Structures and operations of group

generated by Lam Phong

Contents

Articles

References

Article Licenses

Group extension

In mathematics, a **group extension** is a general means of describing a group in terms of a particular normal subgroup and quotient group. If Q and N are two groups, then G is an **extension** of Q by N if there is a short exact sequence

$$1 \to N \to G \to Q \to 1.$$

If G is an extension of Q by N, then G is a group, N is a normal subgroup of G and the quotient group G/N is isomorphic to group Q. Group extensions arise in the context of the **extension problem**, where the groups Q and N are known and the properties of G are to be determined.

An extension is called a **central extension** if the subgroup N lies in the center of G.

Extensions in general

One extension, the direct product, is immediately obvious. If one requires G and Q to be abelian groups, then the set of isomorphism classes of extensions of Q by a given (abelian) group N is in fact a group, which is isomorphic to

$$\mathrm{Ext}^1_{\mathbb{Z}}(Q, N);$$

cf. the Ext functor. Several other general classes of extensions are known but no theory exists which treats all the possible extensions at one time. Group extension is usually described as a hard problem; it is termed the **extension problem**.

To consider some examples, if $G = H \times K$, then G is an extension of both H and K. More generally, if G is a semidirect product of K and H, then G is an extension of H by K, so such products as the wreath product provide further examples of extensions.

Extension problem

The question of what groups G are extensions of H is called the **extension problem**, and has been studied heavily since the late nineteenth century. As to its motivation, consider that the composition series of a finite group is a finite sequence of subgroups $\{A_i\}$, where each A_{i+1} is an extension of A_i by some simple group. The classification of finite simple groups would give us a complete list of finite simple groups; so the solution to the extension problem would give us enough information to construct and classify all finite groups in general.

We can use the language of diagrams to provide a more flexible definition of extension: a group G is an extension of a group H by a group K if and only if there is an exact sequence:

$$1 \to K \to G \to H \to 1$$

where 1 denotes the trivial group with a single element. This definition is more general in that it does not require that K be a subgroup of G; instead, K is isomorphic to a normal subgroup K^* of G, and H is isomorphic to G/K^*.

Classifying extensions

Solving the extension problem amounts to classifying all extensions of H by K; or more practically, by expressing all such extensions in terms of mathematical objects that are easier to understand and compute. In general, this problem is very hard, and all the most useful results classify extensions that satisfy some additional condition.

Classifying split extensions

A **split extension** is an extension

$$1 \to K \to G \to H \to 1$$

for which there is a homomorphism $s\colon H \to G$ such that going from H to G by s and then back to H by the quotient map of the short exact sequence induces the identity map on H. In this situation, it is usually said that s

splits the above exact sequence.

Split extensions are very easy to classify, because the splitting lemma states that an extension is split if and only if the group *G* is a semidirect product of *K* and *H*. Semidirect products themselves are easy to classify, because they are in one-to-one correspondence with homomorphisms from $H \to \mathrm{Aut}(K)$, where Aut(*K*) is the automorphism group of *K*. For a full discussion of why this is true, see semidirect product.

Warning

In general in mathematics, an extension of a structure *K* is usually regarded as a structure *L* of which *K* is a substructure. See for example field extension. However in group theory the opposite terminology has crept in, partly because of the notation $\mathrm{Ext}(Q, N)$, which reads easily as extensions of *Q* by *N*, and the focus is on the group *Q*.

The paper of Brown and Porter (1996) on the Schreier theory of nonabelian extensions (cited below) uses the terminology that an extension of *K* gives a larger structure.

Central extension

A **central extension** of a group *G* is a short exact sequence of groups

$$1 \to A \to E \to G \to 1$$

such that *A* is in *Z*(*E*), the center of the group E. The set of isomorphism classes of central extensions of *G* by *A* (where *G* acts trivially on *A*) is in one-to-one correspondence with the cohomology group $H^2(G,A)$.

Examples of central extensions can be constructed by taking any group *G* and any abelian group *A*, and setting *E* to be *A*×*G*. This kind of *split* example (a split extension in the sense of the extension problem, since *G* is present as a subgroup of *E*) isn't of particular interest, since it corresponds to the element *0* in $H^2(G,A)$ under the above correspondence. More serious examples are found in the theory of projective representations, in cases where the projective representation cannot be lifted to an ordinary linear representation.

In the case of finite perfect groups, there is a universal perfect central extension.

Similarly, the central extension of a Lie algebra is an exact sequence

$$0 \to \mathfrak{a} \to \mathfrak{e} \to \mathfrak{g} \to 0$$

such that $\mathfrak{a}$ is in the center of $\mathfrak{e}$.

There is a general theory of central extensions in Maltsev varieties, see the paper by Janelidze and Kelly listed below.

Generalization to general extensions

The paper on Group Extensions and H^3 given below provides a similar classification of all extensions of *G* by *A* in terms of homomorphisms from $G \to \mathrm{Out}(A)$, a tedious but explicitly checkable existence condition involving $H^3(G,Z(A))$ and the cohomology group $H^2(G,Z(A))$.

Lie groups

In Lie group theory, central extensions arise in connection with algebraic topology. Roughly speaking, central extensions of Lie groups by discrete groups are the same as covering groups. More precisely, a connected covering space *G** of a connected Lie group *G* is naturally a central extension of *G*, in such a way that the projection

$$\pi: G^* \to G$$

is a group homomorphism, and surjective. (The group structure on *G** depends on the choice of an identity element mapping to the identity in *G*.) For example, when *G** is the universal cover of *G*, the kernel of π is the fundamental group of *G*, which is known to be abelian (see H-space). Conversely, given a Lie group *G* and a discrete central subgroup *Z*, the quotient *G*/*Z* is a Lie group and *G* is a covering space of it.

More generally, when the groups A, E and G occurring in a central extension are Lie groups, and the maps between them are homomorphism of Lie groups, then the Lie algebra of E is a central extension of the Lie algebra of G by the Lie algebra of A. In the terminology of theoretical physics, generators of *Lie(A)* are called central charges. These generators are in the center of the Lie algebra of E; by Noether's theorem, generators of symmetry groups correspond to conserved quantities, referred to as charges.

The basic examples of central extensions as covering groups are:

- the spin groups, which double cover the special orthogonal groups, which (in even dimension) double-cover the projective orthogonal group.
- the metaplectic groups, which double cover the symplectic groups.

The case of $SL_2(R)$ involves a fundamental group that is infinite cyclic. Here the central extension involved is well known in modular form theory, in the case of forms of weight ½. A projective representation that corresponds is the Weil representation, constructed from the Fourier transform, in this case on the real line. Metaplectic groups also occur in quantum mechanics.

References

- Mac Lane, Saunders (1975), *Homology*, Classics in Mathematics, Springer Verlag, ISBN 3-540-58662-8
- R.L. Taylor, Covering groups of non connected topological groups, *Proceedings of the American Mathematical Society*, vol. 5 (1954), 753-768.
- R. Brown and O. Mucuk, Covering groups of non-connected topological groups revisited, *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 115 (1994), 97-110.
- R. Brown and T. Porter, On the Schreier theory of non-abelian extensions: generalisations and computations, *Proceedings of the Royal Irish Academy*, vol. 96A (1996), 213-227.
- G. Janelidze and G. M. Kelly, Central extensions in Malt'sev varieties [1], *Theory and Applications of Categories*, vol. 7 (2000), 219-226.
- P. J. Morandi, Group Extensions and H^3 [2]. From his collection of short mathematical notes.

References

[1] http://www.tac.mta.ca/tac/volumes/7/n10/7-10abs.html

[2] http://sierra.nmsu.edu/morandi/notes/GroupExtensions.pdf

Direct product of groups

In the mathematical field of group theory, the **direct product** is an operation that takes two groups G and H and constructs a new group, usually denoted $G \times H$. This operation is the group-theoretic analogue of the Cartesian product of sets, and is one of several important notions of direct product in mathematics.

In the context of abelian groups, the direct product is sometimes referred to as the direct sum, and is denoted $G \oplus H$. Direct sums play an important role in the classification of abelian groups: according to fundamental theorem of finite abelian groups, every finite abelian group can be expressed as the direct sum of cyclic groups.

Definition

Given groups G and H, the **direct product** $G \times H$ is defined as follows:

1. The elements of $G \times H$ are ordered pairs (g, h), where $g \in G$ and $h \in H$. That is, the set of elements of $G \times H$ is the Cartesian product of the sets G and H.
2. The binary operation on $G \times H$ is defined componentwise:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$$

The resulting algebraic object satisfies the axioms for a group. Specifically:

Associativity

The binary operation on $G \times H$ is indeed associative.

Identity

The direct product has an identity element, namely $(1_G, 1_H)$, where 1_G is the identity element of G and 1_H is the identity element of H.

Inverses

The inverse of an element (g, h) of $G \times H$ is the pair (g^{-1}, h^{-1}), where g^{-1} is the inverse of g in G, and h^{-1} is the inverse of h in H.

Examples

- Let $\mathbf{R}$ be the group of real numbers under addition. Then the direct product $\mathbf{R} \times \mathbf{R}$ is the group of all two-component vectors (x, y) under the operation of vector addition:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

- Let G and H be cyclic groups with two elements each:

*	**1**	***a***
1	1	*a*
a	*a*	1

*	**1**	***b***
1	1	*b*
b	*b*	1

Then the direct product $G \times H$ is isomorphic to the Klein four-group:

$$G \times H$$

*	**(1, 1)**	**(*a*, 1)**	**(1, *b*)**	**(*a*, *b*)**
(1, 1)	(1, 1)	(*a*, 1)	(1, *b*)	(*a*, *b*)
(*a*, 1)	(*a*, 1)	(1, 1)	(*a*, *b*)	(1, *b*)
(1, *b*)	(1, *b*)	(*a*, *b*)	(1, 1)	(*a*, 1)
(*a*, *b*)	(*a*, *b*)	(1, *b*)	(*a*, 1)	(1, 1)

Elementary properties

- The order of a direct product $G \times H$ is the product of the orders of G and H:

  $$| G \times H | = | G | | H |.$$

  This follows from the formula for the cardinality of the cartesian product of sets.
- The order of each element (g, h) is the least common multiple of the orders of g and h:

  $$| (g, h) | = \text{lcm}(| g |, | h |).$$

  In particular, if $| g |$ and $| h |$ are relatively prime, then the order of (g, h) is the product of the orders of g and h.
- As a consequence, if G and H are cyclic groups whose orders are relatively prime, then $G \times H$ is cyclic as well. That is, if m and n are relatively prime, then

  $$(\mathbf{Z} / m\mathbf{Z}) \times (\mathbf{Z} / n\mathbf{Z}) \cong \mathbf{Z} / mn\mathbf{Z}.$$

  This fact is closely related to the Chinese remainder theorem.

Algebraic structure

Let G and H be groups, let $P = G \times H$, and consider the following two subsets of P:

$$\text{G'} = \{ (g, 1) : g \in G \} \quad \text{and} \quad \text{H'} = \{ (1, h) : h \in H \}$$

Both of these are in fact subgroups of P, the first being isomorphic to G, and the second being isomorphic to H. If we identify these with G and H, respectively, then we can think of the direct product P as containing the original groups G and H as subgroups.

These subgroups of P have the following three important properties: (Saying again that we identify G' and H' with G and H, respectively.)

1. The intersection $G \cap H$ is trivial.
2. Every element of P can be expressed as the product of an element of G and an element of H.
3. Every element of G commutes with every element of H.

Together, these three properties completely determine the algebraic structure of the direct product P. That is, if P is *any* group having subgroups G and H that satisfy the properties above, then P is necessarily isomorphic to the direct product of G and H. In this situation, P is sometimes referred to as the **internal direct product** of its subgroups G and H.

In some contexts, the third property above is replaced by the following:

3'. Both G and H are normal in P.

This property is equivalent to property 3, since the elements of two normal subgroups with trivial intersection necessarily commute.

Examples

- Let V be the Klein four-group:

V

*	**1**	***a***	***b***	***c***
1	1	*a*	*b*	*c*
a	*a*	1	*c*	*b*
b	*b*	*c*	1	*a*
c	*c*	*b*	*a*	1

  Then V is the internal direct product of the two-element subgroups $\{ 1, a \}$ and $\{ 1, b \}$.

- Let $\langle a \rangle$ be a cyclic group of order mn, where m and n are relatively prime. Then $\langle a^n \rangle$ and $\langle a^m \rangle$ are cyclic subgroups of orders m and n, respectively, and $\langle a \rangle$ is the internal direct product of these subgroups.
- Let $\mathbf{C}^\times$ be the group of nonzero complex numbers under multiplication. Then $\mathbf{C}^\times$ is the internal direct product of the circle group $\mathbf{T}$ of unit complex numbers and the group $\mathbf{R}^+$ of positive real numbers under multiplication.
- If n is odd, then the general linear group $GL(n, \mathbf{R})$ is the internal direct product of the special linear group $SL(n, \mathbf{R})$ and the subgroup consisting of all scalar matrices.
- Similarly, when n is odd the orthogonal group $O(n, \mathbf{R})$ is the internal direct product of the special orthogonal group $SO(n, \mathbf{R})$ and the two-element subgroup $\{ -I, I \}$, where I denotes the identity matrix.
- The symmetry group of a cube is the internal direct product of the subgroup of rotations and the two-element group $\{ -I, I \}$, where I is the identity element and $-I$ is the point reflection through the center of the cube. A similar fact holds true for the symmetry group of a icosahedron.
- Let n be odd, and let D_{4n} be the dihedral group of order $4n$:

$$D_{4n} = \langle\ r, s \mid r^{2n} = s^2 = 1, sr = r^{-1}s\ \rangle\ .$$

  Then D_{4n} is the internal direct product of the subgroup $\langle\ r^2, s\ \rangle$ (which is isomorphic to D_{2n}) and the two-element subgroup $\{ 1, r^n \}$.

Presentations

The algebraic structure of $G \times H$ can be used to give a presentation for the direct product in terms of the presentations of G and H. Specifically, suppose that

$$G = \langle\ S_G \mid R_G\ \rangle \quad \text{and} \quad H = \langle\ S_H \mid R_H\ \rangle\ ,$$

where S_G and S_H are (disjoint) generating sets and R_G and R_H are defining relations. Then

$$G \times H = \langle\ S_G \cup S_H \mid R_G \cup R_H \cup R_P\ \rangle$$

where R_P is a set of relations specifying that each element of S_G commutes with each element of S_H

For example, suppose that

$$G = \langle\ a \mid a^3 = 1\ \rangle \quad \text{and} \quad H = \langle\ b \mid b^5 = 1\ \rangle\ .$$

Then

$$G \times H = \langle\ a, b \mid a^3 = 1, b^5 = 1, ab = ba\ \rangle\ .$$

Normal structure

As mentioned above, the subgroups G and H are normal in $G \times H$. Specifically, define functions $\pi_G\colon G \times H \to G$ and $\pi_H\colon G \times H \to H$ by

$$\pi_G(g, h) = g \quad \text{and} \quad \pi_H(g, h) = h.$$

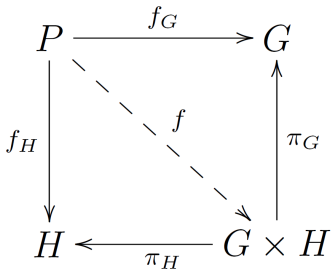
Then π_G and π_H are homomorphisms, known as **projection homomorphisms**, whose kernels are H and G, respectively.

It follows that $G \times H$ is an extension of G by H (or vice-versa). In the case where $G \times H$ is a finite group, it follows that the composition factors of $G \times H$ are precisely the union of the composition factors of G and the composition factors of H.

Further properties

Universal property

The direct product $G \times H$ can be characterized by the following universal property. Let $\pi_G\colon G \times H \to G$ and $\pi_H\colon G \times H \to H$ be the projection homomorphisms. Then for any group P and any homomorphisms $f_G\colon P \to G$ and $f_H\colon P \to H$, there exists a unique homomorphism $f\colon P \to G \times H$ making the following diagram commute:



Specifically, the homomorphism f is given by the formula

$$f(p) = (f_G(p), f_H(p)).$$

This is a special case of the universal property for products in category theory.

Subgroups

If A is a subgroup of G and B is a subgroup of H, then the direct product $A \times B$ is a subgroup of $G \times H$. For example, the isomorphic copy of G in $G \times H$ is the product $G \times \{1\}$, where $\{1\}$ is the trivial subgroup of H.

If A and B are normal, then $A \times B$ is a normal subgroup of $G \times H$. Moreover, the quotient $(G \times H) / (A \times B)$ is isomorphic to the direct product of the quotients G / A and H / B:

$$(G \times H) / (A \times B) \cong (G / A) \times (H / B).$$

Note that it is not true in general that every subgroup of $G \times H$ is the product of a subgroup of G with a subgroup of H. For example, if G is any group, then the product $G \times G$ has a diagonal subgroup

$$\Delta = \{ (g, g) : g \in G \}$$

which is not the direct product of two subgroups of G. Other subgroups include fiber products of G and H (see below). The subgroups of direct products are described by Goursat's lemma.

Conjugacy and centralizers

Two elements (g_1, h_1) and (g_2, h_2) are conjugate in $G \times H$ if and only if g_1 and g_2 are conjugate in G and h_1 and h_2 are conjugate in H. It follows that each conjugacy class in $G \times H$ is simply the Cartesian product of a conjugacy class in G and a conjugacy class in H.

Along the same lines, if $(g, h) \in G \times H$, the centralizer of (g, h) is simply the product of the centralizers of g and h:

$$C_{G\times H}(g, h) = C_G(g) \times C_H(h).$$

Similarly, the center of $G \times H$ is the product of the centers of G and H:

$$Z(G \times H) = Z(G) \times Z(H).$$

Normalizers behave in a more complex manner since not all subgroups of direct products themselves decompose as direct products.

Automorphisms and endomorphisms

If α is an automorphism of G and β is an automorphism of H, then the product function $\alpha \times \beta$: $G \times H \to G \times H$ defined by

$$(\alpha \times \beta)(g, h) = (\alpha(g), \beta(h))$$

is an automorphism of $G \times H$. It follows that $\mathrm{Aut}(G \times H)$ has a subgroup isomorphic to the direct product $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

It is not true in general that every automorphism of $G \times H$ has the above form. (That is, $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$ is often a proper subgroup of $\mathrm{Aut}(G \times H)$.) For example, if G is any group, then there exists an automorphism σ of $G \times G$ that switches the two factors, i.e.

$$\sigma(g_1, g_2) = (g_2, g_1).$$

For another example, the automorphism group of $\mathbf{Z} \times \mathbf{Z}$ is $GL(2, \mathbf{Z})$, the group of all 2×2 matrices with integer entries and determinant ± 1. This automorphism group is infinite, but only finitely many of the automorphisms have the form given above.

In general, every endomorphism of $G \times H$ can be written as a 2×2 matrix

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

where α is an endomorphism of G, δ is an endomorphism of H, and β: $H \to G$ and γ: $G \to H$ are homomorphisms. Such a matrix must have the property that every element in the image of α commutes with every element in the image of β, and every element in the image of γ commutes with every element in the image of δ.

