Quantum Field Theory, D. McMahon, Mc Graw Hill (USA), 2008, ISBN 978-0-07-154382-8

- Griffiths, David J. (2004), *Introduction to Quantum Mechanics* (2nd ed.), Prentice Hall, ISBN 0-13-805326-X
- Liboff, Richard L. (2002), *Introductory Quantum Mechanics*, Addison-Wesley, ISBN 0-8053-8714-5
- McKay, Susan (2000), *Finite p-groups*, Queen Mary Maths Notes, **18**, University of London, ISBN 978-0-902480-17-9, MR1802994

## External links

- More commutator relations with proofs. ([http://physics.bulling.se/commutator\\_relations.pdf](http://physics.bulling.se/commutator_relations.pdf))

# Composition series

---

In abstract algebra, a **composition series** provides a way to break up an algebraic structure, such as a group or a module, into simple pieces. The need for considering composition series in the context of modules arises from the fact that many naturally occurring modules are not semisimple, hence cannot be decomposed into a direct sum of simple modules. A composition series of a module  $M$  is a finite increasing filtration of  $M$  by submodules such that the successive quotients are simple and serves as a replacement of the direct sum decomposition of  $M$  into its simple constituents.

A composition series may not even exist, and when it does, it need not be unique. Nevertheless, a group of results known under the general name **Jordan-Hölder theorem** asserts that whenever composition series exist, the *isomorphism classes* of simple pieces (although, perhaps, not their *location* in the composition series in question) and their multiplicities are uniquely determined. Composition series may thus be used to define invariants of finite groups and Artinian modules.

A related but distinct concept is a chief series: a composition series is a maximal *subnormal* series, while a chief series is a maximal *normal series*.

## For groups

If a group  $G$  has a normal subgroup  $N$ , then the factor group  $G/N$  may be formed, and some aspects of the study of the structure of  $G$  may be broken down by studying the "smaller" groups  $G/N$  and  $N$ . If  $G$  has no normal subgroup that is different from  $G$  and from the trivial group, then  $G$  is a simple group. Otherwise, the question naturally arises as to whether  $G$  can be reduced to simple "pieces", and if so, are there any unique features of the way this can be done?

More formally, a **composition series** of a group  $G$  is a subnormal series

$$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = G,$$

with strict inclusions, such that each  $H_i$  is a maximal normal subgroup of  $H_{i+1}$ . Equivalently, a composition series is a subnormal series such that each factor group  $H_{i+1}/H_i$  is simple. The factor groups are called **composition factors**.

---

A subnormal series is a composition series if and only if it is of maximal length. That is, there are no additional subgroups which can be "inserted" into a composition series. The length  $n$  of the series is called the **composition length**.

If a composition series exists for a group  $G$ , then any subnormal series of  $G$  can be *refined* to a composition series, informally, by inserting subgroups into the series up to maximality. Every finite group has a composition series, but not every infinite group has one. For example, the infinite cyclic group has no composition series.

### Uniqueness: Jordan–Hölder theorem

A group may have more than one composition series. However, the **Jordan–Hölder theorem** (named after Camille Jordan and Otto Hölder) states that any two composition series of a given group are equivalent. That is, they have the same composition length and the same composition factors, up to permutation and isomorphism. This theorem can be proved using the Schreier refinement theorem. The Jordan–Hölder theorem is also true for transfinite *ascending* composition series, but not transfinite *descending* composition series (Birkhoff 1934).

Transfinite *ascending* composition series are related to the concept of *hypertranssimplicity* (Sharipov 2009). A group is called *hypertranssimple* if it has no *ascending* subnormal series (neither finite nor transfinite ) other than the trivial series of the length one.

### Example

For a cyclic group of order  $n$ , composition series correspond to ordered prime factorizations of  $n$ , and in fact yields a proof of the fundamental theorem of arithmetic.

For example, the cyclic group  $C_{12}$  has

$$C_1 \triangleleft C_2 \triangleleft C_6 \triangleleft C_{12},$$

$$C_1 \triangleleft C_2 \triangleleft C_4 \triangleleft C_{12},$$

$$C_1 \triangleleft C_3 \triangleleft C_6 \triangleleft C_{12}$$

as different composition series. The sequences of composition factors obtained in the respective cases are

$$C_2, C_3, C_2$$

$$C_2, C_2, C_3 \text{ and}$$

$$C_3, C_2, C_2.$$

### For modules

The definition of composition series for modules restricts all attention to submodules, ignoring all additive subgroups that are *not* submodules. Given a ring  $R$  and an  $R$ -module  $M$ , a composition series for  $M$  is a series of submodules

$$\{0\} = J_0 \subset \cdots \subset J_n = M$$

where all inclusions are strict and  $J_k$  is a maximal submodule of  $J_{k+1}$  for each  $k$ . As for groups, if  $M$  has a composition series at all, then any finite strictly increasing series of submodules of  $M$  may be refined to a composition series, and any two composition series for  $M$  are equivalent. In that case, the (simple) quotient modules  $J_{k+1}/J_k$  are known as the **composition factors** of  $M$ , and the Jordan–Hölder theorem holds, ensuring that the number of occurrences of each isomorphism type of simple  $R$ -module as a composition factor does not depend on the choice of composition series.

It is well known<sup>[1]</sup> that a module has a finite composition series if and only if it is both an Artinian module and a Noetherian module. If  $R$  is an Artinian ring, then every finitely generated  $R$ -module is Artinian and Noetherian, and thus has a finite composition series. In particular, for any field  $K$ , any finite-dimensional module for a finite-dimensional algebra over  $K$  has a composition series, unique up to equivalence.

## Generalization

Groups with a set of operators generalize group actions and ring actions on an group. A unified approach to both groups and modules can be followed as in (Isaacs 1994, Ch. 10), simplifying some of the exposition. The group  $G$  is viewed as being acted upon by elements (operators) from a set  $\Omega$ . Attention is restricted entirely to subgroups invariant under the action of elements from  $\Omega$ , called  $\Omega$ -subgroups. Thus  $\Omega$ -composition series must use only  $\Omega$ -subgroups, and  $\Omega$ -composition factors need only be  $\Omega$ -simple. The standard results above, such as the Jordan-Hölder theorem, are established with nearly identical proofs.

The special cases recovered include when  $\Omega=G$  so that  $G$  is acting on itself. An important example of this is when elements of  $G$  act by conjugation, so that the set of operators consists of the inner automorphisms. A composition series under this action is exactly a chief series. Module structures are a case of  $\Omega$ -actions where  $\Omega$  is a ring and some additional axioms are satisfied.

## For objects in an abelian category

A **composition series** of an object  $A$  in an abelian category is a sequence of subobjects

$$A = X_0 \supsetneq X_1 \supsetneq \cdots \supsetneq X_n = 0$$

such that each quotient object  $X_i/X_{i+1}$  is simple (for  $0 \leq i < n$ ). If  $A$  has a composition series, the integer  $n$  only depends on  $A$  and is called the length of  $A$ .<sup>[2]</sup>

## Notes

[1] Isaacs 1994, p.146.

[2] Kashiwara & Schapira 2006, exercise 8.20

## References

- Birkhoff, Garrett (1934), "Transfinite subgroup series" (<http://projecteuclid.org/euclid.bams/1183497873>), *Bulletin of the American Mathematical Society* **40** (12): 847–850, doi:10.1090/S0002-9904-1934-05982-2
- Isaacs, I. Martin (1994), *Algebra: A Graduate Course*, Brooks/Cole, ISBN 978-0-534-19002-6
- Kashiwara, Masaki; Schapira, Pierre (2006), *Categories and sheaves*
- Sharipov, Ruslan (2009). "Transfinite normal and composition series of groups". arXiv:0908.2257 [math.GR].

# Conjugacy class

---

In mathematics, especially group theory, the elements of any group may be partitioned into **conjugacy classes**; members of the same conjugacy class share many properties, and study of conjugacy classes of non-abelian groups reveals many important features of their structure.<sup>[1][2]</sup> In all abelian groups every conjugacy class is a set containing one element (singleton set).

Functions that are constant for members of the same conjugacy class are called class functions.

## Definition

Suppose  $G$  is a group. Two elements  $a$  and  $b$  of  $G$  are called **conjugate** if there exists an element  $g$  in  $G$  with

$$gag^{-1} = b.$$

(In linear algebra, this is referred to as similarity of matrices.)

It can be readily shown that conjugacy is an equivalence relation and therefore partitions  $G$  into equivalence classes. (This means that every element of the group belongs to precisely one conjugacy class, and the classes  $\text{Cl}(a)$  and  $\text{Cl}(b)$  are equal if and only if  $a$  and  $b$  are conjugate, and disjoint otherwise.) The equivalence class that contains the element  $a$  in  $G$  is

$$\text{Cl}(a) = \{ gag^{-1} : g \in G \}$$

and is called the **conjugacy class** of  $a$ . The **class number** of  $G$  is the number of distinct (nonequivalent) conjugacy classes.

Conjugacy classes may be referred to by describing them, or more briefly by abbreviations such as "6A", meaning "a certain conjugacy class of order 6 elements", and "6B" would be a different conjugacy class of order 6 elements; the conjugacy class 1A is the conjugacy class of the identity. In some cases, conjugacy classes can be described in a uniform way – for example, in the symmetric group they can be described by cycle structure.

## Examples

The symmetric group  $S_3$ , consisting of all 6 permutations of three elements, has three conjugacy classes:

- no change ( $abc \rightarrow abc$ )
- interchanging two ( $abc \rightarrow acb$ ,  $abc \rightarrow bac$ ,  $abc \rightarrow cba$ )
- a cyclic permutation of all three ( $abc \rightarrow bca$ ,  $abc \rightarrow cab$ )

The symmetric group  $S_4$ , consisting of all 24 permutations of four elements, has five conjugacy classes, listed with their cycle structures and orders:

- $(1)_4$ : no change (1 element)
- $(2)$ : interchanging two (6 elements)
- $(3)$ : a cyclic permutation of three (8 elements)
- $(4)$ : a cyclic permutation of all four (6 elements)
- $(2)(2)$ : interchanging two, and also the other two (3 elements)

In general, the number of conjugacy classes in the symmetric group  $S_n$  is equal to the number of integer partitions of  $n$ . This is because each conjugacy class corresponds to exactly one partition of  $\{1, 2, \dots, n\}$  into cycles, up to permutation of the elements of  $\{1, 2, \dots, n\}$ .

See also the proper rotations of the cube, which can be characterized by permutations of the body diagonals.

---



## Properties

- The identity element is always in its own class, that is  $\text{Cl}(e) = \{e\}$
- If  $G$  is abelian, then  $gag^{-1} = a$  for all  $a$  and  $g$  in  $G$ ; so  $\text{Cl}(a) = \{a\}$  for all  $a$  in  $G$ ; the concept is therefore not very useful in the abelian case. The failure of this thus gives us an idea in what degree the group is nonabelian.
- If two elements  $a$  and  $b$  of  $G$  belong to the same conjugacy class (i.e., if they are conjugate), then they have the same order. More generally, every statement about  $a$  can be translated into a statement about  $b=gag^{-1}$ , because the map  $\varphi(x) = gxg^{-1}$  is an automorphism of  $G$ .
- An element  $a$  of  $G$  lies in the center  $Z(G)$  of  $G$  if and only if its conjugacy class has only one element,  $a$  itself. More generally, if  $C_G(a)$  denotes the *centralizer* of  $a$  in  $G$ , i.e., the subgroup consisting of all elements  $g$  such that  $ga = ag$ , then the index  $[G : C_G(a)]$  is equal to the number of elements in the conjugacy class of  $a$  (by the orbit-stabilizer theorem).
- If  $a$  and  $b$  are conjugate, then so are powers of them,  $a^k$  and  $b^k$  – thus taking  $k$ th powers gives a map on conjugacy classes, and one may speak of which conjugacy classes a given conjugacy class "powers up" into. For example, in the symmetric group, the square of an element of type (3)(2) (a 3-cycle and a 2-cycle) is an element of type (3), while the cube is an element of type (2), so the class (3)(2) powers up into the classes (3) and (2).

## Conjugacy class equation

If  $G$  is a finite group, then for any group element  $a$ , the elements in the conjugacy class of  $a$  are in one-to-one correspondence with cosets of the centralizer  $C_G(a)$ . This can be seen by observing that any two elements  $b$  and  $c$  belonging to the same coset (and hence,  $b=cz$  for some  $z$  in the centralizer  $C_G(a)$ ) give rise to the same element when conjugating  $a$ :  $bab^{-1} = cza(cz)^{-1} = cza z^{-1} c^{-1} = czz^{-1} ac^{-1} = cac^{-1}$ .

Thus the number of elements in the conjugacy class of  $a$  is the index  $[G:C_G(a)]$  of the centralizer  $C_G(a)$  in  $G$ . Thus the size of each conjugacy class is a divisor of the order of the group.

Furthermore, if we choose a single representative element  $x_i$  from every conjugacy class, we infer from the disjointedness of the conjugacy classes that  $|G| = \sum_i [G : C_G(x_i)]$ , where  $C_G(x_i)$  is the centralizer of the element  $x_i$ . Observing that each element of the center  $Z(G)$  forms a conjugacy class containing just itself gives rise to the following important **class equation**:<sup>[3]</sup>

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

where the second sum is over a representative element from each conjugacy class that is not in the center.

Knowledge of the divisors of the group order  $|G|$  can often be used to gain information about the order of the center or of the conjugacy classes.

## Example

Consider a finite  $p$ -group  $G$  (that is, a group with order  $p^n$ , where  $p$  is a prime number and  $n > 0$ ). We are going to prove that: *every finite p-group has a non-trivial center*.

Since the order of any conjugacy class of  $G$  must divide the order of  $G$ , it follows that each conjugacy class  $H_i$  also has order some power of  $p^{(k_i)}$ , where  $0 < k_i < n$ . But then the class equation requires that  $|G| = p^n = |Z(G)| + \sum_i (p^{(k_i)})$ . From this we see that  $p$  must divide  $|Z(G)|$ , so  $|Z(G)| > 1$ .

## Conjugacy of subgroups and general subsets

More generally, given any subset  $S$  of  $G$  ( $S$  not necessarily a subgroup), we define a subset  $T$  of  $G$  to be conjugate to  $S$  if and only if there exists some  $g$  in  $G$  such that  $T = gSg^{-1}$ . We can define  $\text{Cl}(S)$  as the set of all subsets  $T$  of  $G$  such that  $T$  is conjugate to  $S$ .

A frequently used theorem is that, given any subset  $S$  of  $G$ , the index of  $N(S)$  (the normalizer of  $S$ ) in  $G$  equals the order of  $\text{Cl}(S)$ :

$$|\text{Cl}(S)| = [G : N(S)]$$

This follows since, if  $g$  and  $h$  are in  $G$ , then  $gSg^{-1} = hSh^{-1}$  if and only if  $g^{-1}h$  is in  $N(S)$ , in other words, if and only if  $g$  and  $h$  are in the same coset of  $N(S)$ .

Note that this formula generalizes the one given earlier for the number of elements in a conjugacy class (let  $S = \{a\}$ ).

The above is particularly useful when talking about subgroups of  $G$ . The subgroups can thus be divided into conjugacy classes, with two subgroups belonging to the same class if and only if they are conjugate. Conjugate subgroups are isomorphic, but isomorphic subgroups need not be conjugate (for example, an abelian group may have two different subgroups which are isomorphic, but they are never conjugate).

## Conjugacy as group action

If we define

$$g \cdot x = gxg^{-1}$$

for any two elements  $g$  and  $x$  in  $G$ , then we have a group action of  $G$  on  $G$ . The orbits of this action are the conjugacy classes, and the stabilizer of a given element is the element's centralizer.<sup>[4]</sup>

Similarly, we can define a group action of  $G$  on the set of all subsets of  $G$ , by writing

$$g \cdot S = gSg^{-1},$$

or on the set of the subgroups of  $G$ .

## Geometric interpretation

Conjugacy classes in the fundamental group of a path-connected topological space can be thought of as equivalence classes of free loops under free homotopy.

## References

- [1] Dummit, David S.; Foote, Richard M. (2004). *Abstract Algebra* (3rd ed.). John Wiley & Sons. ISBN 0-471-43334-9.
- [2] Lang, Serge (2002). *Algebra*. Graduate Texts in Mathematics. Springer. ISBN 0-387-95385-X.
- [3] Grillet (2007), p. 57 ([http://books.google.com/books?id=LJtyhu8-xYwC&pg=PA57&dq="The+Class+Equation"](http://books.google.com/books?id=LJtyhu8-xYwC&pg=PA57&dq=))
- [4] Grillet (2007), p. 56 ([http://books.google.com/books?id=LJtyhu8-xYwC&pg=PA56&dq="the+orbits+are+the+conjugacy+classes"](http://books.google.com/books?id=LJtyhu8-xYwC&pg=PA56&dq=))
- Grillet, Pierre Antoine (2007). *Abstract algebra*. Graduate texts in mathematics. **242** (2 ed.). Springer. ISBN 9780387715674.

# Conjugate closure

---

In group theory, the **conjugate closure** of a subset  $S$  of a group  $G$  is the subgroup of  $G$  generated by  $S^G$ , i.e. the closure of  $S^G$  under the group operation, where  $S^G$  is the conjugates of the elements of  $S$ :

$$S^G = \{g^{-1}sg \mid g \in G \text{ and } s \in S\}$$

The conjugate closure of  $S$  is denoted  $\langle S^G \rangle$  or  $\langle S \rangle^G$ .

The conjugate closure of any subset  $S$  of a group  $G$  is always a normal subgroup of  $G$ ; in fact, it is the smallest (by inclusion) normal subgroup of  $G$  which contains  $S$ . For this reason, the conjugate closure is also called the **normal closure** of  $S$  or the **normal subgroup generated by  $S$** . The normal closure can also be characterized as the intersection of all normal subgroups of  $G$  which contain  $S$ . Any normal subgroup is equal to its normal closure.

The conjugate closure of a singleton subset  $\{a\}$  of a group  $G$  is a normal subgroup generated by  $a$  and all elements of  $G$  which are conjugate to  $a$ . Therefore, any simple group is the conjugate closure of any non-identity group element. The conjugate closure of the empty set  $\emptyset$  is the trivial group.

Contrast the normal closure of  $S$  with the *normalizer* of  $S$ , which is (for  $S$  a group) the largest subgroup of  $G$  in which  $S$  *itself* is normal. (This need not be normal in the larger group  $G$ , just as  $\langle S \rangle$  need not be normal in its conjugate/normal closure.)

## References

- Derek F. Holt; Bettina Eick, Eamonn A. O'Brien (2005). *Handbook of Computational Group Theory*. CRC Press. pp. 73. ISBN 1584883723.

# Conjugation of isometries in Euclidean space

---

In a group, the **conjugate** by  $g$  of  $h$  is  $ghg^{-1}$ .

## Translation

If  $h$  is a translation, then its conjugate by an isometry can be described as applying the isometry to the translation:

- the conjugate of a translation by a translation is the first translation
- the conjugate of a translation by a rotation is a translation by a rotated translation vector
- the conjugate of a translation by a reflection is a translation by a reflected translation vector

Thus the conjugacy class within the Euclidean group  $E(n)$  of a translation is the set of all translations by the same distance.

The smallest subgroup of the Euclidean group containing all translations by a given distance is the set of *all* translations. Thus this is the conjugate closure of a singleton containing a translation.

Thus  $E(n)$  is a semidirect product of the orthogonal group  $O(n)$  and the subgroup of translations  $T$ , and  $O(n)$  is isomorphic with the quotient group of  $E(n)$  by  $T$ :

$$O(n) \cong E(n)/T$$

Thus there is a partition of the Euclidean group with in each subset one isometry that keeps the origin fixed, and its combination with all translations.

Each isometry is given by an orthogonal matrix  $A$  in  $O(n)$  and a vector  $b$ :

$$x \mapsto Ax + b$$

and each subset in the quotient group is given by the matrix  $A$  only.

---

Similarly, for the special orthogonal group  $SO(n)$  we have

$$SO(n) \cong E^+(n)/T$$

## Inversion

The conjugate of the inversion in a point by a translation is the inversion in the translated point, etc.

Thus the conjugacy class within the Euclidean group  $E(n)$  of inversion in a point is the set of inversions in all points.

Since a combination of two inversions is a translation, the conjugate closure of a singleton containing inversion in a point is the set of all translations and the inversions in all points. This is the generalized dihedral group  $\text{dih}(R^n)$ .

Similarly  $\{I, -I\}$  is a normal subgroup of  $O(n)$ , and we have:

$$E(n)/\text{dih}(R^n) \cong O(n)/\{I, -I\}$$

For odd  $n$  we also have:

$$O(n) \cong SO(n) \times \{I, -I\}$$

and hence not only

$$O(n)/SO(n) \cong \{I, -I\}$$

but also:

$$O(n)/\{I, -I\} \cong SO(n)$$

For even  $n$  we have:

$$E^+(n)/\text{dih}(R^n) \cong SO(n)/\{I, -I\}$$

## Rotation

In 3D, the conjugate by a translation of a rotation about an axis is the corresponding rotation about the translated axis, etc.

Thus the conjugacy class within the Euclidean group  $E(3)$  of a rotation about an axis is a rotation by the same angle about any axis.

The conjugate closure of a singleton containing a rotation in 3D is  $E^+(3)$ .

In 2D it is different in the case of a  $k$ -fold rotation: the conjugate closure contains  $k$  rotations (including the identity) combined with all translations.

