Ministry of Higher Education
and Scientific Research

University of Maysan
college of Education
Mathematics department

عنوان التقرير :

Cyclic group and its subgroups

اشراف الاستاذ :
مرتضى علي العلاق

2019
-
2020

اعداد الطالبة:

زينب اباذر محمد

الدراسة: المسائية

Introduction

In group theory, a branch of abstract algebra, a cyclic group or monogenous group is a group that is generated by a single element.[l] That is, it is a set of invertible elements with a single associative binary operation, and it contains an element g such that every other element of the group may be obtained by repeatedly applying the group operation to g or its inverse. Each element can be written as a power of g in ,multiplicative notation
or as a multiple of g in additive notation. This element g is called a generator of the group.[l]

,Every infinite cyclic group is isomorphic to the additive group of Z
,the integers. Every finite cyclic group of order n is isomorphic to the additive group of Z/nZ
the integers modulo n. Every cyclic group is an abelian group (meaning that its group operation is .commutative), and every finitely generated abelian group is a direct product of cyclic groups

Every cyclic group of prime order is a simple group which cannot be broken ,down into smaller groups. In the classification of finite simple groups

which cannot be broken down into smaller groups. In the classification of finite simple groups, one of the three infinite classes consists of the cyclic groups of prime order. The cyclic groups of prime order are thus among the building blocks from which all groups can be built.

Cyclic Groups

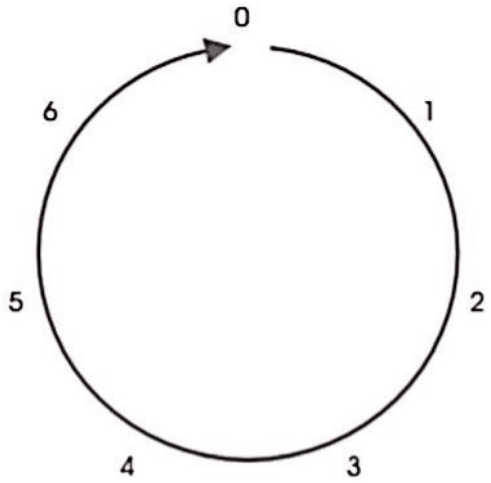
Cyclic groups are groups in which every element is a power of some fixed element
. (If the group is abelian and I 'm using + as the operation,
then I should say instead that every element is a multiple of some fixed element.)
Here are the relevant definitions.
Definition. Let G be a group, g ∈ G.
The order of g is the smallest positive integer n such that gn = I.
If there is no positive integer n such that gn = I, then g has infinite order.
In the case of an abelian group with + as the operation and ·
as the identity, the order of g is the smallest positive integer n such that ng = ·.
Definition. If G is a group and g ∈ G, then the subgroup generated by g is ⟨g⟩={gn In∈Z}.
If the group is abelian and I 'm using + as the operation, then ⟨g⟩ = {ng I n ∈ Z}.

Example. (The integers and the integers mod n are cyclic) Show that Z and Zn for n › · are cyclic.

Z is an infinite cyclic group, because every element is a multiple of I (or of –I).
For instance, IIV = IIV·I.
(Remember that "IIV · I" is really shorthand for I + I + · · · + I — I added to itself IIV times.)
In fact, it is the only infinite cyclic group up to isomorphism.
Notice that a cyclic group can have more than one generator.
If n is a positive integer, Zn is a cyclic group of order n generated by I.
For example, I generates ZV, since

1+1=2
1+1+1=3
1+1+1+1=4
1+1+1+1+1=5
1+1+1+1+1+1=6
1+1+1+1+1+1+1=0

In other words, if you add I to itself repeatedly, you eventually cycle back to ·.



a cyclic group of order 7

3+3=6

3+3+3=2

3+3+3+3=5

3+3+3+3+3=1

3+3+3+3+3+3=4

3+3+3+3+3+3+3=0

The “same” group can be written using multiplicative notation this way: Z7 ={1,a,a2,a3,a4,a5,a6}.

In this form, a is a generator of Z7.

It turns out that in Z7 = {0, 1, 2, 3, 4, 5, 6}, every nonzero element generates the group.

