SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT – III – DISCRETE MATHEMATICS – SMTA 1302

GROUP THEORY

Course Contents: Groups – Properties of groups – Semi group and Monoid (definition and examples only) – Subgroups, Cosets – Lagranges Theorem

Binary Operations

Definition

Let S be a set. A **binary operation** on S is a mapping $*: S \times S \to S$,

which we will usually denote by $*(a, b) = a * b$.

Also, we've written $*$ as a **function** from $S \times S$ to S, which means two things in particular:

1. The operation $*$ is **well-defined**: given $a, b \in S$, there is exactly one $c \in S$ such that $a * b = c$. In other words, the operation is defined for *all* ordered pairs, and there is no ambiguity in the meaning of $a * b$.
2. S is **closed** under $*$: for all $a, b \in S$, $a * b$ is again in S.

Example

Here are some examples of binary operations.

- Addition and multiplication on Z are binary operations.
- Addition and multiplication on Z_n are binary operations.
- Addition and multiplication on $M_n(R)$ are binary operations.

- The following are non -examples.
- Define $*$ on R by $a * b = a/b$. This is not a binary operation, since it is not defined everywhere. In particular, $a * b$ is undefined whenever $b = 0$.
- Define $*$ on R by $a * b = c$, where c is some number larger than $a + b$. This is not well-defined, since it is not clear exactly what $a * b$ should be. This sort of operation is fairly silly, and we will rarely encounter such things in the wild. It's more likely that the given set is not closed under the operation.
- Matrix multiplication *is* a binary operation on $GL_n(R)$. Recall from linear algebra that the determinant is multiplicative, in the sense that

$$\det(AB) = \det(A)\det(B).$$

Properties of binary operation

i) A binary operation $*$ on a set S is **commutative** if

$$a * b = b * a \text{ for all } a, b \in S.$$

Example

Let's ask whether some of our known examples of binary operations are actually commutative.

1. + and $\cdot$ on Z and Z_n are commutative.

2. Matrix multiplication is not commutative (on both $M_n(R)$ and $GL_n(R)$).

ii) A binary operation $*$ on a set S is **associative** if

$$(a * b) * c = a * (b * c) \text{ for all } a, b, c \in S.$$

Example

The following are examples of associative (and non- associative) binary operations.

1. + and $\cdot$ on Z (and Z_n) are associative.
2. Matrix multiplication is associative.
3. Subtraction on Z is a binary operation, but it is not associative. For example,

$$(3 - 5) - 1 = -2 - 1 = -3,$$

$$\text{While } 3 - (5 - 1) = 3 - 4 = -1.$$

4. The **cross product** on R^3 is a binary operation, since it combines two vectors to produce a new vector. However, it is not associative, since

$$a \times (b \times c) = (a \times b) \times c - b \times (c \times a).$$

5. (Composition of functions) Let S be a set, and define

$$F(S) = \{\text{functions } f : S \longrightarrow S\}.$$

if $f, g, h \in F(S)$, then $(f \circ g) \circ h = f \circ (g \circ h)$. To show that two functions are equal, we need to show that their values at any element $x \in S$ are equal.
For any $x \in S$, we have

$$(f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x))) \text{ and}$$

$$f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x)))$$

In other words, $(f \circ g) \circ h(x) = f \circ (g \circ h)(x)$ for all $x \in S$,
so $(f \circ g) \circ h = f \circ (g \circ h)$, and composition of functions is associative.

Groups

A **group** is a set G together with a binary operation $*$: $G \times G \to G$ satisfying

Closure:

For all $a, b \in G$, we have $a * b \in G$

Associativity:

For all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$.

