International Journal of Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.02,Issue.19,
December-2013,
Pages:2223-2234

www.semargroups.org,
www.ijsetr.com

A Study of Extra Special *P*-Group

MURTADHA ALI SHABEEB[1], DR. SWAPNIL SRIVASTAVA[2]

[1]MSc, Dept of Mathematics, SHITAS, Allahabad, UP-INDIA, Email: murtadha.ali2012@gmail.com.

[2]Asst Prof, Dept of Mathematics, SHIATS, Allahabad, UP-INDIA.

Abstract: In this dissertation we have discussed extra special p-group. A finite non- abelian p-group is called extra special p-group if its center is exactly equal to its commutator subgroup. Here we have discussed extra special p-groups and we have find that every non-abelian group of order p^3 is extra special p-group. In particular if $p = 2$ then we have two extra special p-groups one is dihedral group D_4 and another is Hamiltonian group Q_8. Here we have also discussed that if G is non-abelian group of order p^3, then $Z(G)$ has order p. We have thoroughly discussed the following theorem: Let G be a finite extra special group. Then it is central product of non-abelian groups of order p^3. In particular G is of order p^{2m+1} for some m. To prove above theorem we have gone through solvability and nilpotency in groups, Frattini subgroups, and different type of bilinear forms.

Keywords: P-Group, Hamiltonian Group.

I. INTRODUCTION

Algebra is one of the broad parts of Mathematics, together with number theory, geometry and analysis. For historical reasons, the word "algebra" has several related meaning in mathematics, as a single word or with qualifies. The word algebra originated from the title of the book **"**al-Kitab al-mukhtasar fi hisab al-jabr w'al-muqabala**"**, a book written during the ninth century the Arabian mathematician named Al-Khwarizmi. The original title was translated as the science of restoration and reduction, basically meaning transposing and combining similar terms of equations. Translated in Latin to al-jabr (the union of broken parts). led to the term we now refer to as algebra, Algebra was brought from ancient Babylon, Egypt and India to Europe via Italy by the Arabs. One of the most fundamental concept in Mathematics today is that of a group. Germs of group was present , even in ancient times , in the study of congruences of Geometric figures and also in the study of motions in space .It started taking shape in the beginning of the nineteenth century . One of the most challenging problem at this time was the problem of solvability of general polynomial equations of degree, $n \geq 5$ by field and radical operations (addition, subtraction, multiplication, division by non-zero elements and taking m^{th} roots for different m). Abel and Ruffini proved, using the structure of the set of permutations on the set of roots of the polynomials that a general n^{th} degree equation $n \geq 5$ is not solvable by field and radical operations. Galois motivated by the work of Abel , attached , to every polynomial equation a structure (called the Galois group of the polynomial equation) and proved that a polynomial equation is solvable by field and radical operations if and only if the structure (namely the Galois group) possess a property (called the solvability). In the second half of the nineteenth century the notion of the congruences of Geometric objects was generalized. The development during this period was influenced by the work of Lie, Klein, Poincare and Dehn. The importance of the study of permutation Groups, Continuous Groups, Groups of homeomorphisms and Fundamental Groups was realized and this lead to the formulation of an Abstract Group. The notion of an abstract group is present in the works of Caley and Vondyck.

The theory of groups developed slowly but steadily in the first half of the twentieth century with some very significant contributions by Burnside, Schreier, P.Hall and others. Theory of finite groups picked up momentum with the works of Brauer and his students in 1955. Theory of groups, now, has tremendous applications and interest in itself. There are four major sources in the evolution of group theory. They are:

1. Classical algebra. (J.L. Lagrange, 1770).
2. Number theory (C.F. Gauss, 1801).
3. Geometry (F.Klein, 1874).
4. Analysis (S.Lie, 1874, H. Poincare and F. Klein, 1876).

A. Objectives

- To study extra special p −group.
- To find extra special p −groups of different orders.

B. Commutators

Definition 1: Let G be a group. An element of the form, $a^{-1}b^{-1}ab$ which is denoted by (a, b) is called a commutator. The subgroup G' of G generated by all commutators of G is called the commutator Subgroup or the derived subgroup of G and denoted by $[G, G]$. Thus $G'=[G, G]=\langle (a, b) \mid a, b \in G \rangle$.

Definition 2: Let A and B be subsets of a group G.The subgroup generated by $\{(a, b) \mid a \in A, b \in B\}$ is denoted by $[A, B]$.

Proposition: Let G be a group and a, b and c be elements of G.

1. $(a, b)=\{e\}$ if and only if a and b commute.
2. $ba(a, b)=ab$.
3. $(a,b)^{-1}=(b, a)$.
4. $[A, B]=[B, A]$.
5. $(ab, c)=(a, c)^{b}(b, c)$.
6. $(a, bc)=(a,c)\ (a, b)^{c}$.
7. $(a, b)^{c}=(a^{c}, b)=(a, b^{c})$. Where a^{c} means $c^{-1}ac$.

From (above proposition 1), we understand that commutators measure, so to speak, how non-abelian a group is. When the set of commutators consists of 1 only, then the group is abelian. Rather sloppily, the more nonidentity commutators a group has, the more elements of G fail to commute with other elements of G, and the more non-abelian G is.

Corollary: $[G, G] \trianglelefteq G$.

Proof: To prove $G' \trianglelefteq G$, let $(a, b) \in G'$ and $g \in G$.

