**4. Two Important Groups**

**Definition(4-1):** Let $a,b,n\in Z, n>0$. Then $a$ is congruent to $b$ modulo $n$ if $a-b=nk, k\in Z$ and denoted by $a≡b$ or $a≡b$ (mod $n$).

**Examples(4-2):**

1. $17≡5$ (mod$ 6$), since $17-5=12=(6)(2)$.
2. $8≡4$ (mod$ 2$), since $8-4=4=(2)(2)$.
3. $-12≡3$ (mod$ 3$), since $-12-3=-15=(3)(-5)$.
4. $5≢2$ (mod$ 2$), since $5-2=3\ne \left(2\right)\left(k\right), ∀ k\in Z$ .

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

**Proof:** let $a,b,c,n\in Z, n>0$

$a-a=0=(n)(0)⟹a≡a$ ( mod$ n$ )

 $⟹$ the reflexive is a true.

 If $a≡b$ (mod$ n$), to prove $b≡a$ (mod$ n$)

$a≡b$ (mod$ n$)$ ⟹a-b=nk, k\in Z$, so

$b-a=-nk=n\left(-k\right), -k\in Z⟹b≡a$ (mod$ n$)$ $

$⟹$ the symmetric is a true.

If $a≡b$ (mod$ n$) and $b≡c$ (mod$ n$), to prove $a≡c$ (mod$ n$)

Since $a≡b$ (mod$ n$), then $a-b=nk$ and

 $b≡c$ (mod$ n$), then$ b-c=nk^{\*}$

By adding these two equations

$$⟹a-c=n\left(k+k^{\*}\right), k+k^{\*}\in Z $$

$⟹a≡c$ (mod$ n$)

$⟹$ the transitive is a true.

$⟹$ the congruence modulo $n$ is an equivalent relation.

**Definition(4-4):** let $ a\in Z, n>0$. The congruence class of $a$ modulo $n$, denoted by $[a]$ is the set of all integers that are congruent to$ a$ modulo$ n$.

This means, $\left[a\right]=\{z\in Z:z≡a $( mod $n$)$\}$

 $=\{z\in Z:z=a+kn, k\in Z\}$

**Example(4-5):** if $n=2$, find$ [0]$ and $[1]$.

**Solution:** $\left[0\right]=\{z\in Z:z=0+2k, k\in Z\}$

 $=\{0,\pm 2, \pm 4, …\}$

$\left[1\right]=\{z\in Z:z≡1 $( mod $2$)$\}$

 $=\{z\in Z:z=1+2k, k\in Z\}$

 $=\{\pm 1, \pm 3, \pm 5,…\}$.

**Example(4-6):** if $n=3$, find$ [1]$ and $[7]$.

**Solution:** $\left[1\right]=\{z\in Z:z≡1 $( mod $3$)$\}$

 $=\{z\in Z:z=1+3k, k\in Z\}$

 $=\{1,-2,4,7,-5,…\}$

$[7]$ ( **Homework**)

**Definition(4-7):** The set of all congruence classes modulo $n$ is denoted by $Z\_{n}$ ( which is read $Z$ mod $n$). Thus,

$$Z\_{n}=\left\{\left[0\right], \left[1\right], \left[2\right], …, \left[n-1\right]\right\}$$

Or $Z\_{n}=\{0,1,2,…, n-1\}$

$Z\_{n}$ has $n$ elements.

**Example(4-8):** $Z\_{1}=\{0\}$,$Z\_{2}=\left\{0,1\right\},Z\_{3}=\{0,1,3\}$.

Now, we define the addition on $Z\_{n}$ ( write $+\_{n}$ ) by the following: for any $\left[a\right], [b]\in Z\_{n}$, $[a]+\_{n}\left[b\right]=[a+\_{n}b]$.