Identity:

There exists an element $e \in G$ with the property that

$$e * a = a * e = a \text{ for all } a \in G.$$

Inverses:

For every $a \in G$, there is an element $a^{-1} \in G$ with the property that

$$a * a^{-1} = a^{-1} * a = e.$$

Example

Here are some examples of groups and not a group

1. $(\mathbb{Z}, +)$ is a group, as we have already seen.
2. $(M_n(\mathbb{R}), +)$ is a group.
3. $(\mathbb{Z}_n, +_n)$ is a group.
4. $(\mathbb{Z}, \cdot)$ is *not* a group, since inverses do not always exist. However, $(\{1, -1\}, \cdot)$ is a group. We do need to be careful here—the restriction of a binary oper- ation to a smaller set need not be a binary operation, since the set may not be closed under the operation. However, $\{1, -1\}$ is definitely closed under multiplication, so we indeed have a group.
5. $(M_n(\mathbb{R}), \cdot)$ is not a group, since inverses fail. However, $(GL_n(\mathbb{R}), \cdot)$ is a group. We already saw that it is closed, and the other axioms hold as well.
6. $(\mathbb{Z}_n, \cdot_n)$ is not a group, again because inverses fail. However, $(\mathbb{Z}_n^\times, \cdot_n)$ will be a group. Again, we just need to verify closure: if $a, b \in \mathbb{Z}_n^\times$, then a and b are both relatively prime to n. But then neither a nor b shares any prime divisors with n, so ab is also relatively prime to n. Thus $ab \in \mathbb{Z}_n^\times$.

Definition

A group $(G, *)$ is said to be **abelian** if $*$ is commutative, i.e.

$$a * b = b * a$$

for all $a, b \in G$. If a group is not commutative, we'll say that it is **nonabelian**.

Definition

The **order** of a group G, denoted by $|G|$, is the number of elements in G.

If a group G has infinitely many elements, we will write $|G| = \infty$.[3]

Definition

A group G is said to be **finite** if $|G| < \infty$.

Example

For any n, the additive group Z_n is a finite group, with

$|Z_n| = n$.

Cayley Tables

One of the things that makes finite groups easier to handle is that we can write down a table that completely describes the group. We list the elements out and multiply "row by column."

Example

Let's look at Z_3, for example. We'll write down a "multiplication table" that tells us how the group operation works for any pair of elements. As we mentioned, each entry is computed as "row times column":

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

(Of course we have to remember that "times" really means "plus" in this example.) This is called a **group table** (or a **Cayley table**).

Exercise

Show that any group of order 4 is abelian. [Hint: Compute all possible Cayley tables. Up to a reordering of the elements, there are two possible tables.]

Exercise

Show that any group of order 5 is abelian. [Hint: There is only one possible Cayley table, up to relabeling.

Basic Properties of Groups

Property.1

Let G be a group. The identity element $e \in G$ is unique, *i.e., there is only one element e of G with the property that $ae = ea = a$ for all $a \in G$.*

Proof

For this proof, we need to use the standard mathematical trick for proving uniqueness: we assume that there is another gadget that behaves like the one in which we're interested, and we prove that the two actually have to be the same.
Suppose there is another $f \in G$ with the property that

for all $a \in G$. Then in particular, $af = fa = a$

But since e is an identity, Therefore $ef = fe = e$Since e is unique, $f.e = e.f = f$.

Property.2.

(Cancellation laws)**.** *Let G be a group, and let a, b, c ∈ G. Then:*

(a) *If a*b = b*c, then b = c.*

(b) *If b*a = c*a, then b = c.*

Proof. (a) Suppose that $ab = ac$. Multiply both sides on the left by a^{-1}:

$$a^{-1}(ab) = a^{-1}(ac).$$

By associativity, this is the same as

$$(a^{-1}a)b = (a^{-1}a)c,$$

and since $a^{-1}a = e$, we have $eb = ec$

Since e is the identity, $b = c$. The same sort of argument works for (b), except we multiply the equation on the right by a^{-1}.

The cancellation laws actually give us a very useful corollary. You may have already guessed that this result holds, but we will prove here that inverses in a group are unique.

Property 3.

Let G be a group. Every a ∈ G has a unique *inverse, i.e. to each*

a ∈ G there is exactly one element a^{-1} *with the property that*

$$aa^{-1} = a^{-1}a = e.$$

Proof. Let $a \in G$, and suppose that $b \in G$ has the property that $ab = ba = e$. Then in particular,

$$ab = e = aa^{-1},$$

and by cancellation, $b = a^{-1}$. Thus a^{-1} is unique.

