NARAJOLE RAJ COLLEGE

Department of Mathematics

Paper- C6T (unit-4)

semester- 3rd,

— Puja Paul.

Quotient Group

Let H be a normal subgroup of a group G. Then the set of all distinct cosets of H in G forms a group with respect to the binary composition $*$ defined by $aH * bH = abH$, $a, b \in G$.

This group is said to be the quotient group of G or factor group of G by H and is denoted by G/H.

Factor groups from normal subgroups :-

Let, H be a subgroup of a group G. The coset multiplication $(aH)(bH) = (ab)H$ is well defined, independent of the choices a and b from the cosets, and makes the set G/H of left cosets into a group if and only if H is a normal subgroup of G.

EX. Consider the group with addition modulo 6 :

$(G, +_6) = \{0, 1, 2, 3, 4, 5\}$.

Consider the subgroup $N = \{0, 3\}$ which is normal because G is abelian. Then the set of left cosets of size 3 : $G/N = \{a + N : a \in G\} = \{\{0,3\}, \{1,4\}, \{2,5\}\}$

$= \{0+N, 1+N, 2+N\}$

The binary operation defined above makes this set into a group, is known as quotient group or factor group.

Factor groups from homomorphisms :-

Let, $\Phi : G \to G'$ be a group homomorphism with $H = \text{Ker}(\Phi)$. Then the coset multiplication

$$(aH)(bH) = (ab)H$$

is well defined, independent of the choices a and b from the cosets and makes the set G/H of left cosets into a group (factor group).

The map $\mu : G/H \to \Phi[G]$ is defined by

$$\mu(aH) = \Phi(a)$$

is an isomorphism, independent of the choice of a from the coset.

Theorems and Properties on Quotient Group :-

1. If H be a subgroup of a commutative group G, then the quotient group G/H is commutative.

2. If H be a subgroup of a cyclic group G, then the quotient group G/H is cyclic.

3. If G be a non-commutative group with centre Z, then the quotient group G/Z is non-cyclic.

4. If $G/Z(G)$ is cyclic then G is abelian.

5. Let, H be a normal subgroup of a group G. Then the quotient group G/H is abelian if and only if $xyx^{-1}y^{-1} \in H$, $\forall\, x, y \in G$.

6. Every quotient group of a cyclic group is cyclic, but converse is not true.

7. Every quotient group of an abelian group is abelian, but converse is not true.

Let, H be a normal subgroup of a group G. Then the set of all distinct cosets of H in G forms a group with respect to the binary composition '$*$' defined by $aH * bH = abH$, $a, b \in G$.

Proof :- Let, S be the set of all distinct cosets of H in G, Then S is closed under '$*$'.

Now, $aH*(bH*cH) = aH*bcH = a(bc)H$

$(aH*bH)*cH = abH*cH = (ab)cH$

So, $aH*(bH*cH) = (aH*bH)*cH$, [since $a(bc) = (ab)c$]

Therefore, '$*$' is associative.

Let, H is the identity element, because

$H*aH = eH*aH = eaH = aH$

and $aH*H = aH*eH = aeH = aH$.

The inverse of aH is $a^{-1}H$ as

$aH*a^{-1}H = aa^{-1}H = eH = H$.

and $a^{-1}H*aH = a^{-1}aH = eH = H$.

Thus $(S,*)$ is a group. This group is said to be the quotient group (factor group) of G by H and denoted by G/H.

If H be a subgroup of a cyclic group G, then the quotient group G/H is cyclic.

→ Since, G is cyclic, G is commutative. Thus H is is a normal subgroup of G and G/H exists.

Let, $G = \langle a \rangle$. Since H is a subgroup of G, H is also cyclic and $H = \langle a^m \rangle$ where m is the least positive integer such that $a^m \in H$.

First we are to prove that $H, aH, a^2H, \ldots, a^{m-1}H$ is a complete list of distinct cosets of H in G.

Let, $x \in G$, Then $x = a^p$, for some integer p.