$E(2)$  has quotient group  $O(2)/C_k$  and  $E^+(2)$  has quotient group  $SO(2)/C_k$ . For  $k = 2$  this was already covered above.

## Reflection

The conjugates of a reflection are reflections with a translated, rotated, and reflected mirror plane. The conjugate closure of a singleton containing a reflection is the whole  $E(n)$ .

## Rotoreflexion

The left and also the right coset of a reflection in a plane combined with a rotation by a given angle about a perpendicular axis is the set of all combinations of a reflection in the same or a parallel plane, combined with a rotation by the same angle about the same or a parallel axis, preserving orientation

## Isometry groups

Two isometry groups are said to be equal up to conjugacy with respect to affine transformations if there is an affine transformation such that all elements of one group are obtained by taking the conjugates by that affine transformation of all elements of the other group. This applies for example for the symmetry groups of two patterns which are both of a particular wallpaper group type. If we would just consider conjugacy with respect to isometries, we would not allow for scaling, and in the case of a parallelogrammatic lattice, change of shape of the parallelogram. Note however that the conjugate with respect to an affine transformation of an isometry is in general not an isometry, although volume (in 2D: area) and orientation are preserved.

## Cyclic groups

Cyclic groups are Abelian, so the conjugate by every element of every element is the latter.

$$Z_{mn} / Z_m \cong Z_n.$$

$Z_{mn}$  is the direct product of  $Z_m$  and  $Z_n$  if and only if  $m$  and  $n$  are coprime. Thus e.g.  $Z_{12}$  is the direct product of  $Z_3$  and  $Z_4$ , but not of  $Z_6$  and  $Z_2$ .

## Dihedral groups

Consider the 2D isometry point group  $D_n$ . The conjugates of a rotation are the same and the inverse rotation. The conjugates of a reflection are the reflections rotated by any multiple of the full rotation unit. For odd  $n$  these are all reflections, for even  $n$  half of them.

This group, and more generally, abstract group  $Dih_n$ , has the normal subgroup  $Z_m$  for all divisors  $m$  of  $n$ , including  $n$  itself.

Additionally,  $Dih_{2n}$  has two normal subgroups isomorphic with  $Dih_n$ . They both contain the same group elements forming the group  $Z_n$ , but each has additionally one of the two conjugacy classes of  $Dih_{2n} \setminus Z_{2n}$ .

In fact:

$$Dih_{mn} / Z_n \cong Dih_n$$

$$Dih_{2n} / Dih_n \cong Z_2$$

$$Dih_{4n+2} \cong Dih_{2n+1} \times Z_2$$

# Core (group)

---

In group theory, a branch of mathematics, a **core** is any of certain special normal subgroups of a group. The two most common types are the **normal core** of a subgroup and the **p-core** of a group.

## The normal core

### Definition

For a group  $G$ , the **normal core** of a subgroup  $H$  is the largest normal subgroup of  $G$  that is contained in  $H$  (or equivalently, the intersection of the conjugates of  $H$ ). More generally, the core of  $H$  with respect to a subset  $S \subseteq G$  is the intersection of the conjugates of  $H$  under  $S$ , *i.e.*

$$\text{Core}_S(H) := \bigcap_{s \in S} s^{-1} H s.$$

Under this more general definition, the normal core is the core with respect to  $S=G$ . The normal core of any normal subgroup is the subgroup itself.

### Significance

Normal cores are important in the context of group actions on sets, where the normal core of the isotropy subgroup of any point acts as the identity on its entire orbit. Thus, in case the action is transitive, the normal core of any isotropy subgroup is precisely the kernel of the action.

A **core-free subgroup** is a subgroup whose normal core is the trivial subgroup. Equivalently, it is a subgroup that occurs as the isotropy subgroup of a transitive, faithful group action.

The solution for the hidden subgroup problem in the abelian case generalizes to finding the normal core in case of subgroups of arbitrary groups.

## The $p$ -core

In this section  $G$  will denote a finite group, though some aspects generalize to locally finite groups and to profinite groups.

### Definition

For a prime  $p$ , the  **$p$ -core** of a finite group is defined to be its largest normal  $p$ -subgroup. It is the normal core of every Sylow  $p$ -subgroup of the group. The  $p$ -core of  $G$  is often denoted  $O_p(G)$ , and in particular appears in one of the definitions of the Fitting subgroup of a finite group. Similarly, the  **$p'$ -core** is the largest normal subgroup of  $G$  whose order is coprime to  $p$  and is denoted  $O_{p'}(G)$ . In the area of finite insoluble groups, including the classification of finite simple groups, the  $2'$ -core is often called simply the **core** and denoted  $O(G)$ . This causes only a small amount of confusion, because one can usually distinguish between the core of a group and the core of a subgroup within a group. The  **$p', p$ -core**, denoted  $O_{p', p}(G)$  is defined by  $O_{p', p}(G)/O_{p'}(G) = O_p(G/O_{p'}(G))$ .

For a finite group, the  $p', p$ -core is the unique largest normal  $p$ -nilpotent subgroup. The  $p$ -core can also be defined as the unique largest subnormal  $p$ -subgroup; the  $p'$ -core as the unique largest subnormal  $p'$ -subgroup; and the  $p', p$ -core as the unique largest subnormal  $p$ -nilpotent subgroup.

The  $p'$  and  $p', p$ -core begin the **upper  $p$ -series**. For sets  $\pi_1, \pi_2, \dots, \pi_{n+1}$  of primes, one defines subgroups  $O_{\pi_1, \pi_2, \dots, \pi_{n+1}}(G)$  by:

$$O_{\pi_1, \pi_2, \dots, \pi_{n+1}}(G)/O_{\pi_1, \pi_2, \dots, \pi_n}(G) = O_{\pi_{n+1}}(G/O_{\pi_1, \pi_2, \dots, \pi_n}(G))$$


---

The upper  $p$ -series is formed by taking  $\pi_{2i-1} = p'$  and  $\pi_{2i} = p$ ; there is also a lower  $p$ -series. A finite group is said to be  **$p$ -nilpotent** if and only if it is equal to its own  $p',p$ -core. A finite group is said to be  **$p$ -soluble** if and only if it is equal to some term of its upper  $p$ -series; its  **$p$ -length** is the length of its upper  $p$ -series. A finite group  $G$  is said to be  **$p$ -constrained** for a prime  $p$  if  $C_G(O_{p',p}(G)/O_{p'}(G)) \subseteq O_{p',p}(G)$ .

Every nilpotent group is  $p$ -nilpotent, and every  $p$ -nilpotent group is  $p$ -soluble. Every soluble group is  $p$ -soluble, and every  $p$ -soluble group is  $p$ -constrained. A group is  $p$ -nilpotent if and only if it has a **normal  $p$ -complement**, which is just its  $p'$ -core.

## Significance

Just as normal cores are important for group actions on sets,  $p$ -cores and  $p'$ -cores are important in modular representation theory, which studies the actions of groups on vector spaces. The  $p$ -core of a finite group is the intersection of the kernels of the irreducible representations over any field of characteristic  $p$ . For a finite group, the  $p'$ -core is the intersection of the kernels of the ordinary (complex) irreducible representations that lie in the principal  $p$ -block. For a finite group, the  $p',p$ -core is the intersection of the kernels of the irreducible representations in the principal  $p$ -block over any field of characteristic  $p$ . Also, for a finite group, the  $p',p$ -core is the intersection of the centralizers of the abelian chief factors whose order is divisible by  $p$  (all of which are irreducible representations over a field of size  $p$  lying in the principal block). For a finite,  $p$ -constrained group, an irreducible module over a field of characteristic  $p$  lies in the principal block if and only if the  $p'$ -core of the group is contained in the kernel of the representation.

## Solvable radicals

A related subgroup in concept and notation is the solvable radical. The **solvable radical** is defined to be the largest solvable normal subgroup, and is denoted  $O_\infty(G)$ . There is some variance in the literature in defining the  $p'$ -core of  $G$ . A few authors in only a few papers (for instance Thompson's N-group papers, but not his later work) define the  $p'$ -core of an insoluble group  $G$  as the  $p'$ -core of its solvable radical in order to better mimic properties of the  $2'$ -core.

## References

- Aschbacher, M. (2000), *Finite Group Theory*, Cambridge University Press, ISBN 0-521-78675-4
- Doerk, K.; Hawkes, T. (1992). *Finite Soluble Groups*. Walter de Gruyter. ISBN 3-11-012892-6.
- Huppert, B.; Blackburn, N. (1982). *Finite Groups II*. Springer Verlag. ISBN 0-387-10632-4.

# Coset

---

In mathematics, if  $G$  is a group, and  $H$  is a subgroup of  $G$ , and  $g$  is an element of  $G$ , then

$gH = \{gh : h \text{ an element of } H\}$  is a **left coset of  $H$**  in  $G$ , and

$Hg = \{hg : h \text{ an element of } H\}$  is a **right coset of  $H$**  in  $G$ .

Only when  $H$  is normal will the right and left cosets of  $H$  coincide, which is one definition of normality of a subgroup.

A **coset** is a left or right coset of *some* subgroup in  $G$ . Since  $Hg = g(g^{-1}Hg)$ , the right cosets  $Hg$  (of  $H$ ) and the left cosets  $g(g^{-1}Hg)$  (of the conjugate subgroup  $g^{-1}Hg$ ) are the same. Hence it is not meaningful to speak of a coset as being left or right unless one first specifies the underlying subgroup. In other words: a right coset of one subgroup equals a left coset of a different (conjugate) subgroup. If the left cosets and right cosets are the same then  $H$  is a normal subgroup and the cosets form a group called the quotient group.

The map  $gH \rightarrow (gH)^{-1} = Hg^{-1}$  defines a bijection between the left cosets and the right cosets of  $H$ , so the number of left cosets is equal to the number of right cosets. The common value is called the index of  $H$  in  $G$ .

For abelian groups, left cosets and right cosets are always the same. If the group operation is written additively then the notation used changes to  $g+H$  or  $H+g$ .

Cosets are a basic tool in the study of groups; for example they play a central role in Lagrange's theorem.

## Examples

Let  $G$  be the multiplicative group of  $\{-1,1\}$ , and  $H$  the trivial subgroup  $(1,*)$ . Then  $-1H=\{-1\}$ ,  $1H=H$  are the sole cosets of  $H$  in  $G$ .

Let  $G$  be the additive group of integers  $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$  and  $H$  the subgroup  $m\mathbf{Z} = \{\dots, -2m, -m, 0, m, 2m, \dots\}$  where  $m$  is a positive integer. Then the cosets of  $H$  in  $G$  are the  $m$  sets  $m\mathbf{Z}$ ,  $m\mathbf{Z}+1$ ,  $\dots$ ,  $m\mathbf{Z}+(m-1)$ , where  $m\mathbf{Z}+a = \{\dots, -2m+a, -m+a, a, m+a, 2m+a, \dots\}$ . There are no more than  $m$  cosets, because  $m\mathbf{Z}+m = m(\mathbf{Z}+1) = m\mathbf{Z}$ . The coset  $m\mathbf{Z}+a$  is the congruence class of  $a$  modulo  $m$ .<sup>[1]</sup>

Another example of a coset comes from the theory of vector spaces. The elements (vectors) of a vector space form an abelian group under vector addition. It is not hard to show that subspaces of a vector space are subgroups of this group. For a vector space  $V$ , a subspace  $W$ , and a fixed vector  $a$  in  $V$ , the sets

$$\{x \in V : x = a + n, n \in W\}$$

are called affine subspaces, and are cosets (both left and right, since the group is abelian). In terms of geometric vectors, these affine subspaces are all the "lines" or "planes" parallel to the subspace, which is a line or plane going through the origin.

## Definition using equivalence classes

Some authors<sup>[2]</sup> define the left cosets of  $H$  in  $G$  to be the equivalence classes under the equivalence relation on  $G$  given by  $x \sim y$  if and only if  $x^{-1}y \in H$ . The relation can also be defined by  $x \sim y$  if and only if  $xh=y$  for some  $h$  in  $H$ . It can be shown that the relation given is, in fact, an equivalence relation and that the two definitions are equivalent. It follows that any two left cosets of  $H$  in  $G$  are either identical or disjoint — . In other words every element of  $G$  belongs to one and only one left coset and so the left cosets form a partition of  $G$ .<sup>[3]</sup> Corresponding statements are true for right cosets.

---



## Double cosets

Given two subgroups,  $H$  and  $K$  of a group  $G$ , the **double coset** of  $H$  and  $K$  in  $G$  are sets of the form  $HgK = \{h g k : h \text{ an element of } H, k \text{ an element of } K\}$ . These are the left cosets of  $K$  and right cosets of  $H$  when  $H=1$  and  $K=1$  respectively.<sup>[4]</sup>

## General properties

The identity is in precisely one left or right coset, namely  $H$  itself. Thus  $H$  is both a left and right coset of itself.

A **coset representative** is a representative in the equivalence class sense. A set of representatives of all the cosets is called a transversal. There are other types of equivalence relations in a group, such as conjugacy, that form different classes which do not have the properties discussed here. Some books on very applied group theory erroneously identify the conjugacy class as 'the' equivalence class as opposed to a particular type of equivalence class.

## Index of a subgroup

All left cosets and all right cosets have the same order (number of elements, or cardinality in the case of an infinite  $H$ ), equal to the order of  $H$  (because  $H$  is itself a coset). Furthermore, the number of left cosets is equal to the number of right cosets and is known as the **index** of  $H$  in  $G$ , written as  $[G : H]$ . Lagrange's theorem allows us to compute the index in the case where  $G$  and  $H$  are finite, as per the formula:

$$|G| = [G : H] \cdot |H|.$$

This equation also holds in the case where the groups are infinite, although the meaning may be less clear.

## Cosets and normality

If  $H$  is not normal in  $G$ , then its left cosets are different from its right cosets. That is, there is an  $a$  in  $G$  such that no element  $b$  satisfies  $aH = Hb$ . This means that the partition of  $G$  into the left cosets of  $H$  is a different partition than the partition of  $G$  into right cosets of  $H$ . (It is important to note that *some* cosets may coincide. For example, if  $a$  is in the center of  $G$ , then  $aH = Ha$ .)

On the other hand, the subgroup  $N$  is normal if and only if  $gN = Ng$  for all  $g$  in  $G$ . In this case, the set of all cosets form a group called the quotient group  $G/N$  with the operation  $*$  defined by  $(aN) * (bN) = abN$ . Since every right coset is a left coset, there is no need to differentiate "left cosets" from "right cosets".

## Applications

- Cosets of  $\mathbf{Q}$  in  $\mathbf{R}$  are used in the construction of Vitali sets, a type of non-measurable set.
- Cosets are central in the definition of the transfer.
- Cosets are important in computational group theory. For example Thistlethwaite's algorithm for solving Rubik's Cube relies heavily on cosets.
- Coset leaders are used in decoding received data in Linear error-correcting codes.

## References

- [1] Joshi p. 323
- [2] e.g. Zassenhaus
- [3] Joshi Corrolary 2.3
- [4] Scott p. 19
- Scott, W.R. (1987). "§1.7 Cosets and index". *Group Theory*. Courier Dover Publications. pp. 19 ff.. ISBN 0486653773.
- Joshi, K. D. (1989). "§5.2 Cosets of Subgroups". *Foundations of Discrete Mathematics*. New Age International. pp. 322 ff.. ISBN 8122401201.
- Zassenhaus, Hans J. (1999). "§1.4 Subgroups". *The Theory of Groups*. Courier Dover Publications. pp. 10 ff.. ISBN 0486409228.

## External links

- Nicolas Bray, "Coset (<http://mathworld.wolfram.com/Coset.html>)" from MathWorld.
- Weisstein, Eric W., "Left Coset (<http://mathworld.wolfram.com/LeftCoset.html>)" from MathWorld.
- Weisstein, Eric W., "Right Coset (<http://mathworld.wolfram.com/RightCoset.html>)" from MathWorld.
- Ivanova, O.A. (2001), "Coset in a group" (<http://www.encyclopediaofmath.org/index.php?title=C/c026620>), in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1556080104
- *Coset* (<http://planetmath.org/encyclopedia/Coset.html>) at PlanetMath.
- "Coset" (<http://groupprops.subwiki.org/wiki/Coset>). *groupprops*. The Group Properties Wiki.

# Commutator subgroup

---

In mathematics, more specifically in abstract algebra, the **commutator subgroup** or **derived subgroup** of a group is the subgroup generated by all the commutators of the group.<sup>[1][2]</sup>

The commutator subgroup is important because it is the smallest normal subgroup such that the quotient group of the original group by this subgroup is abelian. In other words,  $G/N$  is abelian if and only if  $N$  contains the commutator subgroup. So in some sense it provides a measure of how far the group is from being abelian; the larger the commutator subgroup is, the "less abelian" the group is.

## Commutators

For elements  $g$  and  $h$  of a group  $G$ , the commutator of  $g$  and  $h$  is  $[g, h] := g^{-1}h^{-1}gh$ . The commutator  $[g, h]$  is equal to the identity element  $e$  if and only if  $gh = hg$ , that is, if and only if  $g$  and  $h$  commute. In general,  $gh = hg[g, h]$ . An element of  $G$  which is of the form  $[g, h]$  for some  $g$  and  $h$  is called a commutator. The identity element  $e = [e, e]$  is always a commutator, and it is the only commutator if and only if  $G$  is abelian.

Here are some simple but useful commutator identities, true for any elements  $s, g, h$  of a group  $G$ :

- $[g, h]^{-1} = [h, g]$ .
- $[g, h]^s = [g^s, h^s]$ , where  $g^s = s^{-1}gs$ .
- For any homomorphism  $f: G \rightarrow H$ ,  $f([g, h]) = [f(g), f(h)]$ .

The first and second identities imply that the set of commutators in  $G$  is closed under inversion and under conjugation. If in the third identity we take  $H = G$ , we get that the set of commutators is stable under any endomorphism of  $G$ . This is in fact a generalization of the second identity, since we can take  $f$  to be the conjugation automorphism  $x \mapsto x^s$ .

---

However, the product of two or more commutators need not be a commutator. A generic example is  $[a,b][c,d]$  in the free group on  $a,b,c,d$ . It is known that the least order of a finite group for which there exists two commutators whose product is not a commutator is 96; in fact there are two nonisomorphic groups of order 96 with this property.

## Definition

This motivates the definition of the **commutator subgroup**  $[G,G]$  (also called the **derived subgroup**, and denoted  $G'$  or  $G^{(1)}$ ) of  $G$ : it is the subgroup generated by all the commutators.

It follows from the properties of commutators that any element of  $[G,G]$  is of the form

$$[g_1, h_1] \cdots [g_n, h_n]$$

for some natural number  $n$ . Moreover, since  $([g_1, h_1] \cdots [g_n, h_n])^s = [g_1^s, h_1^s] \cdots [g_n^s, h_n^s]$ , the commutator subgroup is normal in  $G$ . For any homomorphism  $f: G \rightarrow H$ ,

$$f([g_1, h_1] \cdots [g_n, h_n]) = [f(g_1), f(h_1)] \cdots [f(g_n), f(h_n)],$$

so that  $f([G, G]) \leq [H, H]$ .

This shows that the commutator subgroup can be viewed as a functor on the category of groups, some implications of which are explored below. Moreover, taking  $G = H$  it shows that the commutator subgroup is stable under every endomorphism of  $G$ : that is,  $[G,G]$  is a fully characteristic subgroup of  $G$ , a property which is considerably stronger than normality.

The commutator subgroup can also be defined as the set of elements  $g$  of the group which have an expression as a product  $g = g_1 g_2 \cdots g_k$  that can be rearranged to give the identity.

## Derived series

This construction can be iterated:

$$G^{(0)} := G$$

$$G^{(n)} := [G^{(n-1)}, G^{(n-1)}] \quad n \in \mathbf{N}$$

The groups  $G^{(2)}, G^{(3)}, \dots$  are called the **second derived subgroup**, **third derived subgroup**, and so forth, and the descending normal series

$$\cdots \triangleleft G^{(2)} \triangleleft G^{(1)} \triangleleft G^{(0)} = G$$

is called the **derived series**. This should not be confused with the **lower central series**, whose terms are  $G_n := [G_{n-1}, G]$ , not  $G^{(n)} := [G^{(n-1)}, G^{(n-1)}]$ .

For a finite group, the derived series terminates in a perfect group, which may or may not be trivial. For an infinite group, the derived series need not terminate at a finite stage, and one can continue it to infinite ordinal numbers via transfinite recursion, thereby obtaining the **transfinite derived series**, which eventually terminates at the perfect core of the group.

## Abelianization

Given a group  $G$ , a factor group  $G/N$  is abelian if and only if  $[G,G] \leq N$ .

The quotient  $G/[G,G]$  is an abelian group called the **abelianization** of  $G$  or  **$G$  made abelian**. It is usually denoted by  $G^{\text{ab}}$  or  $G_{\text{ab}}$ .

There is a useful categorical interpretation of the map  $\varphi: G \rightarrow G^{\text{ab}}$ . Namely  $\varphi$  is universal for homomorphisms from  $G$  to an abelian group  $H$ : for any abelian group  $H$  and homomorphism of groups  $f: G \rightarrow H$  there exists a unique homomorphism  $F: G^{\text{ab}} \rightarrow H$  such that  $f = F \circ \varphi$ . As usual for objects defined by universal mapping properties, this shows the uniqueness of the abelianization  $G^{\text{ab}}$  up to canonical isomorphism, whereas the explicit construction  $G \rightarrow G/[G,G]$  shows existence.

The abelianization functor is the left adjoint of the inclusion functor from the category of abelian groups to the category of groups.