When G and H are indecomposable, centerless groups, then the automorphism group is relatively straightforward, being $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$ if G and H are not isomorphic, and $\mathrm{Aut}(G)$ wr 2 if $G \cong H$, wr denotes the wreath product. This is part of the Krull–Schmidt theorem, and holds more generally for finite direct products.

Generalizations

Finite direct products

It is possible to take the direct product of more than two groups at once. Given a finite sequence G_1, ..., G_n of groups, the **direct product**

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n$$

is defined as follows:

- The elements of $G_1 \times \cdots \times G_n$ are tuples $(g_1, ..., g_n)$, where $g_i \in G_i$ for each i.
- The operation on $G_1 \times \cdots \times G_n$ is defined componentwise:

$$(g_1, ..., g_n)(g_1', ..., g_n') = (g_1 g_1', ..., g_n g_n').$$

This has many of the same properties as the direct product of two groups, and can be characterized algebraically in a similar way.

Infinite direct products

It is also possible to take the direct product of an infinite number of groups. For an infinite sequence G_1, G_2, ... of groups, this can be defined just like the finite direct product of above, with elements of the infinite direct product being infinite tuples.

More generally, given an indexed family $\{ G_i \}_{i \in I}$ of groups, the **direct product** $\prod_{i \in I} G_i$ is defined as follows:

- The elements of $\prod_{i \in I} G_i$ are the elements of the infinite Cartesian product of the sets G_i, i.e. functions $f: I \to \bigcup_{i \in I} G_i$ with the property that $f(i) \in G_i$ for each i.
- The product of two elements f, g is defined componentwise:

$$(f \cdot g)(i) = f(i) \cdot g(i).$$

Unlike a finite direct product, the infinite direct product $\prod_{i \in I} G_i$ is not generated by the elements of the isomorphic subgroups $\{ G_i \}_{i \in I}$. Instead, these subgroups generate a subgroup of the direct product known as the **infinite direct sum**, which consists of all elements that have only finitely many non-identity components.

Other products

Semidirect products

Recall that a group P with subgroups G and H is isomorphic to the direct product of G and H as long as it satisfies the following three conditions:

1. The intersection $G \cap H$ is trivial.
2. Every element of P can be expressed as the product of an element of G and an element of H.
3. Both G and H are normal in P.

A **semidirect product** of G and H is obtained by relaxing the third condition, so that only one of the two subgroups G, H is required to be normal. The resulting product still consists of ordered pairs (g, h), but with a slightly more complicated rule for multiplication.

It is also possible to relax the third condition entirely, requiring neither of the two subgroups to be normal. In this case, the group P is referred to as a **Zappa–Szép product** of G and H.

Free products

The **free product** of G and H, usually denoted $G * H$, is similar to the direct product, except that the subgroups G and H of $G * H$ are not required to commute. That is, if

$$G = \langle\ S_G \mid R_G\ \rangle \quad \text{and} \quad H = \langle\ S_H \mid R_H\ \rangle\ ,$$

are presentations for G and H, then

$$G * H = \langle\ S_G \cup S_H \mid R_G \cup R_H\ \rangle\ .$$

Unlike the direct product, elements of the free product cannot be represented by ordered pairs. In fact, the free product of any two nontrivial groups is infinite. The free product is actually the coproduct in the category of groups.

Subdirect products

If G and H are groups, a **subdirect product** of G and H is any subgroup of $G \times H$ which maps surjectively onto G and H under the projection homomorphisms. By Goursat's lemma, every subdirect product is a fiber product, and vice versa.

Fiber products

Let G, H, and Q be groups, and let φ: $G \to Q$ and χ: $H \to Q$ be epimorphisms. The **fiber product** of G and H over Q, also known as a **pullback**, is the following subgroup of $G \times H$:

$$G \times_Q H\ =\ \{\ (g, h) \in G \times H : \varphi(g) = \chi(h)\ \}.$$

By Goursat's lemma, every subdirect product is a fiber product, and vice versa.

References

- Artin, Michael (1991), *Algebra*, Prentice Hall, ISBN 978-0-89871-510-1
- Herstein, Israel Nathan (1996), *Abstract algebra* (3rd ed.), Upper Saddle River, NJ: Prentice Hall Inc., ISBN 978-0-13-374562-7, MR1375019.
- Herstein, Israel Nathan (1975), *Topics in algebra* (2nd ed.), Lexington, Mass.: Xerox College Publishing, MR0356988.
- Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR1878556
- Lang, Serge (2005), *Undergraduate Algebra* (3rd ed.), Berlin, New York: Springer-Verlag, ISBN 978-0-387-22025-3.
- Robinson, Derek John Scott (1996), *A course in the theory of groups*, Berlin, New York: Springer-Verlag, ISBN 978-0-387-94461-6.

Direct sum of groups

In mathematics, a group G is called the **direct sum** of a set of subgroups $\{H_i\}$ if

- each H_i is a normal subgroup of G
- each distinct pair of subgroups has trivial intersection, and
- $G = <\{H_i\}>$; in other words, G is generated by the subgroups $\{H_i\}$.

If G is the direct sum of subgroups H and K, then we write $G = H + K$; if G is the direct sum of a set of subgroups $\{H_i\}$, we often write $G = \sum H_i$. Loosely speaking, a direct sum is isomorphic to a weak direct product of subgroups.

In abstract algebra, this method of construction can be generalized to direct sums of vector spaces, modules, and other structures; see the article direct sum of modules for more information.

This notation is commutative; so that in the case of the direct sum of two subgroups, $G = H + K = K + H$. It is also associative in the sense that if $G = H + K$, and $K = L + M$, then $G = H + (L + M) = H + L + M$.

A group which can be expressed as a direct sum of non-trivial subgroups is called *decomposable*; otherwise it is called *indecomposable*.

If $G = H + K$, then it can be proven that:

- for all h in H, k in K, we have that $h*k = k*h$
- for all g in G, there exists unique h in H, k in K such that $g = h*k$
- There is a cancellation of the sum in a quotient; so that $(H + K)/K$ is isomorphic to H

The above assertions can be generalized to the case of $G = \sum H_i$, where $\{H_1\}$ is a finite set of subgroups.

- if $i \neq j$, then for all h_i in H_i, h_j in H_j, we have that $h_i * h_j = h_j * h_i$
- for each g in G, there unique set of $\{h_i \text{ in } H_i\}$ such that

  $g = h_1 * h_2 * \ldots * h_i * \ldots * h_n$
- There is a cancellation of the sum in a quotient; so that $((\sum H_i) + K)/K$ is isomorphic to $\sum H_i$

Note the similarity with the direct product, where each g can be expressed uniquely as

$g = (h_1, h_2, \ldots, h_i, \ldots, h_n)$

Since $h_i * h_j = h_j * h_i$ for all $i \neq j$, it follows that multiplication of elements in a direct sum is isomorphic to multiplication of the corresponding elements in the direct product; thus for finite sets of subgroups, $\sum H_i$ is isomorphic to the direct product $\times\{H_i\}$.

Equivalence of direct sums

The direct sum is not unique for a group; for example, in the Klein group, $V_4 = C_2 \times C_2$, we have that

$V_4 = <(0,1)> + <(1,0)>$ and

$V_4 = <(1,1)> + <(1,0)>$.

However, it is the content of the Remak-Krull-Schmidt theorem that given a finite group $G = \sum A_i = \sum B_j$, where each A_i and each B_j is non-trivial and indecomposable, then the two sums are equivalent up to reordering and isomorphism of the subgroups involved.

The Remak-Krull-Schmidt theorem fails for infinite groups; so in the case of infinite $G = H + K = L + M$, even when all subgroups are non-trivial and indecomposable, we cannot then assume that H is isomorphic to either L or M.

Generalization to sums over infinite sets

If we wish to describe the above properties in the case where *G* is the direct sum of an infinite (perhaps uncountable) set of subgroups, we need to be a bit more careful.

If *g* is an element of the cartesian product $\prod\{H_i\}$ of a set of groups, let g_i be the *i*th element of *g* in the product. The **external direct sum** of a set of groups $\{H_i\}$ (written as $\sum_E\{H_i\}$) is the subset of $\prod\{H_i\}$, where, for each element *g* of $\sum_E\{H_i\}$, g_i is the identity e_{H_i} for all but a finite number of g_i (equivalently, only a finite number of g_i are not the identity). The group operation in the external direct sum is pointwise multiplication, as in the usual direct product.

This subset does indeed form a group; and for a finite set of groups H_i, the external direct sum is identical to the direct product.

Then if $G = \sum H_i$, then *G* is isomorphic to $\sum_E\{H_i\}$. Thus, in a sense, the direct sum is an "internal" external direct sum. We have that, for each element *g* in *G*, there is a unique finite set *S* and unique $\{h_i \text{ in } H_i : i \text{ in } S\}$ such that $g = \prod\{h_i : i \text{ in } S\}$.

Free abelian group

In abstract algebra, a **free abelian group** is an abelian group that has a "basis" in the sense that every element of the group can be written in one and only one way as a finite linear combination of elements of the basis, with integer coefficients. Hence, free abelian groups over a basis *B* are also known as **formal sums** over *B*. Informally, free abelian groups or formal sums may also be seen as signed multisets with elements in B.

Free abelian groups have very nice properties which make them similar to vector spaces and allow a general abelian group to be understood as a quotient of a free abelian group by "relations". Every free abelian group has a rank defined as the cardinality of a basis. The rank determines the group up to isomorphism, and the elements of such a group can be written as finite formal sums of the basis elements. Every subgroup of a free abelian group is itself free abelian, which is important for the description of a general abelian group as a cokernel of a homomorphism between free abelian groups.

Example

For example, let G be the group that is the direct sum $\mathbb{Z} \oplus \mathbb{Z}$ of two copies of the infinite cyclic group $\mathbb{Z}$. Symbolically,

$$G = \{(a, b) | a, b \in \mathbb{Z}\} .$$

One basis for this group is {(1,0),(0,1)}. If we say $e_1 = (1, 0)$ and $e_2 = (0, 1)$, then we can write the element (4,3) as

$(4, 3) = 4e_1 + 3e_2$. Where 'multiplication' is defined in following way: $4e_1 := e_1 + e_1 + e_1 + e_1$.

In this basis, there is no other way to write (4,3), but if we choose our basis to be {(1,0),(1,1)}, where $f_1 = (1, 0)$ and $f_2 = (1, 1)$, then we can write (4,3) as

$$(4, 3) = f_1 + 3f_2.$$

Unlike vector spaces, not all abelian groups have a basis, hence the special name for those that do. (For instance, any group having periodic elements is not a free abelian group because any element can be expressed in an infinite number of ways simply by putting in an arbitrary number of cycles constructed from a periodic element.) The trivial abelian group {0} is also considered to be free abelian, with basis the empty set.

Terminology

Note that a *free abelian* group is *not* a free group except in two cases: a free abelian group having an empty basis (rank 0, giving the trivial group) or having just 1 element in the basis (rank 1, giving the infinite cyclic group). Other abelian groups are not free groups because in free groups ab must be different from ba if a and b are different elements of the basis, while in free abelian groups they must be identical.

Properties

1. For every set B, there exists a free abelian group with basis B, and all such free abelian groups having B as basis are isomorphic. One example may be constructed as the abelian group of functions on B, where each function may take integer values, and all but finitely many of its values are zero. This is the direct sum of copies of $\mathbb{Z}$, one copy for each element of B.
2. If F is a free abelian group with basis B, then we have the following universal property: for every arbitrary function f from B to some abelian group A, there exists a unique group homomorphism from F to A which extends f. This universal property can also be used to define free abelian groups.
3. Given any abelian group A, there always exists a free abelian group F and a surjective group homomorphism from F to A. This follows from the universal property mentioned above.
4. All free abelian groups are torsion-free, and all finitely generated torsion-free abelian groups are free abelian. (The same applies to flatness, since an abelian group is torsion-free if and only if it is flat.) The additive group of rational numbers **Q** is a (not finitely generated) torsion-free group that's not free abelian. The reason: **Q** is divisible but non-zero free abelian groups are never divisible.
5. Free abelian groups are a special case of free modules, as abelian groups are nothing but modules over the ring $\mathbb{Z}$.

Importantly, every subgroup of a free abelian group is free abelian (see below). As a consequence, to every abelian group A there exists a short exact sequence

$$0 \to G \to F \to A \to 0$$

with F and G being free abelian (which means that A is isomorphic to the factor group F/G). This is called a **free resolution** of A. Furthermore, the free abelian groups are precisely the projective objects in the category of abelian groups.[1]

It can be surprisingly difficult to determine whether a concretely given group is free abelian. Consider for instance the Baer–Specker group $\mathbb{Z}^{\mathbb{N}}$, the direct product (not to be confused with the direct sum, which differs from the direct product on an infinite number of summands) of countably many copies of $\mathbb{Z}$. Reinhold Baer proved in 1937 that this group is *not* free abelian; Specker proved in 1950 that every countable subgroup of $\mathbb{Z}^{\mathbb{N}}$ is free abelian.

Rank

Every finitely generated free abelian group is isomorphic to $\mathbb{Z}^n$ for some natural number n called the **rank** of the free abelian group. In general, a free abelian group F has many different bases, but all bases have the same cardinality, and this cardinality is called the rank of F. This rank of free abelian groups can be used to define the rank of all other abelian groups: see rank of an abelian group. The relationships between different bases can be interesting; for example, the different possibilities for choosing a basis for the free abelian group of rank two is reviewed in the article on the fundamental pair of periods.

Formal sum

A **formal sum** of elements of a given set *B* is an element of the free abelian group with basis *B*. In other words, given a set *B*, let *G* be the unique (up to isomorphism) free abelian group with basis *B*. For elements $b_1, b_2, \ldots \in B$ and $a_1, a_2, \ldots \in \mathbb{Z}$ (where there may be an $n \in \mathbb{Z}$ such that $a_i = 0$ iff $i \geq n$),

$$\sum_{i=1}^{\infty} a_i b_i \in G$$

Subgroup closure

Every subgroup of a free abelian group is itself a free abelian group. This is similar to the Nielsen–Schreier theorem that a subgroup of a free group is free.[2]

Theorem: Let F be a free abelian group generated by the set $X = \{x_k \mid k \in I\}$ and let $G \subset F$ be a subgroup. Then G is a free abelian group.

Proof:[3] If $G = \{0\}$, the statement holds, so we can assume that G is nontrivial. First we shall prove this for finite X by induction. When $|X| = 1$, G is isomorphic to $\mathbb{Z}$ (being nontrivial) and clearly free. Assume that if a group is generated by a set of size $\leq k$, then every subgroup of it is free. Let $X = \{x_1, x_2, \ldots, x_k, x_{k+1}\}$, F the free group generated by X and $G \subset F$ a subgroup. Let $\mathrm{pr}\colon G \to F$ be the projection $\mathrm{pr}(a_1 x_1 + \cdots + a_{k+1} x_{k+1}) = a_1 x_1$. If $\mathrm{Rng}(\mathrm{pr}) = \{0\}$, then G is a subset of $\langle x_2, \ldots, x_{k+1} \rangle$ and free by the induction hypothesis. Thus we can assume that the range is nontrivial. Let $m > 0$ be the least such that $mx_1 \in \mathrm{Rng}(\mathrm{pr})$ and choose some x such that $\mathrm{pr}x = mx_1$. It is standard to verify that $x \notin \mathrm{Ker}(\mathrm{pr})$ and if $y \in G$, then $y = nx + k$, where $k \in \mathrm{Ker}(\mathrm{pr})$ and $n \in \mathbb{Z}$. Hence $G = \mathrm{Ker}(\mathrm{pr}) \oplus \langle x \rangle$. By the induction hypothesis $\mathrm{Ker}(\mathrm{pr})$ and $\langle x \rangle$ are free: first is isomorphic to a subgroup of $\langle x_2, \ldots x_{k+1} \rangle$ and the second to $\mathbb{Z}$.

Assume now that $X = \{x_i \mid i \in I\}$ is arbitrary. For each subset J of I let F_J be the free group generated by $\{x_i \mid i \in J\}$, thus $F_J \subset F$ is a free subgroup and denote $G_J = F_J \cap G$.

Now set

$$S = \{(G_J, w) \mid G_J \text{ is a nontrivial free group and } w \text{ is a basis of } G_J\}.$$

Formally w is an injective (one-to-one) map

$$w : J' \to G_J$$

such that $w[J']$ generates G_J .

Clearly S is nonempty: Let us have an element x in G . Then $x = a_1 x_{i_1} + \cdots + a_n x_{i_n}$ and thus the free group generated by $J = \{x_{i_1}, \ldots, x_{i_n}\}$ contains x and the intersection $G \cap F_J$ is a nontrivial subgroup of a finitely generated free abelian group and thus free by the induction above.

If $(G_J, w), (G_K, u) \in S$, define order $(G_J, w) \leq (G_K, u)$ if and only if $J \subset K$ and the basis u is an extension of w ; formally if $w : J' \to G_J$ and $u : K' \to G_K$, then $J' \subset K'$ and $u \restriction w = w$.

If $(G_{J_r}, w_r)_{r \in L}$ is a $\leq$ -chain (L is some linear order) of elements of S , then obviously

$$\left(\bigcup_{r \in L} G_{J_r}, \bigcup_{r \in L} w_r\right) \in S,$$

so we can apply Zorn's lemma and conclude that there exists a maximal (G_J, w). Since $G_I = G$, it is enough to prove now that $J = I$. Assume on contrary that there is $k \in I \setminus J$.

Put $K = J \cup \{k\}$. If $G_K = F_K \cap G = G_J$, then it means that $(G_J, w) \leq (G_K, w)$, but they are not equal, so (G_K, w) is bigger, which contradicts maximality of (G_J, w). Otherwise there is an element $nx_k + y \in G_K$ such that $n \in \mathbb{Z} \setminus \{0\}$ and $y \in F_J$.

The set of $n \in \mathbb{Z}$ for which there exists $y \in F_J$ such that $nx_k + y \in G_K$ forms a subgroup of $\mathbb{Z}$. Let n_0 be a generator of this group and let $w_k = n_0 x_k + y \in G_K$ with $y \in F_J$. Now if $z \in G_K$, then for some $m \in Z$, $z = z - mw_k + mw_k$, where $z - mw_k \in G_J$.
On the other hand clearly $w_k\mathbb{Z} \cap F_J = \{0\}$, so $w' = w \cup \{w_k\}$ is a basis of G_K, so $(G_K, w') \geq (G_J, w)$ contradicting the maximality again. □

Notes

[1] Griffith, p.18

[2] According to Johnson, this result is due to Richard Dedekind. Johnson, D. L. (1980). *Topics in the Theory of Group Presentations*. London Mathematical Society lecture note series. **42**. Cambridge University Press. p. 9. ISBN 9780521231084.

[3] This proof is an application of Zorn's lemma and can be found in Appendix 2 §2, page 880 of Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR1878556.

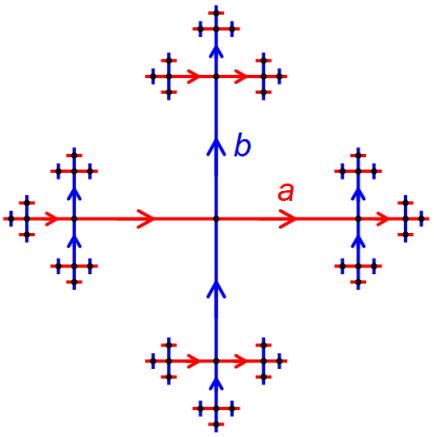
References

- Phillip A. Griffith (1970). *Infinite Abelian group theory*. Chicago Lectures in Mathematics. University of Chicago Press. ISBN 0-226-30870-7.

