**4. Two Important Groups**

**Definition(4-1):** Let . Then is congruent to modulo if and denoted by or (mod ).

**Examples(4-2):**

1. (mod), since .
2. (mod), since .
3. (mod), since .
4. (mod), since .

**Theorem(4-3):** The congruence modulo is an equivalence relation on the set of integers.

**Proof:** let

( mod )

the reflexive is a true.

If (mod), to prove (mod)

(mod), so

(mod)

the symmetric is a true.

If (mod) and (mod), to prove (mod)

Since (mod), then and

(mod), then

By adding these two equations

(mod)

the transitive is a true.

the congruence modulo is an equivalent relation.

**Definition(4-4):** let . The congruence class of modulo , denoted by is the set of all integers that are congruent to modulo.

This means, ( mod )

**Example(4-5):** if , find and .

**Solution:**

( mod )

.

**Example(4-6):** if , find and .

**Solution:** ( mod )

( **Homework**)

**Definition(4-7):** The set of all congruence classes modulo is denoted by ( which is read mod ). Thus,

Or

has elements.

**Example(4-8):** ,.

Now, we define the addition on ( write ) by the following: for any , .

Similarly, we define the multiplication on ( write ) by the following: for any , .

It is easy to note that is an abelian group with identity and for every . This group is called the additive group of integers modulo .

**Example(4-9):** ,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. The closure is a true.
2. The associative is a true.
3. is an identity element.
4. The inverse: .
5. An abelian: .

**Example(4-10):** ,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

It is clear that we cannot have a group, since the number is an identity, but the numbers and have no inverses. Thus isnot group.

**The Permutations:**

**Definition(4-11):** A permutation or symmetric of a set is a function from into that is both one to one and onto. ( one to one and onto) and Symm(one to one and onto the set of all permutation on . If is the finite set, then the set of all permutation of is denoted by where , where .

**Example(4-12):** let . Write all permutation on .

**Solution:**

Symm.

**Example(4-13):** let . Write all permutation on .

**Solution:**

Symm, .

**Theorem(4-14):** If , then the set of all permutation on forms a group with composition of mapping. This means, let , then Symm is a group.

**Proof:** Symmis a mapping

Since there is a permutation on

1. Closure: let Symm
2. The associative is a true, since the composition of the mappings is an associative.
3. The identity: since and , for all in is an identity element.
4. The inverse: and is a group.

**Example(4-15):** let , then and is a group. This group is called a symmetric group.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

is not an abelian group.

**Definition(4-16):** (The dihedral group of order )

The -th dihedral group is the group of symmetries of the regular -gon, .

is the third dihedral group. .

**Example(4-17):** the group of symmetries of square or , , where is a clockwise rotation.

1. Write all elements of as a permutation. (**Homework**)
2. Is an abelian? Use table (**Homework**).

**Definition(4-18):** A permutation of a set is a cycle of length if there exist such that and for but . we write .

**Example(4-19):** If , then

Observe that,

.

**Example(4-20):** Let be a set of a group . Then

And

These permutations above are not cycles.

**Theorem(4-21):** Every permutation of a finite set is a product of disjoint cycles.

**Definition(4-22):** A cycle of length two is a transposition.

**Example(4-23):** The permutation is a transposition.

**Property(4-24):** Any permutation can be expressed as the product of transpositions. This means . Therefore any cycle is a product of transposition.

**Example(4-25):** We note that .

**Definition(4-26):** A permutation is even or odd according as it can be written as the product of an even or odd number of transpositions.

**Example(4-27):** Let . Is even or odd permutation.

**Solution:**

has two transpositions, thus is an even permutation.

**Example(4-28):** Determine an even and odd permutation of . (**Homework**)

**Definition(4-29):** (Alternating group)

The Alternating group on letters denoted by is the group consisting of all even permutations in the symmetric group .

**Example(4-30):** Let , then is a subgroup of .

**Example(4-31):** Find from . (**Homework**)