Another important interpretation of  $G^{\text{ab}}$  is as  $H_1(G, \mathbf{Z})$ , the first homology group of  $G$  with integral coefficients.

### Classes of groups

A group  $G$  is an **abelian group** if and only if the derived group is trivial:  $[G, G] = \{e\}$ . Equivalently, if and only if the group equals its abelianization. See above for the definition of a group's abelianization.

A group  $G$  is a **perfect group** if and only if the derived group equals the group itself:  $[G, G] = G$ . Equivalently, if and only if the abelianization of the group is trivial. This is "opposite" to abelian.

A group with  $G^{(n)} = \{e\}$  for some  $n$  in  $\mathbf{N}$  is called a **solvable group**; this is weaker than abelian, which is the case  $n = 1$ .

A group with  $G^{(\alpha)} = \{e\}$  for some ordinal number, possibly infinite, is called a **hypoabelian group**; this is weaker than solvable, which is the case  $\alpha$  is finite (a natural number).

### Examples

- The commutator subgroup of the alternating group  $A_4$  is the Klein four group.
- The commutator subgroup of the symmetric group  $S_n$  is the alternating group  $A_n$ .
- The commutator subgroup of the quaternion group  $Q = \{1, -1, i, -i, j, -j, k, -k\}$  is  $[Q, Q] = \{1, -1\}$ .

### Map from Out

Since the derived subgroup is characteristic, any automorphism of  $G$  induces an automorphism of the abelianization. Since the abelianization is abelian, inner automorphisms act trivially, hence this yields a map

$$\text{Out}(G) \rightarrow \text{Aut}(G^{\text{ab}})$$

### References

- [1] Dummit, David S.; Foote, Richard M. (2004). *Abstract Algebra* (3rd ed.). John Wiley & Sons. ISBN 0-471-43334-9.
- [2] Lang, Serge (2002). *Algebra*. Graduate Texts in Mathematics. Springer. ISBN 0-387-95385-X.

# Elementary group theory

---

In mathematics and abstract algebra, a group is the algebraic structure  $\{G, \perp\}$ , where  $G$  is a non-empty set and  $\perp$  denotes a binary operation  $\perp: G \times G \rightarrow G$ , called the *group operation*. The notation  $\perp(x, y)$  is normally shortened to the infix notation  $x \perp y$ , or even to  $xy$ .

A group must obey the following rules (or axioms). Let  $a, b, c$  be arbitrary elements of  $G$ . Then:

- **A1, Closure.**  $a \perp b \in G$ . This axiom is often omitted because a binary operation is closed by definition.
- **A2, Associativity.**  $(a \perp b) \perp c = a \perp (b \perp c)$ .
- **A3, Identity.** There exists an identity (or neutral) element  $e \in G$  such that  $a \perp e = e \perp a = a$ . The *identity* of  $G$  is unique by Theorem 1.4 below.
- **A4, Inverse.** For each  $a \in G$ , there exists an inverse element  $x \in G$  such that  $a \perp x = x \perp a = e$ . The *inverse* of  $a$  is unique by Theorem 1.5 below.

An abelian group also obeys the additional rule:

- **A5, Commutativity.**  $a \perp b = b \perp a$ .

## Notation

The group  $\{G, \perp\}$  is often referred to as "the group  $G$ " or more simply as " $G$ ." Nevertheless, the operation " $\perp$ " is fundamental to the description of the group.  $\{G, \perp\}$  is usually read as "the group  $G$  under  $\perp$ ". When we wish to assert that  $G$  is a group (for example, when stating a theorem), we say that " $G$  is a group under  $\perp$ ". The group operation  $\perp$  can be interpreted in a great many ways. The generic notation for the group operation, identity element, and inverse of  $a$  are  $\perp, e, a'$ , respectively. Because the group operation associates, parentheses have only one necessary use in group theory: to set the scope of the inverse operation.

Group theory may also be notated:

- **Additively** by replacing the generic notation by  $+, 0, -a$ , with "+" being infix. Additive notation is typically used when numerical addition or a commutative operation other than multiplication interprets the group operation;
- **Multiplicatively** by replacing the generic notation by  $*, 1, a^{-1}$ . Infix "\*" is often replaced by simple concatenation, as in standard algebra. Multiplicative notation is typically used when numerical multiplication or a noncommutative operation interprets the group operation.

Other notations are of course possible.

## Examples

### Arithmetic

- Take  $G := \mathbb{Z}$  or  $\mathbb{Q}$  or  $\mathbb{R}$  or  $\mathbb{C}$ , then  $\{G, +\}$  is an abelian group.
- Take  $G := \mathbb{Q} \setminus \{0\}$  or  $\mathbb{R} \setminus \{0\}$  or  $\mathbb{C} \setminus \{0\}$ , then  $\{G, *\}$  is an abelian group.

### Function composition

- Let  $E$  be an arbitrary set, and let  $G$  be the set of all bijective functions from  $E$  to  $E$ . Let function composition, notated by infix  $\circ$ , interpret the group operation. Then  $\{G, \circ\}$  is a group whose identity element is  $id_E: E \rightarrow E, x \mapsto x$ . The group inverse of an arbitrary group element  $f \in G$  is the function inverse  $f^{-1}$ .
-

## Alternative Axioms

The pair of axioms A3 and A4 may be replaced either by the pair:

- **A3'**, left neutral. There exists an  $e \in G$  such that for all  $a \in G$ ,  $e \perp a = a$ .
- **A4'**, left inverse. For each  $a \in G$ , there exists an element  $x \in G$  such that  $x \perp a = e$ .

or by the pair:

- **A3''**, right neutral. There exists an  $e \in G$  such that for all  $a \in G$ ,  $a \perp e = a$ .
- **A4''**, right inverse. For each  $a \in G$ , there exists an element  $x \in G$  such that  $a \perp x = e$ .

These evidently weaker axiom pairs are trivial consequences of A3 and A4. We will now show that the nontrivial converse is also true. Given a left neutral element  $e$ , and for any given  $a \in G$ , then A4' says there exists an  $x$  such that  $x \perp a = e$ .

**Theorem 1.2:**  $a \perp x = e$ .

*Proof.* Let  $y \in G$  be an inverse of  $a \perp x$ . Then:

$$\begin{aligned}
 e &= y \perp (a \perp x) && (1) \\
 &= y \perp (a \perp (e \perp x)) && (A3') \\
 &= y \perp (a \perp ((x \perp a) \perp x)) && (A4') \\
 &= y \perp (a \perp (x \perp (a \perp x))) && (A2) \\
 &= y \perp ((a \perp x) \perp (a \perp x)) && (A2) \\
 &= (y \perp (a \perp x)) \perp (a \perp x) && (A2) \\
 &= e \perp (a \perp x) && (1) \\
 &= a \perp x && (A3')
 \end{aligned}$$

This establishes A4 (and hence A4'').

**Theorem 1.2a:**  $a \perp e = a$ .

*Proof.*

$$\begin{aligned}
 a \perp e &= a \perp (x \perp a) && (A4') \\
 &= (a \perp x) \perp a && (A2) \\
 &= e \perp a && (A4) \\
 &= a && (A3')
 \end{aligned}$$

This establishes A3 (and hence A3'').

**Theorem:** Given A1 and A2, A3' and A4' imply A3 and A4.

*Proof.* Theorems 1.2 and 1.2a.

**Theorem:** Given A1 and A2, A3'' and A4'' imply A3 and A4.

*Proof.* Similar to the above.

## Basic theorems

### Identity is unique

**Theorem 1.4:** The identity element of a group  $\{G, \perp\}$  is unique.

*Proof:* Suppose that  $e$  and  $f$  are two identity elements of  $G$ . Then

$$\begin{aligned} e &= e \perp f \quad (A3'') \\ &= f \quad (A3') \end{aligned}$$

As a result, we can speak of *the* identity element of  $\{G, \perp\}$  rather than *an* identity element. Where different groups are being discussed and compared,  $e_G$  denotes the identity of the specific group  $\{G, \perp\}$ .

### Inverses are unique

**Theorem 1.5:** The inverse of each element in  $\{G, \perp\}$  is unique.

*Proof:* Suppose that  $h$  and  $k$  are two inverses of an element  $g$  of  $G$ . Then

$$\begin{aligned} h &= h \perp e \quad (A3) \\ &= h \perp (g \perp k) \quad (A4) \\ &= (h \perp g) \perp k \quad (A2) \\ &= e \perp k \quad (A4) \\ &= k \quad (A3) \end{aligned}$$

As a result, we can speak of *the* inverse of an element  $a$ , rather than *an* inverse. Without ambiguity, for all  $a$  in  $G$ , we denote by  $a'$  the unique inverse of  $a$ .

### Inverting twice takes you back to where you started

**Theorem 1.6:** For all elements  $a$  in a group  $\{G, \perp\}$ ,  $(a')' = a$ .

*Proof:*  $a' \perp a = e$  and  $(a')' \perp a' = e$  are both true by A4. Therefore both  $a$  and  $(a')'$  are inverses of  $a'$ . By Theorem 1.5,  $a = (a')'$ .

Equivalently, inverting is an involution.

### Inverse of $ab$

**Theorem 1.7:** For all elements  $a$  and  $b$  in group  $\{G, \perp\}$ ,  $(a \perp b)' = b' \perp a'$ .

*Proof:*  $(a \perp b) \perp (b' \perp a') = a \perp (b \perp b') \perp a' = a \perp e \perp a' = a \perp a' = e$ . The conclusion follows from Theorem 1.4.

### Cancellation

**Theorem 1.8:** For all elements  $a, x, y$  in a group  $\{G, \perp\}$ , then

$$x = y \Leftrightarrow a \perp x = a \perp y \Leftrightarrow x \perp a = y \perp a.$$

*Proof.*

(1) If  $x = y$ , then multiplying by the same value on either side preserves equality.

(2) If  $a \perp x = a \perp y$  then by (1)

$$\begin{aligned} a' \perp (a \perp x) &= a' \perp (a \perp y) \\ \Rightarrow (a' \perp a) \perp x &= (a' \perp a) \perp y \\ \Rightarrow e \perp x &= e \perp y \\ \Rightarrow x &= y \end{aligned}$$

(3) If  $x \perp a = y \perp a$  we use the same method as in (2).

### Latin square property

**Theorem 1.3:** For all elements  $a, b$  in a group  $\{G, \perp\}$ , there exists a unique  $x \in G$  such that  $a \perp x = b$ , namely  $x = a' \perp b$ .

*Proof.*

Existence: If we let  $x := a' \perp b$ , then  $a \perp (a' \perp b) = (a \perp a') \perp b = e \perp b = b$ .

Unicity: Suppose  $x$  satisfies  $a \perp x = b$ , then by Theorem 1.8,  $a' \perp (a \perp x) = a' \perp b \Leftrightarrow x = a' \perp b$ .

### Powers

For  $n \in \mathbb{Z}$  and  $a$  in group  $\{G, \perp\}$  we define:

$$a^n := \begin{cases} \underbrace{a \perp a \perp \cdots \perp a}_{n \text{ times}}, & \text{if } n > 0 \\ e, & \text{if } n = 0 \\ \underbrace{a' \perp a' \perp \cdots \perp a'}_{-n \text{ times}}, & \text{if } n < 0 \end{cases}$$

**Theorem 1.9:** For all  $a$  in group  $\{G, \perp\}$  and  $n, m \in \mathbb{Z}$ :

$$\begin{aligned} a^m \perp a^n &= a^{m+n} \\ (a^m)^n &= a^{m*n} \end{aligned}$$

## Order

### Of a group element

The order of an element  $a$  in a group  $G$  is the least positive integer  $n$  such that  $a^n = e$ . Sometimes this is written " $\text{o}(a)=n$ ".  $n$  can be infinite.

**Theorem 1.10:** A group whose nontrivial elements all have order 2 is abelian. In other words, if all elements  $g$  in a group  $G$   $g^2=e$  is the case, then for all elements  $a, b$  in  $G$ ,  $a*b=b*a$ .

*Proof.* Let  $a, b$  be any 2 elements in the group  $G$ . By A1,  $a*b$  is also a member of  $G$ . Using the given condition, we know that  $(a*b)*(a*b)=e$ . Hence:

- $b*a$
- $=e*(b*a)*e$
- $=(a*a)*(b*a)*(b*b)$
- $=a*(a*b)*(a*b)*b$
- $=a*e*b$
- $=a*b$ .

Since the group operation  $*$  commutes, the group is abelian



## Of a group

The **order of the group**  $G$ , usually denoted by  $|G|$  or occasionally by  $o(G)$ , is the number of elements in the set  $G$ , in which case  $\langle G, * \rangle$  is a *finite group*. If  $G$  is an infinite set, then the group  $\langle G, * \rangle$  has order equal to the cardinality of  $G$ , and is an *infinite group*.

## Subgroups

A subset  $H$  of  $G$  is called a **subgroup** of a group  $\langle G, * \rangle$  if  $H$  satisfies the axioms of a group, using the same operator "\*", and restricted to the subset  $H$ . Thus if  $H$  is a subgroup of  $\langle G, * \rangle$ , then  $\langle H, * \rangle$  is also a group, and obeys the above theorems, restricted to  $H$ . The *order* of subgroup  $H$  is the number of elements in  $H$ .

A *proper subgroup* of a group  $G$  is a subgroup which is not identical to  $G$ . A *non-trivial* subgroup of  $G$  is (usually) any proper subgroup of  $G$  which contains an element other than  $e$ .

**Theorem 2.1:** If  $H$  is a subgroup of  $\langle G, * \rangle$ , then the identity  $e_H$  in  $H$  is identical to the identity  $e$  in  $\langle G, * \rangle$ .

*Proof.* If  $h$  is in  $H$ , then  $h * e_H = h$ ; since  $h$  must also be in  $G$ ,  $h * e = h$ ; so by theorem 1.8,  $e_H = e$ .

**Theorem 2.2:** If  $H$  is a subgroup of  $G$ , and  $h$  is an element of  $H$ , then the inverse of  $h$  in  $H$  is identical to the inverse of  $h$  in  $G$ .

*Proof.* Let  $h$  and  $k$  be elements of  $H$ , such that  $h * k = e$ ; since  $h$  must also be in  $G$ ,  $h * h^{-1} = e$ ; so by theorem 1.5,  $k = h^{-1}$ .

Given a subset  $S$  of  $G$ , we often want to determine whether or not  $S$  is also a subgroup of  $G$ . A handy theorem valid for both infinite and finite groups is:

**Theorem 2.3:** If  $S$  is a non-empty subset of  $G$ , then  $S$  is a subgroup of  $G$  if and only if for all  $a, b$  in  $S$ ,  $a * b^{-1}$  is in  $S$ .

*Proof.* If for all  $a, b$  in  $S$ ,  $a * b^{-1}$  is in  $S$ , then

- $e$  is in  $S$ , since  $a * a^{-1} = e$  is in  $S$ .
- for all  $a$  in  $S$ ,  $e * a^{-1} = a^{-1}$  is in  $S$
- for all  $a, b$  in  $S$ ,  $a * b = a * (b^{-1})^{-1}$  is in  $S$

Thus, the axioms of closure, identity, and inverses are satisfied, and associativity is inherited; so  $S$  is subgroup.

Conversely, if  $S$  is a subgroup of  $G$ , then it obeys the axioms of a group.

- As noted above, the identity in  $S$  is identical to the identity  $e$  in  $G$ .
- By A4, for all  $b$  in  $S$ ,  $b^{-1}$  is in  $S$
- By A1,  $a * b^{-1}$  is in  $S$ .

The intersection of two or more subgroups is again a subgroup.

**Theorem 2.4:** The intersection of any non-empty set of subgroups of a group  $G$  is a subgroup.

*Proof.* Let  $\{H_i\}$  be a set of subgroups of  $G$ , and let  $K = \cap \{H_i\}$ .  $e$  is a member of every  $H_i$  by theorem 2.1; so  $K$  is not empty. If  $h$  and  $k$  are elements of  $K$ , then for all  $i$ ,

- $h$  and  $k$  are in  $H_i$ .
- By the previous theorem,  $h * k^{-1}$  is in  $H_i$ .
- Therefore,  $h * k^{-1}$  is in  $\cap \{H_i\}$ .

Therefore for all  $h, k$  in  $K$ ,  $h * k^{-1}$  is in  $K$ . Then by the previous theorem,  $K = \cap \{H_i\}$  is a subgroup of  $G$ ; and in fact  $K$  is a subgroup of each  $H_i$ .

Given a group  $\langle G, * \rangle$ , define  $x * x$  as  $x^2$ ,  $x * x * x * \dots * x$  ( $n$  times) as  $x^n$ , and define  $x^0 = e$ . Similarly, let  $x^{-n}$  for  $(x^{-1})^n$ . Then we have:

**Theorem 2.5:** Let  $a$  be an element of a group  $\langle G, * \rangle$ . Then the set  $\{a^n: n \text{ is an integer}\}$  is a subgroup of  $G$ .

A subgroup of this type is called a *cyclic* subgroup; the subgroup of the powers of  $a$  is often written as  $\langle a \rangle$ , and we say that  $a$  *generates*  $\langle a \rangle$ .

## Cosets

If  $S$  and  $T$  are subsets of  $G$ , and  $a$  is an element of  $G$ , we write " $a*S$ " to refer to the subset of  $G$  made up of all elements of the form  $a*s$ , where  $s$  is an element of  $S$ ; similarly, we write " $S*a$ " to indicate the set of elements of the form  $s*a$ . We write  $S*T$  for the subset of  $G$  made up of elements of the form  $s*t$ , where  $s$  is an element of  $S$  and  $t$  is an element of  $T$ .

If  $H$  is a subgroup of  $G$ , then a *left coset* of  $H$  is a set of the form  $a*H$ , for some  $a$  in  $G$ . A *right coset* is a subset of the form  $H*a$ .

If  $H$  is a subgroup of  $G$ , the following useful theorems, stated without proof, hold for all cosets:

- Any  $x$  and  $y$  are elements of  $G$ , then either  $x*H = y*H$ , or  $x*H$  and  $y*H$  have empty intersection.
- Every left (right) coset of  $H$  in  $G$  contains the same number of elements.
- $G$  is the disjoint union of the left (right) cosets of  $H$ .
- Then the number of distinct left cosets of  $H$  equals the number of distinct right cosets of  $H$ .

Define the **index** of a subgroup  $H$  of a group  $G$  (written " $[G:H]$ ") to be the number of distinct left cosets of  $H$  in  $G$ .

From these theorems, we can deduce the important Lagrange's theorem, relating the order of a subgroup to the order of a group:

- **Lagrange's theorem:** If  $H$  is a subgroup of  $G$ , then  $|G| = |H|*[G:H]$ .

For finite groups, this can be restated as:

- **Lagrange's theorem:** If  $H$  is a subgroup of a finite group  $G$ , then the order of  $H$  divides the order of  $G$ .
- If the order of group  $G$  is a prime number,  $G$  is cyclic.

## References

- Jordan, C. R and D.A. *Groups*. Newnes (Elsevier), ISBN 0-340-61045-X
- Scott, W R. *Group Theory*. Dover Publications, ISBN 0-486-65377-3

# Euler's theorem

---

In number theory, **Euler's theorem** (also known as the **Fermat–Euler theorem** or **Euler's totient theorem**) states that if  $n$  and  $a$  are coprime positive integers, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

where  $\varphi(n)$  is Euler's totient function. (The notation is explained in the article Modular arithmetic.) It was first stated and proved by Leonhard Euler in 1736.<sup>[1]</sup>

There is a converse of Euler's theorem: if the above congruence is true then  $a$  and  $n$  must be coprime.

The theorem is a generalization of Fermat's little theorem, and is further generalized by Carmichael's theorem.

The theorem may be used to easily reduce large powers modulo  $n$ . For example, consider finding the ones place decimal digit of  $7^{222}$ , i.e.  $7^{222} \pmod{10}$ . Note that 7 and 10 are coprime, and  $\varphi(10) = 4$ . So Euler's theorem yields  $7^4 \equiv 1 \pmod{10}$ , and we get  $7^{222} \equiv 7^{4 \times 55 + 2} \equiv (7^4)^{55} \times 7^2 \equiv 1^{55} \times 7^2 \equiv 49 \equiv 9 \pmod{10}$ .

In general, when reducing a power of  $a$  modulo  $n$  (where  $a$  and  $n$  are coprime), one needs to work modulo  $\varphi(n)$  in the exponent of  $a$ :

$$\text{if } x \equiv y \pmod{\varphi(n)}, \text{ then } a^x \equiv a^y \pmod{n}.$$

Euler's theorem also forms the basis of the RSA encryption system: encryption and decryption in this system together amount to exponentiating the original text by  $k\varphi(n)+1$  for some positive integer  $k$ , so Euler's theorem shows that the decrypted result is the same as the original.

## Notes

[1] Weisstein, Eric W., "Euler's Totient Theorem (<http://mathworld.wolfram.com/EulersTotientTheorem.html>)" from MathWorld.

## References

The *Disquisitiones Arithmeticae* has been translated from Gauss's Ciceronian Latin into English and German. The German edition includes all of his papers on number theory: all the proofs of quadratic reciprocity, the determination of the sign of the Gauss sum, the investigations into biquadratic reciprocity, and unpublished notes.

