Cyclic group

From Wikipedia, the free encyclopedia

In group theory, a **cyclic group** is a group that can be generated by a single element, in the sense that the group has an element g (called a "generator" of the group) such that, when written multiplicatively, every element of the group is a power of g (a multiple of g when the notation is additive).

Contents

Definition

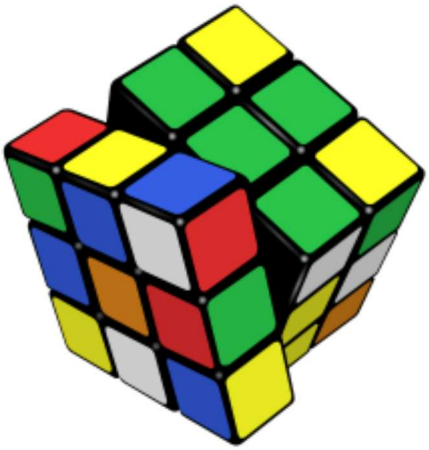
A group G is called cyclic if there exists an element g in G such that $G = \langle g \rangle = \{ g^n \mid n \text{ is an integer} \}$. Since any group generated by an element in a group is a subgroup of that group, showing that the only subgroup of a group G that contains g is G itself suffices to show that G is cyclic.

For example, if $G = \{ g^0, g^1, g^2, g^3, g^4, g^5 \}$ is a group, then $g^6 = g^0$, and G is cyclic. In fact, G is essentially the same as (that is, isomorphic to) the set { 0, 1, 2, 3, 4, 5 } with addition modulo 6. For example, 1 + 2 = 3 (mod 6) corresponds to $g^1 \cdot g^2 = g^3$, and 2 + 5 = 1 (mod 6) corresponds to $g^2 \cdot g^5 = g^7 = g^1$, and so on. One can use the isomorphism φ defined by $\varphi(g^i) = i$.

For every positive integer n there is exactly one cyclic group (up to isomorphism) whose order is n, and there is exactly one infinite cyclic group (the integers under addition). Hence, the cyclic groups are the simplest groups and they are completely classified.

The name "cyclic" may be misleading: it is possible to generate infinitely many elements and not form any literal cycles; that is, every g^n is distinct. (It can be said that it has one infinitely long cycle.) A group

Group theory



Group theory

Basic notions

Subgroup
Normal subgroup
Quotient group
Group homomorphism
(semi-)direct product

Finite groups and classification of finite simple groups

Cyclic group Z_n
Symmetric group, S_n
Dihedral group, D_n
Alternating group A_n
Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24}
Conway groups Co_1, Co_2, Co_3
Janko groups J_1, J_2, J_3, J_4
Fischer groups F_{22}, F_{23}, F_{24}
Baby Monster group B
Monster group M

Discrete groups and lattices

The integers, **Z**
Lattice (group)
Modular groups, PSL(2,**Z**) and SL(2,**Z**)

Topological groups and Lie

generated in this way is called an **infinite cyclic group**, and is isomorphic to the additive group of integers **Z**.

Furthermore, the circle group (whose elements are uncountable) is *not* a cyclic group—a cyclic group always has countable elements.

Since the cyclic groups are abelian, they are often written additively and denoted $\mathbf{Z}_n$. However, this notation can be problematic for number theorists because it conflicts with the usual notation for p-adic number rings or localization at a prime ideal. The quotient notations $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Z}/n$, and $\mathbf{Z}/(n)$ are standard alternatives. We adopt the first of these here to avoid the collision of notation. See also the section Subgroups and notation below.

One may write the group multiplicatively, and denote it by C_n, where n is the order (which can be ∞). For example, $g^3g^4 = g^2$ in C_5, whereas $3 + 4 = 2$ in $\mathbf{Z}/5\mathbf{Z}$.

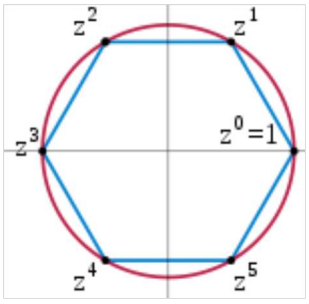
groups

Solenoid (mathematics)
Circle group
General linear group GL(n)
Special linear group SL(n)
Orthogonal group O(n)
Special orthogonal group SO(n)
Unitary group U(n)
Special unitary group SU(n)
Symplectic group Sp(n)

G_2 F_4 E_6 E_7 E_8
Lorentz group
Poincaré group
Conformal group
Diffeomorphism group
Loop group
Infinite-dimensional Lie groups
$O(\infty)$ $SU(\infty)$ $Sp(\infty)$

Properties

The fundamental theorem of cyclic groups states that if G is a cyclic group of order n then every subgroup of G is cyclic. Moreover, the order of any subgroup of G is a divisor of n and for each positive divisor k of n the group G has exactly one subgroup of order k. This property characterizes finite cyclic groups: a group of order n is cyclic if and only if for every divisor d of n the group has at most one subgroup of order d. Sometimes the refined statement is used: a group of order n is cyclic if and only if for every divisor d of n the group has exactly one subgroup of order d.