$g\ (a, b)\ g^{-1}=g(\ a^{-1}\ b^{-1}ab)\ g^{-1}=(g\ \ a^{-1}\ g^{-1})\ (g\ \ b^{-1}\ g^{-1})\ (g\ a\ g^{-1})\ (g\ \ b\ g^{-1})$. Just inserted $g^{-1}g$ between each elements. Now note that $(g\ a\ g^{-1})$ $= (g\ a^{-1}\ g^{-1})^{-1}$.Similarly $(g\ \ b\ g^{-1}) = (g\ b^{-1}\ g^{-1})^{-1}$. So we have $g\ (\ a^{-1}\ b^{-1}ab)\ g^{-1}= (g\ a^{-1}\ g^{-1})^{-1}$ $(g\ b^{-1}\ g^{-1})^{-1}(g\ \ a^{-1}\ g^{-1})(g\ \ a^{-1}\ g^{-1})(g\ \ b^{-1}\ g^{-1})$.

Theorem 1: Let H be a normal subgroup of G. Then G/H is abelian if and only if $G' \subseteq H$. Also if H is any subgroup of G containing G', then it is normal in G.

Proof: G/H is abelian $\Leftrightarrow xH * yH = yH * xH$ for all $x, y \in G \Leftrightarrow\ xyH = yxH \Leftrightarrow x^{-1}y^{-1}xyH = H$ for all $x, y \in G\ \ \Leftrightarrow x^{-1}y^{-1}xy\ y \in H$ for all $x, y \in G \Leftrightarrow$ $(x, y) \in H$ for all $x, y \in G \Leftrightarrow \langle (x, y) \mid x, y \in G \rangle$ is a subgroup of $H \Leftrightarrow G'$ is a subgroup of H.

Remark: The commutator subgroup is the smallest normal subgroup of G by which if we factor we get an abelian group. The quotient group G/G' is the largest quotient group of G which is abelian. The group G/G' is called the abelianizer of G and is denoted by G_{ab}.

Definition 3: If G is nonabelian simple group then $G' = G$. A group G is said to be perfect if its commutator subgroup G' is G itself. Thus a nonabelian simple group is always perfect.

Example 1: $S_3{}'=A_3$: $S_3/A_3 \cong \{1, -1\}$ is abelian group. Hence $S_3{}' \subseteq A_3$. Since S_3 is nonabelian, $S_3{}' \neq \{I\}$ and since A_3 has no nontrivial proper subgroup $S_3{}' = A_3$.

Example 2: $S_4{}'=A_4$: $S_4/A_4 \cong \{1, -1\}$ is abelian and therefore $S_4{}' \subseteq A_4$. The subgroups of A_4 which are normal in S_4 are A_4 ,V_4 and the trivial group. Since S_4 is nonabelian it's commutator subgroup is nontrivial. Further since $S_4/V_4 \cong S_3$ is nonabelian. Thus $S_4{}' = A_4$.

Example 3: For $n \geq 5$, $S_n{}' = A_n$: Since $S_n/A_n \cong \{1, -1\}$ is abelian, $S_n{}' \subseteq A_n$. Further for $n \geq 5$, A_n is simple. Thus A_n has no nontrivial proper normal subgroups and since S_n is nonabelian, $S_n{}' = A_n$.

Proposition: Let f be a surjective homomorphism from H to K. Then $f(H')=K'$.

Proof: Since $f((a, b))=f(a^{-1}b^{-1}ab)=f(a)^{-1}f(b)^{-1}f(a)f(b)$ $=(f(a), f(b))$, it follows that $f(H') \subseteq K'$. Further let (c, d) be a commutator in K. Since f is surjective, there exist $a, b \in H$ such that $f(a)=c$, $f(b)=d$. Then (c, d) $=(f(a), f(b))=f((a, b)) \in f(H')$. Thus all commutators of K are in $f(H')$ and so $K' \subseteq f(H)$.

Corollary: Let $H \trianglelefteq G$. Then $(G/H)'=G'H/H$.

Proof: The quotient map v from G to G/H is a surjective homomorphism and so $(G/H)'=v(G') = \{g'H \mid g' \in G'\}= \{g'hH \mid g' \in G', h \in H\}=G'H/H$.

C. Solvable Groups

Definition1: Let G be a group. Define subgroups G^n of G inductively as follows: Define $G^1 = G'$. Assuming that G^n has already been defined, define $G^{n+1} =[G^n, G^n]$. Thus $G = G^0 \trianglerighteq G^1 \trianglerighteq G^2 \trianglerighteq \ldots \trianglerighteq G^n \trianglerighteq G^{n+1} \trianglerighteq \ldots$of G. This series is called the Commutator Series or the Derrived Series of G and G^n is called the n^{th} term of the derived series.

Definition 2: A group G is said to be Solvable (or Soluble) if the derived series of G terminates to $\{e\}$ after finitely many steps. The smallest n such that $G^n = \{e\}$ is called the derived length of G.

Example 1: The derived series of S_3 is: $S_3^{\,0} = S_3$, $S_3^{\,1} = A_3$, $S_3^{\,2} = \{I\}$. S_3 is solvable of derived length 2.

Example 2: The derived series of S_4 is $S_4^{\,0}=S_4$, $S_4^{\,1}=A_3$, $S_4^{\,2}=V_4$, $S_4^{\,3}=\{I\}$. S_4 is solvable of derived length 3.