- Gauss, Carl Friedrich; Clarke, Arthur A. (translator into English) (1986), *Disquisitiones Arithmeticae (Second, corrected edition)*, New York: Springer, ISBN 0387962549
- Gauss, Carl Friedrich; Maser, H. (translator into German) (1965), *Untersuchungen über höhere Arithmetik (Disquisitiones Arithmeticae & other papers on number theory) (Second edition)*, New York: Chelsea, ISBN 0-8284-0191-8
- Hardy, G. H.; Wright, E. M. (1980), *An Introduction to the Theory of Numbers (Fifth edition)*, Oxford: Oxford University Press, ISBN 978-0198531715
- Ireland, Kenneth; Rosen, Michael (1990), *A Classical Introduction to Modern Number Theory (Second edition)*, New York: Springer, ISBN 0-387-97329-X
- Landau, Edmund (1966), *Elementary Number Theory*, New York: Chelsea

## External links

- Weisstein, Eric W., " Euler's Totient Theorem (<http://mathworld.wolfram.com/EulersTotientTheorem.html>)" from MathWorld.
- Euler's Theorem (<http://planetmath.org/encyclopedia/EulersTheorem.html>) at PlanetMath (<http://planetmath.org>)

# Fitting subgroup

---

In mathematics, especially in the area of algebra known as group theory, the **Fitting subgroup**  $F$  of a finite group  $G$ , named after Hans Fitting, is the unique largest normal nilpotent subgroup of  $G$ . Intuitively, it represents the smallest subgroup which "controls" the structure of  $G$  when  $G$  is solvable. When  $G$  is not solvable, a similar role is played by the **generalized Fitting subgroup**  $F^*$ , which is generated by the Fitting subgroup and the **components** of  $G$ .

For an arbitrary (not necessarily finite) group  $G$ , the Fitting subgroup is defined to be the subgroup generated by the nilpotent normal subgroups of  $G$ . For infinite groups, the Fitting subgroup is not always nilpotent.

The remainder of this article deals exclusively with finite groups.

## The Fitting subgroup

The nilpotency of the Fitting subgroup of a finite group is guaranteed by Fitting's theorem which says that the product of a finite collection of normal nilpotent subgroups of  $G$  is again a normal nilpotent subgroup. It may also be explicitly constructed as the product of the  $p$ -cores of  $G$  over all of the primes  $p$  dividing the order of  $G$ .

If  $G$  is a finite non-trivial solvable group then the Fitting subgroup is always non-trivial, i.e. if  $G \neq 1$  is finite solvable, then  $F(G) \neq 1$ . Similarly the Fitting subgroup of  $G/F(G)$  will be nontrivial if  $G$  is not itself nilpotent, giving rise to the concept of Fitting length. Since the Fitting subgroup of a finite solvable group contains its own centralizer, this gives a method of understanding finite solvable groups as extensions of nilpotent groups by faithful automorphism groups of nilpotent groups.

In a nilpotent group, every chief factor is centralized by every element. Relaxing the condition somewhat, and taking the subgroup of elements of a general finite group which centralize every chief factor, one simply gets the Fitting subgroup again (Huppert 1967, Kap.VI, Satz 5.4, p.686):

$$\text{Fit}(G) = \bigcap \{C_G(H/K) : H/K \text{ a chief factor of } G\}.$$

The generalization to  $p$ -nilpotent groups is similar.

## The generalized Fitting subgroup

A **component** of a group is a subnormal quasisimple subgroup. (A group is **quasisimple** if it is a perfect central extension of a simple group.) The **layer**  $E(G)$  or  $L(G)$  of a group is the subgroup generated by all components. Any two components of a group commute, so the layer is a perfect central extension of a product of simple groups, and is the largest normal subgroup of  $G$  with this structure. The generalized Fitting subgroup  $F^*(G)$  is the subgroup generated by the layer and the Fitting subgroup. The layer commutes with the Fitting subgroup, so the generalized Fitting subgroup is a central extension of a product of  $p$ -groups and simple groups.

The layer is also the maximal normal semisimple subgroup, where a group is called **semisimple** if it is a perfect central extension of a product of simple groups.

The definition of the generalized Fitting subgroup looks a little strange at first. To motivate it, consider the problem of trying to find a normal subgroup  $H$  of  $G$  that contains its own centralizer and the Fitting group. If  $C$  is the centralizer of  $H$  we want to prove that  $C$  is contained in  $H$ . If not, pick a minimal characteristic subgroup  $M/Z(H)$  of

---

$C/Z(H)$ , where  $Z(H)$  is the center of  $H$ , which is the same as the intersection of  $C$  and  $H$ . Then  $M/Z(H)$  is a product of simple or cyclic groups as it is characteristically simple. If  $M/Z(H)$  is a product of cyclic groups then  $M$  must be in the Fitting subgroup. If  $M/Z(H)$  is a product of non-abelian simple groups then the derived subgroup of  $M$  is a normal semisimple subgroup mapping onto  $M/Z(H)$ . So if  $H$  contains the Fitting subgroup and all normal semisimple subgroups, then  $M/Z(H)$  must be trivial, so  $H$  contains its own centralizer. The generalized Fitting subgroup is the smallest subgroup that contains the Fitting subgroup and all normal semisimple subgroups.

The generalized Fitting subgroup can also be viewed as a generalized centralizer of chief factors. A nonabelian semisimple group cannot centralize itself, but it does act on itself as inner automorphisms. A group is said to be **quasi-nilpotent** if every element acts as an inner automorphism on every chief factor. The generalized Fitting subgroup is the unique largest subnormal quasi-nilpotent subgroup, and is equal to the set of all elements which act as inner automorphisms on every chief factor of the whole group (Huppert 1967, Kap.VI, Satz 5.4, p. 686):

$$\text{Fit}^*(G) = \bigcap \{HC_G(H/K) : H/K \text{ a chief factor of } G\}.$$

Here an element  $g$  is in  $HC_G(H/K)$  if and only if there is some  $h$  in  $H$  such that for every  $x$  in  $H$ ,  $x^g \equiv x^h \pmod{K}$ .

## Properties

If  $G$  is a finite solvable group, then the Fitting subgroup contains its own centralizer. The centralizer of the Fitting subgroup is the center of the Fitting subgroup. In this case, the generalized Fitting subgroup is equal to the Fitting subgroup. More generally, if  $G$  is any finite group, the generalized Fitting subgroup contains its own centralizer. This means that in some sense the generalized Fitting subgroup controls  $G$ , because  $G$  modulo the centralizer of  $F^*(G)$  is contained in the automorphism group of  $F^*(G)$ , and the centralizer of  $F^*(G)$  is contained in  $F^*(G)$ . In particular there are only a finite number of groups with given generalized Fitting subgroup.

## Applications

The normalizers of nontrivial  $p$ -subgroups of a finite group are called the  **$p$ -local subgroups** and exert a great deal of control over the structure of the group (allowing what is called local analysis). A finite group is said to be of **characteristic  $p$  type** if  $F^*(G)$  is a  $p$ -group for every  $p$ -local subgroup, because any group of Lie type defined over a field of characteristic  $p$  has this property. In the classification of finite simple groups, this allows one to guess over which field a simple group should be defined. Note that a few groups are of characteristic  $p$  type for more than one  $p$ .

If a simple group is not of Lie type over a field of given characteristic  $p$ , then the  $p$ -local subgroups usually have components in the generalized Fitting subgroup, though there are many exceptions for groups that have small rank, are defined over small fields, or are sporadic. This is used to classify the finite simple groups, because if a  $p$ -local subgroup has a known component, it is often possible to identify the whole group (Aschbacher & Seitz 1976).

The analysis of finite simple groups by means of the structure and embedding of the generalized Fitting subgroups of their maximal subgroups was originated by Helmut Bender (Bender 1970) and has come to be known as Bender's method. It is especially effective in the exceptional cases where components or signalizer functors are not applicable.

## References

- Aschbacher, Michael (2000), *Finite Group Theory*, Cambridge University Press, ISBN 978-0-521-78675-1
- Aschbacher, Michael; Seitz, Gary M. (1976), "On groups with a standard component of known type", *Osaka J. Math.* **13** (3): 439–482
- Huppert, B. (1967) (in German), *Endliche Gruppen*, Berlin, New York: Springer-Verlag, ISBN 978-3-540-03825-2, OCLC 527050, MR0224703
- Bender, Helmut (1970), "On groups with abelian Sylow 2-subgroups", *Mathematische Zeitschrift* **117**: 164–176, doi:10.1007/BF01109839, ISSN 0025-5874, MR0288180

## Hamiltonian group

In group theory, a **Dedekind group** is a group  $G$  such that every subgroup of  $G$  is normal. All abelian groups are Dedekind groups. A non-abelian Dedekind group is called a **Hamiltonian group**.<sup>[1]</sup>

The most familiar (and smallest) example of a Hamiltonian group is the quaternion group of order 8, denoted by  $Q_8$ . It can be shown that every Hamiltonian group is a direct product of the form  $G = Q_8 \times B \times D$ , where  $B$  is the direct sum of some number of copies of the cyclic group  $C_2$ , and  $D$  is a periodic abelian group with all elements of odd order.

Dedekind groups are named after Richard Dedekind, who investigated them in (Dedekind 1897), proving a form of the above structure theorem (for finite groups). He named the non-abelian ones after William Rowan Hamilton, the discoverer of quaternions.

In 1898 George Miller delineated the structure of a Hamiltonian group in terms of its order and that of its subgroups. For instance, he shows "a Hamilton group of order  $2^a$  has  $2^{2a-6}$  quaternion groups as subgroups". In 2005 Horvat *et al.* used this structure to count the number of Hamiltonian groups of any order  $n = 2^e o$  where  $o$  is an odd integer. When  $e \leq 3$  then there are no Hamiltonian groups of order  $n$ , otherwise there are the same number as there are Abelian groups of order  $o$ .

## Notes

[1] Hall (1999), p. 190 ([http://books.google.com/books?id=oyxnWF9ssI8C&pg=PA190&dq="Hamiltonian"](http://books.google.com/books?id=oyxnWF9ssI8C&pg=PA190&dq=)).

## References

- Dedekind, Richard (1897), "Ueber Gruppen, deren sämtliche Theiler Normaltheiler sind" (<http://resolver.sub.uni-goettingen.de/purl?GDZPPN002256258>), *Mathematische Annalen* **48** (4): 548–561, doi:10.1007/BF01447922, ISSN 0025-5831, JFM 28.0129.03, MR1510943
- Hall, Marshall (1999), *The theory of groups*, AMS Bookstore, p. 190, ISBN 9780821819678
- Horvat, Boris; Jaklič, Gašper; Pisanski, Tomaž (2005). "On the number of Hamiltonian groups". *Mathematical Communications* **10** (1): 89–94.
- G. A. Miller (1898) "On the Hamilton groups", *Bulletin of the American Mathematical Society* 4(10):510–15.
- Olga Taussky-Todd (1970) "Sums of squares", *American Mathematical Monthly*: 77:805–30.

# Identity element

In mathematics, an **identity element** (or **neutral element**) is a special type of element of a set with respect to a binary operation on that set. It leaves other elements unchanged when combined with them. This is used for groups and related concepts.

The term *identity element* is often shortened to *identity* (as will be done in this article) when there is no possibility of confusion.

Let  $(S,*)$  be a set  $S$  with a binary operation  $*$  on it (known as a magma). Then an element  $e$  of  $S$  is called a **left identity** if  $e * a = a$  for all  $a$  in  $S$ , and a **right identity** if  $a * e = a$  for all  $a$  in  $S$ . If  $e$  is both a left identity and a right identity, then it is called a **two-sided identity**, or simply an **identity**.

An identity with respect to addition is called an **additive identity** (often denoted as 0) and an identity with respect to multiplication is called a **multiplicative identity** (often denoted as 1). The distinction is used most often for sets that support both binary operations, such as rings. The multiplicative identity is often called the **unit** in the latter context, where, unfortunately, a unit is also sometimes used to mean an element with a multiplicative inverse.

## Examples

set	operation	identity
real numbers	+ (addition)	0
real numbers	· (multiplication)	1
real numbers	$a^b$ (exponentiation)	1 (right identity only)
positive integers	least common multiple	1
nonnegative integers	greatest common divisor	0 (under most definitions of GCD)
$m$ -by- $n$ matrices	+ (addition)	matrix of all zeroes
$n$ -by- $n$ square matrices	· (multiplication)	$I_n$ (matrix with 1 on diagonal and 0 elsewhere)
all functions from a set $M$ to itself	$\square$ (function composition)	identity function
all functions from a set $M$ to itself	$*$ (convolution)	$\delta$ (Dirac delta)
character strings, lists	concatenation	empty string, empty list
extended real numbers	minimum/infimum	$+\infty$
extended real numbers	maximum/supremum	$-\infty$
subsets of a set $M$	$\cap$ (intersection)	$M$
sets	$\cup$ (union)	$\{ \}$ (empty set)
boolean logic	$\wedge$ (logical and)	$\top$ (truth)
boolean logic	$\vee$ (logical or)	$\perp$ (falsity)
boolean logic	$\oplus$ (Exclusive or)	$\perp$ (falsity)
compact surfaces	$\#$ (connected sum)	$S^2$
only two elements $\{e, f\}$	$*$ defined by $e * e = f * e = e$ and $f * f = e * f = f$	both $e$ and $f$ are left identities, but there is no right identity and no two-sided identity

## Properties

As the last example shows, it is possible for  $(S, *)$  to have several left identities. In fact, every element can be a left identity. Similarly, there can be several right identities. But if there is both a right identity and a left identity, then they are equal and there is just a single two-sided identity. To see this, note that if  $l$  is a left identity and  $r$  is a right identity then  $l = l * r = r$ . In particular, there can never be more than one two-sided identity. If there were two,  $e$  and  $f$ , then  $e * f$  would have to be equal to both  $e$  and  $f$ .

It is also quite possible for  $(S, *)$  to have *no* identity element. The most common example of this is the cross product of vectors. The absence of an identity element is related to the fact that the direction of any nonzero cross product is always orthogonal to any element multiplied – so that it is not possible to obtain a non-zero vector in the same direction as the original. Another example would be the additive semigroup of positive natural numbers.

## References

- M. Kilp, U. Knauer, A.V. Mikhalev, *Monoids, Acts and Categories with Applications to Wreath Products and Graphs*, De Gruyter Expositions in Mathematics vol. 29, Walter de Gruyter, 2000, ISBN 3110152487, p. 14-15

# Lagrange's theorem (group theory)

---

**Lagrange's theorem**, in the mathematics of group theory, states that for any finite group  $G$ , the order (number of elements) of every subgroup  $H$  of  $G$  divides the order of  $G$ . The theorem is named after Joseph Lagrange.

## Proof of Lagrange's Theorem

This can be shown using the concept of left cosets of  $H$  in  $G$ . The left cosets are the equivalence classes of a certain equivalence relation on  $G$  and therefore form a partition of  $G$ . Specifically,  $x$  and  $y$  in  $G$  are related if and only if there exists  $h$  in  $H$  such that  $x = yh$ . If we can show that all cosets of  $H$  have the same number of elements, then each coset of  $H$  has precisely  $|H|$  elements. We are then done since the order of  $H$  times the number of cosets is equal to the number of elements in  $G$ , thereby proving that the order of  $H$  divides the order of  $G$ . Now, if  $aH$  and  $bH$  are two left cosets of  $H$ , we can define a map  $f: aH \rightarrow bH$  by setting  $f(x) = ba^{-1}x$ . This map is bijective because its inverse is given by  $f^{-1}(y) = ab^{-1}y$ .

This proof also shows that the quotient of the orders  $|G| / |H|$  is equal to the index  $[G : H]$  (the number of left cosets of  $H$  in  $G$ ). If we write this statement as

$$|G| = [G : H] \cdot |H|,$$

then, seen as a statement about cardinal numbers, it is equivalent to the Axiom of choice.

## Using the theorem

A consequence of the theorem is that the order of any element  $a$  of a finite group (i.e. the smallest positive integer number  $k$  with  $a^k = e$ , where  $e$  is the identity element of the group) divides the order of that group, since the order of  $a$  is equal to the order of the cyclic subgroup generated by  $a$ . If the group has  $n$  elements, it follows

$$a^n = e.$$

This can be used to prove Fermat's little theorem and its generalization, Euler's theorem. These special cases were known long before the general theorem was proved.

The theorem also shows that any group of prime order is cyclic and simple. This in turn can be used to prove Wilson's theorem, that if  $p$  is prime then  $p$  is a factor of  $(p-1)!+1$ .



## Existence of subgroups of given order

Lagrange's theorem raises the converse question as to whether every divisor of the order of a group is the order of some subgroup. This does not hold in general: given a finite group  $G$  and a divisor  $d$  of  $|G|$ , there does not necessarily exist a subgroup of  $G$  with order  $d$ . The smallest example is the alternating group  $G = A_4$  which has 12 elements but no subgroup of order 6. A *CLT group* is a finite group with the property that for every divisor of the order of the group, there is a subgroup of that order. It is known that a CLT group must be solvable and that every supersolvable group is a CLT group: however there exists solvable groups which are not CLT and CLT groups which are not supersolvable.

There are partial converses to Lagrange's theorem. For general groups, Cauchy's theorem guarantees the existence of an element, and hence of a cyclic subgroup, of order any prime dividing the group order; Sylow's theorem extends this to the existence of a subgroup of order equal to the maximal power of any prime dividing the group order. For solvable groups, Hall's theorems assert the existence of a subgroup of order equal to any unitary divisor of the group order (that is, a divisor coprime to its cofactor).

## History

Lagrange did not prove Lagrange's theorem in its general form. He stated, in his article *Réflexions sur la résolution algébrique des équations*,<sup>[1]</sup> that if a polynomial in  $n$  variables has its variables permuted in all  $n!$  ways, the number of different polynomials that are obtained is always a factor of  $n!$ . (For example if the variables  $x$ ,  $y$ , and  $z$  are permuted in all 6 possible ways in the polynomial  $x + y - z$  then we get a total of 3 different polynomials:  $x + y - z$ ,  $x + z - y$ , and  $y + z - x$ . Note that 3 is a factor of 6.) The number of such polynomials is the index in the symmetric group  $S_n$  of the subgroup  $H$  of permutations which preserve the polynomial. (For the example of  $x + y - z$ , the subgroup  $H$  in  $S_3$  contains the identity and the transposition  $(xy)$ .) So the size of  $H$  divides  $n!$ . With the later development of abstract groups, this result of Lagrange on polynomials was recognized to extend to the general theorem about finite groups which now bears his name.

Lagrange did not prove his theorem; all he did, essentially, was to discuss some special cases. The first complete proof of the theorem was provided by Abbati and published in 1803.<sup>[2]</sup>

## Notes

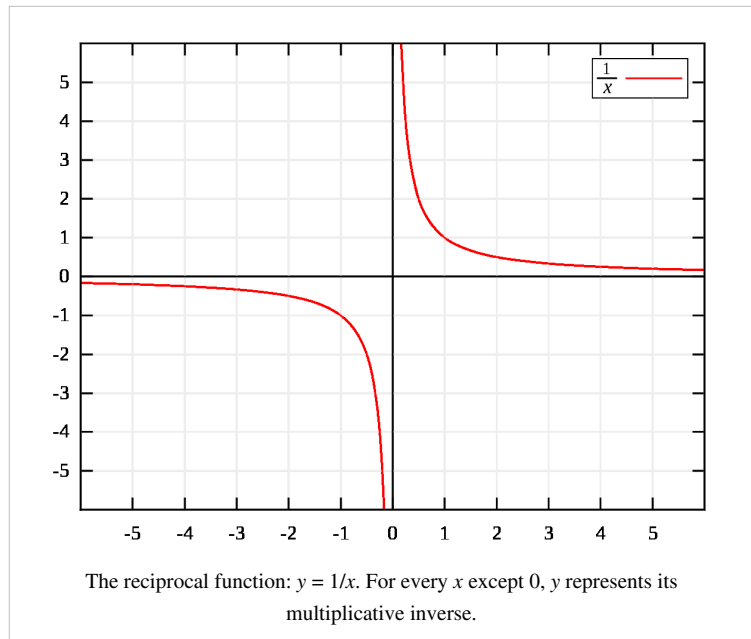
- [1] Lagrange, J. L. (1771) "Réflexions sur la résolution algébrique des équations" [Reflections on the algebraic solution of equations] (part II), *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin*, pages 138-254; see especially pages 202-203. Available on-line (in French, among Lagrange's collected works) at: [http://math-doc.ujf-grenoble.fr/cgi-bin/oeitem?id=OE\\_LAGRANGE\\_\\_3\\_205\\_0](http://math-doc.ujf-grenoble.fr/cgi-bin/oeitem?id=OE_LAGRANGE__3_205_0) [Click on "Section seconde. De la résolution des équations du quatrième degré 254-304"].
- [2] P. Abbati (1803) "Lettera di Pietro Abbati Modenese al socio Paolo Ruffini da questo presentata il di 16. Dicembre 1802" [Letter from Pietro Abbati of Modena to the member Paolo Ruffini, who submitted it on the 16. December 1802], *Memorie di Matematica e di Fisica della Società Italiana delle Scienze*, vol. 10 (part 2), pages 385-409. See also: Richard L. Roth (April 2001) "A history of Lagrange's theorem on groups," *Mathematics Magazine*, vol. 74, no. 2, pages 99-108.

