VIVEKANANDA COLLEGE
THAKURPUKUR
KOLKATA-700063

NAAC ACCREDITED ‘A’ GRADE

Topic: Group Homomorphism

Course Title: Isomorphic Groups and Cayley’s Theorem

Paper: CC4

Unit: 3

Semester: 2

Name of the Teacher: Jayeeta Saha

Name of the Department: Mathematics

MATHEMATICS

(HONOURS)

SEM-II

ISOMORPHIC GROUPS
&
CAYLEY’S THEOREM

Dr. JAYEETA SAHA

ASSISTANT PROFESSOR
DEPARTMENT OF MATHEMATICS,
VIVEKANANDA COLLEGE, THAKURPUKUR

Definition 0.11. Isomorphic Group:

Two groups G and G' are said to be isomorphic if there exists an isomorphism between them. Notationally we write $G \simeq G'$.

Observations

(i) Let $\phi : G \to G'$ be an isomorphism. Then $\phi^{-1} : G' \to G$ is also an isomorphism. i.e $G \simeq G' \implies G' \simeq G$

(ii) Let $\phi : G \to G'$ and $\psi : G' \to G''$ be two isomorphisms. Then $\psi\phi : G \to G''$ is also an isomorphism. i.e $G \simeq G'$ and $G' \simeq G'' \implies G \simeq G''$.

From above observations we can say that the relation of being isomorphic is symmetric and as well as transitive on the collection of all groups. Also the relation is reflexive by considering the identity mapping on a group which is obviously an isomorphism. Thus isomorphism is an equivalence relation on the collection of all groups and therefore it creates a partition on the collection af all groups into the class of isomorphic groups. Thus two groups belonging to the same class are isomorphic.

Again as isomorphism is a bijective map so two isomorphic groups have the same cardinality. Also an isomorphism being a homomorphism ,its preserves algebraic structure. Thus two isomorphic groups are structurally same in group theory.

Theorem 0.12. *Two finite cyclic groups of the same order are isomorphic*

Proof. Let G and G' be two cyclic groups of order n. As G and G' are cyclic there exists two elements $a \in G$ and $b \in G'$ such that $G =< a >$ and $G' =< b >$. Then $o(a) = o(b) = n$ and $G = \{e_G, a, a^2, \ldots, a^{n-1}\}$, $G' = \{e'_G, b, b^2, \ldots, b^{n-1}\}$.

Let us define a mapping $\phi : G \to G'$ by $\phi(a^s) = b^s$, $s = 0, 1, 2, \ldots, n-1$.

We now first show that for any integer k not necessarily belongs to the set $\{0, 1, \ldots, n-1\}$, $\phi(a^k) = b^k$.

Now for any integer k, by division algorothm we get two integer q, r such that $k = nq + r$ where $0 \leq r < n$.

Then $a^k = a^{nq+r} = a^r$ and $b^k = b^{nq+r} = b^r$. Thus $\phi(a^k) = \phi(a^r) = b^r = b^k$.

To show that ϕ is a homomorphism let us take two elements a^p and a^q from G.

Then $\phi(a^p a^q) = \phi(a^{p+q}) = b^{p+q} = b^p b^q = \phi(a^p)\phi(a^q)$.

This shows that ϕ is a homomorphism from G to G'.

Clearly ϕ is bijective, hence ϕ is an isomorphism. □

Corollary 0.13. *A finite cyclic group of order n is isomorphic to* $(\mathbb{Z}_n, +)$

Theorem 0.14. *Two infinite cyclic groups are isomorphic.*

Proof. Let us take two infinite cyclic group G and G'. We now show that G is isomorphic to $(\mathbb{Z}, +)$. Let $G =< a >$. Now define a mapping $\phi : (\mathbb{Z}, +) \to G$ by $\phi(n) = a^n$. $n \in \mathbb{Z}$. We now show that ϕ is an isomorphism. Let us take two elements $p, q \in Z$. Then $\phi(p + q) = a^{p+q} = a^p a^q = \phi(p)\phi(q)$. Thus ϕ is a homomorphism. As G is an infinite cyclic group for two elements m, n from G with $m \neq n$, $\phi(a^m) \neq \phi(a^n)$. Then ϕ is a injective. Again since every element of G is of the form a^r, so ϕ is surjective. Hence ϕ is an isomorphism. Thus G is isomorphic to $(\mathbb{Z}, +)$. Similarly G' is isomorphic to $(\mathbb{Z}, +)$. As relation of being isomorphic is both symmetric and transitive thus G and G' are isomorphic. □

Definition 0.15. Permutation groups: Let A be a non empty set. A bijective mapping on A is said to be a permutation on A.

Let S be the set of all permutations on A. Then S becomes a group with respect to the composition of mapping. This group is said to be the group of all permutation on A.
In particular, if A be a finite set containing n elements then the group is called symmetric group S_n.

Theorem 0.16. *Cayley's Theorem*

A finite group G of order n is isomorphic to a subgroup of S_n.

Proof. Let $(G, \cdot)$ be a group of order n and $g \in G$. Consider a function $f_g : G \to G$ define by $f_g(a) = ga$. Then by property of group it is easy to show that f_g is bijective. Hence $f_g \in S_n$. Let us define a mapping $\phi : G \to S_n$ by $\phi(g) = f_g$. To show ϕ is a homomorphism let us take two elements $x, y \in G$, then $\phi(xy) = f_{xy} = f_x o f_y$ [as for any $a \in G$, $f_{xy}(a) = xya = x(ya) = xf_y(a) = f_x(f_y(a)) \implies f_{xy} = f_x o f_y$]. $= \phi(x) o \phi(y)$. Thus ϕ is a homomorphism. To show ϕ is injective let $x \in \ker\phi \Leftrightarrow \phi(x) = I$ where I is the identity element of $S_n \Leftrightarrow f_x = I \Leftrightarrow f_x(a) = a \; \forall a \in G \Leftrightarrow xa = a \; \forall a \in G \Leftrightarrow x = e_G$. Thus $\ker\phi = \{e_G\}$. Therefore ϕ is injective and hence ϕ is a monomorphism. Also $\phi(G)$ is a subgroup of S_n. Thus G is isomorphic to a subgroup $\phi(G)$ of S_n. □