Free group

In mathematics, a group *G* is called **free** if there is a subset *S* of *G* such that any element of *G* can be written in one and only one way as a product of finitely many elements of *S* and their inverses (disregarding trivial variations such as $st^{-1} = su^{-1}ut^{-1}$). Apart from the existence of inverses no other relation exists between the generators of a free group.

A related but different notion is a free abelian group.



The Cayley graph for the free group on two generators. Each vertex represents an element of the free group, and each edge represents multiplication by *a* or *b*.

History

Free groups first arose in the study of hyperbolic geometry, as examples of Fuchsian groups (discrete groups acting by isometries on the hyperbolic plane). In an 1882 paper, Walther von Dyck pointed out that these groups have the simplest possible presentations.[1] The algebraic study of free groups was initiated by Jakob Nielsen in 1924, who gave them their name and established many of their basic properties.[2][3][4] Max Dehn realized the connection with topology, and obtained the first proof of the full Nielsen–Schreier theorem.[5] Otto Schreier published an algebraic proof of this result in 1927,[6] and Kurt Reidemeister included a comprehensive treatment of free groups in his 1932 book on combinatorial topology.[7] Later on in the 1930s, Wilhelm Magnus discovered the connection between the lower central series of free groups and free Lie algebras.

Examples

The group (**Z**,+) of integers is free; we can take $S = \{1\}$. A free group on a two-element set S occurs in the proof of the Banach–Tarski paradox and is described there.

On the other hand, any nontrivial finite group cannot be free, since the elements of a free generating set of a free group have infinite order.

In algebraic topology, the fundamental group of a bouquet of k circles (a set of k loops having only one point in common) is the free group on a set of k elements.

Construction

The **free group** F_S with **free generating set** S can be constructed as follows. S is a set of symbols and we suppose for every s in S there is a corresponding "inverse" symbol, s^{-1}, in a set S^{-1}. Let $T = S \cup S^{-1}$, and define a **word** in S to be any written product of elements of T. That is, a word in S is an element of the monoid generated by T. The empty word is the word with no symbols at all. For example, if $S = \{a, b, c\}$, then $T = \{a, a^{-1}, b, b^{-1}, c, c^{-1}\}$, and

$$abc^{-1}ca^{-1}c$$

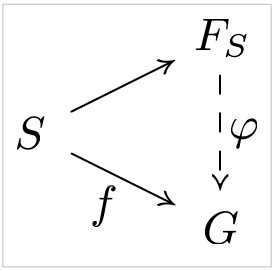
is a word in S. If an element of S lies immediately next to its inverse, the word may be simplified by omitting the s, s^{-1} pair:

$$abc^{-1}ca^{-1}c \quad \longrightarrow \quad ab\,a^{-1}c.$$

A word that cannot be simplified further is called **reduced**. The free group F_S is defined to be the group of all reduced words in S. The group operation in F_S is concatenation of words (followed by reduction if necessary). The identity is the empty word. A word is called **cyclically reduced**, if its first and last letter are not inverse to each other. Every word is conjugate to a cyclically reduced word, and the cyclically reduced conjugates of a cyclically reduced word are all cyclic permutations. For instance $b^{-1}abcb$ is not cyclically reduced, but is conjugate to abc, which is cyclically reduced. The only cyclically reduced conjugates of abc are abc, bca, and cab.

Universal property

The free group F_S is the universal group generated by the set S. This can be formalized by the following universal property: given any function f from S to a group G, there exists a unique homomorphism $\varphi: F_S \to G$ making the following diagram commute:



That is, homomorphisms $F_S \to G$ are in one-to-one correspondence with functions $S \to G$. For a non-free group, the presence of relations would restrict the possible images of the generators under a homomorphism.

To see how this relates to the constructive definition, think of the mapping from S to F_S as sending each symbol to a word consisting of that symbol. To construct φ for given f, first note that φ sends the empty word to identity of G and it has to agree with f on the elements of S. For the remaining words (consisting of more than one symbol) φ can be uniquely extended since it is a homomorphism, i.e., $\varphi(ab) = \varphi(a)\,\varphi(b)$.

The above property characterizes free groups up to isomorphism, and is sometimes used as an alternative definition. It is known as the universal property of free groups, and the generating set S is called a **basis** for F_S. The basis for a free group is not uniquely determined.

Being characterized by a universal property is the standard feature of free objects in universal algebra. In the language of category theory, the construction of the free group (similar to most constructions of free objects) is a functor from the category of sets to the category of groups. This functor is left adjoint to the forgetful functor from groups to sets.

Facts and theorems

Some properties of free groups follow readily from the definition:

1. Any group G is the homomorphic image of some free group F(S). Let S be a set of *generators* of G. The natural map f: F(S) → G is an epimorphism, which proves the claim. Equivalently, G is isomorphic to a quotient group of some free group F(S). The kernel of f is a set of *relations* in the presentation of G. If S can be chosen to be finite here, then G is called **finitely generated**.
2. If S has more than one element, then F(S) is not abelian, and in fact the center of F(S) is trivial (that is, consists only of the identity element).
3. Two free groups F(S) and F(T) are isomorphic if and only if S and T have the same cardinality. This cardinality is called the **rank** of the free group F. Thus for every cardinal number k, there is, up to isomorphism, exactly one free group of rank k.
4. A free group of finite rank $n > 1$ has an exponential growth rate of order $2n - 1$.

A few other related results are:

1. The Nielsen–Schreier theorem: Any subgroup of a free group is free.
2. A free group of rank k clearly has subgroups of every rank less than k. Less obviously, a (*nonabelian!*) free group of rank at least 2 has subgroups of all countable ranks.
3. The commutator subgroup of a free group of rank $k > 1$ has infinite rank; for example for F(a,b), it is freely generated by the commutators $[a^m, b^n]$ for non-zero m and n.
4. The free group in two elements is SQ universal; the above follows as any SQ universal group has subgroups of all countable ranks.
5. Any group that acts on a tree, freely and preserving the orientation, is a free group of countable rank (given by 1 plus the Euler characteristic of the quotient graph).
6. The Cayley graph of a free group of finite rank, with respect to a free generating set, is a tree on which the group acts freely, preserving the orientation.
7. The groupoid approach to these results, given in the work by P.J. Higgins below, is kind of extracted from an approach using covering spaces. It allows more powerful results, for example on Grushko's theorem, and a normal form for the fundamental groupoid of a graph of groups. In this approach there is considerable use of free groupoids on a directed graph.
8. Grushko's theorem has the consequence that if a subset B of a free group F on n elements generates F and has n elements, then B generates F freely.

Free abelian group

Further information: free abelian group

The free abelian group on a set S is defined via its universal property in the analogous way, with obvious modifications: Consider a pair (F, φ), where F is an abelian group and φ: $S \to F$ is a function. F is said to be the **free abelian group on S with respect to φ** if for any abelian group G and any function ψ: $S \to G$, there exists a unique homomorphism f: $F \to G$ such that

$$f(\varphi(s)) = \psi(s), \text{ for all } s \text{ in } S.$$

The free abelian group on S can be explicitly identified as the free group F(S) modulo the subgroup generated by its commutators, [F(S), F(S)], i.e. its abelianisation. In other words, the free abelian group on S is the set of words that

are distinguished only up to the order of letters. The rank of a free group can therefore also be defined as the rank of its abelianisation as a free abelian group.

Tarski's problems

Around 1945, Alfred Tarski asked whether the free groups on two or more generators have the same first order theory, and whether this theory is decidable. Sela (2006) answered the first question by showing that any two nonabelian free groups have the same first order theory, and Kharlampovich & Myasnikov (2006) answered both questions, showing that this theory is decidable.

A similar unsolved (in 2011) question in free probability theory asks whether the von Neumann group algebras of any two non-abelian finitely generated free groups are isomorphic.

Notes

[1] von Dyck, Walther (1882). "Gruppentheoretische Studien" (http://www.springerlink.com/content/t8lx644qm87p3731). *Mathematische Annalen* **20** (1): 1–44. doi:10.1007/BF01443322. .

[2] Nielsen, Jakob (1917). "Die Isomorphismen der allgemeinen unendlichen Gruppe mit zwei Erzeugenden" (http://www.springerlink.com/content/xp12702q30q40381). *Mathematische Annalen* **78** (1): 385–397. doi:10.1007/BF01457113. JFM 46.0175.01. MR1511907. .

[3] Nielsen, Jakob (1921). "On calculation with noncommutative factors and its application to group theory. (Translated from Danish)". *The Mathematical Scientist* **6 (1981)** (2): 73–85.

[4] Nielsen, Jakob (1924). "Die Isomorphismengruppe der freien Gruppen" (http://www.springerlink.com/content/l898u32j37u10671). *Mathematische Annalen* **91** (3): 169–209. doi:10.1007/BF01556078. .

[5] See Magnus, Wilhelm; Moufang, Ruth (1954). "Max Dehn zum Gedächtnis" (http://www.springerlink.com/content/l657774u3w864mp3). *Mathematische Annalen* **127** (1): 215–227. doi:10.1007/BF01361121. ..

[6] Schreier, Otto (1928). "Die Untergruppen der freien Gruppen". *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* **5**: 161–183. doi:10.1007/BF02952517.

[7] Reidemeister, Kurt (1972 (1932 original)). *Einführung in die kombinatorische Topologie*. Darmstadt: Wissenschaftliche Buchgesellschaft.

References

- Kharlampovich, Olga; Myasnikov, Alexei (2006). "Elementary theory of free non-abelian groups". *J. Algebra* **302** (2): 451–552. doi:10.1016/j.jalgebra.2006.03.033. MR2293770
- W. Magnus, A. Karrass and D. Solitar, "Combinatorial Group Theory", Dover (1976).
- P.J. Higgins, 1971, "Categories and Groupoids", van Nostrand, {New York}. Reprints in Theory and Applications of Categories, 7 (2005) pp 1–195.
- Sela, Z. (2006). "Diophantine geometry over groups. VI. The elementary theory of a free group.". *Geom. Funct. Anal. 16* (3): 707–730. MR2238945
- J.-P. Serre, *Trees*, Springer (2003) (English translation of "arbres, amalgames, SL_2", 3rd edition, *astérisque* **46** (1983))
- P.J. Higgins, "The fundamental groupoid of a graph of groups", J. London Math. Soc. (2) {13}, (1976) 145–149.
- Aluffi, Paolo (2009). *Algebra: Chapter 0* (http://books.google.com/books?id=deWkZWYbyHQC&pg=PA70). AMS Bookstore. p. 70. ISBN 978-0-821-84781-7.
- Grillet, Pierre (2007). *Abstract algebra* (http://books.google.com/books?id=LJtyhu8-xYwC&pg=PA27). Springer. p. 27. ISBN 978-0-387-71567-4.

Free product

In mathematics, specifically group theory, the **free product** is an operation that takes two groups G and H and constructs a new group $G * H$. The result contains both G and H as subgroups, is generated by the elements of these subgroups, and is the "most general" group having these properties. Unless one of the groups G and H is trivial, the free product is always infinite. The construction of a free product is similar in spirit to the construction of a free group (the most general group that can be made from a given set of generators).

The free product is the coproduct in the category of groups. That is, the free product plays the same role in group theory that disjoint union plays in set theory, or that the direct sum plays in module theory.

The free product is important in algebraic topology because of van Kampen's theorem, which states that the fundamental group of the union of two path-connected topological spaces is always an **amalgamated free product** of the fundamental groups of the spaces. In particular, the fundamental group of the wedge sum of two spaces (i.e. the space obtained by joining two spaces together at a single point) is simply the free product of the fundamental groups of the spaces.

Free products are also important in Bass–Serre theory, the study of groups acting by automorphisms on trees. Specifically, any group acting with finite vertex stabilizers on a tree may be constructed from finite groups using amalgamated free products and HNN extensions. Using the action of the modular group on a certain tessellation of the hyperbolic plane, it follows from this theory that the modular group is isomorphic to the free product of cyclic groups of orders 4 and 6 amalgamated over a cyclic group of order 2.

Construction

If G and H are groups, a **word** in G and H is a product of the form

$$s_1 s_2 \cdots s_n,$$

where each s_i is either an element of G or an element of H. Such a word may be **reduced** using the following operations:

- Remove an instance of the identity element (of either G or H).
- Replace a pair of the form $g_1 g_2$ by its product in G, or a pair $h_1 h_2$ by its product in H.

Every reduced word is an alternating product of elements of G and elements of H, e.g.

$$g_1 h_1 g_2 h_2 \cdots g_k h_k.$$

The **free product** $G * H$ is the group whose elements are the reduced words in G and H, under the operation of concatenation followed by reduction.

For example, if G is the infinite cyclic group $\langle x \rangle$, and H is the infinite cyclic group $\langle y \rangle$, then every element of $G * H$ is an alternating product of powers of x with powers of y. In this case, $G * H$ is isomorphic to the free group generated by x and y.

Presentation

Suppose that

$$G = \langle R_G \mid S_G \rangle$$

is a presentation for G (where R_G is a set of generators and S_G is a set of relations), and suppose that

$$H = \langle R_H \mid S_H \rangle$$

is a presentation for H. Then

$G * H = \langle R_G \cup R_H \mid S_G \cup S_H \rangle$. That is, $G * H$ is generated by the generators for G together with the generators for H, with relations consisting of the relations from G together with the relations from H (assume here no notational clashes so that these are in fact disjoint unions).

For example, suppose that G is a cyclic group of order 4,

$$G = \langle x \mid x^4 = 1 \rangle,$$

and H is a cyclic group of order 5

$$H = \langle y \mid y^5 = 1 \rangle.$$

Then $G * H$ is the infinite group

$$G * H = \langle x, y \mid x^4 = y^5 = 1 \rangle.$$

Because there are no relations in a free group, the free product of free groups is always a free group. In particular,

$$F_m * F_n \cong F_{m+n},$$

where F_n denotes the free group on n generators.

Generalization: Free product with amalgamation

The more general construction of **free product with amalgamation** is correspondingly a pushout in the same category. Suppose G and H are given as before, along with group homomorphisms

$$\varphi : F \to G \text{ and } \psi : F \to H.$$

where F is some arbitrary group. Start with the free product $G * H$ and adjoin as relations

$$\varphi(f)\psi(f)^{-1} = 1$$

for every f in F. In other words take the smallest normal subgroup N of $G * H$ containing all elements on the left-hand side of the above equation, which are tacitly being considered in $G * H$ by means of the inclusions of G and H in their free product. The free product with amalgamation of G and H, with respect to φ and ψ, is the quotient group

$$(G * H)/N.$$

The amalgamation has forced an identification between $\varphi(F)$ in G with $\psi(F)$ in H, element by element. This is the construction needed to compute the fundamental group of two connected spaces joined along a connected subspace, with F taking the role of the fundamental group of the subspace. See: Seifert–van Kampen theorem.

Free products with amalgamation and a closely related notion of HNN extension are basic building blocks in Bass–Serre theory of groups acting on trees.

In other branches

One may similarly define free products of other algebraic structures than groups, including algebras over a field. Free products of algebras of random variables play the same role in defining "freeness" in the theory of free probability that Cartesian products play in defining statistical independence in classical probability theory.

References

- Free product [1] on PlanetMath
- Free product with amalgamated subgroup [2] on PlanetMath

Notes

[1] http://planetmath.org/?op=getobj&from=objects&id=6574
[2] http://planetmath.org/?op=getobj&from=objects&id=3944

Generating set of a group

In abstract algebra, a **generating set of a group** is a subset that is not contained in any proper subgroup of the group. Equivalently, a generating set of a group is a subset such that every element of the group can be expressed as the combination (under the group operation) of finitely many elements of the subset and their inverses.

More generally, if S is a subset of a group G, then $\langle S \rangle$, the **subgroup generated by S**, is the smallest subgroup of G containing every element of S, meaning the intersection over all subgroups containing the elements of S; equivalently, <S> is the subgroup of all elements of G that can be expressed as the finite product of elements in S and their inverses.

If $G = \langle S \rangle$, then we say S **generates** G; and the elements in S are called **generators** or **group generators**. If S is the empty set, then $\langle S \rangle$ is the trivial group $\{e\}$, since we consider the empty product to be the identity.

When there is only a single element x in S, $\langle S \rangle$ is usually written as $\langle x \rangle$. In this case, $\langle x \rangle$ is the **cyclic subgroup** of the powers of x, a cyclic group, and we say this group is generated by x. Equivalent to saying an element x generates a group is saying that $\langle x \rangle$ equals the entire group G. For finite groups, it is also equivalent to saying that x has order |G|.

Finitely generated group

If S is finite, then a group $G = \langle S \rangle$ is called **finitely generated**. The structure of finitely generated abelian groups in particular is easily described. Many theorems that are true for finitely generated groups fail for groups in general. It has been proven that if a finite group is generated by a subset S, then each group element may be expressed as a word from the alphabet S of length less than or equal to the order of the group.

Every finite group is finitely generated since $\langle G \rangle = G$. The integers under addition are an example of an infinite group which is finitely generated by both 1 and −1, but the group of rationals under addition cannot be finitely generated. No uncountable group can be finitely generated.

Different subsets of the same group can be generating subsets; for example, if p and q are integers with $\gcd(p, q) = 1$, then $\{p, q\}$ also generates the group of integers under addition (by Bézout's identity).

While it is true that every quotient of a finitely generated group is finitely generated (simply take the images of the generators in the quotient), a subgroup of a finitely generated group need not be finitely generated. For example, let G be the free group in two generators, x and y (which is clearly finitely generated, since $G = \langle \{x,y\} \rangle$), and let S be the subset consisting of all elements of G of the form $y^n x y^{-n}$, for n a natural number. Since $\langle S \rangle$ is clearly isomorphic

to the free group in countable generators, it cannot be finitely generated. However, every subgroup of a finitely generated abelian group is in itself finitely generated. Rather more can be said about this though: the class of all finitely generated groups is closed under extensions. To see this, take a generating set for the (finitely generated) normal subgroup and quotient: then the generators for the normal subgroup, together with preimages of the generators for the quotient, generate the group.

Free group

The most general group generated by a set *S* is the group **freely generated** by *S*. Every group generated by S is isomorphic to a quotient of this group, a feature which is utilized in the expression of a group's presentation.

Frattini subgroup

An interesting companion topic is that of **non-generators**. An element *x* of the group *G* is a non-generator if every set *S* containing *x* that generates *G*, still generates *G* when *x* is removed from *S*. In the integers with addition, the only non-generator is 0. The set of all non-generators forms a subgroup of *G*, the Frattini subgroup.