## References

- Bray, Henry G. (1968), "A note on CLT groups", *Pacific J. Math.* **27** (2): 229–231
- Gallian, Joseph (2006), *Contemporary Abstract Algebra* (6th ed.), Boston: Houghton Mifflin, ISBN 978-0-618-51471-7
- Dummit, David S.; Foote, Richard M. (2004), *Abstract algebra* (3rd ed.), New York: John Wiley & Sons, ISBN 978-0-471-43334-7, MR2286236
- Roth, Richard R. (2001), "A History of Lagrange's Theorem on Groups", *Mathematics Magazine* **74** (2): 99–108, doi:10.2307/2690624, JSTOR 2690624

# Multiplicative inverse

In mathematics, a **multiplicative inverse** or **reciprocal** for a number  $x$ , denoted by  $1/x$  or  $x^{-1}$ , is a number which when multiplied by  $x$  yields the multiplicative identity, 1. The multiplicative inverse of a fraction  $a/b$  is  $b/a$ . For the multiplicative inverse of a real number, divide 1 by the number. For example, the reciprocal of 5 is one fifth ( $1/5$  or 0.2), and the reciprocal of 0.25 is 1 divided by 0.25, or 4. The **reciprocal function**, the function  $f(x)$  that maps  $x$  to  $1/x$ , is one of the simplest examples of a function which is self-inverse.



The term *reciprocal* was in common use at least as far back as the third edition of *Encyclopædia Britannica* (1797) to describe

two numbers whose product is 1; geometrical quantities in inverse proportion are described as *reciprocall* in a 1570 translation of Euclid's *Elements*.<sup>[1]</sup>

In the phrase *multiplicative inverse*, the qualifier *multiplicative* is often omitted and then tacitly understood (in contrast to the additive inverse). Multiplicative inverses can be defined over many mathematical domains as well as numbers. In these cases it can happen that  $ab \neq ba$ ; then "inverse" typically implies that an element is both a left and right inverse.

## Practical applications

The multiplicative inverse has innumerable applications in algorithms of computer science, particularly those related to number theory, since many such algorithms rely heavily on the theory of modular arithmetic. As a simple example, consider the *exact division problem* where you have a list of odd word-sized numbers each divisible by  $k$  and you wish to divide them all by  $k$ . One solution is as follows:

1. Use the extended Euclidean algorithm to compute  $k^{-1}$ , the modular multiplicative inverse of  $k \bmod 2^w$ , where  $w$  is the number of bits in a word. This inverse will exist since the numbers are odd and the modulus has no odd factors.
2. For each number in the list, multiply it by  $k^{-1}$  and take the least significant word of the result.

On many machines, particularly those without hardware support for division, division is a slower operation than multiplication, so this approach can yield a considerable speedup. The first step is relatively slow but only needs to be done once.

## Examples and counterexamples

In the field of real numbers, Zero does not have a reciprocal because no real number multiplied by 0 produces 1. With the exception of zero, reciprocals of every complex number are complex, reciprocals of every real number are real, and reciprocals of every rational number are rational. The imaginary units,  $\pm i$ , are the only complex numbers with additive inverse equal to multiplicative inverse. For example, additive and multiplicative inverses of  $i$  are  $-(i) = -i$  and  $1/i = -i$ , respectively.

To approximate the reciprocal of  $x$ , using only multiplication and subtraction, one can guess a number  $y$ , and then repeatedly replace  $y$  with  $2y - xy^2$ . Once the change in  $y$  becomes (and stays) sufficiently small,  $y$  is an approximation of the reciprocal of  $x$ .

In constructive mathematics, for a real number  $x$  to have a reciprocal, it is not sufficient that  $x \neq 0$ . There must instead be given a *rational* number  $r$  such that  $0 < r < |x|$ . In terms of the approximation algorithm in the previous paragraph, this is needed to prove that the change in  $y$  will eventually become arbitrarily small.

In modular arithmetic, the modular multiplicative inverse of  $a$  is also defined: it is the number  $x$  such that  $ax \equiv 1 \pmod{n}$ . This multiplicative inverse exists if and only if  $a$  and  $n$  are coprime. For example, the inverse of 3 modulo 11 is 4 because  $4 \cdot 3 \equiv 1 \pmod{11}$ . The extended Euclidean algorithm may be used to compute it.

The sedenions are an algebra in which every nonzero element has a multiplicative inverse, but which nonetheless has divisors of zero, i.e. nonzero elements  $x, y$  such that  $xy = 0$ .

A square matrix has an inverse if and only if its determinant has an inverse in the coefficient ring. The linear map that has the matrix  $A^{-1}$  with respect to some base is then the reciprocal function of the map having  $A$  as matrix in the same base. Thus, the two distinct notions of the inverse of a function are strongly related in this case, while they must be carefully distinguished in the general case (see below).

The trigonometric functions are related by the reciprocal identity: the cotangent is the reciprocal of the tangent; the secant is the reciprocal of the cosine; the cosecant is the reciprocal of the sine.

It is important to distinguish the reciprocal of a function  $f$  in the multiplicative sense, given by  $1/f$ , from the reciprocal or **inverse function** with respect to composition, denoted by  $f^{-1}$  and defined by  $f \circ f^{-1} = \text{id}$ . Only for linear maps are they strongly related (see above), while they are completely different for all other cases. The terminology difference *reciprocal* versus *inverse* is not sufficient to make this distinction, since many authors prefer the opposite naming convention, probably for historical reasons (for example in French, the inverse function is preferably called *application réciproque*).

A ring in which every nonzero element has a multiplicative inverse is a division ring; likewise an algebra in which this holds is a division algebra.

## Pseudo-random number generation

The expansion of the reciprocal  $1/q$  in any base can also act <sup>[2]</sup> as a source of pseudo-random numbers, if  $q$  is a "suitable" safe prime, a prime of the form  $2p + 1$  where  $p$  is also a prime. A sequence of pseudo-random numbers of length  $q - 1$  will be produced by the expansion.

## Reciprocals of irrational numbers

Every number excluding zero has a reciprocal, and reciprocals of certain irrational numbers often can prove useful for reasons linked to the irrational number in question. Examples of this are the reciprocal of  $e$  which is special because no other positive number can produce a lower number when put to the power of itself, and the golden ratio's reciprocal which, being roughly 0.6180339887, is exactly one less than the golden ratio and in turn illustrates the uniqueness of the number.

There are an infinite number of irrational reciprocal pairs that differ by an integer (giving the curious effect that the pairs share their infinite mantissa). These pairs can be found by simplifying  $n + \sqrt{n^2 + 1}$  for any integer  $n$ , and taking the reciprocal.

## Further remarks

If the multiplication is associative, an element  $x$  with a multiplicative inverse cannot be a zero divisor (meaning for some  $y$ ,  $xy = 0$  with neither  $x$  nor  $y$  equal to zero). To see this, it is sufficient to multiply the equation  $xy = 0$  by the inverse of  $x$  (on the left), and then simplify using associativity. In the absence of associativity, the sedenions provide a counterexample.

The converse does not hold: an element which is not a zero divisor is not guaranteed to have a multiplicative inverse. Within  $\mathbf{Z}$ , all integers except  $-1, 0, 1$  provide examples; they are not zero divisors nor do they have inverses in  $\mathbf{Z}$ . If the ring or algebra is finite, however, then all elements  $a$  which are not zero divisors do have a (left and right) inverse. For, first observe that the map  $f(x) = ax$  must be injective:  $f(x) = f(y)$  implies  $x = y$ :

$$\begin{aligned} ax = ay &\Rightarrow ax - ay = 0 \\ &\Rightarrow a(x - y) = 0 \\ &\Rightarrow x - y = 0 \\ &\Rightarrow x = y. \end{aligned}$$

Distinct elements map to distinct elements, so the image consists of the same finite number of elements, and the map is necessarily surjective. Specifically,  $f$  (namely multiplication by  $a$ ) must map some element  $x$  to 1,  $ax = 1$ , so that  $x$  is an inverse for  $a$ .

The multiplicative inverse of a fraction  $\frac{a}{b}$  is simply  $\frac{b}{a}$ .

## Notes

- [1] "In equal Parallelipedons the bases are reciprocally to their altitudes". *OED* "Reciprocal" §3a. Sir Henry Billingsley translation of Elements XI, 34.
- [2] Mitchell, Douglas W., "A nonlinear random number generator with known, long cycle length," *Cryptologia* 17, January 1993, 55-62.

## References

- Maximally Periodic Reciprocals, Matthews R.A.J. *Bulletin of the Institute of Mathematics and its Applications* vol 28 pp 147–148 1992

# Normal subgroup

---

In abstract algebra, a **normal subgroup** is a subgroup which is invariant under conjugation by members of the group. Normal subgroups can be used to construct quotient groups from a given group. In other words, a subgroup  $H$  of a group  $G$  is normal in  $G$  if and only if  $aH = Ha$  for all  $a$  in  $G$ .

Évariste Galois was the first to realize the importance of the existence of normal subgroups.

## Definitions

A subgroup,  $N$ , of a group,  $G$ , is called a **normal subgroup** if it is invariant under conjugation; that is, for each element  $n$  in  $N$  and each  $g$  in  $G$ , the element  $gng^{-1}$  is still in  $N$ . We write

$$N \triangleleft G \Leftrightarrow \forall n \in N, \forall g \in G, gng^{-1} \in N.$$

For any subgroup, the following conditions are equivalent to normality. Therefore any one of them may be taken as the definition:

- For all  $g$  in  $G$ ,  $gNg^{-1} \subseteq N$ .
- For all  $g$  in  $G$ ,  $gNg^{-1} = N$ .
- The sets of left and right cosets of  $N$  in  $G$  coincide.
- For all  $g$  in  $G$ ,  $gN = Ng$ .
- $N$  is a union of conjugacy classes of  $G$ .
- There is some homomorphism on  $G$  for which  $N$  is the kernel.

The last condition accounts for some of the importance of normal subgroups; they are a way to internally classify all homomorphisms defined on a group. For example, a non-identity finite group is simple if and only if it is isomorphic to all of its non-identity homomorphic images, a finite group is perfect if and only if it has no normal subgroups of prime index, and a group is imperfect if and only if the derived subgroup is not supplemented by any proper normal subgroup.

## Examples

- The subgroup  $\{e\}$  consisting of just the identity element of  $G$  and  $G$  itself are always normal subgroups of  $G$ . The former is called the trivial subgroup, and if these are the only normal subgroups, then  $G$  is said to be simple.
  - The center of a group is a normal subgroup.
  - The commutator subgroup is a normal subgroup.
  - More generally, any characteristic subgroup is normal, since conjugation is always an automorphism.
  - All subgroups  $N$  of an abelian group  $G$  are normal, because  $gN = Ng$ . A group that is not abelian but for which every subgroup is normal is called a Hamiltonian group.
  - The translation group in any dimension is a normal subgroup of the Euclidean group; for example in 3D rotating, translating, and rotating back results in only translation; also reflecting, translating, and reflecting again results in only translation (a translation seen in a mirror looks like a translation, with a reflected translation vector). The translations by a given distance in any direction form a conjugacy class; the translation group is the union of those for all distances.
  - In the Rubik's Cube group, the subgroup consisting of operations which only affect the corner pieces is normal, because no conjugate transformation can make such an operation affect an edge piece instead of a corner. By contrast, the subgroup consisting of turns of the top face only is not normal, because a conjugate transformation can move parts of the top face to the bottom and hence not all conjugates of elements of this subgroup are contained in the subgroup.
-

However, even if  $H$  is a normal subgroup of  $G$ , this does not mean that  $ah=ha$  for all  $h \in H$  and for all  $a \in G$ . As the following example shows: Consider the group  $S_3$ . Let  $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ . Then  $H$  is a subgroup of  $S_3$ . Since  $e, (1\ 2\ 3)$  and  $(1\ 3\ 2)$  are elements of  $H$ , it follows that  $eH = He$ ,  $(1\ 2\ 3)H = H(1\ 2\ 3)$  and  $(1\ 3\ 2)H = H(1\ 3\ 2)$ . Now  $(1\ 2)H = \{(1\ 2), (1\ 2)(1\ 2\ 3), (1\ 2)(1\ 3\ 2)\}$ ,  $H(1\ 2) = \{(1\ 2), (1\ 3\ 2)(1\ 2), (1\ 2\ 3)(1\ 2)\}$ . Hence  $(1\ 2)H \neq H(1\ 2)$ .  $(2\ 3)H = \{(2\ 3), (2\ 3)(1\ 2\ 3), (2\ 3)(1\ 3\ 2)\} = \{(2\ 3), (1\ 3), (1\ 2)\}$ ,  $H(2\ 3) = \{(2\ 3), (1\ 2\ 3)(2\ 3), (1\ 3\ 2)(2\ 3)\} = \{(2\ 3), (1\ 2), (1\ 3)\}$ . Hence  $(2\ 3)H \neq H(2\ 3)$ . Also in the same way this can be shown that  $(1\ 3)H \neq H(1\ 3)$ . Consequently  $H$  is a normal subgroup. However we point out that for  $(1\ 2\ 3) \in H$  and  $(2\ 3) \in G (= S_3)$ ,  $(2\ 3)(1\ 2\ 3) = (1\ 3) \neq (1\ 2\ 3)(2\ 3)$ .

## Properties

- Normality is preserved upon surjective homomorphisms, and is also preserved upon taking inverse images.
- Normality is preserved on taking direct products
- A normal subgroup of a normal subgroup of a group need not be normal in the group. That is, normality is not a transitive relation. However, a characteristic subgroup of a normal subgroup is normal. Also, a normal subgroup of a central factor is normal. In particular, a normal subgroup of a direct factor is normal.
- Every subgroup of index 2 is normal. More generally, a subgroup  $H$  of finite index  $n$  in  $G$  contains a subgroup  $K$  normal in  $G$  and of index dividing  $n!$  called the normal core. In particular, if  $p$  is the smallest prime dividing the order of  $G$ , then every subgroup of index  $p$  is normal.

## Lattice of normal subgroups

The normal subgroups of a group  $G$  form a lattice under subset inclusion with least element  $\{e\}$  and greatest element  $G$ . Given two normal subgroups  $N$  and  $M$  in  $G$ , meet is defined as

$$N \wedge M := N \cap M$$

and join is defined as

$$N \vee M := NM = \{nm \mid n \in N, \text{ and } m \in M\}.$$

The lattice is complete and modular.

## Normal subgroups and homomorphisms

If  $N$  is normal subgroup, we can define a multiplication on cosets by

$$(a_1N)(a_2N) := (a_1a_2)N.$$

This turns the set of cosets into a group called the quotient group  $G/N$ . There is a natural homomorphism  $f: G \rightarrow G/N$  given by  $f(a) = aN$ . The image  $f(N)$  consists only of the identity element of  $G/N$ , the coset  $eN = N$ .

In general, a group homomorphism  $f: G \rightarrow H$  sends subgroups of  $G$  to subgroups of  $H$ . Also, the preimage of any subgroup of  $H$  is a subgroup of  $G$ . We call the preimage of the trivial group  $\{e\}$  in  $H$  the **kernel** of the homomorphism and denote it by  $\ker(f)$ . As it turns out, the kernel is always normal and the image  $f(G)$  of  $G$  is always isomorphic to  $G/\ker(f)$  (the first isomorphism theorem). In fact, this correspondence is a bijection between the set of all quotient groups  $G/N$  of  $G$  and the set of all homomorphic images of  $G$  (up to isomorphism). It is also easy to see that the kernel of the quotient map,  $f: G \rightarrow G/N$ , is  $N$  itself, so we have shown that the normal subgroups are precisely the kernels of homomorphisms with domain  $G$ .

Theorem: If  $H$  and  $K$  are two subgroups of a group  $G$ , then

1. if  $H$  is a normal subgroup of  $G$ , then  $HK = KH$  is a subgroup of  $G$ .
2. if  $H$  and  $K$  are both normal subgroups of  $G$  then  $HK = KH$  is a normal subgroup of  $G$ .
3. if  $H$  and  $K$  are both normal subgroups of  $G$  then  $H \cap K$  is a normal subgroup of  $G$ .

Proof:

1. Let  $b \in K$ . Then  $Hb = bH$  implies  $Hb \leq KH$ . This is true for any  $b \in K$ . Hence  $HK \leq KH$ . Similarly it can be shown that  $KH \leq HK$ . So  $HK = KH$ . So  $HK$  is a subgroup of  $G$ . (Note: it is a theorem that if  $H$  and  $K$  are two subgroups of  $G$  and  $HK = KH$  then  $HK$  is a subgroup of  $G$ .)
2. Suppose that  $H$  and  $K$  are both normal subgroups of  $G$ . Now from (i)  $HK = KH$  is a subgroup of  $G$ . Let  $g \in G$ . Then  $gHKg^{-1} = gHg^{-1}gKg^{-1} = (gHg^{-1})(gKg^{-1}) \leq HK$ . Hence  $HK$  is a normal subgroup of  $G$ .
3. Since  $H$  and  $K$  are subgroups,  $H \cap K$  is also a subgroup. Let  $g \in G$  and  $a \in H \cap K$ . Then  $gag^{-1} \in gHg^{-1} \leq H$  and  $gag^{-1} \in gKg^{-1} \leq K$ . Since  $gag^{-1} \in H \cap K$  for all  $a \in H \cap K$ , we find that  $g(H \cap K)g^{-1} \leq H \cap K$  for all  $g \in G$ . Hence  $H \cap K$  is a normal subgroup of  $G$ .

Theorem: Let  $H$  be a normal subgroup of a group  $G$ . Denote the set of all cosets  $\{aH : a \in G\}$  by  $G/H$  and define  $*$  on  $G/H$  by for all  $aH, bH \in G/H$ ,  $(aH)*(bH) = abH$ . Then  $(G/H, *)$  is a group.

Proof: First of all we have to show that the operation  $*$  is well defined binary operation on  $G/H$ . In other words we have to show that if  $aH = a_1H$  and  $bH = b_1H$  then  $(ab)H = (a_1b_1)H$ , as this will show that  $aH*bH = (ab)H = (a_1b_1)H = a_1H*b_1H$ . Now let  $aH = a_1H$  and  $bH = b_1H$  is given. This imply that  $a = a_1h_1$  and  $b = b_1h_2$  for some  $h_1, h_2 \in H$ . Then  $(a_1b_1)^{-1}ab = (b_1^{-1}a_1^{-1})^{-1}a_1h_1b_1h_2$  (1.1) Since  $H$  is a normal subgroup,  $Hb_1 = b_1H$  and hence  $b_1^{-1}b_1h_2 = b_1h_3$  for some  $h_3 \in H$ . Hence from (1.1)  $(a_1b_1)^{-1}ab = b_1^{-1}b_1h_3h_2 = h_3h_2 \in H$ . This implies that  $(a_1b_1)H = (ab)H$ . Hence  $aH*bH = abH = a_1b_1H = a_1H*b_1H$  and so  $*$  is well defined binary operation on  $G/H$ . Next we show the associativity of  $*$  on  $G/H$ . Let  $aH, bH, cH \in G/H$ . Now  $aH*(bH*cH) = aH*bcH = a(bc)H = (ab)cH = abH*cH = (aH*bH)*cH$ . Hence  $*$  is associative. Now  $eH \in G/H$  and  $aH*eH = aeH = aH = eaH = eH*aH$  for all  $aH \in G/H$ . Hence  $eH$  is the identity of  $(G/H, *)$ . Also for all  $aH \in (G/H)$ ,  $a^{-1}H \in G/H$  and  $aH*a^{-1}H = aa^{-1}H = eH = a^{-1}H*aH$ . Here for all  $aH \in G/H$ ,  $a^{-1}H$  is the inverse of  $aH$ . Thus  $(G/H, *)$  is a group.

#### SOME RESULTS RELATED TO NORMAL SUBGROUPS

- Let  $H$  be a subgroup of  $G$  such that  $[G : H] = 2$ . Then  $H$  is a normal subgroup.

Proof: Since  $[G : H] = 2$ , the group  $G$  has only two distinct left cosets and only two distinct right cosets. Now  $H$  itself is a left as well as right coset in  $G$ . Let  $a \in G$ . If  $a \in H$ , then  $aH = H = Ha$ . Suppose  $a$  does not belong to  $H$ . Then  $aH \neq H$ . Hence  $G = H \cup aH$  and  $H \cap aH = \Phi$ . Then  $aH = G - H$ . Again since  $a$  does not belong to  $H$  and  $G$  has only two right cosets, we find that  $G = H \cup Ha$  where  $H \cap Ha = \Phi$ . Thus  $Ha = G - H$ . Hence  $Ha = aH$ . Thus we find that  $aH = Ha$  for all  $a \in G$  and so  $H$  is a normal subgroup of  $G$ .

- The center of a group  $G$ , given by  $Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$  is a normal subgroup of  $G$ .

Proof: We know that the center of a group is a subgroup of that group. Now for any  $g \in G$  and any  $a \in Z(G)$ ,  $gag^{-1} = agg^{-1} = a \in Z(G)$  and hence,  $gZ(G)g^{-1} \leq Z(G)$ . Consequently  $Z(G)$  is a normal subgroup.

- Let  $H$  be subgroup of the group  $G$ . If  $x^2 \in H$  for all  $x \in G$ , then  $H$  is a normal subgroup of  $G$  and  $G/H$  is commutative.

Proof: Let  $g \in G$  and  $h \in H$ . Consider  $ghg^{-1}$  and note that  $ghg^{-1} = ghgh^{-1}g^{-2} = (gh)^2h^{-1}g^{-2}$ . Now  $h^{-1} \in H$  and by our hypothesis  $(gh)^2, g^{-2} \in H$ . This implies that  $ghg^{-1} \in H$  which in turn shows that  $gHg^{-1} \subseteq H$ . Hence  $H$  is a normal subgroup of  $G$ . To show  $G/H$  is commutative, let  $xH, yH \in G/H$ . We show that  $xHyH = yHxH$  or  $xyH = yxH$  or  $(yx)^{-1}(xy) \in H$ . Now,  $(yx)^{-1}(xy) = (x^{-1}y^{-1})(xy) = (x^{-1}y^{-1})^2(yxy^{-1})^2y^2$ . Since  $a^2 \in H$  for all  $a \in G$ , it follows that  $(x^{-1}y^{-1})^2(yxy^{-1})^2y^2 \in H$  and so  $(yx)^{-1}(xy) \in H$ . Hence  $G/H$  is commutative.