By division algorithm, there exist integers q and r such that $p = qm + r$, where $0 \le r \le m-1$.

Therefore, $a^p = a^{qm+r} = a^r (a^m)^q = a^r h$, $\forall h \in H$.

since, $0 \le r \le m-1$, x belongs to one of the cosets $H, aH, a^2H, \ldots, a^{m-1}H$. No two of these cosets are equal. since $a^iH = a^jH$, with $0 \le i < j \le m$

$\Rightarrow (a^i)^{-1} a^j \in H$, i.e, $a^{j-i} \in H$,

a contradiction, since $0 < j - i < m$.

Therefore, the distinct cosets of H in G are $H, aH, a^2H, \ldots, a^{m-1}H$.

$$a^rH = (a \cdot a \cdot \ldots \cdot a)H$$
$$= (aH) * (aH) * \ldots * (aH) \ (r \text{ factors})$$
$$= (aH)^r$$

Thus G/H is a finite group of m elements $H, aH, (aH)^2, \ldots, (aH)^{m-1}$.

Therefore, G/H is a cyclic group, aH being a generator.

N.B. The converse of the theorem is not true.

Let, $G = S_3$, $H = A_3$, Then G/H being a group of order 2 is cyclic, but S_3 is not cyclic.

—•—

▨ If G be a non-commutative group with centre Z then the quotient group G/Z is non-cyclic.

Proof :- Since Z is normal in G, the quotient group G/Z exists.

Let, G/Z be cyclic. Then $G/Z = \langle aZ \rangle$ for some $a \in G$.

So, each element of G/Z is of the form $(aZ)^i$ i.e., of the form a^iZ, for some integer i.

Let, p, q be arbitrary elements of G.

Let, the cosets of Z to which they belong be a^rZ, a^sZ respectively, where r, s are integers.

Then, $p = a^rz_1$ and $q = a^sz_2$, for some $z_1, z_2 \in Z$

Now, $pq = (a^rz_1)(a^sz_2)$

$= a^ra^sz_1z_2$ (z_1 commutates with a^s, as $z_1 \in Z$)

$= a^{r+s}z_1z_2$

$qp = (a^sz_2)(a^rz_1)$

$= a^sa^rz_2z_1$

$= a^{r+s}z_1z_2$

Hence, $pq = qp$, $\forall\ p, q \in G$, This shows that G is commutative, a contradiction,

Therefore, G/Z is not cyclic.

▨ If G be a commutative group then $Z = G$ and the quotient group G/Z is the trivial subgroup. Thus for an arbitrary group G, the quotient group G/Z cannot be non-trivial cyclic.

Ex.

1. Give an example that the converse of Lagrange's theorem "if d be positive divisor of the order of a finite group G then G has a subgroup of order d" is not true.

2. Let, H be a subgroup of a group G such that the product of any two left cosets of H is a left coset of H. Prove that H is normal in G.

Let G be a cyclic group of order 12 generated by a and H be the cyclic subgroup of G generated by a^4. Prove that H is normal in G. Write all cosets of H in G. Verify that the quotient group G/H is a cyclic group of order 4.

Proof :- $G = \{a, a^2, \cdots, a^{12}(=e)\}$ and $H = \{a^4, a^8, e\}$

Since G is a commutative group, H is normal in G. The quotient group G/H exists and $o(G/H) = 4$.

The elements of G/H are H, $aH(=\{a, a^5, a^9\})$, $a^2H(=\{a^2, a^6, a^{10}\})$, $a^3H(=\{a^3, a^7, a^{11}\})$.

H is the identity element. $o(H) = 1$

$o(aH) = 4$, as $(aH)^4 = a^4H = H$.

$o(a^2H) = 2$, as $(a^2H)^2 = a^4H = H$.

$o(a^3H) = 4$, as $(a^3H)^4 = a^{12}H = H$.

Since, $o(G/H) = 4$ and $o(aH) = 4$, G/H is a cyclic group of order 4 generated by aH. a^3H is also a generator.