Example 3: A_5 is nonabelian simple group, thus $A_5' = A_5$. The derived series of A_5 is $A_5^{\,i} = A_5$ for all i. Thus A_5 insolvable.

Remark: Every abelian group is solvable. Since $G' = \{e\}$, then the derived series of G is $G \rhd \{e\}$ of length 1.

Proposition: A Subgroup of solvable group is solvable.

Proof: Let G be a solvable group, H a subgroup of G. $H = H^0 \subseteq G^0 = G$. $H' = [H,H] \subseteq [G,G] = G'$. Suppose $H^n \subseteq G^n$. Thus $H^{n+1} = [H^n, H^n] \subseteq [G^n, G^n] = G^{n+1}$.

Proposition: Homomorphic image of a solvable group is solvable.

Proof: Suppose that G is a solvable group and f: $G \to H$ is surjective homomrphism . $G' = [G, G] = \langle (a, b) \mid a, b \in G \rangle$. $f((a, b)) = f(a^{-1}b^{-1}ab) = f(a)^{-1}f(b)^{-1}f(a)f(b)$ $= (f(a), f(b))$. Therefore $f([G,G]) = [f(G), fG)]$. Thus $f(G)' = H'$.

Proposition: A group G is solvable if and only if it has a normal series with abelian factors.

Proof: If G is solvable, then the derived series $G = G^0 \trianglerighteq G^1 \trianglerighteq G^2 \trianglerighteq \ldots \trianglerighteq G^n = \{e\}$ is a normal series with abelian factors. Conversely suppose that G has a normal series $G = G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_n = \{ e \}$ with abelian factors, i.e. G_i / G_{i+1} is abelian $\forall i$. We show, by induction, that $G^i \subseteq G_i \forall i$. $= G^0 = G = G_0$. $G_0 / G_1 = G / G_1$ is abelian, then $G^1 \subseteq G_1$. Suppose inductively $G^r \subseteq G_r$. G_r / G_{r+1} is abelian, then $[G_r, G_r] \subseteq G_{r+1}$. Thus $[G^r, G^r] \subseteq [G_r, G_r] \subseteq G_{r+1}$. Then $G^{r+1} \subseteq G_{r+1}$. Hence G is solvable.

Example 4: S_3 is solvable for $S_3 \rhd A_3 \rhd \{ I \}$ is a normal series of S_3 with abelian factors.

Example 5: S_4 is solvable for $S_4 \rhd A_4 \rhd V_4 \rhd \{ I \}$ is a normal series of S_4 with abelian factors.

Example 6: For $n \geq 5$, S_n is not solvable $S_n \rhd A_n \rhd \{ I \}$ and $S_n \rhd \{ I \}$ are the only normal series and none of them are with abelian factors.

Proposition: Quotient group of a solvable group is solvable.

Proposition: Let G be a group and H is a solvable normal subgroup of G such that G/H is solvable. Then G is also solvable.

Proof: Since H is solvable it has a normal series $H = H^0 \trianglerighteq H^1 \trianglerighteq H^2 \trianglerighteq \ldots \trianglerighteq H^s \trianglerighteq \{e\}$. Since G/H is solvable it has a normal series $G/H = (G/H)^0 \trianglerighteq (G/H)^1 \trianglerighteq (G/H)^2 \trianglerighteq \ldots \trianglerighteq (G/H)^t = \{H\}$ for some $s, t \in N$. Since $G^i H/H = (G/H)^i$, so that G^t is a subgroup of H. Thus $G^{(t+s)}$ is a subgroup of $H^s = \{e\}$. Therefore $G^{(t+s)} = \{e\}$.

Proposition: Let G be a group and H, K solvable subgroups of G. Suppose that $K \trianglelefteq G$. Then HK is a solvable subgroup.

Proof: Since $K \trianglelefteq G$, $HK = KH$ and so HK is a subgroup of G. Since H is solvable, $H/H \cap K$ is solvable. Then $H/H \cap K$ is isomorphic to HK/K . Hence HK/K and K both are solvable. Thus HK is solvable.

Proposition: A maximal solvable normal subgroup of a group (if exists) is largest solvable normal subgroup.

Proof: If M is a maximal solvable normal subgroup and H a solvable normal subgroup, then HM is also solvable normal subgroup. Since M supposed to be maximal, $HM = M$ and so $H \subseteq M$.

Corollary: A solvable group is simple if and only if it is a cyclic group of prime order.

Proof: Assume that G is prime cyclic, then it is abelian. So $G' = [G,G] = \{e\}$. Hence the derived series of G is $G \rhd \{e\}$. So G is solvable. Conversely, let G be a solvable which is simple. Then $G' = [G,G]$ is a subgroup of G. Since G is simple, it has no normal subgroup. Thus $[G,G] = \{e\}$ so G is abelian. Hence it is prime cyclic group.

Example 7: Every group of order pq where p and q are prime is solvable: If $p = q$, then $|G| = p^2$ and so it is abelian. Hence it is solvable. Suppose that $p \neq q$ and $p > q$. Then the $Sylow\, p-subgroup\, P$ of G is normal. Then P and G/P (prime cyclic) are solvable. Hence G is solvable.

Example 8: Every group of prime power order is solvable: Let $|G|=p^n$. The proof is by induction on n. If $n=1$, then G is prime cyclic and so solvable. Assume that the result is true for all those groups of orders p^m, $m<n$. Since G is prime power order $Z(G)\neq\{e\}$. Hence $|G/Z(G)|=p^m$ for some $m<n$. By induction hypothesis $G/Z(G)$is solvable. Since $Z(G)$is abelian, thus G is solvable .