Examples

The group of units $U(\mathbf{Z}_9)$ is the group of all integers relatively prime to 9 under multiplication mod 9 ($U_9 = \{1, 2, 4, 5, 7, 8\}$). All arithmetic here is done modulo 9. Seven is not a generator of $U(\mathbf{Z}_9)$, since

$$\{7^i \pmod 9 \mid i \in \mathbb{N}\} = \{7, 4, 1\}.$$

while 2 is, since:

$$\{2^i \pmod 9 \mid i \in \mathbb{N}\} = \{2, 4, 8, 7, 5, 1\}.$$

On the other hand, for $n > 2$ the symmetric group of degree n is not cyclic, so it is not generated by any one element. However, it is generated by the two permutations (1 2) and (1 2 3 ... *n*). For example, for S_3 we have:

$e = (1\ 2)(1\ 2)$

$(1\ 2) = (1\ 2)$

$(1\ 3) = (1\ 2)(1\ 2\ 3)$

$(2\ 3) = (1\ 2\ 3)(1\ 2)$

$(1\ 2\ 3) = (1\ 2\ 3)$

$(1\ 3\ 2) = (1\ 2)(1\ 2\ 3)(1\ 2)$

Infinite groups can also have finite generating sets. The additive group of integers has 1 as a generating set. The element 2 is not a generating set, as the odd numbers will be missing. The two-element subset {3, 5} is a generating set, since (−5) + 3 + 3 = 1 (in fact, any pair of coprime numbers is, as a consequence of Bézout's identity).

References

- Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR1878556

External links

- Mathworld: Group generators [1]

References

[1] http://mathworld.wolfram.com/GroupGenerators.html

Group cohomology

In abstract algebra, homological algebra, algebraic topology and algebraic number theory, as well as in applications to group theory proper, **group cohomology** is a way to study groups using a sequence of functors H^n. The study of fixed points of groups acting on modules and quotient modules is a motivation, but the cohomology can be defined using various constructions. There is a dual theory, group homology, and a generalization to non-abelian coefficients.

These algebraic ideas are closely related to topological ideas. Thus, the group cohomology of a group G can be thought of as, and is motivated by, the singular cohomology of a suitable space having G as its fundamental group, namely the corresponding Eilenberg-MacLane space. Thus, the group cohomology of $\mathbb{Z}$ can be thought of as the singular cohomology of the circle S^1, and similarly for $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{RP}^\infty$.

A great deal is known about the cohomology of groups, including interpretations of low dimensional cohomology, functorality, and how to change groups. The subject of group cohomology began in the 1920s, matured in the late 1940s, and continues as an area of active research today.

Motivation

A general paradigm in group theory is that a group G should be studied via its group representations. A slight generalization of those representations are the G-modules: a G-module is an abelian group M together with a group action of G on M, with every element of G acting as an endomorphism of M. In the sequel we will write G multiplicatively and M additively.

Given such a G-module M, it is natural to consider the subgroup of G-invariant elements:

$$M^G = \{x \in M \mid \forall g \in G : \ gx = x\}.$$

Now, if N is a submodule of M (i.e. a subgroup of M mapped to itself by the action of G), it isn't in general true that the invariants in M/N are found as the quotient of the invariants in M by those in N: being invariant 'modulo N' is broader. The first group cohomology $H^1(G,N)$ precisely measures the difference. The group cohomology functors H^* in general measure the extent to which taking invariants doesn't respect exact sequences. This is expressed by a long exact sequence.

Formal constructions

In this article, G is a finite group. The collection of all G-modules is a category (the morphisms are group homomorphisms f with the property $f(gx) = g(f(x))$ for all g in G and x in M). This category of G-modules is an abelian category with enough injectives (since it is isomorphic to the category of all modules over the group ring $\mathbb{Z}[G]$).

Sending each module M to the group of invariants M^G yields a functor from this category to the category $\mathfrak{Ab}$ of abelian groups. This functor is left exact but not necessarily right exact. We may therefore form its right derived functors; their values are abelian groups and they are denoted by $H^n(G,M)$, "the n-th cohomology group of G with coefficients in M". $H^0(G,M)$ is identified with M^G.

Long exact sequence of cohomology

In practice, one often computes the cohomology groups using the following fact: if

$$0 \to L \to M \to N \to 0$$

is a short exact sequence of G-modules, then a long exact sequence

$$0 \to L^G \to M^G \to N^G \xrightarrow{\delta^0} H^1(G,L) \to H^1(G,M) \to H^1(G,N) \xrightarrow{\delta^1} H^2(G,L) \to \cdots$$

is induced. The maps δ^n are called the "connecting homomorphisms" and can be obtained from the snake lemma.[1]

Cochain complexes

Rather than using the machinery of derived functors, the cohomology groups can also be defined more concretely, as follows.[2] For $n \geq 0$, let $C^n(G, M)$ be the group of all functions from G^n to M. This is an abelian group; its elements are called the (inhomogeneous) ***n*-cochains**. The **coboundary homomorphisms**

$$d^n : C^n(G,M) \to C^{n+1}(G,M)$$

are defined as

$$\begin{aligned}(d^n\varphi)(g_1,\ldots,g_{n+1}) &= g_1 \cdot \varphi(g_2,\ldots,g_{n+1}) \\ &+ \sum_{i=1}^{n}(-1)^i \varphi(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_{n+1}) \\ &+ (-1)^{n+1}\varphi(g_1,\ldots,g_n)\end{aligned}$$

The crucial thing to check here is

$$d^{n+1} \circ d^n = 0$$

thus we have a cochain complex and we can compute cohomology. For $n \geq 0$, define the group of ***n*-cocycles** as:

$$Z^n(G,M) = \ker(d^n)$$

and the group of ***n*-coboundaries** as

$$\begin{cases} B^0(G,M) = 0 \\ B^n(G,M) = \operatorname{im}(d^{n-1}),\ n \geq 1 \end{cases}$$

and

$$H^n(G,M) = Z^n(G,M)/B^n(G,M).$$

The functors Ext^n and formal definition of group cohomology

Yet another approach is to treat G-modules as modules over the group ring $\mathbb{Z}[G]$, which allows one to define group cohomology via Ext functors:

$$H^n(G, M) = \operatorname{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M),$$

where M is a $\mathbb{Z}[G]$-module.

Here $\mathbb{Z}$ is treated as the trivial G-module: every element of G acts as the identity. These Ext groups can also be computed via a projective resolution of $\mathbb{Z}$, the advantage being that such a resolution only depends on G and not on M. We recall the definition of Ext more explicitly for this context. Let F be a projective $\mathbb{Z}[G]$-resolution (e.g. a free $\mathbb{Z}[G]$-resolution) of the trivial $\mathbb{Z}[G]$-module $\mathbb{Z}$:

$$\cdots \to F_n \to F_{n-1} \to \cdots \to F_0 \to \mathbb{Z}.$$

e.g., one may always take the resolution of group rings, $F_n = \mathbb{Z}[G^{n+1}]$, with morphisms

$$f_n : \mathbb{Z}[G^{n+1}] \to \mathbb{Z}[G^n], \quad (g_0, g_1, \ldots, g_n) \mapsto \sum_{i=0}^{n} (-1)^i (g_0, \ldots, \widehat{g_i}, \ldots, g_n).$$

Recall that for $\mathbb{Z}[G]$-modules N and M, $Hom_G(N, M)$ is an abelian group consisting of $\mathbb{Z}[G]$-homomorphisms from N to M. Since $Hom_G(–, M)$ is a contravariant functor and reverses the arrows, applying $Hom_G(–, M)$ to F termwise produces a cochain complex $Hom_G(F, M)$:

$$... \leftarrow \operatorname{Hom}_G(F_n, M) \leftarrow \operatorname{Hom}_G(F_{n-1}, M) \leftarrow \cdots \leftarrow \operatorname{Hom}_G(F_0, M) \leftarrow \operatorname{Hom}_G(\mathbb{Z}, M).$$

The cohomology groups $H^*(G,M)$ of G with coefficients in M are defined as the cohomology of the above cochain complex:

$H^n(G,M)=H^n(Hom_G(F, M))$

for $n \geq 0$.

Group homology

Dually to the construction of group cohomology there is the following definition of **group homology**: given a G-module M, set DM to be the submodule generated by elements of the form $g \cdot m - m$, $g \in G$, $m \in M$. Assigning to M its so-called *coinvariants*, the quotient

$$M_G := M/DM,$$

is a right exact functor. Its left derived functors are by definition the group homology

$$H_n(G, M).$$

Note that the superscript/subscript convention for cohomology/homology agrees with the convention for group invariants/coinvariants, while which is denoted "co-" switches:

- superscripts correspond to cohomology H^* and invariants X^G, while
- subscripts correspond to homology H_* and coinvariants $X_G := X/G$.

The covariant functor which assigns M_G to M is isomorphic to the functor which sends M to $\mathbb{Z} \otimes_{\mathbb{Z}[G]} M$, where $\mathbb{Z}$ is endowed with the trivial G-action. Hence one also gets an expression for group homology in terms of the Tor functors,

$$H_n(G, M) = \operatorname{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

Recall that the tensor product $N \otimes_{\mathbb{Z}[G]} M$ is defined whenever N is a right $\mathbb{Z}[G]$-module and M is a left $\mathbb{Z}[G]$-module. If N is a left $\mathbb{Z}[G]$-module, we turn it into a right $\mathbb{Z}[G]$-module by setting $a\ g = g^{-1}\ a$ for every $g \in G$ and every $a \in N$. This convention allows to define the tensor product $N \otimes_{\mathbb{Z}[G]} M$ in the case where both M and N are left $\mathbb{Z}[G]$-modules.

Specifically, the homology groups $H_n(G, M)$ can be computed as follows. Start with a projective resolution F of the trivial $\mathbb{Z}[G]$-module $\mathbb{Z}$, as in the previous section. Apply the covariant functor $\otimes_{\mathbb{Z}[G]} M$ to F termwise to get a chain complex $F \otimes_{\mathbb{Z}[G]} M$:

$$\cdots \to F_n \otimes_{\mathbb{Z}[G]} M \to F_{n-1} \otimes_{\mathbb{Z}[G]} M \to \cdots \to F_0 \otimes_{\mathbb{Z}[G]} M \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} M.$$

Then $H_n(G, M)$ are the homology groups of this chain complex, $H_n(G, M) = H_n(F \otimes_{\mathbb{Z}[G]} M)$ for $n \geq 0$.
Group homology and cohomology can be treated uniformly for some groups, especially finite groups, in terms of complete resolutions and the Tate cohomology groups.

Functorial maps in terms of cochains

Connecting homomorphisms

For a short exact sequence $0 \to L \to M \to N \to 0$, the connecting homomorphisms $\delta^n : H^n(G, N) \to H^{n+1}(G, L)$ can be described in terms of inhomogeneous cochains as follows.[3] If c is an element of $H^n(G, N)$ represented by an n-cocycle $\varphi : G^n \to N$, then $\delta^n(c)$ is represented by $d^n(\psi)$, where ψ is an n-cochain $G^n \to M$ "lifting" φ (i.e. such that φ is the composition of ψ with the surjective map $M \to N$).

Non-abelian group cohomology

Using the G-invariants and the 1-cochains, one can construct the zeroth and first group cohomology for a group G with coefficients in a non-abelian group. Specifically, a G-group is a (not necessarily abelian) group A together with an action by G.

The *zeroth cohomology of G with coefficients in* A *is defined to be the subgroup*

$$H^0(G, A) = A^G,$$

of A.

The *first cohomology of G with coefficents in A* is defined as 1-cocycles modulo an equivalence relation instead of by 1-coboundaries. The condition for a map φ to be a 1-cocycle is that $\varphi(gh) = \varphi(g)[g\varphi(h)]$ and $\varphi \sim \varphi'$ if there is an a in A such that $a\varphi'(g) = \varphi(g) \cdot (ga)$. In general, $H^1(G, A)$ is not a group when A is non-abelian. It instead has the structure of a pointed set – exactly the same situation arises in the 0th homotopy group, $\pi_0(X; x)$ which for a general topological space is not a group but a pointed set. Note that a group is in particular a pointed set, with the identity element as distinguished point.
Using explicit calculations, one still obtains a *truncated* long exact sequence in cohomology. Specifically, let

$$0 \to A \to B \to C \to 0$$

be a short exact sequence of G-groups, then there is an exact sequence of pointed sets

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C).$$

Connections with topological cohomology theories

Group cohomology can be related to topological cohomology theories: to the topological group G there is an associated classifying space BG. (If G has no topology about which we care, then we assign the discrete topology to G. In this case, BG is an Eilenberg-MacLane space $K(G,1)$, whose fundamental group is G and whose higher homotopy groups vanish). The n-th cohomology of BG, with coefficients in M (in the topological sense), is the same as the group cohomology of G with coefficients in M. This will involve a local coefficient system unless M is a trivial G-module. The connection holds because the total space EG is contractible, so its chain complex forms a projective resolution of M. These connections are explained in (Adem-Milgram 2004), Chapter II.

When M is a ring with trivial G-action, we inherit good properties which are familiar from the topological context: in particular, there is a cup product under which

$$H^*(G;M) = \bigoplus_n H^n(G;M)$$

is a graded module, and a Künneth formula applies.

If, furthermore, $M=k$ is a field, then $H^*(G;k)$ is a graded k-algebra. In this case, the Künneth formula yields

$$H^*(G_1 \times G_2; k) \cong H^*(G_1;k) \otimes H^*(G_2;k).$$

For example, let G be the group with two elements, under the discrete topology. The real projective space $\mathbb{RP}^\infty$ is a classifying space for G. Let $k=\mathbf{F}_2$, the field of two elements. Then

$$H^*(G;k) \cong k[x],$$

a polynomial k-algebra on a single generator, since this is the cellular cohomology ring of $\mathbb{RP}^\infty$.

Hence, as a second example, if G is an elementary abelian 2-group of rank r, and $k=\mathbf{F}_2$, then the Künneth formula gives

$$H^*(G;k) \cong k[x_1, \ldots, x_r],$$

a polynomial k-algebra generated by r classes in $H^1(G;k)$.

Properties

In the following, let M be a G-module.

Functoriality

Group cohomology depends contravariantly on the group G, in the following sense: if $f : H \to G$ is a group homomorphism, then we have a naturally induced morphism $H^n(G,M) \to H^n(H,M)$ (where in the latter, M is treated as an H-module via f).

Given a morphism of G-modules $M \to N$, one gets a morphism of cohomology groups in the $H^n(G,M) \to H^n(G,N)$.

H^1

The first cohomology group is the quotient of the so-called *crossed homomorphisms*, i.e. maps (of sets) $f : G \to M$ satisfying $f(ab) = f(a) + af(b)$ for all a, b in G, modulo the so-called *principal crossed homomorphisms*, i.e. maps $f : G \to M$ given by $f(a) = am - m$ for some fixed $m \in M$. This follows from the definition of cochains above.

If the action of G on M is trivial, then the above boils down to $H^1(G, M) = Hom(G, M)$, the group of group homomorphisms $G \to M$.

H^2

If M is a trivial G-module (i.e. the action of G on M is trivial), the second cohomology group $H^2(G,M)$ is in one-to-one correspondence with the set of central extensions of G by M (up to a natural equivalence relation). More generally, if the action of G on M is nontrivial, $H^2(G,M)$ classifies the isomorphism classes of all extensions of G by M in which the induced action of G on M by inner automorphisms agrees with the given action.

Change of group

The Hochschild-Serre spectral sequence relates the cohomology of a normal subgroup N of G and the quotient G/N to the cohomology of the group G (for (pro-)finite groups G).

Cohomology of finite groups is torsion

The cohomology groups of finite groups are all torsion. Indeed, by Maschke's theorem the category of representations of a finite group is semi-simple over any field of characteristic zero (or more generally, any field whose characteristic does not divide the order of the group), hence, viewing group cohomology as a derived functor in this abelian category, one obtains that it is zero. The other argument is that over a field of characteristic zero, the group algebra of a finite group is a direct sum of matrix algebras (possibly over division algebras which are extensions of the original field), while a matrix algebra is Morita equivalent to its base field and hence has trivial cohomology.

History and relation to other fields

The low dimensional cohomology of a group was classically studied in other guises, long before the notion of group cohomology was formulated in 1943-45. The first theorem of the subject can be identified as Hilbert's Theorem 90 in 1897; this was recast into *Noether's equations* in Galois theory (an appearance of cocycles for H^1). The idea of *factor sets* for the extension problem for groups (connected with H^2) arose in the work of Hölder (1893), in Issai Schur's 1904 study of projective representations, in Schreier's 1926 treatment, and in Richard Brauer's 1928 study of simple algebras and the Brauer group. A fuller discussion of this history may be found in (Weibel 1999, pp. 806–811).

In 1941, while studying $H_2(G, \mathbb{Z})$ (which plays a special role in groups), Hopf discovered what is now called **Hopf's integral homology formula** (Hopf 1942), which is identical to Schur's formula for the Schur multiplier of a finite, finitely presented group:

$H_2(G, \mathbb{Z}) \cong (R \cap [F, F])/[F, R]$, where $G \cong F/R$ and F is a free group.

Hopf's result led to the independent discovery of group cohomology by several groups in 1943-45: Eilenberg and Mac Lane in the USA (Rotman 1995, p. 358); Hopf and Eckmann in Switzerland; and Freudenthal in the Netherlands (Weibel 1999, p. 807). The situation was chaotic because communication between these countries was difficult during World War II.

From a topological point of view, the homology and cohomology of G was first defined as the homology and cohomology of a model for the topological classifying space *BG* as discussed in #Connections with topological cohomology theories above. In practice, this meant using topology to produce the chain complexes used in formal algebraic definitions. From a module-theoretic point of view this was integrated into the Cartan-Eilenberg theory of Homological algebra in the early 1950s.

The application in algebraic number theory to class field theory provided theorems valid for general Galois extensions (not just abelian extensions). The cohomological part of class field theory was axiomatized as the theory of class formations. In turn, this led to the notion of Galois cohomology and étale cohomology (which builds on it) (Weibel 1999, p. 822). Some refinements in the theory post-1960 have been made, such as continuous cocycles and Tate's redefinition, but the basic outlines remain the same. This is a large field, and now basic in the theories of algebraic groups.

The analogous theory for Lie algebras, called Lie algebra cohomology, was first developed in the late 1940s, by Chevalley-Eilenberg, and Koszul (Weibel 1999, p. 810). It is formally similar, using the corresponding definition of *invariant* for the action of a Lie algebra. It is much applied in representation theory, and is closely connected with the BRST quantization of theoretical physics.

