Episteme: an online interdisciplinary, multidisciplinary & multi-cultural journal

Bharat College of Commerce, Badlapur, MMR, India

Volume 3, Issue 1 **June 2014**

CAUCHY THEOREM

By Jayshri Patil

Assistant Professor

Bharat College of Commerce

Badlapur(W), Dist. Thane, MMR

ABSTRACT:

Abstract algebra is not to be confused with the manipulation of formulae that is covered in secondary education. It studies sets together with binary operations defined on them. Sets and their binary operations may be classified according to their properties: for instance, if an operation is associative on a set that contains an identity element and inverses for each member of the set, the set and operation is considered to be a group. Other structures include rings, fields, vector spaces and lattices.

In this section we will begin to make use of the definitions we made in the section about binary operations. In the next few sections, we will study a specific type of binary structure called a group. First, however, we need some preliminary work involving a less restrictive type of binary structure. After that we will study some necessary definitions like order of group, cyclic group, order of an element, subgroup.

DEFINITIONS:

1) **BINARY OPERATION:**

A binary operation on a set S is a function from S X S to S.

i.e. * : S X S → S

for each (a,b) □ S X S, we denote the element *((a,b)) of S by a*b.

e.g. +(usual addition) is a binary operation on IR, C, Z.

2) * is a binary operation on S. H is subset of S then H is closed under * if for all a , b □ H a*b □ H ⟹

3) GROUP:

Let G be a nonempty set together with a binary operation that assigns to each ordered pair (a,b) of element of G an element in G, denoted by ab.

G is said to be a group under this binary operation if following axioms are satisfied:

i) (ab) c = a (bc), for all a,b,c □ G (Associativity)

ii) There exist e □ G such that ae = ea = a, for all a □ G (e is called identity element in G w.r.t. given binary operation)

iii) For each a □ G , there exist b □ G such that ab = ba = e (b is called inverse of 'a' w.r.t. given binary operation.)

e.g. (IR, +), (Q, +), (C, +), (Z,+).

4) ABELIAN GROUP:

A Group G is said to be an **abelian group** if ab = ba, for all

a,b □ G.

5) ORDER OF GROUP:

The number of element of group (finite or infinite) (cardinality) is called **order of a group.** It is denoted by o(G) or | G| .

6) ORDER OF AN ELEMENT:

Order of an element g in a group G is the smallest positive integer 'n' such that $g^n = e$.

If no such integer exist, we say g has infinite order. The order of an element g is denoted as o(g) or | g| .

7) SUBGROUP:

Let G be a group. H is subset of G then H is a subgroup of G if

i) a,b □ H ⟹ ab □ H.

ii) e □ H

iii) for each a □ H, a^{-1} □ H.

8) CYCLIC GROUP:

Group G is called cyclic if there is an element a in G such that

G = { a^n / n □ z } and such an element 'a' is called a generator of g.

9) LANGRANGE'S THEOREM:

If G is a finite group & H is a subgroup of G, then | H| divides | G| . Moreover, the number of distinct left (right) cosets of H in G is | G| / | H| .

10) EXTERNAL DIRECT PRODUCT:

Let G & H be two groups. The external direct product of G & H is defined by taking group partition on the set G×H as

(g,h)(g',h') = (gg',hh') .

REMARK:

If $G_1 \times G_2 \times \ldots\ldots \times G_n$ are finitely many groups then their external direct product $G_1 \times G_2 \times \ldots\ldots \times G_n$ is similarly defined.

11) INTERNAL DIRECT PRODUCT:

Let G be a group, H & K be two subgroups. HK defines as the set

{ hk / hϵH, kϵK }. Let H & K be normal subgroups of a group G. we say that G is the internal direct product of H & K if G=HK &

H ∩ K = {e}

REMARK:

Let H & K be the two groups. Let G = H × K be their external direct product then G has two normal subgroup H × $\{e_K\}$ & $\{e_H\}$ × K & G is internal direct product at these two groups.

THEOREM:

If G is the internal direct product of two subgroups H & K then G is isomorphic to the external direct product of H & k.

Proof: Define a map,

Φ: H × K→ G

$\Phi(h,k) = h.k$

Φ is onto (since G = HK)

Claim: Φ is a homorphism

Subclaim: If h ϵ H & k ϵ K then hk = kh (H,K are non-abelian)

Exercise: Show that $hkh^{-1}k^{-1}$ = identity of G.