- Let  $G$  be a group such that every cyclic subgroup of  $G$  is a normal subgroup of  $G$ . Then every subgroup of  $G$  is a normal subgroup of  $G$ .

Proof: Let  $H$  be a subgroup of  $G$ . Let  $g \in G$  and  $a \in H$ . Then  $gag^{-1} \in \langle a \rangle \subseteq H$ . Hence  $H$  is normal in  $G$ .

- Let  $H$  is a proper subgroup of a group  $G$ . such that for all  $x, y \in G - H$ ,  $xy \in H$ . Then  $H$  is a normal subgroup of  $G$ .

Proof: Let  $x \in G - H$ . Then  $x^{-1} \in G - H$ . Let  $y \in H$ . Then  $xy \in G - H$ , (for otherwise,  $x = xyx^{-1} \in H$ ). Thus  $xy, x^{-1} \in G - H$ . Hence  $yx^{-1} \in H$ . Also for any  $x \in H$ , we have  $yx^{-1} \in H$ . Thus  $H$  is a normal subgroup of  $G$ .

- Let  $H$  be a subgroup of the group  $G$ . Suppose that the product of two left cosets of  $H$  in  $G$  is again a left coset of  $H$  in  $G$ . Then  $H$  is a Normal subgroup of  $G$ .

Proof: Let  $g \in G$ , Then  $gHg^{-1}H = tH$  for some  $t \in G$ . Thus  $e = geg^{-1}e \in tH$ . Hence  $e = th$  for some  $h \in H$ . Thus  $t = h^{-1} \in H$  so that  $tH = H$ . Now  $gHg^{-1} = gHg^{-1}H = H$ . Hence  $H$  is a normal subgroup.

## References

- I. N. Herstein, *Topics in algebra*. Second edition. Xerox College Publishing, Lexington, Mass.-Toronto, Ont., 1975. xi+388 pp.
- David S. Dummit; Richard M. Foote, *Abstract algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991. pp. xiv, 658 ISBN 0-13-004771-6
- Sen, Ghosh, Mokhopadhyay, "Topics in Abstract Algebra". Second edition. Universities Press (India) Private Limited. ISBN 978-81-7371-551-8

## External links

- Weisstein, Eric W., "normal subgroup"<sup>[1]</sup> from MathWorld.
- Normal subgroup in Springer's Encyclopedia of Mathematics<sup>[2]</sup>
- Robert Ash: Group Fundamentals in *Abstract Algebra. The Basic Graduate Year*<sup>[3]</sup>
- John Baez, What's a Normal Subgroup?<sup>[4]</sup>

## References

- [1] <http://mathworld.wolfram.com/NormalSubgroup.html>  
 [2] <http://eom.springer.de/N/n067690.htm>  
 [3] <http://www.math.uiuc.edu/~r-ash/Algebra/Chapter1.pdf>  
 [4] <http://math.ucr.edu/home/baez/normal.html>



# Perfect group

In mathematics, more specifically in the area of modern algebra known as group theory, a group is said to be **perfect** if it equals its own commutator subgroup, or equivalently, if the group has no nontrivial abelian quotients (equivalently, its abelianization, which is the universal abelian quotient, is trivial). In symbols, a perfect group is one such that  $G^{(1)} = G$  (the commutator subgroup equals the group), or equivalently one such that  $G^{\text{ab}} = 1$  (its abelianization is trivial).

## Examples

The smallest (non-trivial) perfect group is the alternating group  $A_5$ . More generally, any non-abelian simple group is perfect since the commutator subgroup is a normal subgroup with abelian quotient. Conversely, a perfect group need not be simple; for example, the special linear group  $\text{SL}(2,5)$  (or the binary icosahedral group which is isomorphic to it) is perfect but not simple (it has a non-trivial center containing  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$ ).

More generally, a quasisimple group (a perfect central extension of a simple group) which is a non-trivial extension (i.e., not a simple group itself) is perfect but not simple; this includes all the insoluble non-simple finite special linear groups  $\text{SL}(n,q)$  as extensions of the projective special linear group  $\text{PSL}(n,q)$  ( $\text{SL}(2,5)$  is an extension of  $\text{PSL}(2,5)$ , which is isomorphic to  $A_5$ ). Similarly, the special linear group over the real and complex numbers is perfect, but the general linear group  $\text{GL}$  is never perfect (except when trivial or over  $\mathbf{F}_2$ , where it equals the special linear group), as the determinant gives a non-trivial abelianization and indeed the commutator subgroup is  $\text{SL}$ .

A non-trivial perfect group, however, is necessarily not solvable.

Every acyclic group is perfect, but the converse is not true:  $A_5$  is perfect but not acyclic (in fact, not even superperfect), see (Berrick & Hillman 2003). In fact, for  $n \geq 5$  the alternating group  $A_n$  is perfect but not superperfect, with  $H_2(A_n; \mathbf{Z}) = \mathbf{Z}/2$  for  $n \geq 8$ .

## Grün's lemma

A basic fact about perfect groups is **Grün's lemma** from (Grün 1935, Satz 4,<sup>[1]</sup> p. 3): the quotient of a perfect group by its center is centerless (has trivial center).

I.e., if  $Z(G)$  denotes the center of a given group  $G$ , and  $G$  is perfect, then the center of the quotient group  $G/Z(G)$  is the trivial group:

$$G \text{ perfect} \implies Z\left(\frac{G}{Z(G)}\right) \cong \{1\}.$$

### Proof

If  $G$  is a perfect group, let  $Z_1$  and  $Z_2$  denote the first two terms of the upper central series of  $G$  (i.e.,  $Z_1$  is the center of  $G$ , and  $Z_2/Z_1$  is the center of  $G/Z_1$ ). If  $H$  and  $K$  are subgroups of  $G$ , denote the commutator of  $H$  and  $K$  by  $[H,K]$  and note that  $[Z_1, G] = 1$  and  $[Z_2, G] \subseteq Z_1$ , and consequently (the convention that  $[X,Y,Z] = [[X,Y],Z]$  is followed):

$$[Z_2, G, G] = [[Z_2, G], G] \subseteq [Z_1, G] = 1$$

$$[G, Z_2, G] = [[G, Z_2], G] = [[Z_2, G], G] \subseteq [Z_1, G] = 1$$

By the three subgroups lemma (or equivalently, by the Hall-Witt identity), it follows that  $[G, Z_2] = [[G, G], Z_2] = [G, G, Z_2] = 1$ . Therefore,  $Z_2 \subseteq Z_1 = Z(G)$ , and the center of the quotient group  $G/Z(G)$  is the trivial group.

As a consequence, all higher centers (that is, higher terms in the upper central series) of a perfect group equal the center.

## Group homology

In terms of group homology, a perfect group is precisely one whose first homology group vanishes:  $H_1(G; \mathbf{Z}) = 0$ , as the first homology group of a group is exactly the abelianization of the group, and perfect means trivial abelianization. An advantage of this definition is that it admits strengthening:

- A superperfect group is one whose first two homology groups vanish:  $H_1(G; \mathbf{Z}) = H_2(G; \mathbf{Z}) = 0$ .
- An acyclic group is one *all* of whose (reduced) homology groups vanish  $\tilde{H}_i(G; \mathbf{Z}) = 0$ . (This is equivalent to all homology groups other than  $H_0$  vanishing.)

## Quasi-perfect group

Especially in the field of algebraic K-theory, a group is said to be **quasi-perfect** if its commutator subgroup is perfect; in symbols, a quasi-perfect group is one such that  $G^{(2)} = G^{(1)}$ , (the commutator of the commutator subgroup is the commutator subgroup), while a perfect group is one such that  $G^{(1)} = G$  (the commutator subgroup is the whole group). See (Karoubi 1973, pp. 301–411) and (Inassaridze 1995, p. 76).

## Notes

[1] *Satz* is German for "theorem".

## References

- A. Jon Berrick and Jonathan A. Hillman, "Perfect and acyclic subgroups of finitely presentable groups", *Journal of the London Mathematical Society* (2) 68 (2003), no. 3, 683–698. MR2009444
- Grün, Otto (1935), "Beiträge zur Gruppentheorie. I." (<http://resolver.sub.uni-goettingen.de/purl?GDZPPN002173409>) (in German), *Journal für Reine und Angewandte Mathematik* **174**: 1–14, ISSN 0075-4102, Zbl 0012.34102
- Inassaridze, Hvedri (1995), *Algebraic K-theory* (<http://books.google.com/?id=rnSE3aoNVY0C>), Mathematics and its Applications, **311**, Dordrecht: Kluwer Academic Publishers Group, ISBN 978-0-7923-3185-8, MR1368402
- Karoubi, M.: *Périodicité de la K-théorie hermitienne, Hermitian K-Theory and Geometric Applications*, Lecture Notes in Math. 343, Springer-Verlag, 1973
- Rose, John S. (1994), *A Course in Group Theory*, New York: Dover Publications, Inc., pp. 61, ISBN 0-486-68194-7, MR1298629

## External links

- Weisstein, Eric W., "Perfect Group (<http://mathworld.wolfram.com/PerfectGroup.html>)" from MathWorld.
- Weisstein, Eric W., "Grün's lemma (<http://mathworld.wolfram.com/GruensLemma.html>)" from MathWorld.

# Schreier refinement theorem

---

In mathematics, the **Schreier refinement theorem** of group theory states that any two normal series of subgroups of a given group have equivalent refinements.

The theorem is named after the Austrian mathematician Otto Schreier who proved it in 1928. It provides an elegant proof of the Jordan–Hölder theorem.

## References

- Rotman, Joseph (1994). *An introduction to the theory of groups*. New York: Springer-Verlag. ISBN 0-387-94285-8.

# Subgroup

---

In group theory, given a group  $G$  under a binary operation  $*$ , a subset  $H$  of  $G$  is called a **subgroup** of  $G$  if  $H$  also forms a group under the operation  $*$ . More precisely,  $H$  is a subgroup of  $G$  if the restriction of  $*$  to  $H \times H$  is a group operation on  $H$ . This is usually represented notationally by  $H \leq G$ , read as " $H$  is a subgroup of  $G$ ".

A **proper subgroup** of a group  $G$  is a subgroup  $H$  which is a proper subset of  $G$  (i.e.  $H \neq G$ ). The **trivial subgroup** of any group is the subgroup  $\{e\}$  consisting of just the identity element. If  $H$  is a subgroup of  $G$ , then  $G$  is sometimes called an *overgroup* of  $H$ .

The same definitions apply more generally when  $G$  is an arbitrary semigroup, but this article will only deal with subgroups of groups. The group  $G$  is sometimes denoted by the ordered pair  $(G, *)$ , usually to emphasize the operation  $*$  when  $G$  carries multiple algebraic or other structures.

This article will write  $ab$  for  $a*b$ , as is usual.

## Basic properties of subgroups

- A subset  $H$  of the group  $G$  is a subgroup of  $G$  if and only if it is nonempty and closed under products and inverses. (The closure conditions mean the following: whenever  $a$  and  $b$  are in  $H$ , then  $ab$  and  $a^{-1}$  are also in  $H$ . These two conditions can be combined into one equivalent condition: whenever  $a$  and  $b$  are in  $H$ , then  $ab^{-1}$  is also in  $H$ .) In the case that  $H$  is finite, then  $H$  is a subgroup if and only if  $H$  is closed under products. (In this case, every element  $a$  of  $H$  generates a finite cyclic subgroup of  $H$ , and the inverse of  $a$  is then  $a^{-1} = a^{n-1}$ , where  $n$  is the order of  $a$ .)
  - The above condition can be stated in terms of a homomorphism; that is,  $H$  is a subgroup of a group  $G$  if and only if  $H$  is a subset of  $G$  and there is an inclusion homomorphism (i.e.,  $i(a) = a$  for every  $a$ ) from  $H$  to  $G$ .
  - The identity of a subgroup is the identity of the group: if  $G$  is a group with identity  $e_G$ , and  $H$  is a subgroup of  $G$  with identity  $e_H$ , then  $e_H = e_G$ .
  - The inverse of an element in a subgroup is the inverse of the element in the group: if  $H$  is a subgroup of a group  $G$ , and  $a$  and  $b$  are elements of  $H$  such that  $ab = ba = e_H$ , then  $ab = ba = e_G$ .
  - The intersection of subgroups  $A$  and  $B$  is again a subgroup.<sup>[1]</sup> The union of subgroups  $A$  and  $B$  is a subgroup if and only if either  $A$  or  $B$  contains the other, since for example 2 and 3 are in the union of  $2\mathbb{Z}$  and  $3\mathbb{Z}$  but their sum 5 is not. Another example is the union of the x-axis and the y-axis in the plane (with the addition operation); each of these objects is a subgroup but their union is not. This also serves as an example of two subgroups, whose intersection is precisely the identity.
  - If  $S$  is a subset of  $G$ , then there exists a minimum subgroup containing  $S$ , which can be found by taking the intersection of all of subgroups containing  $S$ ; it is denoted by  $\langle S \rangle$  and is said to be the subgroup generated by  $S$ .
-

An element of  $G$  is in  $\langle S \rangle$  if and only if it is a finite product of elements of  $S$  and their inverses.

- Every element  $a$  of a group  $G$  generates the cyclic subgroup  $\langle a \rangle$ . If  $\langle a \rangle$  is isomorphic to  $\mathbf{Z}/n\mathbf{Z}$  for some positive integer  $n$ , then  $n$  is the smallest positive integer for which  $a^n = e$ , and  $n$  is called the *order* of  $a$ . If  $\langle a \rangle$  is isomorphic to  $\mathbf{Z}$ , then  $a$  is said to have *infinite order*.
- The subgroups of any given group form a complete lattice under inclusion, called the lattice of subgroups. (While the infimum here is the usual set-theoretic intersection, the supremum of a set of subgroups is the subgroup *generated by* the set-theoretic union of the subgroups, not the set-theoretic union itself.) If  $e$  is the identity of  $G$ , then the trivial group  $\{e\}$  is the minimum subgroup of  $G$ , while the maximum subgroup is the group  $G$  itself.

### Cosets and Lagrange's theorem

Given a subgroup  $H$  and some  $a$  in  $G$ , we define the **left coset**  $aH = \{ah : h \text{ in } H\}$ . Because  $a$  is invertible, the map  $\varphi : H \rightarrow aH$  given by  $\varphi(h) = ah$  is a bijection. Furthermore, every element of  $G$  is contained in precisely one left coset of  $H$ ; the left cosets are the equivalence classes corresponding to the equivalence relation  $a_1 \sim a_2$  if and only if  $a_1^{-1}a_2$  is in  $H$ . The number of left cosets of  $H$  is called the index of  $H$  in  $G$  and is denoted by  $[G : H]$ .

Lagrange's theorem states that for a finite group  $G$  and a subgroup  $H$ ,

$$[G : H] = \frac{|G|}{|H|}$$

where  $|G|$  and  $|H|$  denote the orders of  $G$  and  $H$ , respectively. In particular, the order of every subgroup of  $G$  (and the order of every element of  $G$ ) must be a divisor of  $|G|$ .

**Right cosets** are defined analogously:  $Ha = \{ha : h \text{ in } H\}$ . They are also the equivalence classes for a suitable equivalence relation and their number is equal to  $[G : H]$ .

If  $aH = Ha$  for every  $a$  in  $G$ , then  $H$  is said to be a normal subgroup. Every subgroup of index 2 is normal: the left cosets, and also the right cosets, are simply the subgroup and its complement. More generally, if  $p$  is the lowest prime dividing the order of a finite group  $G$ , then any subgroup of index  $p$  (if such exists) is normal.

### Example: Subgroups of $\mathbf{Z}_8$

Let  $G$  be the cyclic group  $\mathbf{Z}_8$  whose elements are

$$G = \{0, 2, 4, 6, 1, 3, 5, 7\}$$

and whose group operation is addition modulo eight. Its Cayley table is

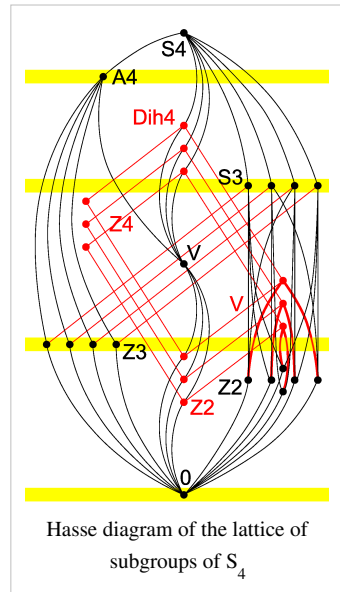
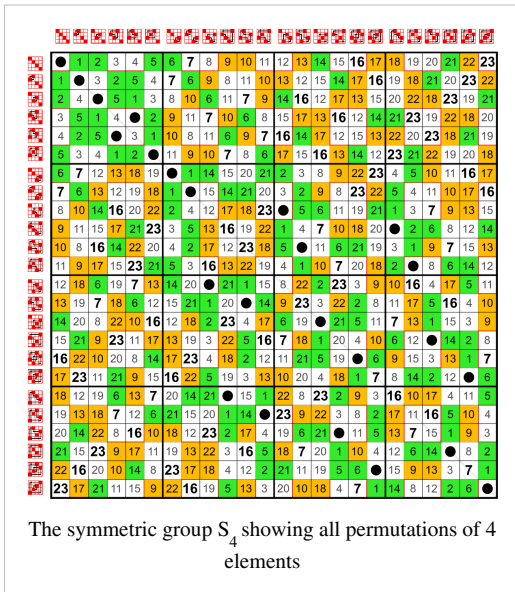
+	0	2	4	6	1	3	5	7
0	0	2	4	6	1	3	5	7
2	2	4	6	0	3	5	7	1
4	4	6	0	2	5	7	1	3
6	6	0	2	4	7	1	3	5
1	1	3	5	7	2	4	6	0
3	3	5	7	1	4	6	0	2
5	5	7	1	3	6	0	2	4
7	7	1	3	5	0	2	4	6

This group has a pair of nontrivial subgroups:  $J = \{0, 4\}$  and  $H = \{0, 2, 4, 6\}$ , where  $J$  is also a subgroup of  $H$ . The Cayley table for  $H$  is the top-left quadrant of the Cayley table for  $G$ . The group  $G$  is cyclic, and so are its subgroups. In general, subgroups of cyclic groups are also cyclic.

### Example: Subgroups of $S_4$

Every group has as many small subgroups as neutral elements on the main diagonal:

The trivial group and two-element groups  $Z_2$ . These small subgroups are not counted in the following list.