The six 6th complex roots of unity form a cyclic group under multiplication. z is a primitive element, but z^2 is not, because the odd powers of z are not a power of z^2.

Every finite cyclic group is isomorphic to the group $\{ [0], [1], [2], ..., [n-1] \}$ of integers modulo n under addition, and any infinite cyclic group is isomorphic to **Z** (the set of all integers) under addition. Thus, one only needs to look at such groups to understand the properties of cyclic groups in general. Hence, cyclic groups are one of the simplest groups to study and a number of nice properties are known.

Given a cyclic group G of order n (n may be infinity) and for every g in G,

- G is abelian; that is, their group operation is commutative: $gh = hg$ (for all h in G). This is so since $g + h \bmod n = h + g \bmod n$.
- If n is finite, then $g^n = g^0$ is the identity element of the group, since $kn \bmod n = 0$ for any integer k.
- If $n = \infty$, then there are exactly two elements that generate the group on their own: namely 1 and -1 for **Z**
- If n is finite, then there are exactly $\varphi(n)$ elements that generate the group on their own, where φ is the Euler totient function
- Every subgroup of G is cyclic. Indeed, each finite subgroup of G is a group of $\{ 0, 1, 2, 3, ... m-1\}$ with addition modulo m. And each infinite subgroup of G is $m\mathbf{Z}$ for some m, which is bijective to (so isomorphic to) **Z**.
- G_n is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ (factor group of **Z** over $n\mathbf{Z}$) since $\mathbf{Z}/n\mathbf{Z} = \{0 + n\mathbf{Z}, 1 + n\mathbf{Z}, 2 + n\mathbf{Z}, 3 + n\mathbf{Z}, 4 + n\mathbf{Z}, ..., n - 1 + n\mathbf{Z}\} \cong \{ 0, 1, 2, 3, 4, ..., n-1\}$ under addition modulo n.

More generally, if d is a divisor of n, then the number of elements in $\mathbf{Z}/n$ which have order d is $\varphi(d)$. 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 or $\mathbf{Z}/p\mathbf{Z}$. There are more numbers with the same property, see cyclic number.

The direct product of two cyclic groups $\mathbf{Z}/n\mathbf{Z}$ and $\mathbf{Z}/m\mathbf{Z}$ is cyclic if and only if n and m are coprime. Thus e.g. $\mathbf{Z}/12\mathbf{Z}$ is the direct product of $\mathbf{Z}/3\mathbf{Z}$ and $\mathbf{Z}/4\mathbf{Z}$, but not the direct product of $\mathbf{Z}/6\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z}$.

The definition immediately implies that cyclic groups have very simple group presentation $C_\infty = < x \mid >$ and $C_n = < x \mid x^n >$ for finite n.

A primary cyclic group is a group of the form $\mathbf{Z}/p^k\mathbf{Z}$ where p is a prime number. The fundamental theorem of abelian groups states that every finitely generated abelian group is the direct product of finitely many finite primary cyclic and infinite cyclic groups.

$\mathbf{Z}/n\mathbf{Z}$ and $\mathbf{Z}$ are also commutative rings. If p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ is a finite field, also denoted by $\mathbf{F}_p$ or $\mathbf{GF}(p)$. Every field with p elements is isomorphic to this one.

The units of the ring $\mathbf{Z}/n\mathbf{Z}$ are the numbers coprime to n. They form a group under multiplication modulo n with $\varphi(n)$ elements (see above). It is written as $(\mathbf{Z}/n\mathbf{Z})^\times$. For example, when $n = 6$, we get $(\mathbf{Z}/n\mathbf{Z})^\times = \{1,5\}$. When $n = 8$, we get $(\mathbf{Z}/n\mathbf{Z})^\times = \{1,3,5,7\}$.

In fact, it is known that $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic if and only if n is 1 or 2 or 4 or p^k or 2 p^k for an odd prime number p and $k \geq 1$, in which case every generator of $(\mathbf{Z}/n\mathbf{Z})^\times$ is called a primitive root modulo n. Thus, $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic for $n = 6$, but not for $n = 8$, where it is instead isomorphic to the Klein four-group.

The group $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic with $p - 1$ elements for every prime p, and is also written $(\mathbf{Z}/p\mathbf{Z})^*$ because it consists of the non-zero elements. More generally, every *finite* subgroup of the multiplicative group of any field is cyclic.

Examples

In 2D and 3D the symmetry group for n-fold rotational symmetry is C_n, of abstract group type Z_n. In 3D there are also other symmetry groups which are algebraically the same, see *Symmetry groups in 3D that are cyclic as abstract group*.

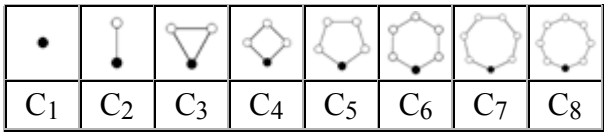
Note that the group S^1 of all rotations of a circle (the circle group) is *not* cyclic, since it is not even countable.