Property 4.

If $a \in G$, then $(a^{-1})^{-1} = a$.

Proof. By definition, $a^{-1}(a^{-1})^{-1} = e$. But $a^{-1}a = aa^{-1} = e$ as well, so by unique-ness of inverses, $(a^{-1})^{-1} = a$.

Property 5.

For any $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. We'll explicitly show that $b^{-1}a^{-1}$ is the inverse of ab by computing:

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= ((ab)b^{-1})a^{-1} \\ &= (a(bb^{-1}))a^{-1} \\ &= (ae)a^{-1} \\ &= aa^{-1} \\ &= e.\end{aligned}$$

Of course we also need to check that $(b^{-1}a^{-1})(ab) = e$, which works pretty much the same way:

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}(ab)) \\ &= b^{-1}((a^{-1}a)b) \\ &= b^{-1}(eb) \\ &= b^{-1}b \\ &= e.\end{aligned}$$

Thus $(ab)^{-1} = b^{-1}a^{-1}$.

Property. 6. *The equations $ax = b$ and $xa = b$ have unique solutions in G.*

Proof. The solution to $ax = b$ is $x = a^{-1}b$, and for $xa = b$ it is $x = ba^{-1}$. These are unique since inverses are unique.

Property.7. *Let G be a group, and let $a, b \in G$. If either $ab = e$ or $ba = e$, then $b = a^{-1}$.*

Proof. This really amounts to solving the equation $ax = e$ (or $xa = e$). We know from Proposition5, that there is a unique solution, namely $x = a^{-1}e = a^{-1}$ (in either case). Therefore, if $ab = e$ or $ba = e$, then b is a solution to either $ax = e$ or $xa = e$, so $b = a^{-1}$.

Exercise

Prove that if G is a group and $a, b \in G$ with $ab = a$, then $b = e$.

The Order of an Element and Cyclic Groups

Let G be a group. We say that an element $a \in G$ has **finite order** if there exists $n \in Z^+$ such that $a^n = e$. The smallest such integer is called the **order** of a, denoted by $o(a)$ (or $|a|$). If no such integer exists, we say that a has **infinite order**.

Example.1

The identity element in any group has order 1.

Example.2

2. In Z_{12}, we see that $o(2) = 6$ and $o(3) = 4$.

We'll calculate the powers of 2 first:

$1 \cdot 2 = 2$
$2 \cdot 2 = 2 +_{12} 2 = 4$
$3 \cdot 2 = 2 +_{12} 2 +_{12} 2 = 6$
$4 \cdot 2 = 8$
$5 \cdot 2 = 10$
$6 \cdot 2 = [12]_{12} = 0$
$7 \cdot 2 = [14]_{12} = 2$
$8 \cdot 2 = [16]_{12} = 4$

and so on. What about powers of 3?

$1 \cdot 3 = 3$
$2 \cdot 3 = 3 +_{12} 3 = 6$
$3 \cdot 3 = 3 +_{12} 3 +_{12} 3 = 9$
$4 \cdot 3 = [12]_{12} = 0$
$5 \cdot 3 = [15]_{12} = 3$
$6 \cdot 3 = [18]_{12} = 6$

and so on. Notice that the lists repeat after a while. In particular, we reach 0 (i.e., the identity) after a certain point. We quantify this phenomenon by saying that these elements have **finite order**.

Proposition

Let G be a finite group. Then every element $a \in G$ has finite order.

Proof. Consider the set $\{a^n : n \geq 0\} = \{e, a, a^2, \ldots\}$. Since G is finite, this list of powers can't be infinite. (This follows from the Pigeon- hole principle, for instance. We have an infinite list of group elements that need to fit into only finitely many slots.) Therefore, two different powers of a must coincide, say $a^i = a^j$, with $j \neq i$. We can assume that $j > i$. Then

$$a^{j-i} = a^j a^{-i} = a^i a^{-i} = e,$$

so a has finite order. (In particular, $o(a) \leq j - i$.) Since $a \in G$ was arbitrary, the result follows.