Claim: $\Phi((h,k).(h',k')) = \Phi(h,k).\Phi(h',k')$

L.H.S = $\Phi((h,k).(h',k'))$

$= \Phi(hh'.kk')$

$= hh'kk'$ ..... (by definition)

$= hkh'k'$

$= \Phi(h,k).\Phi(h',k') = R.H.S$

Ker $\Phi = \{(h,k)/\Phi(h,k)=e\}$

$= \{(h,k)/hk=e\}$

hk=e implies h= k^{-1}

h ϵ H & k^{-1} ϵ K & H∩K={e}

⇨ h = e & k = e

Therefore ker Φ is trivial

Therefore Φ is I-I

So Φ is isomorphism.

CAUCHY'S THEOREM:

Let G be a finite abelian group . If p is a prime dividng the order of G then G has an elements of order P.

Proof: By induction on order of G

Let |G |=n

Let n=1 then result is true

Induction hypothesis: If G is a abelian group of order less than n & p ∣ |G|, P is a prime then G has an elements of order P.

Let z ϵ G z ≠ e, then o(z) > 1

If p|o(z) then we are through.

Assume p does not divide o(z) then there exist a prime q ≠ p, q|o(z)

⇨ ∋ x ϵ G such that o(x) = q

Consider the subgroup <x> of G

Where <x> denotes the cyclic subgroup of G generated by x.

Since G is abelian.

So <x> is a normal subgroup so we can consider quotient group G/<x>.

$G/\langle x\rangle$ is abelian & $|G/\langle x\rangle| < |G|$

$|G| = |G/\langle x\rangle| . |\langle x\rangle|$

$P \mid |G/\langle x\rangle|$ & $|G/\langle x\rangle| < |G|$

So By induction hypothesis there exist $a\langle x\rangle$ whose order is p.

Therefore $(a\langle x\rangle)^p = e_{G/\langle x\rangle}$

$a^p\langle x\rangle = \langle x\rangle$ so $a^p \in \langle x\rangle$

Either $a^p = e$ we are through

or $a^p \in \langle x\rangle$ & $a^p \neq e$ implies $o(a^p) = q$.

$a^{pq} = e$, p,q are prime & $p \neq q$ implies $o(a^q) = p$.

So in either case we have found an element in G whose order is p.

COROLLARY:

If G is finite abelian group & if $p \mid\mid |G|$, p is a prime then G has a subgroup of order p.

This statement is generalized.

THEOREM:

Let G be abelian , $|G| = p^r.m$

(m,p) = 1, G has a subgroup H whose order is p^r.

In fact $H = \{x \in G / x^{pr} = e\}$ & if $K = \{x \in G / x^m = e\}$ then G is internal direct product of H & K.

Proof: Claim: G = HK

Since $(p^r,m)=1$ ..... ($(p,m)=1$)

Therefore $\exists\ \lambda, \mu \in Z$ such that $\lambda p^r + \mu m = 1$

Let $x \in G$, $x = x^1$

$= x^{\lambda pr} . x^{\mu m}$

$= x^{\mu m} . x^{\lambda pr}$

$(x^{\mu m})^{pr} = x^{\mu mpr} = e$ ..... (By Langrange's theorem)

$x^{\mu m} \in H$ & $x^{\lambda pr} \in K$

T.S.T $H \cap K = \{e\}$

Let x belongs to $H \cap K$

Therefore $x \in H$ & $x \in K$

Implies $(x)^{pr} = e$ & $x^m = e$

Implies $o(x) | p^r$ & $o(x) | m$, $(m, p^r) = 1$

Implies $x = e$

Now to prove that $o(H) = p^r$

Therefore By previous theorem,

$G \approx H \times K$

$|G| = |H||K|$

$p^r.m = |H||K|$

If $|H| \neq p^r$ Then $p \| K|$ (Since Z is UFD)

$\exists$ $z \in K$ s.t $o(z)=p$

$K = \{x \in G / x^m = e\}$

$z \in K$ then $z^m = e$

But $o(z) = p$

Implies $p|m$ which is not possible (since $(m,p)=1$)

So $|H| \neq p^r$ then $p \| K|$ is not possible.

therefore $|H| = p^r$.

USES OF CAUCHY'S THEOREM:

A practically immediate consequence of cauchy's theorem is a useful characterisation of finite p-groups, where p is a prime. In particular, a finite group G is a p-group if and only if G has order p^n for some natural number n.

REFERANCES:

1) Basic Abstract Algebra- P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul- Second edition.
2) Contemporary Abstract Algebra- Joseph A. Gallian- forth edition.
3) Algebra- Michael Artin- second edition.
4) (C) G. C. Smith- 12-i-2004.
5) Abstact algebra- David s. Dummit & Richard M. Foote- third edition.
6) www.math.uconn.edu / ~kconrad / blurbs / grouptheory / cauchypdf.