Example 9: Every group G of order pqr where p, q and r are distinct primes is solvable: The $Sylow\,r-subgroup$ R of G is normal which (prime cyclic) is solvable. Also $|G/R|=pq$ and so G/R is also solvable. Hence G is solvable.

D. Nilpotent Groups

Definition 1: Let G be a group. Define subgroups $L_n(G)$ inductively as follows: $L_0(G)=G$, $L_1(G)=[G,L_0(G)]=[G,G]=G'$. Assuming that $L_n(G)$ has already been defined. Define $L_{n+1}(G)=[G,L_n(G)]$. $L_0(G)=G\trianglelefteq G$, $L_1(G)=[G,L_0(G)]=[G,G]\trianglelefteq L_0(G)=G$. Assume $L_n(G)\trianglelefteq G$. Since if A and B are normal in G, then $[A,B]$ is also normal in G. So $L_{n+1}(G)=[G,L_n(G)]\trianglelefteq G$ and $L_{n+1}(G)\trianglelefteq L_n(G)$. Therefore by induction hypothesis this is true for all n. This gives a descending series $G=L_0(G)\trianglerighteq L_1(G)\trianglerighteq L_2(G)\trianglerighteq\ldots\trianglerighteq L_n(G)\trianglerighteq$ ..of G called the **Lower Central Series** of G. $L_0(G)=G=G^0$, $L_1(G)=[G,G]=G'$. Assume $G^n\trianglelefteq L_n(G)$. $L_{n+1}(G)=[G,L_n(G)]$. Since $G^n\trianglelefteq G$ and $G^n\trianglelefteq L_n(G)$. Then $[G^n,G^n]\trianglelefteq[G,L_n(G)]$. Thus $G^{n+1}\trianglelefteq L_{n+1}(G)$. Therefore by induction hypothesis this is true for all n.

Definition 2: Define normal subgroups $Z_n(G)$ of G inductively as follows: Define normal subgroup $Z_0(G)=\{e\}$, $Z_1(G)=Z(G)$ the center of G. Observe that $Z_1(G)/Z_0(G)=Z(G/Z_0(G))$the center of $G/Z_0(G)$. Supposing that $Z_n(G)$ has already been defined, define $Z_{n+1}(G)$ by the equation $Z_{n+1}(G)/Z_n(G)=Z(G/Z_n(G))$. Thus we get an ascending series $\{e\}=Z_0(G)\trianglelefteq Z_1(G)\trianglelefteq Z_2(G)\trianglelefteq\ldots\trianglelefteq Z_n(G)\trianglelefteq\ldots$ of normal subgroups of G . This series is called the Upper Central Series of G .

Example 1: S_3, $Z_0(S_3)=\{I\}$, $Z_1(S_3)=\{I\}$, $Z(S_3/Z_1(S_3))=Z_2(S_3)/Z_1(S_3)=Z_2(S_3)/\{I\}=Z(S_3/\{I\})=Z_1(S_3)=Z_2(S_3)$.

Theorem 1: The lower central series of G terminates to $\{e\}$ at the n^{th} step if and only if the upper central series terminates to G at the n^{th} step (i.e. $L_n(G)=\{e\}$ if and only if $Z_n(G)=G$).

proof: Suppose that $L_n(G)=\{e\}$. We show, by induction on i, that $L_{n-i}(G)\subseteq Z_i(G)\ \forall\ i$. For $i=0$, $L_{n-0}(G)=L_n(G)=\{e\}=Z_0(G)$ and so the result is true for 0. Assume that $L_{n-i}(G)\subseteq Z_i(G)$. We show that $L_{n-(i+1)}(G)\subseteq Z_{i+1}(G)$. Let $a\in L_{n-i-1}(G)$. Since $L_{n-i}(G)=[G,L_{n-i-1}(G)]$, $xax^{-1}a^{-1}\in L_{n-i}(G)\subseteq Z_i(G)\forall\ x\in G$. This shows that $xZ_i(G)aZ_i(G)=aZ_i(G)xZ_i(G)\ \forall\ x\in G$.Thus $aZ_i(G)$ belongs to the center of $G/Z_i(G)$. By the definition $a\in Z_{i+1}(G)$. Putting $i=n$ we find that $Z_n(G)$. Conversely suppose that $Z_n(G)=G$. We show, by induction, that $L_i(G)\subseteq Z_{n-i}(G)\forall\ i$. For $i=0$, $L_0(G)=Z_n(G)$ and so the result is true for $i=0$. Assume that $L_i(G)\subseteq Z_{n-i}(G)$. We show that $L_{i+1}(G)\subseteq Z_{n-i-1}(G)$. From the definition of $L_{i+1}(G)$, it suffices to show that $xax^{-1}a^{-1}\in Z_{n-i-1}(G)\ \forall\ x\in G$ and $a\in L_i(G)$. Let $a\in L_i(G)$. Since $L_i(G)$ is assumed to be contained in $Z_{n-i}(G)$, $a\in Z_{n-i}(G)$. But, then by the definition of Z_{n-i}, $aZ_{n-i-1}(G)$ belongs to the center of $G/Z_{n-i-1}(G)$. Thus $xZ_{n-i-1}(G)aZ_{n-i-1}(G)=aZ_{n-i-1}(G)xZ_{n-i-1}(G)$ for all $x\in G$ .This means that $xa(ax)^{-1}\in Z_{n-i-1}(G)$ $\forall x\in G$. This completes the proof of the fact that $L_i(G)\subseteq Z_{n-i}(G)\ \forall i$. Putting $i=n$, we get that $L_n(G)=Z_0(G)=\{e\}$.