Let's get on with proving some facts about order. First, we'll relate the order of an element to that of its inverse.

Proposition

Let G be a group and let $a \in G$. Then $o(a) = o(a^{-1})$.

Proof. Suppose first that a has finite order, with $o(a) = n$. Then

$$(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e,$$

so $o(a^{-1}) \leq n = o(a)$. On the other hand, if we let $m = o(a^{-1})$, then

$$a^m = ((a^{-1})^{-1})^m = (a^{-1})^{-m} = ((a^{-1})^m)^{-1} = e,$$

so $n \leq m$. Thus $n = m$, or $o(a) = o(a^{-1})$.

Now suppose that a has infinite order. Then for all $n \in \mathbb{Z}^+$, we have $a^n \neq e$.
But then

$$(a^{-1})^n = a^{-n} = (a^n)^{-1} \neq e$$

for all $n \in \mathbb{Z}^+$, so a^{-1} must have infinite order as well.

Let's continue with our investigation of basic properties of order. The first one says that the only integers m for which $a^m = e$ are the multiples of $o(a)$.

Proposition

If $o(a) = n$ and $m \in \mathbb{Z}$, then $a^m = e$ if and only if n divides

m.

Proof. If $n \mid m$, it is easy. Write $m = nd$ for some $d \in \mathbb{Z}$. Then

$$a^m = a^{nd} = (a^n)^d = e^d = e.$$

On the other hand, if $m \geq n$, we can use the Division Algorithm to write

$m = qn + r$ with $0 \leq r < n$. Then

$$e = a^m = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = ea^r = a^r,$$

so $a^r = e$. But $r < n$, and n is the smallest positive power of a which yields the identity. Therefore r must be 0, and n divides m.

Note that this tells us something more general about powers of a: when we proved that elements of finite groups have finite order, we saw that $a^i = a^j$ implied that $a^{j-i} = e$. This means that $n = o(a)$ divides $j - i$. In other words, i and j must be congruent mod n.

Proposition

Let G be a group, $a \in G$ an element of finite order n. Then

$a^i = a^j$ *if and only if* $i \equiv j (\mathrm{mod} n)$.

Along the same lines, we observed that if $a^i = a^j$ with $j > i$, then $a^{j-i} = e$, so a has to have finite order. Taking the contrapositive of this statement, we get the following result.

Cyclic Groups

Let's take a few steps back now and look at the bigger picture. That is, we want to investigate the structure of the set (a) for $a \in G$. What do you notice about it?

- **Closure:** $a^i a^j = a^{i+j} \in (a)$ for all $i, j \in \mathbb{Z}$.
- **Identity:** $e = a^0 \in (a)$
- **Inverses:** Since $(a^j)^{-1} = a^{-j}$, we have $(a^j)^{-1} \in (a)$ for all $j \in \mathbb{Z}$.

It other words, (a) is itself a group. That is, the set of all powers of a group element is a group in its own right. We will investigate these sorts of objects further in the next section, but let's make the following definition now anyway.

Definition

For $a \in G$, the set (a) is called the **cyclic subgroup** generated by a.

For now, let's look at a particular situation. Is G ever a cyclic subgroup of itself? That is, can a "generate" the whole group G? Yes, this does happen some times, and such groups are quite special.

Definition

A group G is called **cyclic** if $G = (a)$ for some $a \in G$. The element a is called a **generator** for G.

Example

1. One of our first examples of a group is actually a cyclic one: Z forms a cyclic group under addition. What is a generator for Z? Both 1 and −1 generate it, since every integer $n \in \mathbb{Z}$ can be written as a "power" of 1 (or −1):

   These are actually the only two generators.

2. How about a finite cyclic group? For any n, $\mathbb{Z}_n$ is cyclic, and 1 is a generator in much the same way that 1 generates Z. There are actually plenty of other generators, and we can characterize them by using our knowledge of greatest common divisors. We'll postpone this until we've made a couple of statements regarding cyclic groups.