Similarly, we define the multiplication on $Z\_{n}$ ( write $∙\_{n}$ ) by the following: for any $\left[a\right], [b]\in Z\_{n}$, $[a]∙\_{n}\left[b\right]=\left[a∙\_{n}b\right], ∀ \left[a\right], [b]\in Z\_{n}$.

It is easy to note that $(Z\_{n}, +\_{n})$ is an abelian group with identity $[0]$ and for every $\left[a\right]\in Z\_{n}, \left[a\right]^{-1}=[n-a]$. This group is called the additive group of integers modulo $n$.

**Example(4-9):** $(Z\_{4}, +\_{4})$, $Z\_{4}=\{0,1,2,3\}$

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $$+\_{4}$$ | $$0$$ | $$1$$ | $$2$$ | $$3$$ |
| $$0$$ | $$0$$ | $$1$$ | $$2$$ | $$3$$ |
| $$1$$ | $$1$$ | $$2$$ | $$3$$ | $$0$$ |
| $$2$$ | $$2$$ | $$3$$ | $$0$$ | $$1$$ |
| $$3$$ | $$3$$ | $$0$$ | $$1$$ | $$2$$ |

1. The closure is a true.
2. The associative is a true.
3. $0$ is an identity element.
4. The inverse: $1^{-1}=4-1=3, 2^{-1}=4-2=2, 3^{-1}=4-3=1$.
5. An abelian: $1+\_{4}2=3=2+\_{4}1, 1+\_{4}3=0=3+\_{4}1$.

**Example(4-10):** $(Z\_{4}, ∙\_{4})$,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $$∙\_{4}$$ | $$0$$ | $$1$$ | $$2$$ | $$3$$ |
| $$0$$ | $$0$$ | $$0$$ | $$0$$ | $$0$$ |
| $$1$$ | $$0$$ | $$1$$ | $$2$$ | $$3$$ |
| $$2$$ | $$0$$ | $$2$$ | $$0$$ | $$2$$ |
| $$3$$ | $$0$$ | $$3$$ | $$2$$ | $$1$$ |

It is clear that we cannot have a group, since the number $1$ is an identity, but the numbers $0$ and $2$ have no inverses. Thus $(Z\_{4}, ∙\_{4})$ isnot group.

**The Permutations:**

**Definition(4-11):** A permutation or symmetric of a set $A$ is a function from $A$ into $A$ that is both one to one and onto. $f:A⟼A$ ( one to one and onto) and Symm($A)=\{f:f:A⟼A, f $one to one and onto$\}$ the set of all permutation on $A$. If $A$ is the finite set$ \{1,2,…,n\}$, then the set of all permutation of $A$ is denoted by $S\_{n}$ where $O(S\_{n})=n!$, where $n!=n\left(n-1\right)…(3)(2)(1)$.

**Example(4-12):** let $A=\{1,2\}$. Write all permutation on $A$.

**Solution:**$ f\_{1}=\left(\begin{matrix}1&2\\1&2\end{matrix}\right), f\_{2}=\left(\begin{matrix}1&2\\2&1\end{matrix}\right)$

$S\_{2}=$Symm$\left(A\right)=\{ f\_{1}=\left(\begin{matrix}1&2\\1&2\end{matrix}\right), f\_{2}=\left(\begin{matrix}1&2\\2&1\end{matrix}\right)\}$.

**Example(4-13):** let $A=\{1,2,3\}$. Write all permutation on $A$.

**Solution:**$ f\_{1}=\left(\begin{matrix}1&2&3\\1&2&3\end{matrix}\right), f\_{2}=\left(\begin{matrix}1&2&3\\1&2&3\end{matrix}\right), f\_{3}=\left(\begin{matrix}1&2&3\\3&1&2\end{matrix}\right),$

$$f\_{4}=\left(\begin{matrix}1&2&3\\1&3&2\end{matrix}\right), f\_{5}=\left(\begin{matrix}1&2&3\\3&2&1\end{matrix}\right), f\_{6}=\left(\begin{matrix}1&2&3\\2&1&3\end{matrix}\right),$$

$S\_{3}=$Symm$\left(A\right)=\{ f\_{1}, f\_{2},f\_{3},f\_{4},f\_{5},f\_{6}\}$, $O(S\_{3})=\left(3\right)\left(2\right)=6$.