12 elements

The alternating group  $A_4$  showing only the even permutations

Subgroups:

8 elements

Dihedral group of order 8

Subgroups:


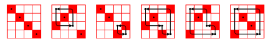
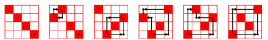





Dihedral group of order 8

Subgroups:

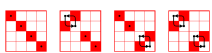
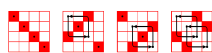
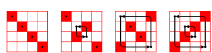
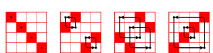
Dihedral group of order 8

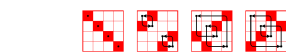
Subgroups:

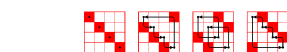
6 elements

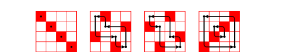
																																																																																																																																																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr> <tr><td>1</td><td>●</td><td>3</td><td>2</td><td>5</td><td>4</td></tr> <tr><td>2</td><td>4</td><td>●</td><td>5</td><td>1</td><td>3</td></tr> <tr><td>3</td><td>5</td><td>1</td><td>4</td><td>●</td><td>2</td></tr> <tr><td>4</td><td>2</td><td>5</td><td>●</td><td>3</td><td>1</td></tr> <tr><td>5</td><td>3</td><td>4</td><td>1</td><td>2</td><td>●</td></tr> </table>	●	1	2	3	4	5	1	●	3	2	5	4	2	4	●	5	1	3	3	5	1	4	●	2	4	2	5	●	3	1	5	3	4	1	2	●	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>5</td><td>6</td><td>11</td><td>19</td><td>21</td></tr> <tr><td>5</td><td>●</td><td>11</td><td>6</td><td>21</td><td>19</td></tr> <tr><td>6</td><td>19</td><td>●</td><td>21</td><td>5</td><td>11</td></tr> <tr><td>11</td><td>21</td><td>5</td><td>19</td><td>●</td><td>6</td></tr> <tr><td>19</td><td>6</td><td>21</td><td>●</td><td>11</td><td>5</td></tr> <tr><td>21</td><td>11</td><td>19</td><td>5</td><td>6</td><td>●</td></tr> </table>	●	5	6	11	19	21	5	●	11	6	21	19	6	19	●	21	5	11	11	21	5	19	●	6	19	6	21	●	11	5	21	11	19	5	6	●	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>1</td><td>14</td><td>15</td><td>20</td><td>21</td></tr> <tr><td>1</td><td>●</td><td>15</td><td>14</td><td>21</td><td>20</td></tr> <tr><td>14</td><td>20</td><td>●</td><td>21</td><td>1</td><td>15</td></tr> <tr><td>15</td><td>21</td><td>1</td><td>20</td><td>●</td><td>14</td></tr> <tr><td>20</td><td>14</td><td>21</td><td>●</td><td>15</td><td>1</td></tr> <tr><td>21</td><td>15</td><td>20</td><td>1</td><td>14</td><td>●</td></tr> </table>	●	1	14	15	20	21	1	●	15	14	21	20	14	20	●	21	1	15	15	21	1	20	●	14	20	14	21	●	15	1	21	15	20	1	14	●	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>2</td><td>6</td><td>8</td><td>12</td><td>14</td></tr> <tr><td>2</td><td>●</td><td>8</td><td>6</td><td>14</td><td>12</td></tr> <tr><td>6</td><td>12</td><td>●</td><td>14</td><td>2</td><td>8</td></tr> <tr><td>8</td><td>14</td><td>2</td><td>12</td><td>●</td><td>6</td></tr> <tr><td>12</td><td>6</td><td>14</td><td>●</td><td>8</td><td>2</td></tr> <tr><td>14</td><td>8</td><td>12</td><td>2</td><td>6</td><td>●</td></tr> </table>	●	2	6	8	12	14	2	●	8	6	14	12	6	12	●	14	2	8	8	14	2	12	●	6	12	6	14	●	8	2	14	8	12	2	6	●
●	1	2	3	4	5																																																																																																																																														
1	●	3	2	5	4																																																																																																																																														
2	4	●	5	1	3																																																																																																																																														
3	5	1	4	●	2																																																																																																																																														
4	2	5	●	3	1																																																																																																																																														
5	3	4	1	2	●																																																																																																																																														
●	5	6	11	19	21																																																																																																																																														
5	●	11	6	21	19																																																																																																																																														
6	19	●	21	5	11																																																																																																																																														
11	21	5	19	●	6																																																																																																																																														
19	6	21	●	11	5																																																																																																																																														
21	11	19	5	6	●																																																																																																																																														
●	1	14	15	20	21																																																																																																																																														
1	●	15	14	21	20																																																																																																																																														
14	20	●	21	1	15																																																																																																																																														
15	21	1	20	●	14																																																																																																																																														
20	14	21	●	15	1																																																																																																																																														
21	15	20	1	14	●																																																																																																																																														
●	2	6	8	12	14																																																																																																																																														
2	●	8	6	14	12																																																																																																																																														
6	12	●	14	2	8																																																																																																																																														
8	14	2	12	●	6																																																																																																																																														
12	6	14	●	8	2																																																																																																																																														
14	8	12	2	6	●																																																																																																																																														
Symmetric group $S_3$	Symmetric group $S_3$	Symmetric group $S_3$	Symmetric group $S_3$																																																																																																																																																
Subgroup: 	Subgroup: 	Subgroup: 	Subgroup: 																																																																																																																																																

4 elements

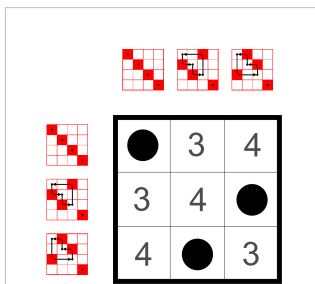
																																																																			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>1</td><td>6</td><td>7</td></tr> <tr><td>1</td><td>●</td><td>7</td><td>6</td></tr> <tr><td>6</td><td>7</td><td>●</td><td>1</td></tr> <tr><td>7</td><td>6</td><td>1</td><td>●</td></tr> </table>	●	1	6	7	1	●	7	6	6	7	●	1	7	6	1	●	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>5</td><td>14</td><td>16</td></tr> <tr><td>5</td><td>●</td><td>16</td><td>14</td></tr> <tr><td>14</td><td>16</td><td>●</td><td>5</td></tr> <tr><td>16</td><td>14</td><td>5</td><td>●</td></tr> </table>	●	5	14	16	5	●	16	14	14	16	●	5	16	14	5	●	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>2</td><td>21</td><td>23</td></tr> <tr><td>2</td><td>●</td><td>23</td><td>21</td></tr> <tr><td>21</td><td>23</td><td>●</td><td>2</td></tr> <tr><td>23</td><td>21</td><td>2</td><td>●</td></tr> </table>	●	2	21	23	2	●	23	21	21	23	●	2	23	21	2	●	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>7</td><td>16</td><td>23</td></tr> <tr><td>7</td><td>●</td><td>23</td><td>16</td></tr> <tr><td>16</td><td>23</td><td>●</td><td>7</td></tr> <tr><td>23</td><td>16</td><td>7</td><td>●</td></tr> </table>	●	7	16	23	7	●	23	16	16	23	●	7	23	16	7	●
●	1	6	7																																																																
1	●	7	6																																																																
6	7	●	1																																																																
7	6	1	●																																																																
●	5	14	16																																																																
5	●	16	14																																																																
14	16	●	5																																																																
16	14	5	●																																																																
●	2	21	23																																																																
2	●	23	21																																																																
21	23	●	2																																																																
23	21	2	●																																																																
●	7	16	23																																																																
7	●	23	16																																																																
16	23	●	7																																																																
23	16	7	●																																																																
Klein four-group	Klein four-group	Klein four-group	Klein four-group																																																																

																
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>7</td><td>17</td><td>22</td></tr> <tr><td>7</td><td>●</td><td>22</td><td>17</td></tr> <tr><td>17</td><td>22</td><td>7</td><td>●</td></tr> <tr><td>22</td><td>17</td><td>●</td><td>7</td></tr> </table>	●	7	17	22	7	●	22	17	17	22	7	●	22	17	●	7
●	7	17	22													
7	●	22	17													
17	22	7	●													
22	17	●	7													
Cyclic group $Z_4$																

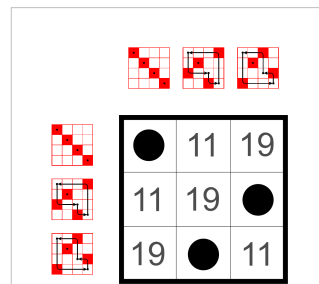
																
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>9</td><td>16</td><td>18</td></tr> <tr><td>9</td><td>●</td><td>18</td><td>16</td></tr> <tr><td>16</td><td>18</td><td>●</td><td>9</td></tr> <tr><td>18</td><td>●</td><td>9</td><td>16</td></tr> </table>	●	9	16	18	9	●	18	16	16	18	●	9	18	●	9	16
●	9	16	18													
9	●	18	16													
16	18	●	9													
18	●	9	16													
Cyclic group $Z_4$																

																
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>●</td><td>10</td><td>13</td><td>23</td></tr> <tr><td>10</td><td>●</td><td>23</td><td>13</td></tr> <tr><td>13</td><td>23</td><td>●</td><td>10</td></tr> <tr><td>23</td><td>13</td><td>10</td><td>●</td></tr> </table>	●	10	13	23	10	●	23	13	13	23	●	10	23	13	10	●
●	10	13	23													
10	●	23	13													
13	23	●	10													
23	13	10	●													
Cyclic group $Z_4$																

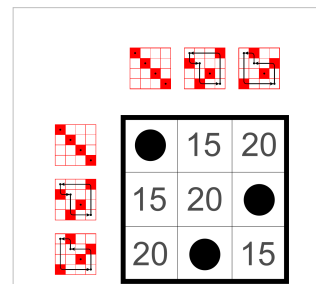
### 3 elements



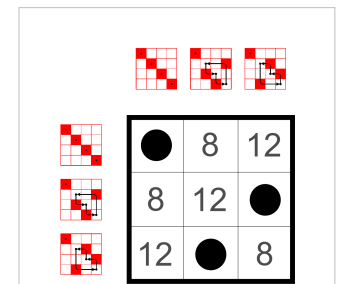
Cyclic group  $Z_3$



Cyclic group  $Z_3$



Cyclic group  $Z_3$



Cyclic group  $Z_3$

## Notes

[1] Jacobson (2009), p. 41

## References

- Jacobson, Nathan (2009), *Basic algebra*, **1** (2nd ed.), Dover, ISBN 978-0-486-47189-1.

## Transversal (combinatorics)

In combinatorial mathematics, given a collection  $C$  of sets, a **transversal** is a set containing exactly one element from each member of the collection. When the sets of the collection are mutually disjoint, each element of the transversal corresponds to exactly one member of  $C$  (the set it is a member of). If the original sets are not disjoint, there are two possibilities for the definition of a transversal. One variation, the one that mimics the situation when the sets are mutually disjoint, is that there is a bijection  $f$  from the transversal to  $C$  such that  $x$  is an element of  $f(x)$  for each  $x$  in the transversal. In this case, the transversal is also called a **system of distinct representatives**. The other, less commonly used, possibility does not require a one-to-one relation between the elements of the transversal and the sets of  $C$ . Loosely speaking, in this situation the members of the *system of representatives* are not necessarily distinct.<sup>[1][2]</sup>

A **partial transversal** is a set containing at most one element from each member of the collection, or (in the stricter form of the concept) a set with an injection from the set to  $C$ .

The transversals of a finite collection  $C$  of finite sets form the basis sets of a matroid, the "transversal matroid" of  $C$ . The independent sets of the transversal matroid are the partial transversals of  $C$ .<sup>[3]</sup>

A generalization of the concept of a transversal would be a set that just has a non-empty intersection with each member of  $C$ . An example of this would be a Bernstein set, which is defined as a set that has a non-empty intersection with each set of  $C$ , but contains no set of  $C$ , where  $C$  is the collection of all perfect sets of a topological Polish space.



## Examples

In group theory, given a subgroup  $H$  of a group  $G$ , a right (respectively left) transversal is a set containing exactly one element from each right (respectively left) coset of  $H$ . In this case, the "sets" (cosets) are mutually disjoint.

Given a direct product of groups  $G = H \times K$ , then  $H$  is a transversal for the cosets of  $K$ .

- Hall's marriage theorem gives necessary and sufficient conditions for a finite collection of not necessarily distinct, but non-empty sets to have a transversal.

## Category theory

In the language of category theory, a **transversal** of a collection of mutually disjoint sets is a section of the quotient map induced by the collection.

## Notes

[1] Roberts & Tesman 2009, pg. 692

[2] Brualdi 2010, pg. 322

[3] Oxley, James G. (2006), *Matroid Theory*, Oxford graduate texts in mathematics, **3**, Oxford University Press, p. 48, ISBN 9780199202508.

## References

- Brualdi, Richard A. (2010), *Introductory Combinatorics* (5th ed.), Upper Saddle River, NJ: Prentice Hall, ISBN 0-13-602040-2
- Lawler, E. L. *Combinatorial Optimization: Networks and Matroids*. 1976.
- Mirsky, Leon (1971). *Transversal Theory: An account of some aspects of combinatorial mathematics*. Academic Press. ISBN 0-12-498550-5.
- Roberts, Fred S.; Tesman, Barry (2009), *Applied Combinatorics* (2nd ed.), Boca Raton: CRC Press, ISBN 978-1-4200-9982-9

# Torsion subgroup

---

In the theory of abelian groups, the **torsion subgroup**  $A_T$  of an abelian group  $A$  is the subgroup of  $A$  consisting of all elements that have finite order. An abelian group  $A$  is called a **torsion** (or **periodic**) group if every element of  $A$  has finite order and is called **torsion-free** if every element of  $A$  except the identity is of infinite order.

The proof that  $A_T$  is closed under addition relies on the commutativity of addition (see examples section).

If  $A$  is abelian, then the torsion subgroup  $T$  is a fully characteristic subgroup of  $A$  and the factor group  $A/T$  is torsion-free. There is a covariant functor from the category of abelian groups to the category of torsion groups that sends every group to its torsion subgroup and every homomorphism to its restriction to the torsion subgroup. There is another covariant functor from the category of abelian groups to the category of torsion-free groups that sends every group to its quotient by its torsion subgroup, and sends every homomorphism to the obvious induced homomorphism (which is easily seen to be well-defined).

If  $A$  is finitely generated and abelian, then it can be written as the direct sum of its torsion subgroup  $T$  and a torsion-free subgroup (but this is not true for all infinitely generated abelian groups). In any decomposition of  $A$  as a direct sum of a torsion subgroup  $S$  and a torsion-free subgroup,  $S$  must equal  $T$  (but the torsion-free subgroup is not uniquely determined). This is a key step in the classification of finitely generated abelian groups.

## $p$ -power torsion subgroups

For any abelian group  $(A, +)$  and any prime number  $p$  the set  $A_{T_p}$  of elements of  $A$  that have order a power of  $p$  is a subgroup called the  **$p$ -power torsion subgroup** or, more loosely, the  **$p$ -torsion subgroup**:

$$A_{T_p} = \{g \in A \mid \exists n \in \mathbb{N}, p^n g = 0\}.$$

The torsion subgroup  $A_T$  is isomorphic to the direct sum of its  $p$ -power torsion subgroups over all prime numbers  $p$ :

$$A_T = \bigoplus_{p \in P} A_{T_p}.$$

When  $A$  is a finite abelian group,  $A_{T_p}$  coincides with the unique Sylow  $p$ -subgroup of  $A$ .

Each  $p$ -power torsion subgroup of  $A$  is a fully characteristic subgroup. More strongly, any homomorphism between abelian groups sends each  $p$ -power torsion subgroup into the corresponding  $p$ -power torsion subgroup.

For each prime number  $p$ , this provides a functor from the category of abelian groups to the category of  $p$ -power torsion groups that sends every group to its  $p$ -power torsion subgroup, and restricts every homomorphism to the  $p$ -torsion subgroups. The product over the set of all prime numbers of the restriction of these functors to the category of torsion groups, is a faithful functor from the category of torsion groups to the product over all prime numbers of the categories of  $p$ -torsion groups. In a sense, this means that studying  $p$ -torsion groups in isolation tells us everything about torsion groups in general.

## Examples and further results

- The torsion subset of a non-abelian group is not, in general, a subgroup. For example, in the infinite dihedral group, which has presentation:

$$\langle x, y \mid x^2 = y^2 = 1 \rangle$$

the element  $xy$  is a product of two torsion elements, but has infinite order.

- The torsion elements in a nilpotent group form a normal subgroup.<sup>[1]</sup>
- Obviously, every finite abelian group is a torsion group. Not every torsion group is finite however: consider the direct sum of a countable number of copies of the cyclic group  $C_2$ ; this is a torsion group since every element has order 2. Nor need there be an upper bound on the orders of elements in a torsion group if it isn't finitely generated,

as the example of the factor group  $\mathbf{Q}/\mathbf{Z}$  shows.

- Every free abelian group is torsion-free, but the converse is not true, as is shown by the additive group of the rational numbers  $\mathbf{Q}$ .
- Even if  $A$  is not finitely generated, the *size* of its torsion-free part is uniquely determined, as is explained in more detail in the article on rank of an abelian group.
- An abelian group  $A$  is torsion-free if and only if it is flat as a  $\mathbf{Z}$ -module, which means that whenever  $C$  is a subgroup of some abelian group  $B$ , then the natural map from the tensor product  $C \otimes A$  to  $B \otimes A$  is injective.
- Tensoring an abelian group  $A$  with  $\mathbf{Q}$  (or any divisible group) kills torsion. That is, if  $T$  is a torsion group then  $T \otimes \mathbf{Q} = 0$ . For a general abelian group  $A$  with torsion subgroup  $T$  one has  $A \otimes \mathbf{Q} \cong A/T \otimes \mathbf{Q}$ .

## Notes

[1] See Epstein & Cannon (1992) p. 167 (<http://books.google.com/books?id=DQ84QITr-EgC&pg=PA167>)

## References

- Epstein, D. B. A., Cannon, James W.. *Word processing in groups*. A K Peters, 1992. ISBN 0867202440

# Article Sources and Contributors

**Zassenhaus lemma** *Source:* <http://en.wikipedia.org/w/index.php?oldid=474249191> *Contributors:* Ahills60, Brad7777, Charles Matthews, DRLB, David Eppstein, FF2010, Giftlite, Helder.wiki, Jason Recliner, Esq., Jeepday, Julien Tuerlinckx, Mat cross, MathMartin, Michael Hardy, Nbarth, RDBury, Schneelocke, Silly rabbit, Silverfish, Waltpohl, 5 anonymous edits

**Center (group theory)** *Source:* <http://en.wikipedia.org/w/index.php?oldid=482612287> *Contributors:* Alberto da Calvaire, Albmont, Arobic, AxelBoldt, CharlotteWebb, Chas zzz brown, Conversion script, Domination989, Fropuff, Giftlite, Goochelaar, Graham87, Grubber, Gubbubu, IhorLiv, Inquam, JackSchmidt, Jim.belk, Lipedia, MathMartin, Meand, Michael Hardy, Nbarth, Obondu, Patrick, Paul Ebermann, Phys, Pi.C.Noizecehx, Sanderling, Sporgp, Stolee, Sławomir Biały, Tannutuva, Tjschuck, Tobias Bergemann, TomyDuby, Tong, Vipul, Ygramul, Zero0000, Zundark, 33 anonymous edits

**Centralizer and normalizer** *Source:* <http://en.wikipedia.org/w/index.php?oldid=471579721> *Contributors:* 417.417, AxelBoldt, Bernard Hurley, Chas zzz brown, Crisófilax, Cwitty, Denisarona, Derek Ross, EoGuy, Hans Adler, Helder.wiki, Joriki, KDesk, LOL, MathMartin, Michael Hardy, Michael Slone, Oleg Alexandrov, Pratik.mallya, Quondum, Rschwieb, Skullfission, Sullivan.tj, Tong, Triona, Tyomitch, Vivacissimamente, Woscafrench, Zeimusu, Zundark, 16 anonymous edits

**Characteristic subgroup** *Source:* <http://en.wikipedia.org/w/index.php?oldid=482613084> *Contributors:* Ahoerstemeyer, AxelBoldt, Bibekmaths, Charles Matthews, Chas zzz brown, Conversion script, Dan Hoey, Derek Ross, Edgar181, Fropuff, GB fan, Giftlite, Goochelaar, Graham87, JackSchmidt, Jim.belk, Lethe, Linas, Michael Hardy, Nbarth, Patrick, Qetuth, Tesseran, Toobaz, Vipul, Zundark, 18 anonymous edits

**Commutator** *Source:* <http://en.wikipedia.org/w/index.php?oldid=482611588> *Contributors:* AlainD, Algebraist, Anne Bauval, Anville, Atlant, AugPi, AxelBoldt, BenFrantzDale, Bryan Derksen, Charles Matthews, CompuChip, Conversion script, Cuzkatzimhut, Dan Granahan, Daniele.tampieri, Dominus, Dori, Dysprosia, El C, Elansey, EthanCho, F=q(E+v^b), Fropuff, Gareth Owen, Gauss, Georgelulu, Giftlite, Glenn, Goochelaar, Gormendo, Grubber, Hans Adler, HappyCamper, Harold f, Headbomb, Henry Delforn (old), Huppybanny, JabberWok, JackSchmidt, JadeNB, JeffBobFrank, JohnBlackburne, KSmrq, Kcordina, Krasnoludek, Lambiam, Larryisgood, Lethe, LokiClock, MFH, Melchoir, Mewt, Mfrosz, Michael Hardy, Modify, Mon4, Ms2ger, Nickj, Nlu, Omnipaedista, PasswOrd, Paul D. Anderson, PaulTanenbaum, Phil Boswell, Polyade, Puuroppysy, Quentar, Reddi, RoboJesus, Salix alba, Seb35, StarLight, Strange but untrue, Tesi1700, Tesseran, Tobias Bergemann, Turgidson, Ub3rm4th, Whaa?, Yahya Abdal-Aziz, Мыша, 55 anonymous edits

**Composition series** *Source:* <http://en.wikipedia.org/w/index.php?oldid=480665372> *Contributors:* Arcfrk, C S, Camrn86, ChKa, Charles Matthews, Docu, Dominus, Dylan Moreland, ElNuevoEinstein, Fropuff, Giftlite, JackSchmidt, Jay Gatsby, Kotasik, LokiClock, MathMartin, Mct mht, Messagetolove, Michael Hardy, Nbarth, Oleg Alexandrov, P Ingerson, Phys, Quietbritishjim, R'n'B, Rjwilmsi, RobHar, Rschwieb, Ruslan Sharipov, Thehotelambush, Tobias Bergemann, Zundark, 12 anonymous edits

**Conjugacy class** *Source:* <http://en.wikipedia.org/w/index.php?oldid=463694831> *Contributors:* Adam majewski, Archelon, AutomaticWriting, AxelBoldt, Charles Matthews, Chas zzz brown, Derek Ross, Dominus, Dysprosia, Fropuff, Giftlite, Helder.wiki, Howard McCay, JackSchmidt, Jim.belk, Jiy, Juan Marquez, Katzmik, Marc van Leeuwen, MathMartin, Michael Hardy, Mpd1989, Nbarth, Nd12345, Nsalven, Oleg Alexandrov, Patrick, Pietro KC, Pjacobi, Pyrop, Quuxplusone, Sandeep.murthy, SantoBugito, Schutz, TakuyaMurata, Tong, Tyomitch, VKokielov, Welsh, Wesley1610, Wpoely86, XJamRastafire, Zundark, 33 anonymous edits

**Conjugate closure** *Source:* <http://en.wikipedia.org/w/index.php?oldid=468925402> *Contributors:* AxelBoldt, CDN99, CZeke, Chas zzz brown, Fropuff, Jay Gatsby, Mhss, Michael Slone, Mike Segal, Qetuth, Roentgenium111, Tobias Bergemann, Vanish2, 6 anonymous edits