3. The group (Q, +) is not cyclic. (This is proven in Saracino.)

4. The dihedral group D_3 is not cyclic. The rotations all have order 3, so

$$(r_1) = (r_2) = \{i, r_1, r_2\}.$$

On the other hand, all of the reflections have order 2, so

$$(m_1) = \{i, m_1\}, \quad (m_2) = \{i, m_2\}, (m_3) = \{i, m_3\}.$$

Now let's start making some observations regarding cyclic groups. First, if $G = (a)$ is cyclic, how big is it? It turns out that our overloading of the word "order" was fairly appropriate after all, for $|G| = o(a)$.

Theorem

If $G = (a)$ is cyclic, then $|G| = o(a)$.

Proof. If a has infinite order, then $|G|$ must be infinite. On the other hand, if $o(a) = n$, then we know that $a^i = a^j$ if and only if $i \equiv j \bmod n$, so the elements of G are $\{e, a, a^2, \ldots, a^{n-1}\}$ of which there are $n = o(a)$.

If we pair this result with Theorem, we can characterize the generators of any finite cyclic group.

Proposition

Let G be a finite cyclic group. Then for any $b \in G$, we have

$o(b) \mid |G|$.

Theorem 1.

Every cyclic group is abelian.

Proof. Let G be a cyclic group and let a be a generator for G, i.e. $G = (a)$. Then given two elements $x, y \in G$, we must have $x = a^i$ and $y = a^j$ for some $i, j \in \mathbb{Z}$. Then

$$xy = a^i a^j = a^{i+j} = a^{j+i} = a^j a^i = yx,$$

and it follows that G is abelian.

Remark

The converse to Theorem1 is not true. That is, there are abelian groups that are not cyclic. Saracino gives the example of the non-cyclic group (Q, +). However, this is a good place to introduce a different group—the **Klein 4-group**, denoted V_4. The Klein 4-group is an abelian group of order 4. It has elements $V_4 = \{e, a, b, c\}$, with

$$a^2 = b^2 = c^2 = e \text{ and } ab = c,\ bc = a,\ ca = b.$$

Note that it is abelian by a previous exercise (Exercise 2.1).[8] However, it is not cyclic, since every element has order 2 (except for the identity, of course). If it were cyclic, there would necessarily be an element of order 4.

Subgroups

Let $(G, *)$ be a group. A **subgroup** of G is a nonempty subset

$H \subseteq G$ with the property that $(H, *)$ is a group.

Note that in order for H to be a subgroup of G, H needs to be a group with respect to the operation that it inherits from G. That is, H and G *always* carry the same binary operation. Also, we'll write

$$H \leq G$$

to denote that H is a subgroup of G. Finally, if we want to emphasize that $H \leq G$ but $H \neq G$, we will say that H is a **proper** subgroup of G.

le

Let's look at the group Z (under addition, of course). Define 2Z = {even integers} = $\{2n : n \in \mathbb{Z}\}$. Is 2Z a subgroup of Z? We need to check that 2Z itself forms a group under addition:

- **Closure:** If $a, b \in 2\mathbb{Z}$, then $a = 2n$ and $b = 2m$ for some $n, m \in \mathbb{Z}$. Then $a + b = 2n + 2m = 2(n + m) \in 2\mathbb{Z}$, so 2Z is indeed closed under addition.
- **Associativity:** Z is already associative, so nothing changes when we pass to a subset of Z.
- **Identity:** The identity for addition on Z is 0, which is even: $0 = 2 \cdot 0 \in 2\mathbb{Z}$.
- **Inverses:** If $a \in 2\mathbb{Z}$, then $a = 2n$ for some $n \in \mathbb{Z}$, and $-a = -2n = 2(-n) \in 2\mathbb{Z}$.

Therefore, $(2\mathbb{Z}, +)$ is a group, hence a subgroup of Z.

Examples:.