**Theorem(4-14):** If $A\ne ∅$, then the set of all permutation on $A$ forms a group with composition of mapping. This means, let $A\ne ∅$, then $($Symm$\left(A\right),∘)$ is a group.

**Proof:** Symm$\left(A\right)=\{f:f:A⟼A $is a mapping$\}$

Since there is $i\_{A}:A⟼A$ a permutation on $A$

$$i\_{A}\in Symm\left(A\right)⟹Symm\left(A\right)\ne ∅$$

1. Closure: let $f, g \in $ Symm$\left(A\right)$

$$f:A⟼A, g:A⟼A⟹f∘g:A⟼A⟹f∘g\in Symm\left(A\right)$$

1. The associative is a true, since the composition of the mappings is an associative.
2. The identity: since $i\_{A}\in Symm\left(A\right)$ and $i\_{A}∘f=f∘i\_{A}=f$, for all $f$ in $Symm\left(A\right)⟹i\_{A}$ is an identity element.
3. The inverse: $∀ f:A⟼A, ∃ f^{-1}:A⟼A⟹f^{-1}\in Symm\left(A\right)$ and $f∘f^{-1}=f^{-1}∘f=i\_{A}⟹(Symm\left(A\right),∘)$ is a group.

**Example(4-15):** let $A=\{1,2,3\}$, then $S\_{3}=\{ f\_{1}, f\_{2},f\_{3},f\_{4},f\_{5},f\_{6}\}$ and $(S\_{3},∘)$ is a group. This group is called a symmetric group.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| $$∘$$ | $$f\_{1}$$ | $$f\_{2}$$ | $$f\_{3}$$ | $$f\_{4}$$ | $$f\_{5}$$ | $$f\_{6}$$ |
| $$f\_{1}$$ | $$f\_{1}$$ | $$f\_{2}$$ | $$f\_{3}$$ | $$f\_{4}$$ | $$f\_{5}$$ | $$f\_{6}$$ |
| $$f\_{2}$$ | $$f\_{2}$$ | $$f\_{3}$$ | $$f\_{1}$$ | $$f\_{5}$$ | $$f\_{6}$$ | $$f\_{4}$$ |
| $$f\_{3}$$ | $$f\_{3}$$ | $$f\_{1}$$ | $$f\_{2}$$ | $$f\_{6}$$ | $$f\_{4}$$ | $$f\_{5}$$ |
| $$f\_{4}$$ | $$f\_{4}$$ | $$f\_{6}$$ | $$f\_{5}$$ | $$f\_{1}$$ | $$f\_{3}$$ | $$f\_{2}$$ |
| $$f\_{5}$$ | $$f\_{5}$$ | $$f\_{4}$$ | $$f\_{6}$$ | $$f\_{2}$$ | $$f\_{1}$$ | $$f\_{3}$$ |
| $$f\_{6}$$ | $$f\_{6}$$ | $$f\_{5}$$ | $$f\_{4}$$ | $$f\_{3}$$ | $$f\_{2}$$ | $$f\_{1}$$ |

$(S\_{3},∘)$ is not an abelian group.

**Definition(4-16):** (The dihedral group $D\_{n}$ of order $2n$)

The $n$-th dihedral group is the group of symmetries of the regular $n$-gon, $O(D\_{n})=2n$.

$D\_{3}:$ is the third dihedral group. $O(D\_{3})=\left(2\right)\left(3\right)=6$.

**Example(4-17):** the group of symmetries of square $D\_{4}$ or $G\_{S}, O\left(D\_{4}\right)=8$, $G\_{S}=D\_{4}=\{r\_{1},r\_{2},r\_{3},r\_{4},v,h,D\_{1},D\_{2}\}$, where $r\_{i}$ is a clockwise rotation.