Definition 3: A group G is said to be nilpotent if $L_n(G)=\{e\}$ or equivalently $Z_n(G)=G$ for some n . A group G is said to be nilpotent of class n if $L_n(G)=\{e\}$ but $L_{n-1}(G)\neq\{e\}$ or equivalently $Z_n(G)=G$ but $Z_{n-1}(G)\neq G$.

Proposition: Every nilpotent group is solvable.

Proof: Let G be a nilpotent group. Therefore the lower central series must terminates to $\{e\}$ at the n^{th} step, i.e. $L_n(G)=\{e\}$. Then $G=L_0(G)\trianglerighteq L_1(G)\trianglerighteq L_2(G)\trianglerighteq\ldots\trianglerighteq L_n(G)=\{e\}$. Since $G^n\trianglelefteq L_n(G)$. Thus $G^n=\{e\}$. Hence $G=G^0\trianglerighteq G^1\trianglerighteq G^2\trianglerighteq\ldots\trianglerighteq G^n\trianglerighteq=\{e\}$. Which shows that G is solvable.

Remark: A solvable group need not be nilpotent. For example in S_3, $L_0(S_3)=S_3$, $L_1(S_3)=[S_3,S_3]=A_3$, $L_2(S_3)=[S_3,A_3]=A_3$. Therefore lower central series not terminates to $\{e\}$.

Proposition: A Subgroup of nilpotent group is nilpotent.

Proof: Let H be a subgroup of nilpotent group G. Since $H\subseteq G$. Thus $L_0(H)\subseteq L_0(G)$. Assume that $L_i(H)\subseteq L_i(G)$. $L_{i+1}(H)=[H,L_i(H)]\subseteq[G,L_i(G)]$. Thus $L_{i+1}(H)\subseteq L_i(G)\forall i$.

Proposition: Homomorphic image of a nilpotent group is nilpotent.

proof: Suppose $f: G_1 \to G_2$ be a surjective homomorphism. i.e. $f(G_1)=G_2$ and G is a nilpotent group .Therefore lower central series $G=L_0(G_1) \trianglerighteq L_1(G_1) \trianglerighteq L_2(G_1) \trianglerighteq \ldots \trianglerighteq L_n(G_1)=\{e_1\}$ is terminate at n^{th} step. $f(L_0(G_1))=f(G_1)=G_2=L_0(G_2)$. Assume that $f(L_n(G_1))=L_n(G_2)$. $f(L_{n+1}(G_1))=f([G_1,L_n(G_1)])=[f(G_1),f(L_n(G_1)]=[G_2,L_n(G_2)]=L_{n+1}(G_2)$. Therefore by induction hypothesis $f(L_n(G_1))=L_n(G_2)\ \forall\ n$. Since $L_n(G_1)=\{e_1\}$, $f(e_1)=e_2=L_n(G_2)$. So G_2 is also nilpotent.

Proposition: Quotient group of a nilpotent is nilpotent .

proof: Let G be a nilpotent group and $H \trianglelefteq G$. Let aH, $bH \in G/H$.

$[G/H,\ G/H]=\langle (aH)^{-1}.(bH)^{-1}.\ aH.bH \mid a,b\in G\rangle=\langle a^{-1}H.b^{-1}H\ \ aH.bH. \mid a,b\in G\rangle=\langle a^{-1}b^{-1}abH \mid a,b\in G\rangle=[G,G]H/H$ ($\because a^{-1}b^{-1}\ ab\in[G,G]$). $L_0(G/H)=G/H=L_0(G)H/H$. Assume that $L_n(G/H)=L_n(G)H/H$. $L_{n+1}(G/H)=[G/H,\ L_n(G/H)=[G/H,L_n(G)H/H]=[G,L_n(G)]H/H$ (from above)$=L_{n+1}(G)H/H=L_{n+1}(G)H/H$. Therefore by induction hypothesis, $L_n(G/H)=L_n(G)H/H$. Since G is a nilpotent group so at n^{th} step, $L_n(G)=\{e\}$. Thus $L_n(G/H)=\{e\}H/H=H/H=H$. Therefore G/H is also nilpotent.

Remark: If H and G/H are nilpotent. Then G is need not be nilpotent. For example, S_3. $A_3 \trianglelefteq S_3$, Since A_3 is abelian so it is nilpotent. $S_3/A_3 \cong \{1,-1\}$ is also abelian, so S_3/A_3 is also nilpotent. But S_3 is not nilpotent.