Prove that the symmetric group S_3 has a trivial centre.

Proof :- Let, Z be the centre of S_3. Since S_3 is non-commutative, $Z \neq S_3$.

By Lagrange's theorem, $o(Z)$ is a divisor of 6.

since, $Z \neq S_3$, $o(Z)$ is either 1 or 2 or 3.

If $o(Z) = 3$, then $o(S_3/Z) = o(S_3)/o(Z) = 2$ this implies that the quotient group S_3/Z is a cyclic group. which is impossible, so $o(Z) \neq 3$.

If $o(Z) = 2$, then $o(S_3/Z) = 3$, which is also impossible. so, $o(Z) \neq 2$.

Now, $o(Z) = 1$, and hence Z is the trivial subgroup.

If each non-identity element in a group G be of order 2, prove that $o(G) = 2^n$, for some natural number n.

Proof :- Since the order of each non-identity element in G is 2, G is a commutative group.

Let, a be a non-identity element in G. Then, $H = \langle a \rangle$ is a normal subgroup of G of order 2.

By Lagrange's theorem, $o(G) = 2k$, for some natural number k.

The quotient group G/H has k elements.

Let, $bH\ (\neq H) \in G/H$

Then, $(bH)^2 = b^2H = H$, as $o(b) = 2$,

Thus, the order of each non-identity element in G/H is 2 and therefore G/H is a commutative group.

Let, $G_1 = G/H$ and a_1 be a non-identity element in G_1. Then $H_1 = \langle a_1 \rangle$ is a normal subgroup of G_1 of order 2.

By Lagrange's theorem, $o(G_1) = 2k_1$, for some natural number k_1, so $o(G) = 2^2 k_1$,

The quotient group G_1/H_1 has k_1 elements. and $G_2 = G_1/H_1$ comes to be a commutative group of even over $2k_2$, consequently $o(G) = 2^3 k_2$, for some natural number k_2.

Since $o(G)$ is finite, after a finite number of steps we have $o(G) = 2^n$, for some natural number n.

Ref :- Abstract Algebra, S.K. Mapa.
Abstract Algebra, Ghosh & Chakraborty.

Let, H be a subgroup of a group G and $[G:H] = 2$. Prove that for every $x \in G$, $x^2 \in H$.

Deduce that A_4 has no subgroup of order 6.

Proof :- H is a normal subgroup of G. The cosets of H in G are H and $G-H$.

The quotient group is a group of order 2. Therefore $(G-H)^2 = H$, H being the identity element in the quotient group.

Let, $x \in H$. Then $x^2 \in H$ since H is a subgroup.

If $x \in G-H$, then $xH = G-H$ and therefore, $(xH)^2 = (G-H)^2 = H$.

$$(xH)^2 = H \Rightarrow (xH)(xH) = H \Rightarrow x^2H = H \Rightarrow x^2 \in H$$

Therefore for every $x \in G \Rightarrow x^2 \in H$.

Now, if possible let H be a subgroup of A_4 of index 2. Then the square of each element of A_4 must belongs to H.

A_4 is a group of order 12. The elements of A_4 are, $-i$, $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$, $(1,2,3)$, $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, $(2,4,3)$.

Denoting these by $f_1, f_2, \ldots, f_{12}$ respectively we get,

$f_1^2 = f_2^2 = f_3^2 = f_4^2 = i$, $f_5^2 = f_6$, $f_6^2 = f_5$,

$f_7^2 = f_8$, $f_8^2 = f_7$, $f_9^2 = f_{10}$, $f_{10}^2 = f_9$, $f_{11}^2 = f_{12}$,

$f_{12}^2 = f_{11}$.

There are more than 6 squares in A_4 and each of them must belong to H of order 6. — This is impossible.

Thus, A_4 has no subgroup of order 6.

— This shows that the converse of the Lagrange's theorem is not true.

—•—

conjugacy relation :-

Let, G be a group and $x, y \in G$. y is said to be conjugate to x if there exists an element g in G such that $y = gxg^{-1}$.