**Conjugation of isometries in Euclidean space** *Source:* <http://en.wikipedia.org/w/index.php?oldid=353817849> *Contributors:* Archelon, Charles Matthews, Huku-chan, Jim.belk, Mhss, Noobert1234, PV=nRT, Patrick, Pontificake

**Core (group)** *Source:* <http://en.wikipedia.org/w/index.php?oldid=470632636> *Contributors:* Charles Matthews, Cobaltcigs, E Wing, Emmanuel93, Fropuff, Galoubet, Gauge, J.delanoy, JackSchmidt, MAntioch, Michael Hardy, Michael Slone, Nbarth, Omnipaedista, Xma, RayBirks, Reetep, Superminja, Zundark, 6 anonymous edits

**Coset** *Source:* <http://en.wikipedia.org/w/index.php?oldid=482163396> *Contributors:* Adan, Allanhalme, AtomicDragon, AxelBoldt, Balrog-kun, Calle, Charles Matthews, Chokfung, Chzz, Deewiant, Deimos 28, Dinosaur puppy, Dmharvey, Dysprosia, Eric Kvaalen, Fropuff, Gianluigi, Giftlite, Grubber, Hawthorn, HonoreDB, JackSchmidt, Jim.belk, Kjartan, Kragen, La goutte de pluie, Leycecc, LokiClock, MathMartin, Motmahp, Nsk92, OneWeirdDude, Onevim, Patrick, Pyrop, RDBury, Revolver, RexxS, Schutz, Superminja, Tobias Bergemann, Tong, Tyomitch, VKokielov, Wshun, Xantharius, Yuide, 36 anonymous edits

**Commutator subgroup** *Source:* <http://en.wikipedia.org/w/index.php?oldid=482629961> *Contributors:* Andi5, AxelBoldt, Charles Matthews, Chas zzz brown, Conversion script, DYLAN LENNON, Dysprosia, Felipe Gonçalves Assis, Gaius Cornelius, Geminatae, Giftlite, Goochelaar, Graham87, Henning Makhholm, JackSchmidt, Jim.belk, Kurykh, Lupin, Magister Mathematicae, MarSch, MathMartin, Mattbuck, Michael Hardy, Michael Slone, Mistamagic28, Nbarth, Originalbigj, Pclark, Schildt.a, Thazett, TobinFricke, Tosha, Turgidson, Vipul, W3asal, Weregberil, Zero sharp, Zundark, 45 anonymous edits

**Elementary group theory** *Source:* <http://en.wikipedia.org/w/index.php?oldid=470654553> *Contributors:* 130.182.129.xxx, Armeth, Auximines, AxelBoldt, Barsamin, Beroal, Brad7777, Calum, Ceroklis, Charles Matthews, Felipe Groves, Chas zzz brown, Conversion script, David.kaplan, Derek Ross, Ducnm, Dysprosia, Giftlite, Graham87, Hammerite, JackSchmidt, Jim.belk, JohnBlackburne, Keenan Pepper, Kurykh, Lisp21, Marc van Leeuwen, MattTait, Mav, Mhss, Michael Hardy, Michael Slone, N8chz, Naddy, Oleg Alexandrov, P0807670, Pizzadeliveryboy, Reetep, Salix alba, Sam Hocevar, Schutz, TakuyaMurata, Usien6, Vecter, Zundark, 48 anonymous edits

**Euler's theorem** *Source:* <http://en.wikipedia.org/w/index.php?oldid=481299199> *Contributors:* AB, Algebraist, Almit39, Andre Engels, AndrewKepert, Arthur Rubin, Avavrin, AxelBoldt, BeteNoir, BiT, CRGreathouse, CYD, Christoffel K, CryptoDerk, Daqu, David Eppstein, Dcoetzee, Devnullnor, Dicklyon, Dirac1933, Drmies, Dysprosia, Edemaine, Estel, Excerial, Fama Clamosa, Gandalf61, Giftlite, Guysoft, Haham hanuka, JayC, JensG, Konradek, Luk3, Lupin, MagnusPI, Marek69, Maxim Razin, Michael Hardy, Misof, Nguyễn Thanh Quang, Nikai, Nonagonal Spider, Oleg Alexandrov, Pako, Pleasantville, Pred, Pyrop, RDBury, SDaniel, Smyth, Supermint, Talouv, Tomaxer, Tromer, Virginia-American, Wayne Slam, Wikieditor06, Wmaham, WojciechSwiderski, Yukke123, Zdrlik, مسمي, 72 anonymous edits

**Fitting subgroup** *Source:* <http://en.wikipedia.org/w/index.php?oldid=389989830> *Contributors:* Bird of paradox, Charles Matthews, Echocampfire, Gauge, Giftlite, JackSchmidt, Joriki, Michael Hardy, Nbarth, Polyade, R.e.b., SetaLyas, Sporgp, TakuyaMurata, Vanish2, Vipul, Zundark

**Hamiltonian group** *Source:* <http://en.wikipedia.org/w/index.php?oldid=451615111> *Contributors:* AxelBoldt, Charles Matthews, Chas zzz brown, Headbomb, Helder.wiki, JackSchmidt, Jim.belk, Michael Slone, Rgdboer, Rjwilmsi, Seb35, Tomo, Uranographer, Vipul, Zundark, 1 anonymous edits

**Identity element** *Source:* <http://en.wikipedia.org/w/index.php?oldid=472414457> *Contributors:* 2D, ABCD, Acroterion, Aeons, Andres, AxelBoldt, Baumgaertner, Belinrahs, Beremiz, Bggoldie, BiT, Bkkbrad, Bombshell, Charles Matthews, Conversion script, Dan653, Davehi 1, David Shay, Dreish, Dysprosia, EdC, EmiI, GLaDOS, Giftlite, Gubbubu, Haza-w, Helix84, Hyacinth, Ideyal, Jay-Sebastos, Jiddisch, Jim.belk, Jokes Free4Me, Keilana, Lethe, Luokehao, MattGiuca, Mattblack82, Melchoir, Mindmatrix, Neelix, Obradovic Goran, Octahedron80, Paul August, Pcap, Pcb21, Philip Hazelden, Philip Trueman, R'n'B, Riojajar, RobertG, Sajjad.r, Salix alba, Sandman, SebastianHelm, Tim Starling, Toby, Toby Bartels, TooMuchMath, Unyoyega, Varuna, WaysToEscape, Woodstone, XJamRastafire, Xyctka, Zundark, 43 anonymous edits

**Lagrange's theorem (group theory)** *Source:* <http://en.wikipedia.org/w/index.php?oldid=474239464> *Contributors:* Aboalbiss, AdamSmithee, Avik21, AxelBoldt, BeteNoir, Brad7777, Bryan Derksen, Calle, Charles Matthews, Chas zzz brown, Chromosome, Conversion script, Courcelles, Creidieki, Cwkmail, Dcoetzee, Dysprosia, Eric119, Giftlite, Goochelaar, Graham87, GregorB, Grubber, Hyju, Ixf64, JCSantos, JackSchmidt, Joth, Kila, Leycecc, Lhf, Lowellian, Lupin, Mathsci, Miaow Miaow, Michael Hardy, Obradovic Goran, Plasticup, Quotient group, Reaper Eternal, Rghthndsl, Salvatore Ingala, Sodin, Superminja, Tarquin, Timwi, Tsemii, Xantharius, Youandme, Yuval Madaar, 40 anonymous edits

**Multiplicative inverse** *Source:* <http://en.wikipedia.org/w/index.php?oldid=468266617> *Contributors:* Alansohn, Algebraist, Anaxial, ArnoldReinhold, Arthur Rubin, Avant Guard, BarretB, Ben Boldt, Ben Tillman, Bo Jacoby, Bobo192, CBM, CRGreathouse, Calabe1992, Cb4astro, Chrisjwmartin, Coolbeans39, Copistopplayer, Dan Hoey, David Eppstein, Dcoetzee, Dmcq, Doctormatt, Dogah, Dreadstar, Duoduoduo, Dysepion, EmiIJ, Eppr123, Eric119, Frazzydee, FreeKresge, Frigator, Fropuff, Gesslein, Ghazer, Giftlite, Glane23, Glenn, Goffrie, GraemeMcRae, Greensburger, Haham hanuka, He Who Is, HoodedMan, Ixf64, JLaTondre, JackSchmidt, Jackpots, Jersey Devil, Jheald, Jim.belk, Josh Parris, Jshadias, Justin W Smith, KSmrq, Kingpin13, Kmhhkmh, Lawilkin, Leon2323, Levineps, Logan, Lyleq, MFH, Madmath789, Marc van Leeuwen, Mets501, Mggiganteus1, Mhaitham.shammaa, Michael Hardy, Michael Slone, Mike.lifeguard, Moipaulocho, Montchav, Mothernessfather, MyNamesNeo, Narnaja, Natalya, No Guru, Notthepainter, OMGsplosion, Octahedron80, Omicronpersei8, OohBunnies!, Oxymoron83, Pandelon, Patrick, Philip Trueman, Piano non troppo, Pmanderson, Quondum, R00723r0, Ramu50, Rettetast, Rich Farmbrough, Rigadoun, Robma, Robo37, Ronhones, Rror, Ruud Koot, Salgueiro, Slakr, Smoby10, Square87, Stephen Poppitt, Tbjw, Tide rolls, Timwi, Toby Bartels, Tobych, Toomai Glittershine, UU, WadeSimiser, WarthogDemon, Wknight94, Wood Thrush, Zorakoid, 214 anonymous edits

**Normal subgroup** *Source:* <http://en.wikipedia.org/w/index.php?oldid=481787330> *Contributors:* Adan, Albmont, Andre Engels, Archelon, AxelBoldt, C S, CDN99, Calle, Cambyses, Charles Matthews, Cmouse, Conversion script, Dbenbenn, Dysprosia, Eck, Eef (A), El C, Fedandr, Fibonacci, Fropuff, Giftlite, Git2010, Goochelaar, Graham87, Grubber, Imnotminkus, Infodonor, JackSchmidt, Jakob.scholbach, Jim.belk, Jmdx, Jorend, Jwuthe2, KSmrq, Kmhmh, Lament, MathMartin, Michael Hardy, Netheril96, Nishantjr, Number 0, Obradovic Goran, Patrick, Pyrop, RedAcer, Revolver, Ringspectrum, Spliffy, Stifle, Svick, TakuyaMurata, Tarquin, The Anome, Thehotelambush, Vipul, Weialawaga, Wikipedist, Wshun, XDorksiclex, Zundark, Мыша, 66 anonymous edits

**Perfect group** *Source:* <http://en.wikipedia.org/w/index.php?oldid=482164044> *Contributors:* Charles Matthews, Cyde, Der Shim, Headbomb, JackSchmidt, Michael Hardy, Nbarth, Point-set topologist, Sullivan.t.j, Turgidson, Vipul, Zundark, 16 anonymous edits

**Schreier refinement theorem** *Source:* <http://en.wikipedia.org/w/index.php?oldid=474249304> *Contributors:* BeteNoir, Brad7777, CBM, Charles Matthews, David Eppstein, Gauge, Geometry guy, ImPerfectHacker, Jaakko Seppälä, Michael Slone, Qetuth, Spartanfox86, Tobias Bergemann, 1 anonymous edits

**Subgroup** *Source:* <http://en.wikipedia.org/w/index.php?oldid=473773156> *Contributors:* Adan, Arturj, Arved, AugPi, Augurar, AxelBoldt, Charles Matthews, Chas zzz brown, Conversion script, David Eppstein, Dcoetzee, Dysprosia, Fredrik, Gaius Cornelius, Giftlite, Grubber, Helder.wiki, Jakob.scholbach, Jim.belk, Jotomicron, Kilva, Lethe, Lipedia, LokiClock, MathMartin, Mets501, Michael Hardy, Michael Slone, Nbarth, Obradovic Goran, OktayD, Patrick, Point-set topologist, Pred, Pyrop, Revolver, SLi, Schutz, Storm Rider, TakuyaMurata, Tanner Swett, Topology Expert, VKokielov, Vipul, Viriditas, Wakimakirolls, West.andrew.g, Zero0000, Zundark, 25 anonymous edits

**Transversal (combinatorics)** *Source:* <http://en.wikipedia.org/w/index.php?oldid=474145816> *Contributors:* Altenmann, Ark'ay, BertSeghers, Booyabazooka, Charles Matthews, Cullinane, David Eppstein, Discospinster, Flegmon, Ghazer, Hillman, Imperial Monarch, J.delanoy, JackSchmidt, Jim.belk, Jleedev, Khazar, Lantonov, Michael Hardy, Michael Slone, NHJG, Nbarth, Ott2, RDBury, Salix alba, Scottfisher, Superminja, Wcherowi, Xlgr2007, Zaslav, Zero0000, 29 anonymous edits

**Torsion subgroup** *Source:* <http://en.wikipedia.org/w/index.php?oldid=423089770> *Contributors:* AxelBoldt, Bryan Derksen, Charles Matthews, Chas zzz brown, Derek Ross, Didivan, Elroch, Fibonacci, Fropuff, Gelingvistoj, Giftlite, Helder.wiki, Jcreed, Keenan Pepper, Konradek, Lenthe, MathMartin, Navilluskram, PV=nRT, Paul August, Zundark, Мыша, 7 anonymous edits

# Image Sources, Licenses and Contributors

**Image:Butterfly lemma.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Butterfly\\_lemma.svg](http://en.wikipedia.org/w/index.php?title=File:Butterfly_lemma.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Claudio Rocchini

**File:Dihedral group of order 8; Cayley table (element orders 1,2,2,2,4,4,2); subgroup of S4.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Dihedral\\_group\\_of\\_order\\_8;\\_Cayley\\_table\\_\(element\\_orders\\_1,2,2,2,4,4,2\);\\_subgroup\\_of\\_S4.svg](http://en.wikipedia.org/w/index.php?title=File:Dihedral_group_of_order_8;_Cayley_table_(element_orders_1,2,2,2,4,4,2);_subgroup_of_S4.svg) *License:* GNU Free Documentation License *Contributors:* User:Lipedia

**Image:Hyperbola one over x.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Hyperbola\\_one\\_over\\_x.svg](http://en.wikipedia.org/w/index.php?title=File:Hyperbola_one_over_x.svg) *License:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contributors:* Anarkman, Darapti, Juiced lemon, Ktiims, Myself488, 6 anonymous edits

**File:Symmetric group 4; Cayley table; numbers.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Symmetric\\_group\\_4;\\_Cayley\\_table;\\_numbers.svg](http://en.wikipedia.org/w/index.php?title=File:Symmetric_group_4;_Cayley_table;_numbers.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Symmetric group 4; Lattice of subgroups Hasse diagram.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Symmetric\\_group\\_4;\\_Lattice\\_of\\_subgroups\\_Hasse\\_diagram.svg](http://en.wikipedia.org/w/index.php?title=File:Symmetric_group_4;_Lattice_of_subgroups_Hasse_diagram.svg) *License:* GNU Free Documentation License *Contributors:* User:Lipedia

**File:Klein four-group; Cayley table; subgroup of S4 (elements 0,7,16,23).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Klein\\_four-group;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,7,16,23\).svg](http://en.wikipedia.org/w/index.php?title=File:Klein_four-group;_Cayley_table;_subgroup_of_S4_(elements_0,7,16,23).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Cyclic group 3; Cayley table; subgroup of S4 (elements 0,3,4).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Cyclic\\_group\\_3;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,3,4\).svg](http://en.wikipedia.org/w/index.php?title=File:Cyclic_group_3;_Cayley_table;_subgroup_of_S4_(elements_0,3,4).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Cyclic group 3; Cayley table; subgroup of S4 (elements 0,11,19).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Cyclic\\_group\\_3;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,11,19\).svg](http://en.wikipedia.org/w/index.php?title=File:Cyclic_group_3;_Cayley_table;_subgroup_of_S4_(elements_0,11,19).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Cyclic group 3; Cayley table; subgroup of S4 (elements 0,15,20).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Cyclic\\_group\\_3;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,15,20\).svg](http://en.wikipedia.org/w/index.php?title=File:Cyclic_group_3;_Cayley_table;_subgroup_of_S4_(elements_0,15,20).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Cyclic group 3; Cayley table; subgroup of S4 (elements 0,8,12).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Cyclic\\_group\\_3;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,8,12\).svg](http://en.wikipedia.org/w/index.php?title=File:Cyclic_group_3;_Cayley_table;_subgroup_of_S4_(elements_0,8,12).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Alternating group 4; Cayley table; numbers.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Alternating\\_group\\_4;\\_Cayley\\_table;\\_numbers.svg](http://en.wikipedia.org/w/index.php?title=File:Alternating_group_4;_Cayley_table;_numbers.svg) *License:* GNU Free Documentation License *Contributors:* Lipedia

**File:Klein four-group; Cayley table; subgroup of S4 (elements 0,1,6,7).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Klein\\_four-group;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,1,6,7\).svg](http://en.wikipedia.org/w/index.php?title=File:Klein_four-group;_Cayley_table;_subgroup_of_S4_(elements_0,1,6,7).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Cyclic group 4; Cayley table (element orders 1,2,4,4); subgroup of S4.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Cyclic\\_group\\_4;\\_Cayley\\_table\\_\(element\\_orders\\_1,2,4,4\);\\_subgroup\\_of\\_S4.svg](http://en.wikipedia.org/w/index.php?title=File:Cyclic_group_4;_Cayley_table_(element_orders_1,2,4,4);_subgroup_of_S4.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Klein four-group; Cayley table; subgroup of S4 (elements 0,5,14,16).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Klein\\_four-group;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,5,14,16\).svg](http://en.wikipedia.org/w/index.php?title=File:Klein_four-group;_Cayley_table;_subgroup_of_S4_(elements_0,5,14,16).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Cyclic group 4; Cayley table (element orders 1,4,2,4); subgroup of S4.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Cyclic\\_group\\_4;\\_Cayley\\_table\\_\(element\\_orders\\_1,4,2,4\);\\_subgroup\\_of\\_S4.svg](http://en.wikipedia.org/w/index.php?title=File:Cyclic_group_4;_Cayley_table_(element_orders_1,4,2,4);_subgroup_of_S4.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Dihedral group of order 8; Cayley table (element orders 1,2,2,4,2,2,4,2); subgroup of S4.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Dihedral\\_group\\_of\\_order\\_8;\\_Cayley\\_table\\_\(element\\_orders\\_1,2,2,4,2,2,4,2\);\\_subgroup\\_of\\_S4.svg](http://en.wikipedia.org/w/index.php?title=File:Dihedral_group_of_order_8;_Cayley_table_(element_orders_1,2,2,4,2,2,4,2);_subgroup_of_S4.svg) *License:* GNU Free Documentation License *Contributors:* User:Lipedia

**File:Klein four-group; Cayley table; subgroup of S4 (elements 0,2,21,23).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Klein\\_four-group;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,2,21,23\).svg](http://en.wikipedia.org/w/index.php?title=File:Klein_four-group;_Cayley_table;_subgroup_of_S4_(elements_0,2,21,23).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Cyclic group 4; Cayley table (element orders 1,4,4,2); subgroup of S4.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Cyclic\\_group\\_4;\\_Cayley\\_table\\_\(element\\_orders\\_1,4,4,2\);\\_subgroup\\_of\\_S4.svg](http://en.wikipedia.org/w/index.php?title=File:Cyclic_group_4;_Cayley_table_(element_orders_1,4,4,2);_subgroup_of_S4.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Dihedral group of order 8; Cayley table (element orders 1,2,2,4,4,2,2,2); subgroup of S4.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Dihedral\\_group\\_of\\_order\\_8;\\_Cayley\\_table\\_\(element\\_orders\\_1,2,2,4,4,2,2,2\);\\_subgroup\\_of\\_S4.svg](http://en.wikipedia.org/w/index.php?title=File:Dihedral_group_of_order_8;_Cayley_table_(element_orders_1,2,2,4,4,2,2,2);_subgroup_of_S4.svg) *License:* GNU Free Documentation License *Contributors:* User:Lipedia

**File:Symmetric group 3; Cayley table; subgroup of S4 (elements 0,1,2,3,4,5).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Symmetric\\_group\\_3;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,1,2,3,4,5\).svg](http://en.wikipedia.org/w/index.php?title=File:Symmetric_group_3;_Cayley_table;_subgroup_of_S4_(elements_0,1,2,3,4,5).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Symmetric group 3; Cayley table; subgroup of S4 (elements 0,5,6,11,19,21).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Symmetric\\_group\\_3;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,5,6,11,19,21\).svg](http://en.wikipedia.org/w/index.php?title=File:Symmetric_group_3;_Cayley_table;_subgroup_of_S4_(elements_0,5,6,11,19,21).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Symmetric group 3; Cayley table; subgroup of S4 (elements 0,1,14,15,20,21).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Symmetric\\_group\\_3;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,1,14,15,20,21\).svg](http://en.wikipedia.org/w/index.php?title=File:Symmetric_group_3;_Cayley_table;_subgroup_of_S4_(elements_0,1,14,15,20,21).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

**File:Symmetric group 3; Cayley table; subgroup of S4 (elements 0,2,6,8,12,14).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Symmetric\\_group\\_3;\\_Cayley\\_table;\\_subgroup\\_of\\_S4\\_\(elements\\_0,2,6,8,12,14\).svg](http://en.wikipedia.org/w/index.php?title=File:Symmetric_group_3;_Cayley_table;_subgroup_of_S4_(elements_0,2,6,8,12,14).svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Lipedia

# License

---

Creative Commons Attribution-Share Alike 3.0 Unported  
[//creativecommons.org/licenses/by-sa/3.0/](https://creativecommons.org/licenses/by-sa/3.0/)

---