Proposition Direct product of finitely many nilpotent groups is nilpotent

proof: It is sufficient to prove that direct product of two nilpotent groups is nilpotent . Suppose H and K be two groups.

$$(H\times K)'=[H\times K, H\times K]$$
$$=\langle (h_1,k_1)^{-1}(h_2,k_2)^{-1}(h_1,k_1)(h_2,k_2) \mid (h_1,k_1),(h_2,k_2)\in H\times K\rangle$$
$$=\langle ({h_1}^{-1},{k_1}^{-1})({h_2}^{-1},{k_2}^{-1})(h_1,k_1)(h_2,k_2) \mid (h_1,k_1),(h_2,k_2)\in H\times K\rangle$$
$$\langle ({h_1}^{-1}{h_2}^{-1}h_1h_2,{k_1}^{-1}{k_2}^{-1}k_1k_2) \mid (h_1,k_1),(h_2,k_2)\rangle \quad (1)$$

$\in H\times K\rangle=[H,H]\times[K,K]=L_0(H\times K)=H\times K=L_0(H)\times L_0(K)$. By induction on n we have to show that $L_n(H\times K)=L_n(H)\times L_n(K)\ \forall\ n$. Assume that $L_n(H\times K)=L_n(H)\times L_n(K)$. $L_{n+1}(H\times K)=[H\times K,\ L_n(H\times K)]=[H\times K,L_n(H)\times L_n(K)]=[H,L_n(H)]\times[K,L_n(K)]$(from above). $L_{n+1}(H)\times L_{n+1}(K)$. So by induction hypothesis, $L_n(H\times K)=L_n(H)\times L_n(K)\ \forall\ n$. Since H and K are nilpotent. So suppose $L_n(H)=\{e\}$ and $L_n(K)=\{e\}$. Let $k=max(m,n)$. Then $L_k(H\times K)=L_k(H)\times L_k(K)=\{e\}\times\{e\}=\{(e,e)\}$.

Proposition Let G be a nontrivial nilpotent group. Then $Z(G)\neq\{e\}$. Thus in a nontrivial nilpotent group there is an element different from identity which commute with each elements of the group.

Proof: Suppose that $Z(G)=\{e\}$. Then $Z_1(G)=Z(G)=\{e\}$. Since $Z_2(G)/Z_1(G)=Z_2(G)/\{e\}=Z(G/Z_1(G))=Z(G/\{e\})=Z(G)/\{e\}=\{e\}/\{e\}$, $Z_2(G)=\{e\}$. Proceeding inductively, we see that $Z_n(G)=\{e\}$ for all n. Hence $Z_n(G)$ can never be G and so G is not nilpotent.

Remark: A solvable group need not be nilpotent: S_3 is solvable but, since $Z(S_3)=\{I\}$, it is not nilpotent .

Proposition: Let H be a normal subgroup of a group G contained in the center $Z(G)$ of G such that G/H is nilpotent. Then G is nilpotent.

Corollary: A group G is nilpotent if and only if $G/Z(G)$ is nilpotent.

Corollary: Every finite $p-group$ is nilpotent.

Proof: Every finite $p-group$ is of order p^n for some n .The proof is by induction on n. If $|G|=p$, then G is prime cyclic and so nilpotent. Assume that every group of order p^m, $m<n$ is nilpotent . Let G be a group of order p^n. Then $Z(G)\neq\{e\}$. Hence $|G/Z(G)|=p^m$, $m<n$. by induction hypothesis $G/Z(G)$ is nilpotent and so G is nilpotent.

Corollary: If All sylow subgroups of a finite group are normal, then the group is nilpotent.

Proof: If All sylow subgroups are normal, then it is direct product of it's sylow subgroups which are prime power ordered groups. Since prime power ordered groups are nilpotent and direct product of nilpotent groups are nilpotent, then the group is nilpotent.

Corollary: Maximal normal nilpotent subgroup is the largest nilpotent subgroup.

Definition 4: Let H be a subgroup of a group G. Define a sequence $\{N_G^{\ n}(H) \mid n\in N\cup\{0\}\}$ of subgroups of G inductively as follows: Define $N_G^{\ 0}(H)=H$. Assuming that

$N_G^n(H)$ has already been defined, define $N_G^{n+1}(H) = N_G(N_G^n(H))$. Thus we get a ascending chain $H=N_G^0(H)\trianglelefteq N_G^1(H)\trianglelefteq N_G^2(H)\trianglelefteq \ldots \trianglelefteq N_G^n(H)\trianglelefteq \ldots$

Proposition: Let G be a nilpotent group of order n . Then $N_G^n(H)=G$ for all subgroups H of G .

Proof: We show by induction on i that $N_G^i(H)\supseteq Z_i(G)$ $\forall i$. $Z_0(G)=\{e\}\subseteq H=N_G^0(H)$, $Z_1(G)=Z(G)\subseteq N_G(H)$ ($\because a \in Z(G)\Longrightarrow aH= Ha$). Assume that $N_G^i(H)\supseteq Z_i(G)$. Then to show that $Z_{i+1}(G)\subseteq N_G^{i+1}(H)$, or $a\, Z_{i+1}(G)\Rightarrow a\, N_G^i(H)=N_G^i(H)\, a$, or $axa^{-1}\in N_G^i(H)$ $\forall x\in N_G^i(H)$. $Z_{i+1}(G)/Z_i(G)=Z(G/Z_i(G))$. $a\in Z_{i+1}(G)\Rightarrow aZ_i(G)\cdot xZ_i(G)= xZ_i(G)\cdot aZ_i(G)\Rightarrow axZ_i(G)=xaZ_i(G)\forall x\in G\Rightarrow Z_i(G)ax =Z_i(G)xa$ $\forall x\in G\Rightarrow axa^{-1}x^{-1}\in Z_i(G)\forall x\in G\Rightarrow axa^{-1}x^{-1}$ $\in Z_i(G)$ $\forall x\in N_G^i(H)$ ($N_G^i(H)\subseteq G$)$\Rightarrow axa^{-1}x^{-1}\in N_G^i(H)$ ($\because Z_i(G)\subseteq N_G^i(H)$)$\Rightarrow axa^{-1}\in N_G^i(H)\forall x\in N_G^i(H)\Rightarrow a\in N_G$ ($N_G^i(H)$) $\forall x\in N_G^i(H)\Rightarrow a\in N_G^{i+1}(H)\forall i$. Thus $Z_{i+1}(G)$ $\subseteq N_G^{i+1}(H)$. Since G is nilpotent group of index n. Therefore $Z_n(G)=G$. Since $Z_n(G)\subseteq N_G^n(H)$. $G\subseteq$ $N_G^n(H)\subseteq G$. Thus $G=N_G^n(H)\forall$ subgroup H of G.

