Dr. O. P. Raman

Deptt. of Mathematics

For T.D.C. Part III

Paper-6

GT—[redacted] A

① Q. *show that if G is a finite group, then* $c_a = \dfrac{o(G)}{o[N(a)]}$, *i.e., the number of elements conjugate to a in G is the index of the normalizer of a in G.*

(Nagarjuna 1978; I.A.S. 72; Meerut 74; Kanpur 87; B.H.U. 88)

Proof. We have

$x, y \in G$ are in the same right coset of $N(a)$ in G

$\Leftrightarrow N(a)x = N(a)y$ [$\because$ $x \in N(a)x$, $y \in N(a)y$. Note that if H is a subgroup, then $x \in Hx$.]

$\Leftrightarrow xy^{-1} \in N(a)$ [$\because$ if H is a subgroup, then $Ha = Hb \Leftrightarrow ab^{-1} \in H$]

$\Leftrightarrow axy^{-1} = xy^{-1}a$ [by def. of $N(a)$]

$\Leftrightarrow x^{-1}(axy^{-1})y = x^{-1}(xy^{-1}a)y$

$\Leftrightarrow x^{-1}ax = y^{-1}ay$

$\Leftrightarrow x, y$ give rise to the same conjugate of a.

Hence the first result follows.

Now consider the right coset decomposition of G with respect to the subgroup $N(a)$. We have just proved that if $x, y \in G$ are in the same right coset of $N(a)$ in G, then they give the same conjugate of a. Further if x, y are in different right cosets of $N(a)$ in G, then they give rise to different conjugates of a. The reason is that if x, y give the same conjugate of a, then they must belong to the same right coset of $N(a)$ in G. Thus **there is a one-to-one correspondence between the right cosets $N(a)$ in G and the conjugates of a.** So if G is a finite group, then

$$\begin{aligned} c_a &= \text{the number of distinct elements in } C(a) \\ &= \text{the number of distinct right cosets of } N(a) \text{ in } G \\ &= \text{the index of } N(a) \text{ in } G = \frac{o(G)}{o[N(a)]}. \end{aligned}$$

C[illegible]y. *If G is a finite group, then*

$$o(G) = \Sigma \frac{o(G)}{o[N(a)]}$$

where this sum runs over one element a in each conjugate class.

(Punjab 1970; Meerut 84P)

Proof. We know that the relation of conjugacy is an equivalence relation on G. Therefore it partitions G into disjoint conjugate classes. The union of all distinct conjugate classes will be equal to G and two distinct conjugate classes will have no common element. Since G is a finite group, therefore the number of distinct conjugate classes of G will be finite, say equal to k. Suppose $C(a)$ denotes the conjugate class of a in G and c_a denotes the number of elements in this class. If $C(a_1), C(a_2), \ldots\ldots, C(a_k)$ are the k distinct conjugate classes of G, then

$$G = C(a_1) \cup C(a_2) \cup \ldots\ldots \cup C(a_k)$$

$\Rightarrow$ the number of elements in G = the number of elements in

$C(a_1)$ + the number of elements in $C(a_2)$ + ... + the number of elements in $C(a_k)$.

[$\because$ two distinct conjugate classes have no common element]

$\Rightarrow o(G) = \Sigma\, c_a$, the summation being run over one element a in each conjugate class

$\Rightarrow o(G) = \Sigma \dfrac{o(G)}{o[N(a)]}$ by previous theorem.

Th[illegible] **6.** *Let G be a finite group and Z be the centre of G. Then the class equation of G can be written as*

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o[N(a)]},$$

where the summation runs over one element a in each conjugate class containing more than one element.

Proof. The class equation of G is

$o(G) = \Sigma \dfrac{o(G)}{o[N(a)]}$, the summation being extended over one element a in each conjugate class.

Now $a \in Z \Leftrightarrow o[N(a)] = o(G) \Leftrightarrow o(G)/o[N(a)] = 1 \Leftrightarrow$ the conjugate class of a in G contains only one element. Thus the number of conjugate classes each having only one element is equal to $o(Z)$. If a is an element of any one of these conjugate classes, we have $o(G)/o[N(a)] = 1$. Hence the class equation of G takes the desired form

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o[N(a)]}.$$

Theorem 7. *If $o(G) = p^n$ where p is a prime number, then the centre $Z \neq \{e\}$.*

(Agra 1986; I.A.S. 72; Guru Nanak 90; Meerut 74; B.H.U. 87)

Proof. By the class equation of G, we have

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o[N(a)]}, \qquad \ldots(1)$$

where the summation runs over one element a in each conjugate class containing more than one element.

Now $\forall\, a \in G$, $N(a)$ is a subgroup of G. Therefore by Lagrange's theorem, $o[N(a)]$ is a divisor of $o(G)$. Also $a \notin Z \Rightarrow N(a) \neq G \Rightarrow o[N(a)] < o(G)$. Therefore if $a \notin Z$, then $o[N(a)]$ must be of the form p^{n_a} where n_a is some integer such that $1 \leqslant n_a < n$. Suppose there are exactly z elements in Z *i.e.*, let $o(Z) = z$. Then the class equation (1) gives

$$p^n = z + \Sigma \frac{p^n}{p^{n_a}}, \text{ where each } n_a \text{ is some integer such that } 1 \leqslant n_a < n.$$

$$\therefore \quad z = p^n - \Sigma \frac{p^n}{p^{n_a}}, \qquad \ldots(2)$$

where n_a's are some positive integers each being less than n.

Now $p \mid p^n$. Also p divides each term in the Σ of the right hand side of (2) because each $n_a < n$. Thus we see that p is a divisor of the right hand side of (2). Therefore p is a divisor of z. Now $e \in Z$. Therefore $z \neq 0$. Therefore z is a positive integer divisible by the prime p. Therefore $z > 1$. Hence Z must contain an element besides e. Therefore $Z \neq \{e\}$.

C 8/ *y.* *If $o(G) = p^2$ where p is a prime number, then G is abelian.* **(Agra 1986; Kumayun 77; Kanpur 80; Meerut 81; B.H.U. 87; G.N.D.U. Amritsar 87)**

Proof. We shall show that the centre Z of G is equal to G itself. Then obviously G will be an abelian group.

Since p is a prime number, therefore by the previous theorem $Z \neq \{e\}$. Therefore $o(Z) > 1$. But Z is a subgroup of G, therefore $o(Z)$ must be a divisor of $o(G)$ *i.e.*, $o(Z)$ must be a divisor of p^2. Since p is prime, therefore either $o(Z) = p$ or p^2.

If $o(Z) = p^2$, then $Z = G$ and our proof is complete.

Now suppose that $o(Z) = p$. Then $o(Z) < o(G)$ because $p < p^2$. Therefore there must be an element which is in G but which is not in Z. Let $a \in G$ and $a \notin Z$.

Now $N(a)$ is a subgroup of G and $a \in N(a)$. Also $x \in Z \Rightarrow xa = ax$ and this implies $x \in N(a)$. Thus $Z \subseteq N(a)$. Since $a \notin Z$, therefore the number of elements in $N(a)$ is $> p$ *i.e.*, $o[N(a)] > p$. But order of $N(a)$ must be a divisor of p^2. Therefore

$o\,[N(a)]$ must be equal to p^2. Then $N(a)=G$. Therefore $a \in Z$ and thus we get a contradiction.

Therefore it is not possible that $o\,(Z)=p$. Hence the only possibility is that

$$o\,(Z)=p^2 \Rightarrow Z=G \Rightarrow G \text{ is abelian.}$$