Generating set of a group

From Wikipedia, the free encyclopedia

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 <*S*>, 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* = <S>, then we say *S* **generates** *G*; and the elements in S are called **generators** or **group generators**. If *S* is the empty set, then <*S*> 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, <*S*> is usually written as <*x*>. In this case, <*x*> 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 <*x*> equals the entire group G. For finite groups, it is also equivalent to saying that *x* has order |G|.

Contents

Finitely generated group

If *S* is finite, then a group *G* = <*S*> 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 <*G*> = *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* = <{*x*,*y*}>), 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 <*S*> 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).

See also

- Cayley graph
- Generating set for related meanings in other structures
- Presentation of a group

References

- Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR1878556 (http://www.ams.org/mathscinet-getitem?mr=1878556)

External links

- Mathworld: Group generators (http://mathworld.wolfram.com/GroupGenerators.html)