Cyclic group

In mathematics, a **cyclic group** is a group that can be generated by a single element, in the sense that the group has an element *a* (called a "generator" of the group) such that all elements of the group are powers of *a*. Equivalently, an element *a* of a group *G* generates *G* precisely if *G* is the only subgroup of itself that contains *a*.

The cyclic groups are the simplest groups and they are completely known: for any positive integer *n*, there is a cyclic group C_n of order *n*, and then there is the infinite cyclic group, the additive group of integers **Z**. Every other cyclic group is isomorphic to one of these.

Examples of cyclic groups

The finite cyclic groups can be introduced as a series of symmetry groups, or as the groups of rotations of a regular n-gon: for example C_3 can be represented as the group of rotations of an equilateral triangle. While this example is concise and graphical, it is important to remember that each element of C_3 represent an *action* and not a position. Note also that the group S^1 of all rotations of a circle is *not* cyclic.

The cyclic group C_n is isomorphic to the group **Z**/*n***Z** of integers modulo *n* with addition as operation; an isomorphism is given by the discrete logarithm. One typically writes the group C_n multiplicatively, while **Z**/*n***Z** is written additively. Sometimes $\mathbf{Z}_n$ is used instead of **Z**/*n***Z**.

Properties

All cyclic groups are abelian, that is they are commutative.

The element *a* mentioned above in the definition is called a *generator* of the cyclic group. A cyclic group can have several generators. The generators of **Z** are +1 and -1, the generators of **Z**/*n***Z** are the residue classes of the integers which are coprime to *n*; the number of those generators is known as φ(*n*), where φ is Euler's phi function.

More generally, if *d* is a divisor of *n*, then the number of elements in **Z**/*n***Z** which have order *d* is φ(*d*). The order of the residue class of *m* is *n* /gcd(*n*,*m*).

If *p* is a prime number, then the only group (up to isomorphism) with *p* elements is the cyclic group C_p.

The direct product of two cyclic groups C_n and C_m is cyclic if and only if *n* and *m* are coprime.

Every finitely generated abelian group is the direct product of finitely many cyclic groups.

Subgroups

All subgroups and factor groups of cyclic groups are cyclic. Specifically, the subgroups of **Z** are of the form *m***Z**, with *m* a natural number. All these subgroups are different, and the non-zero ones are all isomorphic to **Z**. The lattice of subgroups of **Z** is isomorphic to the dual of the lattice of natural numbers ordered by divisibility. All factor groups of **Z** are finite, except for the trivial exception **Z** / {0}. For every positive divisor *d* of *n*, the group **Z**/*n***Z** has precisely one subgroup of order *d*, the one generated by the residue class of *n*/*d*. There are no other subgroups. The lattice of subgroups is thus isomorphic to the set of divisors of n, ordered by divisibility.

In particular: a cyclic group is simple if and only if the number of its elements is prime.

As a practical problem, one may be given a finite subgroup C of order n, generated by an element g, and asked to find the size m of the subgroup generated by g^k for some integer k. Here m will be the smallest integer > 0 such that $m.k$ is divisible by n. It is therefore n/a where $a = (k, n)$ is the hcf of k and n. Put another way, the index of the subgroup generated by g^k is a. This reasoning is known as the **index calculus**, in number theory.

Endomorphisms

The endomorphism ring of the abelian group C_n is isomorphic to the ring $\mathbf{Z}/n\mathbf{Z}$. Under this isomorphism, the residue class of r in $\mathbf{Z}/n\mathbf{Z}$ corresponds to the endomorphism of C_n which raises every element to the r-th power. As a consequence, the automorphism group of C_n is isomorphic to the group $(\mathbf{Z}/n\mathbf{Z})^\times$, the group of units of the ring $\mathbf{Z}/n\mathbf{Z}$. This is the group of numbers coprime to n under multiplication modulo n; it has $\varphi(n)$ elements.

Similarly, the endomorphism ring of the infinite cyclic group is isomorphic to the ring $\mathbf{Z}$, and its automorphism group is isomorphic to the group of units of the ring $\mathbf{Z}$, i.e. to $\{-1, +1\} \cong C_2$.

Advanced examples

If n is a positive integer, then $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic if and only if n is 2 or 4 or p^k or 2 p^k for an odd prime number p and $k \geq 1$. The generators of this cyclic group are called primitive roots modulo n.

In particular, the group $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic with p -1 elements for every prime p. More generally, every *finite* subgroup of the multiplicative group of any field is cyclic.

The Galois group of every finite field extension of a finite field is finite and cyclic; conversely, given a finite field F and a finite cyclic group G, there is a finite field extension of F whose Galois group is G.