On the other hand, in Z6 = {0, 1, 2, 3, 4, 5}, only 1 and 5 generate

Lemma . Let G = ⟨g⟩ be a finite cyclic group, where g has order n. Then the powers {1, g, . . . , gn−1} are distinct.

proof . Since g has order n, g, g2, . . . gn−1 are all different from 1.

Now I'll show that the powers {1,g,...,gn−1} are distinct. Suppose gi = gj where 0 ≤ j ⟨ i ⟨ n. Then

0 ⟨ i − j ⟨ n and gi−j = 1, contrary to the preceding observation. Therefore, the powers {1, g, . . . , gn−1} are distinct.

Lemma: Let $G = \langle g \rangle$ be infinite cyclic. If m and n are integers and $m \neq n$, then $g^m \neq g^n$.

proof: One of m, n is larger — suppose without loss of generality that $m > n$. I want to show that $g^m \neq g^n$; suppose this is false, so $g^m = g^n$. Then $g^{m-n} = 1$, so g has finite order. This contradicts the fact that a generator of an infinite cyclic group has infinite order. Therefore, $g^m \neq g^n$. The next result characterizes subgroups of cyclic groups. The proof uses the Division Algorithm for integers in an important way.

Theorem: Subgroups of cyclic groups are cyclic.

Proof: Let $G = \langle g \rangle$ be a cyclic group, where $g \in G$. Let $H < G$. If $H = \{1\}$, then H is cyclic with generator 1. So assume $H \neq \{1\}$

Example. (Subgroups of the integers) Describe the subgroups of Z.

Every subgroup of Z has the form nZ for $n \in Z$.
For example, here is the subgroup generated by 13:
$13Z = \langle 13 \rangle = \{\ldots -26, -13, 0, 13, 26, \ldots\}$.

Proposition.

Let G = ⟨g⟩ be a cyclic group of order n, and let m < n. Then g has order n/ (m, n)

Remark:

Note that the order of gm (the element) is the same as the order of ⟨gm⟩ (the subgroup).

proof:

Since (m, n) divides m, it follows that m/(m,n) is an integer.

Therefore, n divides mn/(m,n) and by the last lemma.

Example. (Finding the order of an element) Find the order of the element a32 in the cyclic group

G= {1, a, a2, . . . a37}.

(Thus, G is cyclic of order 38 with generator a.)

In the notation of the Proposition, n = 38 and m = 32.

Since (38, 32) = 2, it follows that a32 has order 38/2=19

Example. (Finding the order of an element) Find the order of the element 18 ∈ Z30.

In this case, I'm using additive notation instead of multiplicative notation. The group is cyclic with order n = 30, and the element 18 ∈ Z30 corresponds to a18 in the Proposition — so m = 18.

18,30)=6, so the order of of 18 is 30/6=5

Subgroups

All subgroups and quotient groups of cyclic groups ,are cyclic. Specifically, all subgroups of Z are of the form ⟨m⟩ = mZ with m a positive integer. All of these subgroups are distinct ,from each other, and apart from the trivial group {0} = 0Z they all are isomorphic to Z. The lattice of subgroups of Z is isomorphic to the dual of the lattice of natural numbers ordered by divisibility.[10] Thus, since a prime number p has no nontrivial divisors, pZ is a maximal proper subgroup, and the quotient group Z/pZ is simple; in fact, a cyclic group is simple if and only if its order is prime.[11]

All quotient groups Z/nZ are finite, with the exception Z/0Z = Z/{0}. For every positive divisor d of n, the quotient group Z/nZ has precisely one subgroup of order d, generated .by the residue class of n/d. There are no other subgroups

Additional properties

Every cyclic group is abelian.[1] That is, its group .operation is commutative: gh = hg (for all g and h in G) This is clear for the groups of integer and modular addition since r + s ≡ s + r (mod n), and it follows for all cyclic groups since they are all isomorphic to these ,standard groups. For a finite cyclic group of order n .gn is the identity element for any element g This again follows by using the isomorphism to modular addition, since kn ≡ 0 (mod n) for every integer k. (This is also true for a general group of order n, due to Lagrange's theorem.)

For a prime power pk, the group Z/pkZ is called a primary cyclic group. The fundamental theorem of abelian groups states that every finitely generated abelian group is a finite .direct product of primary cyclic and infinite cyclic groups

Because a cyclic group is abelian, each of its conjugacy classes consists of a single element. A cyclic group of order n

Tensor product and Hom of cyclic groups

The tensor product $Z/mZ \otimes Z/nZ$ can be shown to be isomorphic to $Z / \gcd(m, n)Z$. So we can form the collection of group homomorphisms from Z/mZ to Z/nZ, denoted $\hom(Z/mZ, Z/nZ)$, which is itself a group.