1. Every group G has two special subgroups, namely

$$\{e\} \text{ and } G.$$

These are called the **trivial subgroups** of G.[9]

2. We saw earlier that 2Z is a subgroup of Z. There is nothing special about 2 in this example: for any $n \in \mathbb{Z}^+$,

$$n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$$

is a subgroup of Z. The exact same computations that we performed for 2Z will show that $n\mathbb{Z} \leq \mathbb{Z}$.

3. The rational numbers Q form an additive subgroup of R.

4. Here is an example from linear algebra. Consider the n-dimensional vector space $\mathbb{R}^n$. Then $\mathbb{R}^n$ is, in particular, an abelian group under addition, and any vector subspace of $\mathbb{R}^n$ is a subgroup of $\mathbb{R}^n$.[10] If H is a subspace of $\mathbb{R}^n$, then it is closed under addition, and closure under scalar multiplication guarantees that $0 \in H$ and for $v \in H$, $-v = -1 \cdot v \in H$.

Definition

The group (a) is called the **cyclic subgroup** generated by a.

When we say that a "generates" (a), we mean that that (a) is created entirely out of the element a. In a certain sense, (a) is the *smallest* possible subgroup of G which contains a. Let's try to make this more precise. If $H \leq G$ and $a \in H$, then H must contain the elements

$$a, a^2, a^3, \ldots,$$

since H is closed. It also must contain e and a^{-1}, hence all of the elements

$$\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots,$$

i.e. all powers of a. That is, $(a) \subset H$, and we have proven the following fact:

Theorem

Let G be a group and let $a \in G$. Then (a) is the smallest subgroup of G containing a, in the sense that if $H \leq G$ and $a \in H$, then $(a) \subseteq H$.

Of course we've already encountered several examples of cyclic subgroups in our studies thus far.

Example

1. Our first example of a subgroup, $2\mathbb{Z} \leq \mathbb{Z}$, is a cyclic sub- group, namely (2). Similarly, $n\mathbb{Z}$ is cyclic for any $n \in \mathbb{Z}$.

2. The subgroup consisting of rotations on D_n,

$$H = \{i, r_1, r_2, \ldots, r_{n-1}\} \leq D_n,$$

is cyclic since $H = (r_1)$.

3. All the proper subgroups of Z_4 and V_4 that we listed are cyclic. In addition, Z_4 is a cyclic subgroup of itself, but V_4 is not.
4. The trivial subgroup $\{e\}$ is always a cyclic subgroup, namely (e).

Theorem

Let G be a group. A nonempty subset $H \subseteq G$ is a subgroup if and only if whenever $a, b \in H$, $ab^{-1} \in H$.

Proof. Suppose that $H \leq G$, and let $a, b \in H$. Then $b^{-1} \in H$, so $ab^{-1} \in H$ since H

is closed.

Conversely, suppose that $ab^{-1} \in H$ for all $a, b \in H$. Then for any $a \in H$, we can take $a = b$ and conclude that

$$e = aa^{-1} \in H,$$

so H contains the identity. Since $e \in H$, for any $a \in H$ we have

$$a^{-1} = ea^{-1} \in H,$$

so H is closed under taking inverses. Finally, we claim that H is closed under the group operation. If $a, b \in H$, then $b^{-1} \in H$, so $b^{-1}a^{-1} \in H$, and therefore

$$ab = (ab)^{-1^{-1}} = (b^{-1}a^{-1})^{-1} \in H.$$

Thus H is closed, hence a subgroup of G.

The next criterion is quite interesting. It obviously reduces the number of things that one needs to check, but it only works for a *finite* subset of a group G.

Theorem

*Let G be a group and H a nonempty **finite** subset of G. Then H*

is a subgroup if and only if H is closed under the operation on G.

Proof. If H is a subgroup, then it is obviously closed by hypothesis.