Definition 5: A group G is said to satisfy Normalizer Condition if every proper subgroup is properly contained in its normalizer.

Corollary: Every nilpotent group satisfies normalizer condition.

Proof: Let G be a nilpotent group of class n. Then $N_G^n(H)=G$ for all subgroups H. If H is a proper subgroup and it is not properly contained in $N_G(H)$ then $N_G(H) = H$ and so $N_G^n(H)=H\neq G$, a contradiction.

Proposition: If a finite group satisfies normalizer condition, then all its sylow subgroups are normal.

Proof: Suppose that G satisfies normalizer condition. Let P be a sylow subgroups of G. Consider $N_G(P)$ the normalizer of P. Then N_G $(N_G(P))=N_G(P)$. Hence $N_G^n(P)=N_G(P)\,\forall n\geq 1$. Since the group satisfies the normalizer condition, $N_G(P)$ cannot be a proper subgroup of G. Thus $N_G(P)=G$ and so P is normal in G.

Corollary: A finite group G is nilpotent if and only if all it's sylow subgroups are normal in G.

Proof: Suppose G is nilpotent then all it is Sylow subgroups are normal. Thus G is direct product of it is sylow subgroups. Conversely suppose all sylow subgroups are normal. So G is direct product of it is Sylow subgroups. We know that every finite $p-groups$ are nilpotent. So all sylow subgroups are nilpotent. Since direct product of nilpotent groups are nilpotent. Thus G is nilpotent.

Corollary: A finite nilpotent group is direct product of it's sylow subgroups.

Theorem 2: ($Wielandt$)**.** A finite group is nilpotent if and only if all it's maximal subgroups are normal.

Proof: Let G be a finite nilpotent group and M a maximal subgroup of G. Then, since it satisfies normalizer condition, $N_G(M)$ properly contains M. Since M is maximal, $N_G(M)=G$ and so M is normal. Conversely suppose that all maximal subgroups of G are normal. We show that all sylow subgroups are normal. Let P be a $Sylow\ p-subgroup$ of G. Suppose that $N_G(P)\neq G$. Since G is finite there is a maximal subgroup M containing $N_G(P)$. But then, $N_G(M)=M$ a contradiction to the supposition that all maximal subgroups are normal. Hence all sylow subgroups are normal and so G is nilpotent.

E. Frattini Subgroup

Definition 1: Let G be a group. If G has no maximal subgroup, then we define the Frattini subgroup of G denoted by $\Phi(G)$ to be G itself. If G has maximal subgroup then Frattini subgroup $\Phi(G)$ of G is defined to be the intersection of all maximal subgroup of G. Thus if M denotes the family of all maximal subgroups of G, then $\Phi(G)=\bigcap_{H\in M} H$.

Example 1: $\Phi(S_2)=\{I\}$ for A_2 and $\{I,(12)\}$ are maximal subgroups of S_2. $\Phi(S_4)=\{I\}$ for A_4 and V_4, $\{I,(12)\}$ are maximal subgroups and their intersection is trivial. Also $\Phi(S_n)=\{I\}, n\geq 5$ for the only nontrivial proper normal subgroup of S_n is A_n which is not largest**.**

Definition 2: Let G be a group and $x \in G$. Then x is said to be a non-generator if whenever G is generated by x and a set X, then $G=\langle X\rangle$.

Theorem 1: The Frattini subgroup $\Phi(G)$ is the set of all non-generators of G.

proof: Suppose a is a non-generators of G and H is a maximal subgroup. If $a\notin H$, then H is a proper subgroup of $\langle H, a\rangle$, and so by maximality $\langle H, a\rangle = G$. But a is a non-generator, and hence $H = G$ which contradicts the maximality of H (maximal subgroups are always proper). Therefore $a\in H$ and as this holds for all maximal subgroups H. Thus $a\in\Phi(G)$. Conversely, suppose $a\in\Phi(G)$, so a belongs to all maximal subgroups of G; we show that a is non-generator. Assume that, for some set X, $a\in X$ and $\{a\}\cup H$ generates G. If $\langle X\rangle\neq G$, then

there exists a maximal subgroup K of Gwhich contains $\langle X \rangle$, possibly $\langle X \rangle$ itself, that is, $\langle X \rangle \leq K < G$. By supposition, $a \in K$ and so $\langle a, H \rangle = G$, hence $G \leq K$ which is impossible. Hence $\langle X \rangle = G$ and a is a non-generator.

Proposition: $\Phi(G) \trianglelefteq G$.