The n^{th} roots of unity form a cyclic group of order n under multiplication. e.g.,
$0 = z^3 - 1 = (z - s^0)(z - s^1)(z - s^2)$ where $s^i = e^{2\pi i / 3}$ and a group of $\{s^0,s^1,s^2\}$ under multiplication 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.

Representation

The cycle graphs of finite cyclic groups are all n-sided polygons with the elements at the vertices. The dark vertex in the cycle graphs below stand for the identity element, and the other vertices are the other elements of the group. A cycle consists of successive powers of either of the elements connected to the identity element.



The representation theory of the cyclic group is a critical base case for the representation theory of more general finite groups. In the complex case, a representation of a cyclic group decomposes into a direct sum of linear characters, making the connection between character theory and representation theory transparent. In the positive characteristic case, the indecomposable representations of the cyclic group form a model and inductive basis for the representation theory of groups with cyclic Sylow subgroups and more generally the representation theory of blocks of cyclic defect.

Subgroups and notation

All subgroups and quotient groups of cyclic groups are cyclic. Specifically, all subgroups of $\mathbf{Z}$ are of the form $m\mathbf{Z}$, with m an integer ≥ 0. All of these subgroups are different, and apart from the trivial group (for $m=0$) all are isomorphic to $\mathbf{Z}$. The lattice of subgroups of $\mathbf{Z}$ is isomorphic to the dual of the lattice of natural numbers ordered by divisibility. All factor groups of $\mathbf{Z}$ are finite, except for the trivial exception $\mathbf{Z}/\{0\} = \mathbf{Z}/0\mathbf{Z}$. For every positive divisor d of n, the quotient group $\mathbf{Z}/n\mathbf{Z}$ 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 its order (the number of its elements) is prime.[1]

Using the quotient group formalism, $\mathbf{Z}/n\mathbf{Z}$ is a standard notation for the additive cyclic group with n elements. In ring terminology, the subgroup $n\mathbf{Z}$ is also the ideal (n), so the quotient can also be written $\mathbf{Z}/(n)$ or $\mathbf{Z}/n$ without abuse of notation. These alternatives do not conflict with the notation for the p-adic integers. The last form is very common in informal calculations; it has the additional advantage that it reads the same way that the group or ring is often described verbally, "Zee mod en".

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 mk is divisible by n. It is therefore n/m where $m = (k, n)$ is the greatest common divisor of k and n. Put another way, the index of the subgroup generated by g^k is m. This reasoning is known as the **index calculus algorithm**, in number theory.

Endomorphisms

The endomorphism ring of the abelian group $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ itself as a ring. Under this isomorphism, the number r corresponds to the endomorphism of $\mathbf{Z}/n\mathbf{Z}$ that maps each element to the sum of r copies of it. This is a bijection if and only if r is coprime with n, so the automorphism group of $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to the unit group $(\mathbf{Z}/n\mathbf{Z})^\times$ (see above).

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

Virtually cyclic groups

A group is called **virtually cyclic** if it contains a cyclic subgroup of finite index (the number of cosets that the subgroup has). In other words, any element in a virtually cyclic group can be arrived at by applying a member of the cyclic subgroup to a member in a certain finite set. Every cyclic group is virtually cyclic, as is every finite group. It is known that a finitely generated discrete group with exactly two *ends* is virtually cyclic (for instance the product of $\mathbf{Z}/n$ and $\mathbf{Z}$). Every abelian subgroup of a Gromov hyperbolic group is virtually cyclic.

See also

- Cyclic extension
- Cyclic module
- Modular arithmetic
- Locally cyclic group, a group in which each finitely generated subgroup is cyclic

External links

- An introduction to cyclic groups (http://members.tripod.com/~dogschool/cyclic.html)

Notes

1. ^ Gannon (2006), p. 18 (http://books.google.com/books?id=ehrUt21SnsoC&pg=PA18&dq=%22Zn+is+simple+iff+n+is+prime%22)

References

- Gallian, Joseph (1998), *Contemporary abstract algebra* (4th ed.), Boston: Houghton Mifflin, ISBN 978-0-669-86179-2, especially chapter 4.
- Herstein, I. N. (1996), *Abstract algebra* (3rd ed.), Prentice Hall, ISBN 978-0-13-374562-7, MR1375019 (http://www.ams.org/mathscinet-getitem?mr=1375019) , especially pages 53–60.
- Gannon, Terry (2006), *Moonshine beyond the monster: the bridge connecting algebra, modular forms and physics*, Cambridge monographs on mathematical physics, Cambridge University Press, ISBN 9780521835312

Retrieved from "http://en.wikipedia.org/wiki/Cyclic_group"
Categories: Abelian group theory | Finite groups | Properties of groups

- This page was last modified on 5 April 2011 at 11:15.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of Use for details.
Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.