Notes

[1] Section VII.2 of Serre 1979
[2] Page 62 of Milne 2008 or section VII.3 of Serre 1979
[3] Remark II.1.21 of Milne 2008

References

- Adem, Alejandro; R. James Milgram (2004), *Cohomology of Finite Groups*, Grundlehren der Mathematischen Wissenschaften, **309**, Springer-Verlag, ISBN 3-540-20283-8, MR2035696
- Brown, Kenneth S. (1972), *Cohomology of Groups*, Graduate Texts in Mathematics, **87**, Springer Verlag, ISBN 0-387-90688-6, MR0672956
- Hopf, Heinz (1942), "Fundamentalgruppe und zweite Bettische Gruppe" (http://www.digizeitschriften.de/index.php?id=166&ID=132355&L=2), *Comment. Math. Helv.* **14** (1): 257–309, doi:10.1007/BF02565622, MR6510
- Chapter II of Milne, James (5/2/2008), *Class Field Theory* (http://www.jmilne.org/math), **v4.00**, retrieved 8/9/2008
- Rotman, Joseph (1995), *An Introduction to the Theory of Groups*, Springer-Verlag, ISBN 978-0-387-94285-8, MR1307623
- Chapter VII of Serre, Jean-Pierre (1979), *Local fields*, Graduate Texts in Mathematics, **67**, Berlin, New York: Springer-Verlag, ISBN 978-0-387-90424-5, MR554237
- Serre, Jean-Pierre (1994), *Cohomologie galoisienne*, Lecture Notes in Mathematics, **5** (Fifth ed.), Berlin, New York: Springer-Verlag, ISBN 978-3-540-58002-7, MR1324577
- Shatz, Stephen S. (1972), *Profinite groups, arithmetic, and geometry*, Princeton, NJ: Princeton University Press, ISBN 978-0-691-08017-8, MR0347778
- Chapter 6 of Weibel, Charles A. (1994), *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, **38**, Cambridge University Press, ISBN 978-0-521-55987-4, OCLC 36131259, MR1269324
- Weibel, Charles A. (1999), "History of homological algebra", *History of Topology*, Cambridge University Press, pp. 797–836, ISBN 0-444-82375-1, MR1721123

Presentation of a group

In mathematics, one method of defining a group is by a **presentation**. One specifies a set *S* of **generators** so that every element of the group can be written as a product of powers of some of these generators, and a set *R* of **relations** among those generators. We then say *G* has presentation

$$\langle S \mid R \rangle.$$

Informally, *G* has the above presentation if it is the "freest group" generated by S subject only to the relations *R*. Formally, the group *G* is said to have the above presentation if it is isomorphic to the quotient of a free group on *S* by the normal subgroup generated by the relations *R*.

As a simple example, the cyclic group of order *n* has the presentation

$$\langle a \mid a^n = 1 \rangle.$$

where 1 is the group identity. This may be written equivalently as

$$\langle a \mid a^n \rangle,$$

since terms that don't include an equals sign are taken to be equal to the group identity. Such terms are called **relators**, distinguishing them from the relations that include an equals sign.

Every group has a presentation, and in fact many different presentations; a presentation is often the most compact way of describing the structure of the group.

A closely related but different concept is that of an absolute presentation of a group.

Background

A free group on a set *S* is a group where each element can be *uniquely* described as a finite length product of the form:

$$s_1^{a_1} s_2^{a_2} \ldots s_n^{a_n}$$

where the s_i are elements of S, adjacent s_i are distinct, and a_i are non-zero integers (but *n* may be zero). In less formal terms, the group consists of words in the generators *and their inverses*, subject only to canceling a generator with its inverse.

If *G* is any group, and *S* is a generating subset of *G*, then every element of *G* is also of the above form; but in general, these products will not uniquely describe an element of *G*.

For example, the dihedral group *D* of order sixteen can be generated by a rotation, *r*, of order 8; and a flip, *f*, of order 2; and certainly any element of *D* is a product of *r* 's and *f* 's.

However, we have, for example, $r\,f\,r = f$, $r^7 = r^{-1}$, etc.; so such products are not unique in *D*. Each such product equivalence can be expressed as an equality to the identity; such as

$$r\,f\,r\,f = 1$$
$$r^8 = 1$$
$$f^2 = 1.$$

Informally, we can consider these products on the left hand side as being elements of the free group $F = \langle r,f \rangle$, and can consider the subgroup *R* of *F* which is generated by these strings; each of which would also be equivalent to 1 when considered as products in *D*.

If we then let *N* be the subgroup of *F* generated by all conjugates $x^{-1} R\, x$ of *R*, then it is straightforward to show that every element of *N* is a finite product $x_1^{-1} r_1 x_1 \ldots x_m^{-1} r_m x_m$ of members of such conjugates. It follows that *N* is a normal subgroup of *F*; and that each element of *N*, when considered as a product in *D*, will also evaluate to 1. Thus *D* is isomorphic to the quotient group *F* /*N*. We then say that *D* has presentation

$$\langle r, f \mid r^8 = f^2 = (rf)^2 = 1 \rangle.$$

Definition

Let *S* be a set and let F_S be the free group on *S*. Let *R* be a set of words on *S*, so *R* naturally gives a subset of F_S. To form a group with presentation <*S*|*R*>, the idea is to take F_S quotient by the smallest normal subgroup such that each element of *R* gets identified with the identity. Note that *R* might not be a subgroup, let alone a normal subgroup of F_S, so we cannot take a quotient by *R*. The solution is to take the normal closure *N* of *R* in F_S. The group <*S*|*R*> is then defined as the quotient group

$$\langle S \mid R \rangle = F_S/N.$$

The elements of *S* are called the **generators** of <*S*|*R*> and the elements of *R* are called the **relators**. A group *G* is said to have the presentation <*S*|*R*> if *G* is isomorphic to <*S*|*R*>.

It is a common practice to write relators in the form $x = y$ where x and y are words on S. What this means is that $y^{-1}x \in R$. This has the intuitive meaning that the images of *x* and *y* are supposed to be equal in the quotient group. Thus e.g. r^n in the list of relators is equivalent with $r^n = 1$. Another common shorthand is to write $[x, y]$ for a commutator $xyx^{-1}y^{-1}$.

A presentation is said to be **finitely generated** if S is finite and **finitely related** if R is finite. If both are finite it is said to be a **finite presentation**. A group is **finitely generated** (respectively **finitely related**, **finitely presented**) if it has a presentation that is finitely generated (respectively finitely related, a finite presentation).

If S is indexed by a set I consisting of all the natural numbers $\mathbb{N}$ or a finite subset of them, then it is easy to set up a simple one to one coding (or Gödel numbering) $f : F_S \to \mathbb{N}$ from the free group on S to the natural numbers, such that we can find algorithms that, given $f(w)$, calculate w, and vice versa. We can then call a subset U of F_S recursive (respectively recursively enumerable) if $f(U)$ is recursive (respectively recursively enumerable). If S is indexed as above and R recursively enumerable, then the presentation is a **recursive presentation** and the corresponding group is **recursively presented**. This usage may seem odd, but it is possible to prove that if a group has a presentation with R recursively enumerable then it has another one with R recursive.

For a finite group G, the multiplication table provides a presentation. We take S to be the elements g_i of G and R to be all words of the form $g_i g_j g_k^{-1}$, where $g_i g_j = g_k$ is an entry in the multiplication table. A presentation can then be thought of as a generalization of a multiplication table.

Every finitely presented group is recursively presented, but there are recursively presented groups that cannot be finitely presented. However a theorem of Graham Higman states that a finitely generated group has a recursive presentation if and only if it can be embedded in a finitely presented group. From this we can deduce that there are (up to isomorphism) only countably many finitely generated recursively presented groups. Bernhard Neumann has shown that there are uncountably many non-isomorphic two generator groups. Therefore there are finitely generated groups that cannot be recursively presented.

Examples

History

One of the earliest presentations of a group by generators and relations was given by the Irish mathematician William Rowan Hamilton in 1856, in his Icosian Calculus – a presentation of the icosahedral group.[1]

The first systematic study was given by Walther von Dyck, student of Felix Klein, in the early 1880s, laying the foundations for combinatorial group theory.[2]

Common examples

The following table lists some examples of presentations for commonly studied groups. Note that in each case there are many other presentations that are possible. The presentation listed is not necessarily the most efficient one possible.

Group	Presentation	Comments
the free group on S	$\langle S \mid \varnothing \rangle$	A free group is "free" in the sense that it is subject to no relations.
C_n, the cyclic group of order n	$\langle a \mid a^n \rangle$	
D_{2n}, the dihedral group of order $2n$	$\langle r, f \mid r^n, f^2, (rf)^2 \rangle$	Here r represents a rotation and f a reflection
D_∞, the infinite dihedral group	$\langle r, f \mid r^2, f^2 \rangle$	
Dic_n, the dicyclic group	$\langle r, f \mid r^{2n} = 1, r^n = f^2, frf^{-1} = r^{-1} \rangle$	The quaternion group is a special case when $n = 2$
$\mathbf{Z} \times \mathbf{Z}$	$\langle x, y \mid xy = yx \rangle$	
$\mathbf{Z}_m \times \mathbf{Z}_n$	$\langle x, y \mid x^m = 1, y^n = 1, xy = yx \rangle$	
the free abelian group on S	$\langle S \mid R \rangle$ where R is the set of all commutators of elements of S	
the symmetric group, S_n	generators: $\sigma_1, \ldots, \sigma_{n-1}$ relations: • $\sigma_i^2 = 1$, • $\sigma_i\sigma_j = \sigma_j\sigma_i$ if $j \neq i \pm 1$, • $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ The last set of relations can be transformed into • $(\sigma_i\sigma_{i+1})^3 = 1$ using $\sigma_i^2 = 1$.	Here σ_i is the permutation that swaps the ith element with the i+1 one. The product $\sigma_i\sigma_{i+1}$ is a 3-cycle on the set $\{i, i+1, i+2\}$.
the braid group, B_n	generators: $\sigma_1, \ldots, \sigma_{n-1}$ relations: • $\sigma_i\sigma_j = \sigma_j\sigma_i$ if $j \neq i \pm 1$, • $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$	Note the similarity with the symmetric group; the only difference is the removal of the relation $\sigma_i^2 = 1$.
the tetrahedral group, $T \cong A_4$	$\langle s, t \mid s^2, t^3, (st)^3 \rangle$	
the octahedral group, $O \cong S_4$	$\langle s, t \mid s^2, t^3, (st)^4 \rangle$	
the icosahedral group, $I \cong A_5$	$\langle s, t \mid s^2, t^3, (st)^5 \rangle$	

the quaternion group, Q_8	$\langle i, j \mid jij = i, iji = j \rangle$	For an alternative presentation see Dic_n above.
$SL_2(\mathbb{Z})$	$\langle a, b \mid aba = bab, (aba)^4 \rangle$	topologically you can visualize *a* and *b* as Dehn twists on the torus
$GL_2(\mathbb{Z})$	$\langle a, b, j \mid aba = bab, (aba)^4, j^2, (ja)^2, (jb)^2 \rangle$	non trivial $\mathbb{Z}_2$- group extension of $SL_2(\mathbb{Z})$
$PSL_2(\mathbb{Z})$	$\langle a, b \mid a^2, b^3 \rangle$	$\mathrm{PSL}_2(\mathbf{Z})$ is the free product of the cyclic groups $\mathbf{Z}_2$ and $\mathbf{Z}_3$
Heisenberg group	$\langle x, y, z \mid z = xyx^{-1}y^{-1}, xz = zx, yz = zy \rangle$	
Baumslag-Solitar group, *B*(*m*,*n*)	$\langle a, b \mid a^n = ba^m b^{-1} \rangle$	
Tits group	$\langle a, b \mid a^2, b^3, (ab)^{13}, [a, b]^5, [a, bab]^4, (abababababab^{-1})^6 \rangle$	[*a*, *b*] is the commutator

An example of a finitely generated group that is not finitely presented is the wreath product $\mathbb{Z} \wr \mathbb{Z}$ of the group of integers with itself.

Some theorems

Every group *G* has a presentation. To see this, consider the free group F_G on *G*. By the universal property of free groups, there exists a unique group homomorphism $\varphi : F_G \to G$ whose restriction to *G* is the identity map. Let *K* be the kernel of this homomorphism. Then *K* is normal in F_G, therefore is equal to its normal closure, so <*G*|*K*> = F_G/K. Since the identity map is surjective, φ is also surjective, so by the First Isomorphism Theorem, <*G*|*K*> $\cong \mathrm{im}\varphi = G$.

Note that this presentation may be highly inefficient if both *G* and *K* are much larger than necessary.

Every finite group has a finite presentation.

The negative solution to the word problem for groups states that there is a finite presentation <*S*|*R*> for which there is no algorithm which, given two words *u*, *v*, decides whether *u* and *v* describe the same element in the group.

Constructions

Suppose *G* has presentation <*S*|*R*> and *H* has presentation <*T*|*Q*> with *S* and *T* being disjoint. Then

- the **free product** $G * H$ has presentation <*S,T*|*R,Q*> and
- the **direct product** $G \times H$ has presentation <*S,T*|*R,Q, [S,T]*>, where [*S,T*] means that every element from *S* commutes with every element from *T* (cf. commutator).

Geometric group theory

Further information: Cayley graph

Further information: Word metric

A presentation of a group determines a geometry, in the sense of geometric group theory: one has the Cayley graph, which has a metric, called the word metric. These are also two resulting orders, the *weak order* and the *Bruhat order,* and corresponding Hasse diagrams. An important example is in the Coxeter groups.

Further, some properties of this graph (the coarse geometry) are intrinsic, meaning independent of choice of generators.

Notes

[1] Sir William Rowan Hamilton (1856). "Memorandum respecting a new System of Roots of Unity" (http://www.maths.tcd.ie/pub/HistMath/People/Hamilton/Icosian/NewSys.pdf). *Philosophical Magazine* **12**: 446. .

[2] Stillwell, John (2002). *Mathematics and its history*. Springer. p. 374 (http://books.google.com/books?id=WNjRrqTm62QC&pg=PA374). ISBN 978-0-38795336-6

References

- Johnson, D. L. (1990). *Presentations of Groups*. Cambridge: Cambridge University Press. ISBN 0-521-37824-9. Schreier's method, Nielsen's method, free presentations, subgroups and HNN extensions, Golod-Shafarevich theorem, etc.
- Coxeter, H. S. M. and Moser, W. O. J. (1980). *Generators and Relations for Discrete Groups*. New York: Springer-Verlag. ISBN 0-387-09212-9. This useful reference has tables of presentations of all small finite groups, the reflection groups, and so forth.

Product of group subsets

In mathematics, one can define a **product of group subsets** in a natural way. If *S* and *T* are subsets of a group *G* then their product is the subset of *G* defined by

$$ST = \{st : s \in S \text{ and } t \in T\}$$

Note that *S* and *T* need not be subgroups. The associativity of this product follows from that of the group product. The product of group subsets therefore defines a natural monoid structure on the power set of *G*.

If *S* and *T* are subgroups of *G* their product need not be a subgroup. It will be a subgroup if and only if *ST* = *TS* and the two subgroups are said to permute. In this case *ST* is the group generated by *S* and *T*, i.e. *ST* = *TS* = <*S* ∪ *T*>. If either *S* or *T* is normal then this condition is satisfied and *ST* is a subgroup. Suppose *S* is normal. Then according to the second isomorphism theorem *S* ∩ *T* is normal in *T* and *ST*/*S* ≅ *T*/(*S* ∩ *T*).

If *G* is a finite group and *S* and *T* and subgroups of *G* then *ST* is a subset of *G* of size |*ST*| given by the *product formula*:

$$|ST| = \frac{|S||T|}{|S \cap T|}$$

Note that this applies even if neither *S* nor *T* is normal.

In particular, if *S* and *T* (subgroups now) intersect only in the identity, then every element of *ST* has a unique expression as a product *st* with *s* in *S* and *t* in *T*. If *S* and *T* also permute, then *ST* is a group, and is called a Zappa-Szep product. Even further, if *S* or *T* is normal in *ST*, then *ST* is called a semidirect product. Finally, if both *S* and *T* are normal in *ST*, then *ST* is called a direct product.

References

- Rotman, Joseph (1995). *An Introduction to the Theory of Groups* (4th ed.). Springer-Verlag. ISBN 0-387-94285-8.

Schur multiplier

In mathematical group theory, the **Schur multiplier** or **Schur multiplicator** is the second homology group $H_2(G;\mathbb{Z})$ of a group G. It was introduced by Issai Schur (1904) in his work on projective representations.

Examples and properties

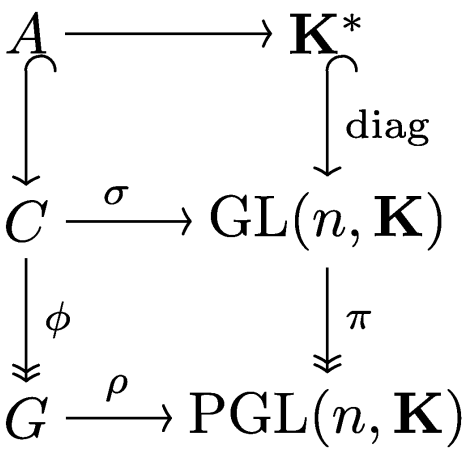
The Schur multiplier M(G) of a finite group G is a finite abelian group whose exponent divides the order of G. If a Sylow p-subgroup of G is cyclic for some p, then order of M(G) is not divisible by p. In particular, if all Sylow p-subgroups of G are cyclic, then M(G) is trivial.

For instance, the Schur multiplier of the nonabelian group of order 6 is the trivial group since every Sylow subgroup is cyclic. The Schur multiplier of the elementary abelian group of order 16 is an elementary abelian group of order 64, showing that the multiplier can be strictly larger than the group itself. The Schur multiplier of the quaternion group is trivial, but the Schur multiplier of dihedral 2-groups has order 2.

The Schur multipliers of the finite simple groups are given at the list of finite simple groups. The covering groups of the alternating and symmetric groups are of considerable recent interest.

Relation to projective representations

Schur's original motivation for studying the multiplier was to classify projective representations of a group, and the modern formulation of his definition is the second cohomology group $H^2(G,\mathbf{C}^\times)$. A projective representation is much like a group representation except that instead of a homomorphism into the general linear group GL(n,$\mathbf{C}$), one takes a homomorphism into the projective general linear group PGL(n,$\mathbf{C}$). In other words, a projective representation is a representation modulo the center.



A projective representation of G can be pulled back to a linear representation of a central extension C of G.

Schur (1904, 1907) showed that every finite group G has associated to it at least one finite group C, called a **Schur cover**, with the property that every projective representation of G can be lifted to an ordinary representation of C. The Schur cover is also known as a **covering group** or **Darstellungsgruppe**. The Schur covers of the finite simple groups are known, and each is an example of a quasisimple group. The Schur cover of a perfect group is uniquely determined up to isomorphism, but the Schur cover of a general finite group is only determined up to isoclinism.

Relation to central extensions

The study of such covering groups led naturally to the study of central and **stem extensions**.

A central extension of a group G is an extension

$$1 \to K \to C \to G \to 1$$

where $K \leq Z(C)$ is a subgroup of the center of C.

A **stem extension** of a group G is an extension

$$1 \to K \to C \to G \to 1$$

where $K \leq Z(C) \cap C'$ is a subgroup of the intersection of the center of C and the derived subgroup of C; this is more restrictive than central.

If the group G is finite and one considers only stem extensions, then there is a largest size for such a group C, and for every C of that size the subgroup K is isomorphic to the Schur multiplier of G. If the finite group G is moreover perfect, then C is unique up to isomorphism and is itself perfect. Such C are often called **universal perfect central extensions** of G, or **covering group** (as it is a discrete analog of the universal covering space in topology). If the finite group G is not perfect, then its Schur covering groups (all such C of maximal order) are only isoclinic.

It is also called more briefly a **universal central extension**, but note that there is no largest central extension, as the direct product of G and an abelian group form a central extension of G of arbitrary size.

Stem extensions have the nice property that any lift of a generating set of G is a generating set of C. If the group G is presented in terms of a free group F on a set of generators, and a normal subgroup R generated by a set of relations on the generators, so that $G \cong F/R$, then the covering group itself can be presented in terms of F but with a smaller normal subgroup S, $C \cong F/S$. Since the relations of G specify elements of K when considered as part of C, one must have $S \leq [F,R]$.