On the other hand, we are assuming that H is closed, so we need to verify that $e \in H$ and that for every $a \in H$, $a^{-1} \in H$ as well. Since $\{e\} \leq G$, we may assume that H is nontrivial, i.e. that H contains an element a distinct from the identity. Since H is closed, the elements

$$a, a^2, a^3, \ldots$$

are all in H, and since H is finite, this list cannot go on forever. That is, we must eventually have duplicates on this list, so

$$a^i = a^j$$

for some $1 \leq i < j \leq |H|$. Since $i < j$, $j - i \geq 0$ and we have

$$a^i = a^j = a^{j-i}a^i,$$

and using cancellation, we get
$a^{j-i} = e$.

Therefore, $e \in H$. Now observe that $j - i - 1 \geq 0$, so $a^{j-i-1} \in H$, and

$$aa^{j-i-1} = a^{j-i} = e,$$

so $a^{-1} = a^{j-i-1} \in H$. Therefore, H is a subgroup of G.

This theorem has an easy corollary, which is useful when the group is finite.

Corollary

*If G is a **finite** group, a subset $H \subseteq G$ is a subgroup of G if and only if it is closed under the operation on G.*

Definition

The number of distinct (right) cosets of H in G is called the

index of H in G, denoted by

$$[G : H].$$

The set of all right cosets of H in G is denoted by G/H, so

$$\#(G/H) = [G : H].$$

Subgroups of Cylic Groups

Let's return now to the cyclic case. There is one very important thing that we can say about cyclic groups, namely that their subgroups are always cyclic.

Theorem

A subgroup of a cyclic group is cyclic.

Proof. Let $G = (a)$ be a cyclic group and let H be a subgroup of G. We may assume that $H \neq \{e\}$, since $\{e\}$ is already known to be cyclic. Then H contains an element other than e, which must have the form a^m for some $m \in \mathbb{Z}$ since G is cyclic. Assume that m is the *smallest* positive integer for which $a^m \in H$. We claim that $H = (a^m)$. To do this, we need to show that if $a^n \in H$, then a^n is a power of a^m.

Suppose that $a^n \in H$, and use the Division Algorithm to write $n = qm + r$, where $0 \leq r < m$. Then

$$a^n = a^{qm+r} = a^{qm}a^r = (a^m)^q a^r.$$

Since H is a subgroup, $(a^m)^{-q} \in H$, hence $(a^m)^{-q}a^n \in H$, and it follows that

$$a^r = (a^m)^{-q}a^n$$

is in H. But $r < m$ and we have assumed that m is the smallest positive integer such that $a^m \in H$, so we must have $r = 0$. In other words, $a^n = (a^m)^q$, so $a^n \in (a^m)$. Since a^n was an arbitrary element of H, we have shown that $H \subseteq (a^m)$. Since $a^m \in H$, we also have $(a^m) \subseteq H$, so $H = (a^m)$, and H is cyclic. This theorem has a particularly nice corollary, which tells us a lot about the structure of Z as an additive group.

Lagrange's Theorem

Theorem

Let G be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.

Proof. Let $Ha_1, \ldots, Ha_k$ denote the distinct cosets of H in G. That is, $a_1, \ldots, a_k$ all represent different cosets of H, and these are all the cosets. We know that the cosets of H partition G, so

$$|G| = \mathrm{O}(Ha_1) + \cdots + \mathrm{O}(Ha_k).$$

(Here O means the *cardinality* of the set, or simply the number of elements in that set.) Therefore, it will be enough to show that each coset has the same number of elements as H.

We need to exhibit a bijection between H and Ha_i for each i. For each $i = 1, \ldots, k$, define a function $f_i : H \to Ha_i$ by

$$f(h) = ha_i.$$

If we can prove that f is a bijection, then we will have

$$|H| = \mathrm{O}(Ha_i)$$

for all i. if $h_1, h_2 \in H$ with $f(h_1) = f(h_2)$, then

$$h_1a_i = h_2a_i,$$

which implies that $h_1 = h_2$, so f is one-to-one. To see that it is onto, take $h \in H$; then $f(h) = ha_i$.

Thus all the cosets have the same number of elements, namely $|H|$, and really says that

$$|G| = \underbrace{|H| + \cdots + |H|}_{k \text{ times}} = k|H|.$$

this implies $|H|$ *divides* $|G|$.