Order (group theory)

In group theory, a branch of mathematics, the term *order* is used in two unrelated senses:

- The **order** of a group is its cardinality, i.e., the number of elements in its set. Also, the **order**, sometimes **period**, of an element a of a group is the smallest positive integer m such that $a^m = e$ (where e denotes the identity element of the group, and a^m denotes the product of m copies of a). If no such m exists, a is said to have infinite order
- The ordering relation of a partially or totally ordered group

This article is about the first sense of order.

The order of a group G is denoted by $\operatorname{ord}(G)$ or $|G|$ and the order of an element a is denoted by $\operatorname{ord}(a)$ or $|a|$.

Contents

Example

Example. The symmetric group S_3 has the following Cayley table.

•	***e***	***s***	***t***	***u***	***v***	***w***
e	*e*	*s*	*t*	*u*	*v*	*w*
s	*s*	*e*	*v*	*w*	*t*	*u*
t	*t*	*u*	*e*	*s*	*w*	*v*
u	*u*	*t*	*w*	*v*	*e*	*s*
v	*v*	*w*	*s*	*e*	*u*	*t*
w	*w*	*v*	*u*	*t*	*s*	*e*

This group has six elements, so $\operatorname{ord}(S_3) = 6$. By definition, the order of the identity, e, is 1. Each of s, t, and w squares to e, so these group elements have order 2. Completing the enumeration, both u and v have order 3, for $u^2 = v$ and $u^3 = vu = e$, and $v^2 = u$ and $v^3 = uv = e$.

Order and structure

The order of a group and that of an element tend to speak about the structure of the group. Roughly speaking, the more complicated the factorization of the order the more complicated the group.

If the order of group G is 1, then the group is called a trivial group. Given an element a, ord(a) = 1 if and only if a is the identity. If every (non-identity) element in G is the same as its inverse (so that $a^2 = e$), then ord(a) = 2 and consequently G is abelian since $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ by Elementary group theory. The converse of this statement is not true; for example, the (additive) cyclic group $\mathbf{Z}_6$ of integers modulo 6 is abelian, but the number 2 has order 3:

$$2 + 2 + 2 = 6 \equiv 0 \pmod 6.$$

The relationship between the two concepts of order is the following: if we write

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

for the subgroup generated by a, then

$$\operatorname{ord}(a) = \operatorname{ord}(\langle a \rangle).$$

For any integer k, we have

$a^k = e$ if and only if ord(a) divides k.

In general, the order of any subgroup of G divides the order of G. More precisely: if H is a subgroup of G, then

ord(G) / ord(H) = [G : H], where [G : H] is called the index of H in G, an integer. This is Lagrange's theorem. (This is, however, only true when G has finite order. If ord(G) = ∞, the quotient ord(G) / ord(H) does not make sense.)

As an immediate consequence of the above, we see that the order of every element of a group divides the order of the group. For example, in the symmetric group shown above, where ord(S_3) = 6, the orders of the elements are 1, 2, or 3.

The following partial converse is true for finite groups: if d divides the order of a group G and d is a prime number, then there exists an element of order d in G (this is sometimes called Cauchy's theorem). The statement does not hold for composite orders, e.g. the Klein four-group does not have an element of order four). This can be shown by inductive proof.[1] The consequences of the theorem include: the order of a group G is a power of a prime p if and only if ord(a) is some power of p for every a in G.[2]

If a has infinite order, then all powers of a have infinite order as well. If a has finite order, we have the following formula for the order of the powers of a:

ord(a^k) = ord(a) / gcd(ord(a), k)

for every integer k. In particular, a and its inverse a^{-1} have the same order.

In any group,

$$\operatorname{ord}(ab) = \operatorname{ord}(ba)$$

There is no general formula relating the order of a product ab to the orders of a and b. In fact, it is possible that both a and b have finite order while ab has infinite order, or that both a and b have infinite order while ab has finite order. An example of the former is $a(x) = 2-x$, $b(x) = 1-x$ with $ab(x) = x-1$ in the group $Sym(\mathbb{Z})$. An example of the latter is $a(x) = x+1$, $b(x) = x-1$ with $ab(x) = x$. If $ab = ba$, we can at least say that ord(ab) divides lcm(ord(a), ord(b)). As a consequence, one can prove that in a finite abelian group, if m denotes the maximum of all the orders of the group's elements, then every element's order divides m.

Counting by order of elements

Suppose G is a finite group of order n, and d is a divisor of n. The number of order-d-elements in G is a multiple of $\varphi(d)$ (possibly zero), where φ is Euler's totient function, giving the number of positive integers no larger than d and coprime to it. For example, in the case of S_3, $\varphi(3) = 2$, and we have exactly two elements of order 3. The theorem provides no useful information about elements of order 2, because $\varphi(2) = 1$, and is only of limited utility for composite d such as d=6, since $\varphi(6)$=2, and there are zero elements of order 6 in S_3.

In relation to homomorphisms

Group homomorphisms tend to reduce the orders of elements: if f: $G \to H$ is a homomorphism, and a is an element of G of finite order, then ord(f(a)) divides ord(a). If f is injective, then ord(f(a)) = ord(a). This can often be used to prove that there are no (injective) homomorphisms between two concretely given groups. (For example, there can be no nontrivial homomorphism h: $S_3 \to \mathbf{Z}_5$, because every number except zero in $\mathbf{Z}_5$ has order 5, which does not divide the orders 1, 2, and 3 of elements in S_3.) A further consequence is that conjugate elements have the same order.

Class equation

An important result about orders is the class equation; it relates the order of a finite group G to the order of its center $Z(G)$ and the sizes of its non-trivial conjugacy classes:

$$|G| = |Z(G)| + \sum_i d_i$$

where the d_i are the sizes of the non-trivial conjugacy classes; these are proper divisors of $|G|$ bigger than one, and they are also equal to the indices of the centralizers in G of the representatives of the non-trivial conjugacy classes. For example, the center of S_3 is just the trivial group with the single element e, and the equation reads $|S_3| = 1+2+3$.

See also

- Torsion subgroup
- Lagrange's theorem (group theory)

References

1. Conrad, Keith. "Proof of Cauchy's Theorem" (http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/cauchypf.pdf) (PDF). Retrieved May 14, 2011.
2. Conrad, Keith. "Consequences of Cauchy's Theorem" (http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/cauchyapp.pdf) (PDF). Retrieved May 14, 2011.