In fact if G is perfect, this is all that is needed: $C \cong [F,F]/[F,R]$ and $M(G) \cong K \cong R/[F,R]$. Because of this simplicity, expositions such as (Aschbacher 2000, §33) handle the perfect case first. The general case for the Schur multiplier is similar but ensures the extension is a stem extension by restricting to the derived subgroup of F: $M(G) \cong (R \cap [F, F])/[F, R]$. These are all slightly later results of Schur, who also gave a number of useful criteria for calculating them more explicitly.

Relation to efficient presentations

In combinatorial group theory, a group often originates from a presentation. One important theme in this area of mathematics is to study presentations with as few relations as possible, such as one relator groups like Baumslag-Solitar groups. These groups are infinite groups with two generators and one relation, and an old result of Schreier shows that in any presentation with more generators than relations, the resulting group is infinite. The borderline case is thus quite interesting: finite groups with the same number of generators as relations are said to have an **efficient presentation**. For a group to have an efficient presentation, the group must have a trivial Schur multiplier because the minimum number of generators of the Schur multiplier is always less than or equal to the difference between the number of relations and the number of generators.

A fairly recent topic of research is to find efficient presentations for all finite simple groups with trivial Schur multipliers. Such presentations are in some sense nice because they are usually short, but they are difficult to find and to work with because they are ill-suited to standard methods such as coset enumeration.

Relation to topology

In topology, groups can often be described as finitely presented groups and a fundamental question is to calculate their integral homology $H_n(G, \mathbb{Z})$. In particular, the second homology plays a special role and this led Hopf to find an effective method for calculating it. The method in (Hopf 1942) is also known as **Hopf's integral homology formula** and is identical to Schur's formula for the Schur multiplier of a finite, finitely presented group:

$$H_2(G, \mathbb{Z}) \cong (R \cap [F, F])/[F, R]$$

where $G \cong F/R$ and F is a free group. The same formula also holds when G is a perfect group.[1]

The recognition that these formulas were the same led Eilenberg and Mac Lane to the creation of cohomology of groups. In general, $H_2(G, \mathbb{Z}) \cong \left(H^2(G, \mathbb{C}^\times)\right)^*$ where the star denotes the algebraic dual group, and when G is finite, there is an unnatural isomorphism $\left(H^2(G, \mathbb{C}^\times)\right)^* \cong H^2(G, \mathbb{C}^\times)$.

A perfect group is one whose first integral homology vanishes. A superperfect group is one whose first two homology groups vanish. The Schur covers of finite perfect groups are superperfect. An acyclic group is a group all of whose reduced integral homology vanishes.

Applications

The second algebraic K-group $K_2(R)$ of a commutative ring R can be identified with the second homology group

$$H_2(E(R), \mathbb{Z})$$

of the group $E(R)$ of (infinite) elementary matrices with entries in R.[2]

References

[1] Rosenberg, Jonathan (1994), *Algebraic K-theory and its applications* (http://books.google.com/books?id=TtMkTEZbYoYC), Graduate Texts in Mathematics, **147**, Berlin, New York: Springer-Verlag, ISBN 978-0-387-94248-3, MR1282290 Errata (http://www-users.math.umd.edu/~jmr/KThy_errata2.pdf), , Theorems 4.1.3, 4.1.19

[2] Rosenberg, Jonathan (1994), *Algebraic K-theory and its applications* (http://books.google.com/books?id=TtMkTEZbYoYC), Graduate Texts in Mathematics, **147**, Berlin, New York: Springer-Verlag, ISBN 978-0-387-94248-3, MR1282290 Errata (http://www-users.math.umd.edu/~jmr/KThy_errata2.pdf), , Corollary 4.2.10

- Aschbacher, Michael (2000), *Finite group theory*, Cambridge Studies in Advanced Mathematics, **10** (2nd ed.), Cambridge University Press, ISBN 978-0-521-78145-9; 978-0-521-78675-1, MR1777008
- Hopf, Heinz (1942), "Fundamentalgruppe und zweite Bettische Gruppe", *Commentarii Mathematici Helvetici* **14**: 257–309, doi:10.1007/BF02565622, ISSN 0010-2571, MR0006510
- Kuzmin, L.V. (2001), "Schur multiplicator" (http://www.encyclopediaofmath.org/index.php?title=S/s083460), in Hazewinkel, Michiel, *Encyclopedia of Mathematics*, Springer, ISBN 978-1556080104
- Rotman, Joseph J. (1994), *An introduction to the theory of groups*, Berlin, New York: Springer-Verlag, ISBN 978-0-387-94285-8
- Schur, J. (1904), "Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen." (http://resolver.sub.uni-goettingen.de/purl?GDZPPN002165511) (in German), *Journal für die reine und angewandte Mathematik* **127**: 20–50, ISSN 0075-4102, JFM 35.0155.01
- Schur, J. (1907), "Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen." (http://resolver.sub.uni-goettingen.de/purl?GDZPPN00216633X) (in German), *Journal für die reine und angewandte Mathematik* **132**: 85–137, ISSN 0075-4102, JFM 38.0174.02
- Van der Kallen, Wilberd (1984), "Review: F. Rudolf Beyl and Jürgen Tappe, Group extensions, representations, and the Schur multiplicator" (http://projecteuclid.org/euclid.bams/1183551591), *Bulletin of the American Mathematical Society* **10** (2): 330–333
- Wiegold, J. (1982), "The Schur multiplier: an elementary approach", *Groups–St. Andrews 1981 (St. Andrews, 1981)*, London Math. Soc. Lecture Note Ser., **71**, Cambridge University Press, pp. 137–154, MR679156

Semidirect product

In mathematics, specifically in the area of abstract algebra known as group theory, a **semidirect product** is a particular way in which a group can be put together from two subgroups, one of which is a normal subgroup. A semidirect product is a generalization of a direct product. It is a cartesian product as a set, but with a particular multiplication operation.

Some equivalent definitions

Let G be a group with identity element e, N a normal subgroup of G (i.e., $N \lhd G$) and H a subgroup of G. The following statements are equivalent:

- $G = NH$ and $N \cap H = \{e\}$.
- $G = HN$ and $N \cap H = \{e\}$.
- Every element of G can be written as a unique product of an element of N and an element of H.
- Every element of G can be written as a unique product of an element of H and an element of N.
- The natural embedding $H \to G$, composed with the natural projection $G \to G / N$, yields an isomorphism between H and the quotient group G / N.
- There exists a homomorphism $G \to H$ which is the identity on H and whose kernel is N.

If one (and therefore all) of these statements hold, we say that G is a **semidirect product** of N and H, written $G = N \rtimes H$, or that G *splits* over N; one also says that G is a **semidirect** product of H acting on N, or even a semidirect product of H and N. In order to avoid ambiguities, it is advisable to specify which of the two subgroups is normal.

Elementary facts and caveats

If G is the semidirect product of the normal subgroup N and the subgroup H, and both N and H are finite, then the order of G equals the product of the orders of N and H.

Note that, as opposed to the case with the direct product, a semidirect product of two groups is not, in general, unique; if G and G' are two groups which both contain isomorphic copies of N as a normal subgroup and H as a subgroup, and both are a semidirect product of N and H, then it does *not* follow that G and G' are isomorphic. This remark leads to an extension problem, of describing the possibilities.

Semidirect products and group homomorphisms

Let G be a semidirect product of the normal subgroup N and the subgroup H. Let Aut(N) denote the group of all automorphisms of N. The map $\varphi : H \to \mathrm{Aut}(N)$ defined by $\varphi(h) = \varphi_h$, where $\varphi_h(n) = hnh^{-1}$ for all h in H and n in N, is a group homomorphism. Together N, H and φ determine G up to isomorphism, as we show now.

Given any two groups N and H (not necessarily subgroups of a given group) and a group homomorphism $\varphi : H \to \mathrm{Aut}(N)$, there is a new group $N \rtimes_\varphi H$ (or simply $N \times_\varphi H$), called the **semidirect product of N and H with respect to φ**, defined as follows.

- As a set, $N \rtimes_\varphi H$ is the cartesian product $N \times H$.
- Multiplication of elements in $N \rtimes_\varphi H$ is determined by the homomorphism φ. The operation is

$$*\colon (N \rtimes_\varphi H) \times (N \rtimes_\varphi H) \to N \rtimes_\varphi H$$

  defined by

$$(n_1, h_1) * (n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2)$$

  for n_1, n_2 in N and h_1, h_2 in H.

This defines a group in which the identity element is (e_N, e_H) and the inverse of the element (n, h) is $(\varphi_h{-}1(n^{-1}), h^{-1})$. Pairs (n,e_H) form a normal subgroup isomorphic to N, while pairs (e_N, h) form a subgroup isomorphic to H. The full group is a semidirect product of those two subgroups in the sense given above.

Conversely, suppose that we are given a group G with a normal subgroup N and a subgroup H, such that every element g of G may be written uniquely in the form $g=nh$ where n lies in N and h lies in H. Let $\varphi : H \to \mathrm{Aut}(N)$ be the homomorphism given by $\varphi(h) = \varphi_h$, where

$$\varphi_h(n) = hnh^{-1}$$

for all n in N and h in H. Then G is isomorphic to the semidirect product $N \rtimes_\varphi H$; the isomorphism sends the product nh to the tuple (n,h). In G, we have the multiplication rule

$$(n_1, h_1)(n_2, h_2) = (n_1(h_1 n_2 h_1^{-1}), h_1 h_2).$$

A version of the splitting lemma for groups states that a group G is isomorphic to a semidirect product of the two groups N and H if and only if there exists a short exact sequence

$$1 \longrightarrow N \xrightarrow{\beta} G \xrightarrow{\alpha} H \longrightarrow 1$$

and a group homomorphism $\gamma : H \to G$ such that $\alpha \circ \gamma = \mathrm{id}_H$, the identity map on H. In this case, $\varphi : H \to \mathrm{Aut}(N)$ is given by $\varphi(h) = \varphi_h$, where

$$\varphi_h(n) = \beta^{-1}(\gamma(h)\beta(n)\gamma(h^{-1})).$$

If φ is the trivial homomorphism, sending every element of H to the identity automorphism of N, then $N \rtimes_\varphi H$ is the direct product $N \times H$.

Examples

The dihedral group D_{2n} with $2n$ elements is isomorphic to a semidirect product of the cyclic groups C_n and C_2. Here, the non-identity element of C_2 acts on C_n by inverting elements; this is an automorphism since C_n is abelian. The presentation for this group is:

$$\langle a,\ b \mid a^2 = e,\ b^n = e,\ aba^{-1} = b^{-1} \rangle.$$

More generally, a semidirect product of any two cyclic groups C_m with generator a and C_n with generator b is given by a single relation $aba^{-1} = b^k$ with k and n coprime, i.e. the presentation:

$$\langle a,\ b \mid a^m = e,\ b^n = e,\ aba^{-1} = b^k \rangle.$$

If r and m are coprime, a^r is a generator of C_m and $a^r b a^{-r} = b^{k^r}$, hence the presentation:

$$\langle a,\ b \mid a^m = e,\ b^n = e,\ aba^{-1} = b^{k^r} \rangle$$

gives a group isomorphic to the previous one.

The fundamental group of the Klein bottle can be presented in the form

$$\langle a,\ b \mid aba^{-1} = b^{-1} \rangle$$

and is therefore a semidirect product of the group of integers, $\mathbb{Z}$, with itself.

The Euclidean group of all rigid motions (isometries) of the plane (maps $f : \mathbf{R}^2 \to \mathbf{R}^2$ such that the Euclidean distance between x and y equals the distance between $f(x)$ and $f(y)$ for all x and y in $\mathbf{R}^2$) is isomorphic to a semidirect product of the abelian group $\mathbf{R}^2$ (which describes translations) and the group O(2) of orthogonal 2×2 matrices (which describes rotations and reflections which keep the origin fixed). n is a translation, h a rotation or reflection. Applying a translation and then a rotation or reflection corresponds to applying the rotation or reflection first and then a translation by the rotated or reflected translation vector (i.e. applying the conjugate of the original translation). Every orthogonal matrix acts as an automorphism on $\mathbf{R}^2$ by matrix multiplication.

The orthogonal group O(n) of all orthogonal real n×n matrices (intuitively the set of all rotations and reflections of n-dimensional space which keep the origin fixed) is isomorphic to a semidirect product of the group SO(n) (consisting of all orthogonal matrices with determinant 1, intuitively the rotations of n-dimensional space) and C_2. If

we represent C_2 as the multiplicative group of matrices $\{I, R\}$, where R is a reflection of n dimensional space which keeps the origin fixed (i.e. an orthogonal matrix with determinant -1 representing an involution), then $\varphi : C_2 \to \mathrm{Aut}(\mathrm{SO}(n))$ is given by $\varphi(H)(N) = H\,N\,H^{-1}$ for all H in C_2 and N in $\mathrm{SO}(n)$. In the non-trivial case (H is not the identity) this means that $\varphi(H)$ is conjugation of operations by the reflection (a rotation axis and the direction of rotation are replaced by their "mirror image").

Relation to direct products

Suppose G is a semidirect product of the normal subgroup N and the subgroup H. If H is also normal in G, or equivalently, if there exists a homomorphism $G \to N$ which is the identity on N, then G is the direct product of N and H.

The direct product of two groups N and H can be thought of as the outer semidirect product of N and H with respect to $\varphi(h) = \mathrm{id}_N$ for all h in H.

Note that in a direct product, the order of the factors is not important, since $N \times H$ is isomorphic to $H \times N$. This is not the case for semidirect products, as the two factors play different roles.

Generalizations

The construction of semidirect products can be pushed much further. The Zappa-Szep product of groups is a generalization which, in its internal version, does not assume that either subgroup is normal. There is also a construction in ring theory, the crossed product of rings. This is seen naturally as soon as one constructs a group ring for a semidirect product of groups. There is also the semidirect sum of Lie algebras. Given a group action on a topological space, there is a corresponding crossed product which will in general be non-commutative even if the group is abelian. This kind of ring (see crossed product for a related construction) can play the role of the *space of orbits* of the group action, in cases where that space cannot be approached by conventional topological techniques - for example in the work of Alain Connes (cf. noncommutative geometry).

There are also far-reaching generalisations in category theory. They show how to construct *fibred categories* from *indexed categories*. This is an abstract form of the outer semidirect product construction.

Groupoids

Another generalisation is for groupoids. This occurs in topology because if a group G acts on a space X it also acts on the fundamental groupoid $\pi_1(X)$ of the space. The semidirect product $\pi_1(X) \rtimes G$ is then relevant to finding the fundamental groupoid of the orbit space X/G . For full details see Chapter 11 of the book referenced below, and also some details in semidirect product[1] in ncatlab.

Abelian categories

Non-trivial semidirect products do *not* arise in abelian categories, such as the category of modules. In this case, the splitting lemma shows that every semidirect product is a direct product. Thus the existence of semidirect products reflects a failure of the category to be abelian.

Notation

Usually the semidirect product of a group H acting on a group N (in most cases by conjugation as subgroups of a common group) is denoted by $N \rtimes H$ or $H \ltimes N$. However, some sources may use this symbol with the opposite meaning. In case the action $\phi : H \to \mathrm{Aut}(N)$ should be made explicit, one also writes $N \rtimes_\phi H$. One way of thinking about the $N \rtimes H$ symbol is as a combination of the symbol for normal subgroup ($\triangleleft$) and the symbol for the product ($\times$).

Unicode lists four variants:[2]

	value	MathML	Unicode description
⋉	U+22C9	ltimes	LEFT NORMAL FACTOR SEMIDIRECT PRODUCT
⋊	U+22CA	rtimes	RIGHT NORMAL FACTOR SEMIDIRECT PRODUCT
⋋	U+22CB	lthree	LEFT SEMIDIRECT PRODUCT
⋌	U+22CC	rthree	RIGHT SEMIDIRECT PRODUCT

Here the Unicode description of the rtimes symbol says "right normal factor", in contrast to its usual meaning in mathematical practice.

In LaTeX, the commands \rtimes and \ltimes produce the corresponding characters.

Notes

[1] Ncatlab.org (http://ncatlab.org/nlab/show/semidirect+product)
[2] See unicode.org (http://www.unicode.org/charts/symbols.htm)

References

- R. Brown, Topology and groupoids, Booksurge 2006. ISBN 1-4196-2722-8

Sylow theorems

In mathematics, specifically in the field of finite group theory, the **Sylow theorems** are a collection of theorems named after the Norwegian mathematician Ludwig Sylow (1872) that give detailed information about the number of subgroups of fixed order that a given finite group contains. The Sylow theorems form a fundamental part of finite group theory and have very important applications in the classification of finite simple groups.

For a prime number p, a **Sylow p-subgroup** (sometimes **p-Sylow subgroup**) of a group G is a maximal p-subgroup of G, i.e., a subgroup of G which is a p-group (so that the order of any group element is a power of p), and which is not a proper subgroup of any other p-subgroup of G. The set of all Sylow p-subgroups for a given prime p is sometimes written $\mathrm{Syl}_p(G)$.

The Sylow theorems assert a partial converse to Lagrange's theorem that for any finite group G the order (number of elements) of every subgroup of G divides the order of G. For any prime factor p of the order of a finite group G, there exists a Sylow p-subgroup of G. The order of a Sylow p-subgroup of a finite group G is p^n, where n is the multiplicity of p in the order of G, and any subgroup of order p^n is a Sylow p-subgroup of G. The Sylow p-subgroups of a group (for fixed prime p) are conjugate to each other. The number of Sylow p-subgroups of a group for fixed prime p is congruent to 1 mod p.

Sylow theorems

Collections of subgroups which are each maximal in one sense or another are common in group theory. The surprising result here is that in the case of $\mathrm{Syl}_p(G)$, all members are actually isomorphic to each other and have the largest possible order: if $|G| = p^n m$ with $n > 0$ where p does not divide m, then any Sylow p-subgroup P has order $|P| = p^n$. That is, P is a p-group and $\gcd(|G:P|, p) = 1$. These properties can be exploited to further analyze the structure of G.

The following theorems were first proposed and proven by Ludwig Sylow in 1872, and published in *Mathematische Annalen*.

Theorem 1: For any prime factor p with multiplicity n of the order of a finite group G, there exists a Sylow p-subgroup of G, of order p^n.

The following weaker version of theorem 1 was first proved by Cauchy.

Corollary: Given a finite group G and a prime number p dividing the order of G, then there exists an element of order p in G .

Theorem 2: Given a finite group G and a prime number p, all Sylow p-subgroups of G are conjugate to each other, i.e. if H and K are Sylow p-subgroups of G, then there exists an element g in G with $g^{-1}Hg = K$.

Theorem 3: Let p be a prime factor with multiplicity n of the order of a finite group G, so that the order of G can be written as $p^n \cdot m$, where $n > 0$ and p does not divide m. Let n_p be the number of Sylow p-subgroups of G. Then the following hold:

- n_p divides m, which is the index of the Sylow p-subgroup in G.
- $n_p \equiv 1 \bmod p$.
- $n_p = |G : N_G(P)|$, where P is any Sylow p-subgroup of G and N_G denotes the normalizer.

Consequences

The Sylow theorems imply that for a prime number p every Sylow p-subgroup is of the same order, p^n. Conversely, if a subgroup has order p^n, then it is a Sylow p-subgroup, and so is isomorphic to every other Sylow p-subgroup. Due to the maximality condition, if H is any p-subgroup of G, then H is a subgroup of a p-subgroup of order p^n.

