Dr. O. P. Raman

Dept. of Mathematics

For T.D.C. Part III

Paper-6

Gr—[redacted] A

Theorem 2. Cauchy's theorem. *Suppose G is a finite group and $p \mid o(G)$ where p is a prime number. Then there is an element a in G such that $o(a)=p$.* **(Meerut 1980)**

Proof. We shall prove the theorem by induction on $o(G)$. Assuming that the theorem is true for groups of order less than that of G, we shall prove that it is also true for G. To start the induction we note that the theorem is vacuously true for groups of order one.

If there exists a subgroup $H \neq G$ of G such that $p \mid o(H)$, then by our induction hypothesis the theorem is true for H because $o(H) < o(G)$. Therefore there exists an element $a \in G$ such that $o(a)=p$. But $a \in H \Rightarrow a \in G$ because $H \subset G$. Therefore there exists an element $a \in G$ such that $o(a)=p$.

So let us now assume that p is not a divisor of the ordet of any proper subgroup of G. Let Z be the centre of G. We write the class equation for G in the form :

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

[See theorem 6, page 201]

Now $N(a)$ is a subgroup of G. If $a \notin Z$, then $N(a) \neq G$ and so p is not a divisor of $o[N(a)]$. But $p \mid o(G)$. Therefore

$$p \mid \frac{o(G)}{o[N(a)]} \text{ if } a \notin Z.$$

$$\therefore \; p \mid \sum_{a \notin Z} \frac{o(G)}{o[N(a)]}.$$

But $p \mid o(G)$. Therefore $p \mid \left[o(G) - \sum_{a \notin Z} \frac{o(G)}{o[N(a)]} \right]$. Then from (1), we conclude that $p \mid o(Z)$. Thus Z is a subgroup of G and the order of Z is divisible by p. But according to our assumption p is not a divisor of the order of any proper subgroup of G. Consequently $Z = G$. But then G is abelian. Therefore by Cauchy's theorem for abelian groups there exists an element in G of order p.

Theorem 3. Sylow's theorem. *Suppose G is a group of finite order and p is a prime number. If $p^m \mid o(G)$ and p^{m+1} is not a divisor of $o(G)$, then G has a subgroup of order p^m.*

(Kanpur 1986; I.A.S. 72; Vikram 76; Calicut 75; Meerut 91; B.H.U. 88)

Proof. We shall prove the theorem by induction on $o(G)$.

$$\therefore \quad o(S')=o(S/N)=\frac{o(S)}{o(N)}.$$

Therefore $o(S)=o(S').o(N)=p^{m-1}p=p^m$.

Thus S is a subgroup of G of order p^m.

This completes the proof of the theorem.

Assuming that the theorem is true for groups of order less than that of G, we shall show that it is also true for G. To start the induction we see that the theorem is obviously true if $o(G)=1$.

Let $o(G)=p^m n$ where p is not a divisor of n. If $m=0$, the theorem is obviously true. If $m=1$, the theorem is true by Cauchy's theorem. So let $m>1$. Then G is a group of composite order and so G must possess a subgroup H such that $H \neq G$.

If p is not a divisor of $\dfrac{o(G)}{o(H)}$, then $p^m \mid o(H)$ because

$$o(G)=p^m n=o(H).\frac{o(G)}{o(H)}.$$

Also p^{m+1} cannot be a divisor of $o(H)$ because then p^{m+1} will be a divisor of $o(G)$ of which $o(H)$ is a divisor. Further $o(H) < o(G)$. Therefore by our induction hypothesis, the theorem is true for H. Therefore H has a subgroup of order p^m and this will also be a subgroup of G. So let us assume that for every subgroup H of G where $H \neq G$, p is a divisor of $\dfrac{o(G)}{o(H)}$.

Consider the class equation,

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

Since $a \notin Z \Rightarrow N(a) \neq G$, therefore according to our assumption p is a divisor of $\displaystyle\sum_{a \notin Z} \frac{o(G)}{o[N(a)]}$. Also $p \mid o(G)$.

Therefore from (1), we conclude that p is a divisor of $o(Z)$. Then by Cauchy's theorem, Z has an element b of order p. Z is the centre of G. Also $N=\{b\}$ is a cyclic subgroup of Z of order p. Therefore N is a cyclic subgroup of G of order p. Since $b \in Z$, therefore N is a normal subgroup of G of order p.

[Ex. 7 on page 208 after § 4]

Now consider the quotient group $G'=G/N$.

We have $\quad o(G')=o(G)/o(N)=p^m n/p=p^{m-1}n$.

Thus $o(G') < o(G)$. Also $p^{m-1} \mid o(G')$ but p^m is not a divisor of $o(G')$. Therefore by our induction hypothesis G' has a subgroup, say S' of order p^{m-1}. We know that the natural mapping $\phi : G \to G/N$ defined by $\phi(x)=Nx \ \forall \ x \in G$ is a homomorphism of G onto G/N with kernel N. Let $S=\{x \in G : \phi(x) \in S'\}$.

Then S is a subgroup of G and $S' \cong S/N$. [See theorem 4 of § 10]