For the tensor product, this is a consequence of the general fact that $R/I \otimes_R R/J \cong R/(I + J)$, where R is a commutative ring with unit and I and J are ideals of the ring. For the Hom group, recall that it is isomorphic to the subgroup of Z / nZ consisting of the elements of order dividing m. That subgroup is cyclic of order $\gcd(m, n)$, which completes the proof.

Related classes of groups

Several other classes of groups have been defined by their relation to the cyclic groups:

1-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. An infinite group is virtually cyclic if and only if it is finitely generated and has exactly two ends; an example of such a group is the direct product of Z/nZ and Z, in which the factor Z has finite index n. Every abelian subgroup of a Gromov hyperbolic group is virtually cyclic.

2-Locally cyclic groups

A locally cyclic group is a group in which each finitely generated subgroup is cyclic. An example is the additive group of the rational numbers: every finite set of rational numbers is a set of integer multiples of a single unit fraction, the inverse of their lowest common denominator, and generates as a subgroup a cyclic group of integer multiples of this unit fraction. A group is locally cyclic if and only if its lattice of subgroups is a distributive lattice.

3-Cyclically ordered groups

A cyclically ordered group is a group together with a cyclic order preserved by the group structure. Every cyclic group can be given a structure as a cyclically ordered group, consistent with the ordering of the integers (or the integers modulo the order of the group). Every finite subgroup of a cyclically ordered group is cyclic

4-Metacyclic and polycyclic groups

A metacyclic group is a group containing a cyclic normal subgroup whose quotient is also cyclic.These groups include the cyclic groups, the dicyclic groups, and the direct products of two cyclic groups. The polycyclic groups generalize metacyclic groups by allowing more than one level of group extension. A group is polycyclic if it has a finite descending sequence of subgroups, each of which is normal in the previous subgroup with a cyclic quotient, ending in the trivial group. Every finitely generated abelian group or nilpotent group is polycyclic.

Conclusion

A cyclic group is a group which is equal to one of its cyclic subgroups: $G = \langle g \rangle$ for some element g, called a generator.

For a finite cyclic group G of order n we have $G = \{e, g, g2, \ldots, gn-1\}$, where e is the identity element and $gi = gj$ whenever $i \equiv j \pmod{n}$; in particular $gn = g0 = e$, and $g-1 = gn-1$. An abstract group defined by this multiplication is often denoted Cn, and we say that G is isomorphic to the standard cyclic group Cn. Such a group is also isomorphic to Z/nZ, the group of integers modulo n with the addition operation, which is the standard cyclic group in additive notation. Under the isomorphism χ defined by $\chi(gi) = i$ the identity element e corresponds to 0, products correspond to sums, and powers correspond to multiples.

Summary

1-A group is called monogenous if it admits a system of generators consisting of a single element. A finite monogenous group is called cyclic.

2-This implication remains true even if only prime values of n are considered. (And observe that when n is prime, there is exactly one element whose order is a proper divisor of n, namely the identity.)

3-If G has two ends, the explicit structure of G is well known: G is an extension of a finite group by either the infinite cyclic group or the infinite dihedral group

References

1- Alonso, J. M.; et al. (1991), "Notes on word hyperbolic groups", Group theory from a geometrical viewpoint (Trieste, 1990)

2- Alspach, Brian (1997), "Isomorphism and Cayley graphs on abelian groups", Graph symmetry (Montreal, PQ, 1996)

3- Aluffi, Paolo (2009), "6.4 Example: Subgroups of Cyclic Groups", Algebra, Chapter 0, Graduate Studies in ,Mathematics, 104, American Mathematical Society

4- ,Bourbaki, Nicolas (1998-08-03) [1970] Algebra I: Chapters 1-3, Elements of Mathematics

5- ,Coxeter, H. S. M.; Moser, W. O. J. (1980) ,Generators and Relations for Discrete Groups ,New York: Springer-Verlag, p. 1

6- ,Rotman, Joseph J. (1998), Galois Theory Universitext, Springer, Theorem 62, p. 65