B.sc(H) part 2 paper 2
Topic: isomorphism theorem for cyclic group
subject:mathematics
Dr hari kant singh

Theorem 1

If the generator of a cylic group G is of order infinity, then G is isomorphic to the additive group of integers.

That is, every cyclic group of infinite order is isomorphic to the additive group $(Z, +)$ of integers.

Proof : Let a be the generator of the cyclic group G. If the order of a be infinity, then no two powers of a are equal. If possible, let $a^n = a^m$ where $n > m$.

Then $a^{n-m} = e$ which is not possible since the order of a is infinity.

Hence $a^n \neq a^m$.

Thus G contains infinite number of terms.

Let $G = \{\ldots a^{-2}, a^{-1}, a^0, a, a^2, a^3, \ldots a^n \ldots\}$

The additive group of integers is

$$Z = \{\ldots -2, -1, 0, 1, 2, 3, \ldots n \ldots\}$$

Let the function $f : G \to Z$ be defined as $f(a^n) = n$, $n \in Z$.

We want to show that f is an isomorphism.

***f* preserves operations.**

Let $a^m, a^n \in G$.

Then $f(a^m \cdot a^n) = f(a^{m+n}) = m + n = f(a^m) + f(a^n)$.

Therefore f is a homomorphism.

***f* is onto :** Again, f is onto since the image point of any point $a^k \in G$ is k which $\in Z$.

f is one-one : Also, f is one-one since

$$f(a^m) = f(a^n) \Rightarrow m = n.$$

Hence f is an isomorphism. Hence $G \cong Z$.

Theorem 2

If a generator of a cyclic group is of order $n(> 0)$, then G is isomorphic to the additive group of residue classes modulo n.

Proof : Let a be a generator of a cyclic group and let its order be n.

It has been proved before that if a generator of a cyclic group is of order n, then the order of the group will be n.

Thus G contains exactly n elements $a, a^2, a^3, \ldots a^n = e$.

Let Z_n be the additive group of residue classes (mod n), that is

$$Z_n = \{\{1\}, \{2\}, \{3\} \ldots \{n\} = \{0\}\}.$$

Let the mapping $f : G \to Z_n$ be defined as

$$f(a^r) = \{r\}, \text{ where } a^r \in G.$$

We want to show that f is an isomorphism.

f preserves operations.

Let $a^r, a^s \in G$.

Then $f(a^r \cdot a^s) = f(a^{r+s}) = (r + s)$

$$= \{r\} + \{s\} = f(a^r) + f(a^s).$$

Therefore f is a homomorphism.

f is onto : Again f is onto, since the preimage point of any element $\{r\} \in Z_n$ is a^r which $\in G$.

f is one-one : Also f is one-one since $f(a^r) = f(a^s) \Rightarrow \{r\} = \{s\}$.

$\Rightarrow$ $r - s$ is divisible by n

$\Rightarrow$ $r - s = kn$ where $k \in I$

$\Rightarrow$ $a^{r-s} = a^{kn} \Rightarrow a^{r-s} = (a^n)^k$

$\Rightarrow$ $a^{r-s} = e^k \Rightarrow a^{r-s} = e \Rightarrow a^r = a^s$

∴ f is one-one. Thus f is an isomorphism.

Hence $G \cong Z_n$.