A very important consequence of Theorem 2 is that the condition $n_p = 1$ is equivalent to saying that the Sylow p-subgroup of G is a normal subgroup (there are groups which have normal subgroups but no normal Sylow subgroups, such as S_4).

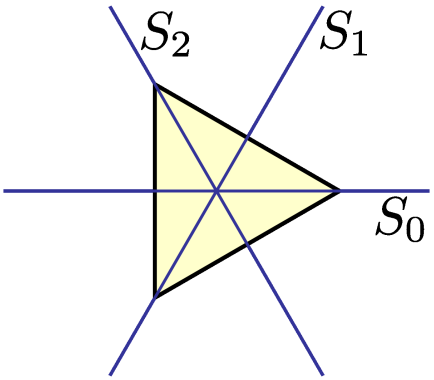
Sylow theorems for infinite groups

There is an analogue of the Sylow theorems for infinite groups. We define a Sylow p-subgroup in an infinite group to be a p-subgroup (that is, every element in it has p-power order) which is maximal for inclusion among all p-subgroups in the group. Such subgroups exist by Zorn's lemma.

Theorem: If K is a Sylow p-subgroup of G, and $n_p = |\mathrm{Cl}(K)|$ is finite, then every Sylow p-subgroup is conjugate to K, and $n_p \equiv 1 \bmod p$, where $\mathrm{Cl}(K)$ denotes the conjugacy class of K.

Examples

A simple illustration of Sylow subgroups and the Sylow theorems are the dihedral group of the n-gon, D_{2n}. For n odd, $2 = 2^1$ is the highest power of 2 dividing the order, and thus subgroups of order 2 are Sylow subgroups. These are the groups generated by a reflection, of which there are n, and they are all conjugate under rotations; geometrically the axes of symmetry pass through a vertex and a side. By contrast, if n is even, then 4 divides the order of the group, and these are no longer Sylow subgroups, and in fact they fall into two conjugacy classes, geometrically according to whether they pass through two vertices or two faces. These are related by an outer automorphism, which can be represented by rotation through π/n, half the minimal rotation in the dihedral group.

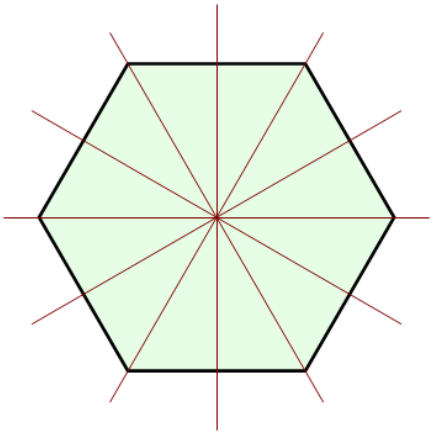


In D_6, all reflections are conjugate, as reflections correspond to Sylow 2-subgroups.

Example applications

Cyclic group orders

Some numbers n are such that every group of order n is cyclic. One can show that n = 15 is such a number using the Sylow theorems: Let G be a group of order 15 = 3 · 5 and n_3 be the number of Sylow 3-subgroups. Then $n_3 \mid 5$ and $n_3 \equiv 1 \pmod 3$. The only value satisfying these constraints is 1; therefore, there is only one subgroup of order 3, and it must be normal (since it has no distinct conjugates). Similarly, n_5 must divide 3, and n_5 must equal 1 (mod 5); thus it must also have a single normal subgroup of order 5. Since 3 and 5 are coprime, the intersection of these two subgroups is trivial, and so G must be the internal direct product of groups of order *3* and *5*, that is the cyclic group of order 15. Thus, there is only one group of order 15 (up to isomorphism).



In D_{12}, reflections no longer correspond to Sylow 2-subgroups, and fall into two conjugacy classes.

Small groups are not simple

A more complex example involves the order of the smallest simple group which is not cyclic. Burnside's p^aq^b theorem states that if the order of a group is the product of two prime powers, then it is solvable, and so the group is not simple, or is of prime order and is cyclic. This rules out every group up to order 30 (= 2 · 3 · 5).

If G is simple, and |G| = 30, then n_3 must divide 10 (= 2 · 5), and n_3 must equal 1 (mod 3). Therefore n_3 = 10, since neither 4 nor 7 divides 10, and if n_3 = 1 then, as above, G would have a normal subgroup of order 3, and could not be simple. G then has 10 distinct cyclic subgroups of order 3, each of which has 2 elements of order 3 (plus the identity). This means G has at least 20 distinct elements of order 3. As well, n_5 = 6, since n_5 must divide 6 (= 2 · 3), and n_5 must equal 1 (mod 5). So G also has 24 distinct elements of order 5. But the order of G is only 30, so a simple group of order 30 cannot exist.

Next, suppose |G| = 42 = 2 · 3 · 7. Here n_7 must divide 6 (= 2 · 3) and n_7 must equal 1 (mod 7), so n_7 = 1. So, as before, G can not be simple.

On the other hand for |G| = 60 = 2^2 · 3 · 5, then n_3 = 10 and n_5 = 6 is perfectly possible. And in fact, the smallest simple non-cyclic group is A_5, the alternating group over 5 elements. It has order 60, and has 24 cyclic permutations

of order 5, and 20 of order 3.

Fusion results

Frattini's argument shows that a Sylow subgroup of a normal subgroup provides a factorization of a finite group. A slight generalization known as **Burnside's fusion theorem** states that if G is a finite group with Sylow p-subgroup P and two subsets A and B normalized by P, then A and B are G-conjugate if and only if they are $N_G(P)$-conjugate. The proof is a simple application of Sylow's theorem: If $B=A^g$, then the normalizer of B contains not only P but also P^g (since P^g is contained in the normalizer of A^g). By Sylow's theorem P and P^g are conjugate not only in G, but in the normalizer of B. Hence gh^{-1} normalizes P for some h that normalizes B, and then $A^{gh}-1 = B^h-1 = B$, so that A and B are $N_G(P)$-conjugate. Burnside's fusion theorem can be used to give a more power factorization called a semidirect product: if G is a finite group whose Sylow p-subgroup P is contained in the center of its normalizer, then G has a normal subgroup K of order coprime to P, $G = PK$ and $P \cap K = 1$, that is, G is p-nilpotent.

Less trivial applications of the Sylow theorems include the focal subgroup theorem, which studies the control a Sylow p-subgroup of the derived subgroup has on the structure of the entire group. This control is exploited at several stages of the classification of finite simple groups, and for instance defines the case divisions used in the Alperin–Brauer–Gorenstein theorem classifying finite simple groups whose Sylow 2-subgroup is a quasi-dihedral group. These rely on J. L. Alperin's strengthening of the conjugacy portion of Sylow's theorem to control what sorts of elements are used in the conjugation.

Proof of the Sylow theorems

The Sylow theorems have been proved in a number of ways, and the history of the proofs themselves are the subject of many papers including (Waterhouse 1980), (Scharlau 1988), (Casadio & Zappa 1990), (Gow 1994), and to some extent (Meo 2004).

One proof of the Sylow theorems exploit the notion of group action in various creative ways. The group G acts on itself or on the set of its p-subgroups in various ways, and each such action can be exploited to prove one of the Sylow theorems. The following proofs are based on combinatorial arguments of (Wielandt 1959). In the following, we use $a \mid b$ as notation for "a divides b" and $a \nmid b$ for the negation of this statement.

> **Theorem 1**: A finite group G whose order $|G|$ is divisible by a prime power p^k has a subgroup of order p^k.

Proof: Let $|G| = p^k m = p^{k+r} u$ such that p does not divide u, and let Ω denote the set of subsets of G of size p^k. G acts on Ω by left multiplication. The orbits $G\omega = \{g\omega \mid g \in G\}$ of the $\omega \in \Omega$ are the equivalence classes under the action of G.

For any $\omega \in \Omega$ consider its stabilizer subgroup G_ω. For any fixed element $\alpha \in \omega$ the function $[g \mapsto g\alpha]$ maps G_ω to ω injectively: for any two $g,h \in G_\omega$ we have that $g\alpha = h\alpha$ implies $g = h$, because $\alpha \in \omega \in G$ means that one may cancel on the right. Therefore $p^k = |\omega| \geq |G_\omega|$.

On the other hand

$$|\Omega| = \binom{p^k m}{p^k} = m \prod_{j=1}^{p^k-1} \frac{p^k m - j}{p^k - j} = m \prod_{j=1}^{p^k-1} \frac{p^{k-\nu_p(j)} m - j/p^{\nu_p(j)}}{p^{k-\nu_p(j)} - j/p^{\nu_p(j)}}$$

and no power of p remains in any of the factors inside the product on the right. Hence $\nu_p(|\Omega|) = \nu_p(m) = r$. Let $R \subset \Omega$ be a complete representation of all the equivalence classes under the action of G. Then,

$$|\Omega| = \sum_{\omega \in R} |G\omega|.$$

Thus, there exists an element $\omega \in R$ such that $s := \nu_p(|G\omega|) \leq \nu_p(|\Omega|) = r$. Hence $|G\omega| = p^s v$ where p does not divide v. By the stabilizer-orbit-theorem we have $|G_\omega| = |G| / |G\omega| = p^{k+r-s} u / v$. Therefore $p^k \mid |G_\omega|$, so $p^k \leq |G_\omega|$ and G_ω is

the desired subgroup.

> **Lemma**: Let G be a finite p-group, let G act on a finite set Ω, and let Ω_0 denote the set of points of Ω that are fixed under the action of G. Then $|\Omega| \equiv |\Omega_0| \bmod p$.

Proof: Write Ω as a disjoint sum of its orbits under G. Any element $x \in \Omega$ not fixed by G will lie in an orbit of order $|G|/|G_x|$ (where G_x denotes the stabilizer), which is a multiple of p by assumption. The result follows immediately.

> **Theorem 2**: If H is a p-subgroup of G and P is a Sylow p-subgroup of G, then there exists an element g in G such that $g^{-1}Hg \leq P$. In particular, all Sylow p-subgroups of G are conjugate to each other (and therefore isomorphic), i.e. if H and K are Sylow p-subgroups of G, then there exists an element g in G with $g^{-1}Hg = K$.

Proof: Let Ω be the set of left cosets of P in G and let H act on Ω by left multiplication. Applying the Lemma to H on Ω, we see that $|\Omega_0| \equiv |\Omega| = [G : P] \bmod p$. Now $p \nmid [G : P]$ by definition so $p \nmid |\Omega_0|$, hence in particular $|\Omega_0| \neq 0$ so there exists some $gP \in \Omega_0$. It follows that for some $g \in G$ and $\forall\ h \in H$ we have $hgP = gP$ so $g^{-1}hgP \subseteq P$ and therefore $g^{-1}Hg \leq P$. Now if H is a Sylow p-subgroup, $|H| = |P| = |gPg^{-1}|$ so that $H = gPg^{-1}$ for some $g \in G$.

> **Theorem 3**: Let q denote the order of any Sylow p-subgroup of a finite group G. Then $n_p \mid |G|/q$ and $n_p \equiv 1 \bmod p$.

Proof: By Theorem 2, $n_p = [G : N_G(P)]$, where P is any such subgroup, and $N_G(P)$ denotes the normalizer of P in G, so this number is a divisor of $|G|/q$. Let Ω be the set of all Sylow p-subgroups of G, and let P act on Ω by conjugation. Let $Q \in \Omega_0$ and observe that then $Q = xQx^{-1}$ for all $x \in P$ so that $P \leq N_G(Q)$. By Theorem 2, P and Q are conjugate in $N_G(Q)$ in particular, and Q is normal in $N_G(Q)$, so then $P = Q$. It follows that $\Omega_0 = \{P\}$ so that, by the Lemma, $|\Omega| \equiv |\Omega_0| = 1 \bmod p$.

Algorithms

The problem of finding a Sylow subgroup of a given group is an important problem in computational group theory.

One proof of the existence of Sylow p-subgroups is constructive: if H is a p-subgroup of G and the index $[G:H]$ is divisible by p, then the normalizer $N = \mathrm{N}_G(H)$ of H in G is also such that $[N:H]$ is divisible by p. In other words, a polycyclic generating system of a Sylow p-subgroup can be found by starting from any p-subgroup H (including the identity) and taking elements of p-power order contained in the normalizer of H but not in H itself. The algorithmic version of this (and many improvements) is described in textbook form in (Butler 1991, Chapter 16), including the algorithm described in (Cannon 1971). These versions are still used in the GAP computer algebra system.

In permutation groups, it has been proven in (Kantor 1985a, 1985b, 1990; Kantor & Taylor 1988) that a Sylow p-subgroup and its normalizer can be found in polynomial time of the input (the degree of the group times the number of generators). These algorithms are described in textbook form in (Seress 2003), and are now becoming practical as the constructive recognition of finite simple groups becomes a reality. In particular, versions of this algorithm are used in the Magma computer algebra system.

Notes

References

- Sylow, L. (1872), "Théorèmes sur les groupes de substitutions" (http://resolver.sub.uni-goettingen.de/purl?GDZPPN002242052) (in French), *Math. Ann.* **5** (4): 584–594, doi:10.1007/BF01442913, JFM 04.0056.02

Proofs

- Casadio, Giuseppina; Zappa, Guido (1990), "History of the Sylow theorem and its proofs" (in Italian), *Boll. Storia Sci. Mat.* **10** (1): 29–75, ISSN 0392-4432, MR1096350, Zbl 0721.01008
- Gow, Rod (1994), "Sylow's proof of Sylow's theorem", *Irish Math. Soc. Bull.* (33): 55–63, ISSN 0791-5578, MR1313412, Zbl 0829.01011
- Kammüller, Florian; Paulson, Lawrence C. (1999), "A formal proof of Sylow's theorem. An experiment in abstract algebra with Isabelle HOL" (http://www.cl.cam.ac.uk/users/lcp/papers/Kammueller/sylow.pdf), *J. Automat. Reason.* **23** (3): 235–264, doi:10.1023/A:1006269330992, ISSN 0168-7433, MR1721912, Zbl 0943.68149
- Meo, M. (2004), "The mathematical life of Cauchy's group theorem", *Historia Math.* **31** (2): 196–221, doi:10.1016/S0315-0860(03)00003-X, ISSN 0315-0860, MR2055642, Zbl 1065.01009
- Scharlau, Winfried (1988), "Die Entdeckung der Sylow-Sätze" (in German), *Historia Math.* **15** (1): 40–52, doi:10.1016/0315-0860(88)90048-1, ISSN 0315-0860, MR931678, Zbl 0637.01006
- Waterhouse, William C. (1980), "The early proofs of Sylow's theorem", *Arch. Hist. Exact Sci.* **21** (3): 279–290, doi:10.1007/BF00327877, ISSN 0003-9519, MR575718, Zbl 0436.01006
- Wielandt, Helmut (1959), "Ein Beweis für die Existenz der Sylowgruppen" (in German), *Arch. Math.* **10** (1): 401–402, doi:10.1007/BF01240818, ISSN 0003-9268, MR0147529, Zbl 0092.02403

Algorithms

- Butler, G. (1991), *Fundamental Algorithms for Permutation Groups*, Lecture Notes in Computer Science, **559**, Berlin, New York: Springer-Verlag, doi:10.1007/3-540-54955-2, ISBN 978-3-540-54955-0, MR1225579, Zbl 0785.20001
- Cannon, John J. (1971), "Computing local structure of large finite groups", *Computers in Algebra and Number Theory (Proc. SIAM-AMS Sympos. Appl. Math., New York, 1970)*, SIAM-AMS Proc., **4**, Providence, RI: AMS, pp. 161–176, ISSN 0160-7634, MR0367027, Zbl 0253.20027
- Kantor, William M. (1985a), "Polynomial-time algorithms for finding elements of prime order and Sylow subgroups", *J. Algorithms* **6** (4): 478–514, doi:10.1016/0196-6774(85)90029-X, ISSN 0196-6774, MR813589, Zbl 0604.20001
- Kantor, William M. (1985b), "Sylow's theorem in polynomial time", *J. Comput. System Sci.* **30** (3): 359–394, doi:10.1016/0022-0000(85)90052-2, ISSN 1090-2724, MR805654, Zbl 0573.20022
- Kantor, William M.; Taylor, Donald E. (1988), "Polynomial-time versions of Sylow's theorem", *J. Algorithms* **9** (1): 1–17, doi:10.1016/0196-6774(88)90002-8, ISSN 0196-6774, MR925595, Zbl 0642.20019
- Kantor, William M. (1990), "Finding Sylow normalizers in polynomial time", *J. Algorithms* **11** (4): 523–563, doi:10.1016/0196-6774(90)90009-4, ISSN 0196-6774, MR1079450, Zbl 0731.20005
- Seress, Ákos (2003), *Permutation Group Algorithms*, Cambridge Tracts in Mathematics, **152**, Cambridge University Press, ISBN 978-0-521-66103-4, MR1970241, Zbl 1028.20002

Hall subgroup

In mathematics, a **Hall subgroup** of a finite group G is a subgroup whose order is coprime to its index. They are named after the group theorist Philip Hall.

Definitions

A **Hall divisor** of an integer n is a divisor d of n such that d and n/d are coprime. The easiest way to find the Hall divisors is to write the **prime factorization** for the number in question and take any product of the multiplicative terms (the full power of any of the prime factors), including 0 of them for a product of 1 or all of them for a product equal to the original number. For example, to find the Hall divisors of 60, show the prime factorization is $2^2 \cdot 3 \cdot 5$ and take any product of {3,4,5}. Thus, the Hall divisors of 60 are 1, 3, 4, 5, 12, 15, 20, and 60.

A **Hall subgroup** of G is a subgroup whose order is a Hall divisor of the order of G. In other words, it is a subgroup whose order is coprime to its index.

If π is a set of primes, then a **Hall π-subgroup** is a subgroup whose order is a product of primes in π, and whose index is not divisible by any primes in π.

Examples

- Any Sylow subgroup of a group is a Hall subgroup.
- If $G = A_5$, the only simple group of order 60, then 15 and 20 are Hall divisors of the order of G, but G has no subgroups of these orders.
- The simple group of order 168 has two different conjugacy classes of Hall subgroups of order 24 (though they are conjugate under an outer automorphism of G).
- The simple group of order 660 has two Hall subgroups of order 12 that are not isomorphic.

Hall's theorem

Hall proved that if G is a finite solvable group and π is any set of primes, then G has a Hall π-subgroup, and any two Hall π-subgroups are conjugate. Moreover any subgroup whose order is a product of primes in π is contained in some Hall π-subgroup. This result can be thought of as a generalization of Sylow's Theorem to Hall subgroups, but the examples above show that such a generalization is false when the group is not solvable.

Hall's theorem can be proved by induction on the order of G, using the fact that every finite solvable group has a normal elementary abelian subgroup.

A converse to Hall's theorem

Any finite group that has a Hall π-subgroup for every set of primes π is solvable. This is a generalization of Burnside's theorem that any group whose order is of the form $p^a q^b$ for primes p and q is solvable, because Sylow's theorem implies that all Hall subgroups exist. This does not (at present) give another proof of Burnside's theorem, because Burnside's theorem is used to prove this converse.