Let, a relation ρ be defined on G by "$x \rho y$ if and only if y is conjugate to x". Then ρ is an equivalence relation on G.

Proof :- Let, $x \in G$. Then $x \rho x$ as $x = exe^{-1}$, e be the identity element in G. Thus ρ is reflexive.

Let, $x, y \in G$ and $x \rho y$. There there exists an element g in G such that $y = gxg^{-1}$.

Hence, $x = g^{-1}yg = pyp^{-1}$, where $p(= g^{-1}) \in G$.

Thus $x \rho y \Rightarrow y \rho x$, so, ρ is symmetric.

Let, $x, y, z \in G$, and $x \rho y$ and $y \rho z$

Then, $y = gxg^{-1}$ for some g in G and $z = hyh^{-1}$ for some h in G.

Hence, $z = (hg)x(hg)^{-1} = qxq^{-1}$, where $q(= hg) \in G$.

Thus $x \rho y$ and $y \rho z \Rightarrow x \rho z$,

so, ρ is transitive.

Therefore, ρ is an equivalence relation on G.

ρ is said to be the conjugacy relation on G. The set G is partitioned into ρ-equivalence which are called the conjugacy classes. The conjugacy class of a is denoted $cl(a)$.

Let, $a \in G$. The conjugacy class of a is the set of those elements of G which are conjugate to a. Therefore $cl(a) = \{gag^{-1} : g \in G\}$.

class equation :-

Let, G be a finite group and Z be it's centre. Let, $C_1, C_2, \cdots, C_m$ be the distinct multi-membered conjugacy classes of G. Then, $o(G) = o(Z) + \sum_{i=1}^{m} |C_i|$, where $|C_i|$ denotes the number of distinct elements in the conjugacy class C_i.

Proof :- Let, $C_i = cl(a_i)$, $a_i \in G$.

If $a \in Z$, then $|cl(a)| = 1$, if $a \in G - Z$, then $cl(a)$ is a multimembered conjugacy class. $cl(a) = [G : c(a)]$, where $c(a)$ is the centraliser of a.

G is partitioned into distinct conjugacy classes. The elements of Z form single-membered conjugacy classes and the elements of $G - Z$ belongs to multimembered conjugacy classes.

Hence, $o(G) = o(Z) + |G - Z|$

$= o(Z) + |cl(a_1)| + |cl(a_2)| + \cdots + |cl(a_m)|$

where, $cl(a_1), cl(a_2), cl(a_3), \cdots, cl(a_m)$ are distinct conjugacy classes of $G - Z$,

i.e, $o(G) = o(Z) + \sum_{i=1}^{m} |cl(a_i)|$

$o(G) = o(Z) + \sum_{i=1}^{m} |C_i|$; this is called the class equation of G.

———•———

■ Let, G be a group and $Z(G)$ be the centre of G. If $a \in Z(G)$ then $cl(a) = \{a\}$ and conversely.

Proof:- Let, $a \in Z(G)$. Then a commutes with each $g \in G$.

Thus $gag^{-1} = a, \forall g \in G \Rightarrow cl(a) = \{a\}$.

conversely, let $cl(a) = \{a\}$.

Then, $gag^{-1} = a, \forall g \in G$

$\Rightarrow ga = ag, \forall g \in G$.

$\Rightarrow a \in Z(G)$.

■ The elements of $Z(G)$ are self-conjugate elements. If $a \in Z(G)$ the conjugacy class of a is said to be a trivial conjugacy class because it contains a only.

■ In a finite group G, $\forall a \in G$, the number of different conjugates of a in G equals the number of distinct left cosets of the subgroup $C(a)$ in G. i.e, $|cl(a)| = |G : C(a)|$, where $|cl(a)|$ denotes the number of elements in $cl(a)$.

Proof:- Two conjugates of a determined by g and h in G are gag^{-1} and hah^{-1} respectively.

so, $gag^{-1} = hah^{-1} \Leftrightarrow (h^{-1}g)a = a(h^{-1}g)$

$\Leftrightarrow h^{-1}g \in C(a)$, the centraliser of $a \in G$.