1. Write all elements of $G\_{S}$ as a permutation. (**Homework**)
2. Is $(G\_{S}, ∘)$ an abelian? Use table (**Homework**).

**Definition(4-18):** A permutation $f$ of a set $A$ is a cycle of length $n$ if there exist $a\_{1}, a\_{2}, …, a\_{n}\in A$ such that$f\left(a\_{1}\right)=a\_{2}, f\left(a\_{2}\right)=a\_{3},…, f\left(a\_{n-1}\right)=a\_{n}, f\left(a\_{n}\right)=a\_{1}$ and $f\left(x\right)=x$ for $x\in A$ but $x\notin \{a\_{1}, a\_{2}, …, a\_{n}\}$. we write $f=(a\_{1}, a\_{2}, …, a\_{n})$.

**Example(4-19):** If $A=\{1,2,3,4,5\}$, then

$$\left(\begin{matrix}1&2&3\\3&2&5\end{matrix} \begin{matrix}4&5\\1&4\end{matrix}\right)=\left(1,3,5,4\right)∘\left(2\right)=\left(1,3,5,4\right)$$

Observe that,

$\left(1,3,5,4\right)=\left(3,5,4,1\right)=\left(5,4,1,3\right)=(4,1,3,5)$.

**Example(4-20):** Let $A=\{1,2,3,4,5,6\}$ be a set of a group $S\_{6}$. Then

$$\left(\begin{matrix}1&2&3\\4&1&3\end{matrix} \begin{matrix}4&5&6\\2&6&5\end{matrix}\right)=\left(1,4,2\right)∘\left(3\right)∘\left(5,6\right)=(1,4,2)∘(5,6)$$

And

$$\left(\begin{matrix}1&2&3\\6&4&3\end{matrix} \begin{matrix}4&5&6\\5&2&1\end{matrix}\right)=\left(1,6\right)∘\left(2,4,5\right)∘\left(3\right)=(1,6)∘(2,4,5)$$

These permutations above are not cycles.

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

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

**Example(4-23):** The permutation $f=\left(\begin{matrix}1&2\\1&4\end{matrix} \begin{matrix}3&4\\3&2\end{matrix}\right)=(24)$ is a transposition.

**Property(4-24):** Any permutation can be expressed as the product of transpositions. This means $(a\_{1}, a\_{2}, …, a\_{n})=(a\_{1}a\_{2})(a\_{1}a\_{3})…(a\_{1}a\_{n})$. Therefore any cycle is a product of transposition.

**Example(4-25):** We note that $\left(16\right)\left(253\right)=(16)(25)(23)$.

**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 $f=\left(\begin{matrix}1&2&3\\3&1&2\end{matrix}\right)\in S\_{3}$. Is $f$ even or odd permutation.

**Solution:** $f=\left(\begin{matrix}1&2&3\\3&1&2\end{matrix}\right)=\left(132\right)=(13)(12)$

$f$ has two transpositions, thus$ f$ is an even permutation.

**Example(4-28):** Determine an even and odd permutation of $D\_{4}$. (**Homework**)

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

The Alternating group on $n$ letters denoted by $A\_{n}$ is the group consisting of all even permutations in the symmetric group $S\_{n}$.

$$O\left(A\_{n}\right)=\frac{n!}{2}, A\_{n}⊂S\_{n}$$

**Example(4-30):** Let $S\_{3}=\{ f\_{1}, f\_{2},f\_{3},f\_{4},f\_{5},f\_{6}\}$, then $A\_{3}=\{i,f\_{2},f\_{3}\}$ is a subgroup of $S\_{3}$. $O\left(A\_{3}\right)=\frac{6}{2}=3$

**Example(4-31):** Find $A\_{4}$ from $S\_{4}$. (**Homework**)