Sylow systems

A **Sylow system** is a set of Sylow p-subgroups S_p for each prime p such that $S_p S_q = S_q S_p$ for all p and q. If we have a Sylow system, then the subgroup generated by the groups S_p for p in π is a Hall π-subgroup. A more precise version of Hall's theorem says that any solvable group has a Sylow system, and any two Sylow systems are conjugate.

Normal Hall subgroups

Any normal Hall subgroup H of a finite group G possesses a complement, that is there is some subgroup K of G which intersects H trivially and such that HK=G (so G is isomorphic to a semi-direct product of H and K).

References

- Gorenstein, Daniel (1980), *Finite groups*, Boston: Amer Mathematical Society, ISBN 0828403015.

Wreath product

In mathematics, the **wreath product** of group theory is a specialized product of two groups, based on a semidirect product. Wreath products are an important tool in the classification of permutation groups and also provide a way of constructing interesting examples of groups.

Given two groups A and H there exist two variations of the wreath product: the **unrestricted wreath product** A Wr H (also written $A \wr H$) and the **restricted wreath product** A wr H. Given a set Ω with an H-action there exists a generalisation of the wreath product which is denoted by $A \operatorname{Wr}_\Omega H$ or $A \operatorname{wr}_\Omega H$ respectively.

Definition

Let A and H be groups and Ω a set with H acting on it. Let K be the direct product

$$K \equiv \prod_{\omega \in \Omega} A_\omega$$

of copies of $A_\omega := A$ indexed by the set Ω. The elements of K can be seen as arbitrary sequences (a_ω) of elements of A indexed by Ω with component wise multiplication. Then the action of H on Ω extends in a natural way to an action of H on the group K by

$$h(a_\omega) \equiv (a_{h^{-1}\omega}).$$

Then the **unrestricted wreath product** $A \operatorname{Wr}_\Omega H$ of A by H is the semidirect product $K \rtimes H$. The subgroup K of $A \operatorname{Wr}_\Omega H$ is called the **base** of the wreath product.

The **restricted wreath product** $A \operatorname{wr}_\Omega H$ is constructed in the same way as the unrestricted wreath product except that one uses the direct sum

$$K \equiv \bigoplus_{\omega \in \Omega} A_\omega$$

as the base of the wreath product. In this case the elements of K are sequences (a_ω) of elements in A indexed by Ω of which all but finitely many a_ω are the identity element of A.

The group H acts in a natural way on itself by left multiplication. Thus we can choose $\Omega := H$. In this special (but very common) case the unrestricted and restricted wreath product may be denoted by $A \operatorname{Wr} H$ and $A \operatorname{wr} H$ respectively. We say in this case that the wreath product is **regular**.

Notation and Conventions

The structure of the wreath product of A by H depends on the H-set Ω and in case Ω is infinite it also depends on whether one uses the restricted or unrestricted wreath product. However, in literature the notation used may be deficient and one needs to pay attention on the circumstances.

- In literature $A \wr_\Omega H$ may stand for the unrestricted wreath product $A \operatorname{Wr}_\Omega H$ or the restricted wreath product $A \operatorname{wr}_\Omega H$.
- Similarly, $A \wr H$ may stand for the unrestricted regular wreath product $A \operatorname{Wr} H$ or the restricted regular wreath product $A \operatorname{wr} H$.
- In literature the H-set Ω may be omitted from the notation even if $\Omega \neq H$.
- In the special case that $H = S_n$ is the symmetric group of degree n it is common in the literature to assume that $\Omega = \{1,\ldots,n\}$ (with the natural action of S_n) and then omit Ω from the notation. That is, $A \wr S_n$ commonly denotes $A \wr_{\{1,\ldots,n\}} S_n$ instead of the regular wreath product $A \wr_S nS_n$. In the first case the base group is the product of n copies of A, in the latter it is the product of $n!$ copies of A.

Properties

- Since the finite direct product is the same as the finite direct sum of groups it follows that the unrestricted $A \operatorname{Wr}_\Omega H$ and the restricted wreath product $A \operatorname{wr}_\Omega H$ agree if the H-set Ω is finite. In particular this is true when $\Omega = H$ is finite.
- $A \operatorname{wr}_\Omega H$ is always a subgroup of $A \operatorname{Wr}_\Omega H$.
- Universal Embedding Theorem: If G is an extension of A by H, then there exists a subgroup of the unrestricted wreath product $A \wr H$ which is isomorphic to G.[1]
- If A, H and Ω are finite, then

$$|A \wr_\Omega H| = |A|^{|\Omega|}|H|.$$[2]

Canonical Actions of Wreath Products

If the group A acts on a set Λ then there are two canonical ways to construct sets from Ω and Λ on which $A \operatorname{Wr}_\Omega H$ (and therefore also $A \operatorname{wr}_\Omega H$) can act.

- The **imprimitive** wreath product action on $\Lambda \times \Omega$.

  If $((a_\omega),h) \in A \operatorname{Wr}_\Omega H$ and $(\lambda,\omega') \in \Lambda \times \Omega$, then

$$((a_\omega), h) \cdot (\lambda, \omega') := (a_{h(\omega')}\lambda, h\omega').$$

- The **primitive** wreath product action on Λ^Ω.

  An element in Λ^Ω is a sequence (λ_ω) indexed by the H-set Ω. Given an element $((a_\omega), h) \in A \operatorname{Wr}_\Omega H$ its operation on $(\lambda_\omega) \in \Lambda^\Omega$ is given by

$$((a_\omega), h) \cdot (\lambda_\omega) := (a_{h^{-1}\omega}\lambda_{h^{-1}\omega}).$$

Examples

- The Lamplighter group is the restricted wreath product $\mathbb{Z}_2 \wr \mathbb{Z}$.
- $\mathbb{Z}_m \wr S_n$ (Generalized symmetric group).

  The base of this wreath product is the n-fold direct product

  $$\mathbb{Z}_m^{\,n} = \mathbb{Z}_m \times \ldots \times \mathbb{Z}_m$$

  of copies of $\mathbb{Z}_m$ where the action $\varphi : S_n \to \mathrm{Aut}(\mathbb{Z}_m^{\,n})$ of the symmetric group S_n of degree n is given by

  $\varphi(\sigma)(\alpha_1,\ldots, \alpha_n) := (\alpha_{\sigma(1)},\ldots, \alpha_{\sigma(n)})$.[3]
- $S_2 \wr S_n$ (Hyperoctahedral group).

  The action of S_n on $\{1,\ldots,n\}$ is as above. Since the symmetric group S_2 of degree 2 is isomorphic to $\mathbb{Z}_2$ the hyperoctahedral group is a special case of a generalized symmetric group.[4]
- Let p be a prime and let $n \leq 1$. Let P be a Sylow p-subgroup of the symmetric group S_{p^n} of degree p^n. Then P is isomorphic to the iterated regular wreath product $W_n = \mathbb{Z}_p \wr \mathbb{Z}_p \wr \ldots \wr \mathbb{Z}_p$ of n copies of $\mathbb{Z}_p$. Here $W_1 := \mathbb{Z}_p$ and $W_k := W_{k-1} \wr \mathbb{Z}_p$ for all $k \geq 2$.[5][6]
- The Rubik's cube group is a subgroup of small index in the product of wreath products, $(\mathbb{Z}_3 \wr S_8) \times (\mathbb{Z}_2 \wr S_{12})$, the factors corresponding to the symmetries of the 8 corners and 12 edges.

References

[1] M. Krasner and L. Kaloujnine, "Produit complet des groupes de permutations et le problème d'extension de groupes III", Acta Sci. Math. Szeged 14, pp. 69-82 (1951)

[2] Joseph J. Rotman, An Introduction to the Theory of Groups, p. 172 (1995)

[3] J. W. Davies and A. O. Morris, "The Schur Multiplier of the Generalized Symmetric Group", J. London Math. Soc (2), 8, (1974), pp. 615-620

[4] P. Graczyk, G. Letac and H. Massam, "The Hyperoctahedral Group, Symmetric Group Representations and the Moments of the Real Wishart Distribution", J. Theoret. Probab. 18 (2005), no. 1, 1-42.

[5] Joseph J. Rotman, An Introduction to the Theory of Groups, p. 176 (1995)

[6] L. Kaloujnine, "La structure des p-groupes de Sylow des groupes symétriques finis", Annales Scientifiques de l'École Normale Supérieure. Troisième Série 65, pp. 239–276 (1948)

External links

- PlanetMath page (http://planetmath.org/encyclopedia/WreathProduct.html)
- Springer Online Reference Works (http://www.encyclopediaofmath.org/index.php/Wreath_product)

Article Sources and Contributors

Group extension *Source*: http://en.wikipedia.org/w/index.php?oldid=474261411 *Contributors*: Agol, Brad7777, Charles Matthews, D3, DKleinecke, Giftlite, Jakito, Jim.belk, Juan Marquez, KSmrq, Lethe, LilHelpa, Linas, Maksim-e, MarSch, Metterklume, Mike Segal, NatusRoma, Nbarth, Phys, QBobWatson, RonnieBrown, Silly rabbit, Silverfish, Sim, Tyomitch, VectorPosse, Vegasprof, Zaslav, Zundark, 22 anonymous edits

Direct product of groups *Source*: http://en.wikipedia.org/w/index.php?oldid=462427235 *Contributors*: Anne Bauval, BlackFingolfin, Dalant019, Fropuff, Giftlite, Headbomb, Inalokasimera, JackSchmidt, Jim.belk, 3 anonymous edits

Direct sum of groups *Source*: http://en.wikipedia.org/w/index.php?oldid=370879816 *Contributors*: AxelBoldt, Chas zzz brown, Ciphers, Gauge, Jim.belk, Jorend, Kaoru Itou, Mhss, Michael Slone, Mwanner, Oleg Alexandrov, Paul August, Revolver, Soumyasch, Yworo, 1 anonymous edits

Free abelian group *Source*: http://en.wikipedia.org/w/index.php?oldid=480553852 *Contributors*: Albmont, Artie p, AxelBoldt, Charles Matthews, Chiapr, Ciphers, Classicalecon, Commator, David Eppstein, El C, Elroch, Eric Kvaalen, Giftlite, Ignirtoq, JackSchmidt, Jim.belk, Keenan Pepper, Linas, MathKnight, MathMartin, Michael Hardy, Omarct1989, Rjwilmsi, RobHar, Sam Coskey, Silly rabbit, Skittleys, Thesm, Tobias Bergemann, Vadik, Vanish2, Vaughan Pratt, Vincent Semeria, Vipul, Waltpohl, Zundark, 17 anonymous edits

Free group *Source*: http://en.wikipedia.org/w/index.php?oldid=481546518 *Contributors*: ATC2, Altenmann, Archelon, AxelBoldt, C S, Charles Matthews, Chris Pressey, David Eppstein, Dbenbenn, Dysprosia, Fadereu, Foobarnix, Giftlite, HUnTeR4subs, HenrikRueping, Hyginsberg, Iorsh, JackSchmidt, Jim.belk, Kapitolini, Kidburla, LachlanA, Larsbars, Laurentius, Linas, Marozols, MathMartin, Mathsci, Mct mht, Michael Hardy, Mikeblas, Mohan ravichandran, Omnipaedista, Punainen Nörtti, R.e.b., RJFJR, Ralamosm, Reedy, Rjwilmsi, Robert Illes, RonnieBrown, Sam nead, Tiphareth, Tobias Bergemann, Tomo, Tosha, Trovatore, Turgidson, Vipul, Virginia-American, ZeroOne, Ziyuang, Zundark, Мыша, 35 anonymous edits

Free product *Source*: http://en.wikipedia.org/w/index.php?oldid=474498479 *Contributors*: Bomazi, Charles Matthews, Fibonacci, Fropuff, J.delanoy, JackSchmidt, Jim.belk, Jowa fan, Juan Marquez, Kidburla, Linas, Michael Hardy, Michael Kinyon, Nsk92, Quinnculver, RobHar, Rror, Tesseran, 17 anonymous edits

Generating set of a group *Source*: http://en.wikipedia.org/w/index.php?oldid=470684196 *Contributors*: ArnoldReinhold, Artem M. Pelenitsyn, AxelBoldt, CRGreathouse, Charles Matthews, Chas zzz brown, Chinju, Dbenbenn, Dcoetzee, Dr.enh, Dysprosia, Emperorbma, Eyal0, Fibonacci, Giftlite, Herbee, JackSchmidt, Lenthe, Lipedia, Mhss, Michael Hardy, Michael Slone, Optimisteo, RobHar, Romanm, Tobias Bergemann, Tomo, Vp loreta, Zundark, 16 anonymous edits

Group cohomology *Source*: http://en.wikipedia.org/w/index.php?oldid=479848297 *Contributors*: Alexander Chervov, AxelBoldt, CBM, CRGreathouse, Charles Matthews, CharlesGillingham, Cohomology, David Eppstein, DealPete, Dysprosia, ElNuevoEinstein, Etale, Expz, Gauge, Giftlite, Hesam7, JackSchmidt, Jakob.scholbach, JarahE, Jaswenso, Joriki, LkNsngth, MSGJ, Maproom, MathKnight, Michael Hardy, Msh210, Nbarth, Nsk92, Oleg Alexandrov, Omarct1989, Owenjonesuk, Quasicharacter, R.e.b., RedWolf, Rich Farmbrough, Rjwilmsi, RobHar, Silly rabbit, Tkuvho, Tob, Vivacissamamente, Waltpohl, Yimuyin, Zaslav, Zundark, 60 anonymous edits

Presentation of a group *Source*: http://en.wikipedia.org/w/index.php?oldid=472962486 *Contributors*: 4pq1injbok, Agradman, Artem M. Pelenitsyn, AxelBoldt, Baccyak4H, Benja, Bernard Hurley, Beroal, Bkonrad, BlackFingolfin, Bobo192, CBM, Charles Matthews, Charvest, Chas zzz brown, Creative1985, Cronian, Dan Hoey, Dbenbenn, Dean P Foster, Dominus, Dr.enh, Elementaro, Fropuff, Giftlite, HUnTeR4subs, Helder.wiki, Hillman, Hmackiernan, JackSchmidt, Jan Hidders, Jay Gatsby, Jim.belk, Juan Marquez, Konradek, Ligulem, Linas, MathMartin, Mhss, Michael Hardy, Mike Segal, Nbarth, Number 0, Patrick, Petersont, PierreAbbat, Quondum, RandomP, Sam nead, Tesseran, That Guy, From That Show!, The Duke of Waltham, Tomo, Turgidson, Virginia-American, Wapcaplet, Yakirr, Zundark, 37 anonymous edits

Product of group subsets *Source*: http://en.wikipedia.org/w/index.php?oldid=461007411 *Contributors*: Andi5, Conversion script, Fropuff, Gauge, Goochelaar, Graham87, JackSchmidt, Jim.belk, Kilva, Konradek, Melchoir, Michael Hardy, Rich Farmbrough, Sandeepr.murthy, Suitangi, That Guy, From That Show!, 1 anonymous edits

Schur multiplier *Source*: http://en.wikipedia.org/w/index.php?oldid=477040407 *Contributors*: BlackFingolfin, Bubba73, Charles Matthews, Gene Ward Smith, Headbomb, JackSchmidt, Jakob.scholbach, Jim.belk, Maproom, Michael Hardy, Nbarth, R.e.b., STyx, Tobias Bergemann, WWGB, Zundark, 11 anonymous edits

Semidirect product *Source*: http://en.wikipedia.org/w/index.php?oldid=471845312 *Contributors*: ATC2, Aeginn, Aghitza, Algebraist, Algebran, AxelBoldt, Bryan Derksen, CESSMASTER, Calculuslover, Charles Matthews, Chas zzz brown, Edward, Elroch, Firsfron, Fropuff, Gauge, Giftlite, Grubber, JackSchmidt, Jakob.scholbach, Jim.belk, Jjalexand, Jleedev, Juan Marquez, KSmrq, Kundor, Lethe, Lotje, Lupin, MSGJ, Materialscientist, Mathisreallycool, Melchoir, Michael Hardy, Michael Kinyon, Nbarth, Patrick, PeterKoroteev, Phys, RonnieBrown, Sabalka, Spacepotato, TheTito, Tijfo098, TommasoT, Tosha, Tyrrell McAllister, Zaslav, Zundark, Мыша, 55 anonymous edits

Sylow theorems *Source*: http://en.wikipedia.org/w/index.php?oldid=463342641 *Contributors*: 01001, Aholtman, Alecobbe, Amitushtush, Ams80, Ank0ku, AxelBoldt, BenF, BeteNoir, CZeke, Charles Matthews, Chas zzz brown, Chochopk, Conversion script, Crisófilax, Cwkmail, David Eppstein, Derek Ross, Dominus, Druiffic, EmilJ, Eramesan, Functor salad, GTBacchus, Gauge, Geometry guy, Giftlite, Goochelaar, Graham87, Grubber, Haham hanuka, Hank hu, Headbomb, Hesam7, JackSchmidt, Japanese Searobin, Joelsims80, Jonathanzung, Kilva, Lzur, MathMartin, Mav, Michael Hardy, Nbarth, Ossido, PappyK, PierreAbbat, Pladdin, Pmanderson, Point-set topologist, Pyrop, R.e.b., Reedy, Schutz, Siroxo, Sl, Spoon!, Stove Wolf, Superninja, TakuyaMurata, Tarquin, Tobias Bergemann, Twilsonb, WLior, Welsh, Zundark, Zvika, 77 anonymous edits

Hall subgroup *Source*: http://en.wikipedia.org/w/index.php?oldid=476139697 *Contributors*: Charles Matthews, Gauge, JackSchmidt, Jim.belk, Marvoir, Michael Hardy, Nihixul, R.e.b., Rjwilmsi, Vipul, 10 anonymous edits

Wreath product *Source*: http://en.wikipedia.org/w/index.php?oldid=478676244 *Contributors*: Alecobbe, C1wang, Charles Matthews, Chas zzz brown, DeaconJohnFairfax, Dysprosia, G2.0 USA, Gauge, Giftlite, Helder.wiki, JackSchmidt, Lagelspeil, LilHelpa, MaximH, Melchoir, Mfluch, Nbarth, Rswarbrick, The Anome, Tomgally, Tyomitch, 29 anonymous edits

Image Sources, Licenses and Contributors

Image:DirectProductDiagram.png *Source*: http://en.wikipedia.org/w/index.php?title=File:DirectProductDiagram.png *License*: Public Domain *Contributors*: Jim.belk

Image:F2 Cayley Graph.png *Source*: http://en.wikipedia.org/w/index.php?title=File:F2_Cayley_Graph.png *License*: Public Domain *Contributors*: Jim.belk

Image:Free Group Universal.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Free_Group_Universal.svg *License*: Public Domain *Contributors*: Jim.belk

File:Projective-representation-lifting.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Projective-representation-lifting.svg *License*: Creative Commons Zero *Contributors*: Nils R. Barth

File:Labeled Triangle Reflections.svg *Source*: http://en.wikipedia.org/w/index.php?title=File:Labeled_Triangle_Reflections.svg *License*: Public Domain *Contributors*: Jim.belk

File:Hexagon Reflections.png *Source*: http://en.wikipedia.org/w/index.php?title=File:Hexagon_Reflections.png *License*: Public Domain *Contributors*: Grafite, Incnis Mrsi, Lipedia, Nbarth

License