$\Leftrightarrow g, h$ are in same left coset of $C(a)$ in G.

Thus, two conjugates gag^{-1} and hah^{-1} of a are

(i) same if g and $h \in$ the same left coset of $C(a)$ in G.

(ii) different if g and h belongs to the different left cosets of $C(a)$ in G.

Hence, the number of distinct conjugates of a in G equals the number of different left cosets of the subgroup $C(a)$ in G.

—·—

● In a finite group G, the number of elements in the conjugacy class of a is a divisor of the order of the group.

■ If G be a group of order p^n where p is a prime and n is a positive integer, then G has a non-trivial centre.

Proof :- If the group G be abelian, $Z(G) = G$. In this case the theorem is true.

Let us assume that G is a non-abelian group and Z be its centre. Let us consider the conjugacy classes of G. The elements of Z from single-membered conjugacy classes and the elements of $G-Z$ are partitioned into multimembered conjugacy classes.

As G is a finite group, the number of conjugacy classes is finite.

Let the distinct multimembered conjugacy classes be $cl(a_1), cl(a_2), \ldots, cl(a_m)$.

Each $a_i \in G-Z$ and $|cl(a_i)| = [G : c(a_i)]$, where $c(a_i)$ is the centraliser of a_i in G.

Thus $o(G) = o(Z) + |cl(a_1)| + |cl(a_2)| + \cdots + |cl(a_m)|$.

Each $|cl(a_i)|$ is a divisor of $o(G)$ and each $|cl(a_i)| > 1$.

It follows that each $|cl(a_i)|$ is p or $p^2, \ldots,$ or p^n.

Since p is a divisor of $o(G)$ and p is a divisor of each $|cl(a_i)|$, it follows that p is a divisor of $o(Z)$. Thus Z is a subgroup having at least p elements and therefore non-trivial.

■ If G be a group of order p^2, where p is a prime, then G is abelian.

Proof :- Let Z be the centre of G. By Lagrange's theorem, $o(Z)$ is a divisor of p^2.

Since p is a prime, $o(Z) = 1$ or p or p^2. But $o(Z) \neq 1$, since G, being a group of order p^2 has a non-trivial centre.

If possible, let $o(Z) = p$, Then the quotient group G/Z is of prime order p and is therefore cyclic.

This is impossible because for any group G the quotient group G/Z cannot be non-trivial cyclic.

Hence $o(Z) = p^2$ and therefore $Z = G$.

Thus G is abelian.

Cauchy's theorem for finite abelian group :-

If G has an element of order m, then for every divisor d of m, G has an element of order d. Where G be a finite group.

If $|g| = m$ and $d|m$ then,

$$|g^{m/d}| = \frac{|g|}{|(g), (m/d)|} = \frac{m}{(m, m/d)} = \frac{m}{m/d} = d.$$

Let, G be an abelian group of order $1 < |G| = n < \infty$. Then if p is a prime dividing n, we have that there is an element $g \in G$ of order p.

A commutative group G has subgroups of order m and n. Prove that G has a subgroup of order $[m,n]$, the l.c.m. of m and n.

➡ Let, H and K be subgroups of G such that $O(H) = m$ and $O(K) = n$.

As H and K are commutative subgroups, HK is a subgroup of G and $O(HK) = \frac{O(H) \cdot O(K)}{O(H \cap K)}$

$$= \frac{mn}{O(H \cap K)}$$

Since, $H \cap K$ is a subgroup of K, $O(H \cap K) | n$.

Thus m is a divisor of $O(HK)$.

Similarly, n is a divisor of $O(HK)$, so $[m,n]$ is a divisor of $O(HK)$.

Since HK is finite commutative group and $[m,n]$ is a divisor of $O(HK)$, it follows that HK has a subgroup of order $[m,n]$ and G has a subgroup of order $[m,n]$.

—•—