Proof: Let $\Phi(G) = \bigcap_{H \in M} H$. $g\Phi(G)g^{-1} = g(\bigcap_{H \in M} H)g^{-1}$ $= \bigcap_{H \in M}(gHg^{-1})$ (conjugate of maximal subgroup is maximal)$= \Phi(G)$. Hence $\Phi(G) \trianglelefteq G$.

Proposition: Let G is a finite group, H is a subgroup of G and $G = H\,\Phi(G)$ then $G = H$.

Proof: If $G \neq H$, then there exists a maximal subgroup K of G which contains H poosibly H itself. Now $\Phi(G) \leq K$ by definition, therefore $G = H\,\Phi(G) \leq K$, which is impossible. The result follows.

Proposition: (Frattini Argument)**.** If G is a finite group, $K \trianglelefteq G$ and P is a sylow subgroups of K, then $G = N_G(P)K$.

Proof: For $g \in G$, $g^{-1}Pg \subseteq g^{-1}Kg = K$, as $P \leq K \trianglelefteq G$. Hence both P and $g^{-1}Pg$ are sylow subgroups of K (they have the same order, and so by $Sylow\ 2$ they are conjugate in K). Therefore, we can find $k \in K$ to satisfy $k^{-1}(g^{-1}Pg)k = (gk)^{-1}P(gk) = P$. Thus $gk \in N_G(P)$, and so $g \in N_G(P)\,k^{-1} \subseteq N_G(P)K \subseteq G$. The result follows because this argument applies to all $g \in G$.

Theorem 2: Frattini subgroup of a finite group is nilpotent.

Proof: Let G be a finite group and P a sylow $p-subgroup$ of the Frattini subgroup. It is sufficient to show that P is normal in $\Phi(G)$. If $\Phi(G) = \{e\}$ there is nothing to do. Suppose that $\Phi(G) \neq \{e\}$. Using the Frattini Argument we have $G = N_G(P)\Phi(G)$, as $\Phi(G) \trianglelefteq G$. By with $H = N_G(P)$, we obtain $N_G(P) = G$, which gives $P \trianglelefteq \Phi(G)$. The result follows as this holds for all sylow subgroups of $\Phi(G)$.

Theorem 3: $(Wielandt)$. A finite group G is nilpotent if and only if $G' \subseteq \Phi(G)$.

Proof: Let G be a finite nilpotent and H a maximal subgroup. Then from of Wielandt H is normal subgroup of G. Since H is maximal, G/H is a group without proper subgroup and so it is prime cyclic, in particular abelian. But then $G' \subseteq H$. This show that $G' \subseteq \Phi(G)$. Conversely suppose that $G' \subseteq \Phi(G)$. Then every maximal subgroup of G contains G' and so every maximal subgroup is normal. By the of Wielandt G is nilpotent.

II. BASIC FROM LINEAR ALGEBRA

Definition 1: A ring $(R, +, \cdot)$ is a nonempty set containing at least two elements with two binary operations satisfies the following conditions:

1. $(R, +)$ is commutative group whose identity element is denoted by 0.
2. $(R, \cdot)$ is a semigroup group.
3. The binary operation $\cdot$ distributes over + from left as well as from right.

Definition 2: A field $(F,+, \cdot)$ is a nonempty set at least two elements with two binary operations satisfies the following conditions:

1. $(F,+)$ is commutative group whose identity element is denoted by 0.
2. $(F \setminus \{0\}, \cdot)$ is a commutative group whose identity element is denoted by 1.
3. The binary operation $\cdot$ distributes over + from left as well as from right.

Definition 3: Let R be a ring with identity 1. A left R –module is an abelian group $(M, +)$ together with a map $\cdot$ from $R \times M$ to M (the image of (a, m) under $\cdot$ is denoted by $a \cdot m$) such that.

1. $(a + b) \cdot m = a \cdot m + b \cdot m$
2. $a \cdot (m + n) = a \cdot m + a \cdot n$
3. $(ab) \cdot m = a \cdot (b \cdot m)$
4. $1 \cdot m = m$ for all $a, b \in R$ and $m, n, \in M$.

In the similar manner we can define right modules. We say that M is a left(right) R –module or M is a left(right) module over R.

Remark: If R is a commutative ring, then every left R –module can also be considered as a right R –module. In this case we simply say that M a R –module.

Definition 4: A module over a field F is called a vector space over F.

Example 1: Every abelian group $(A,+)$ is a Z –module.

Example 2: Let R be a ring with identity. Then $(R,+)$ is an R –module.

Definition 5: Let M be a left R –module. A subset N of M is called a submodule of M if:

1. N is a subgroup of $(M,+)$
2. The map $\cdot$ from $R \times M$ to M induces a map from $R \times N$ to N. In other words $a \cdot x \in N\ \forall a \in R$ and $x \in N$. Thus a submodule is a module at it's own right. In case of vector space submodule are called Subspace.

Definition 6: A left R –module M is said to be finitely generated if it has a finite set of generators. A finitely generated vector space V over a field K is also said to be finite dimensional.

Definition 7: Let S be a nonempty subset of a left R –module M. An element $x \in M$ is called a linear combination of members of S if:

$x = a_1x_1 + a_2x_2 + \ldots + a_nx_n$ for some $a_1, a_2, \ldots, a_n \in R$ and $x_1, x_2, \ldots, x_n \in M$.

Definition 8: A subset S of a left R –module M is called independent if:

1. $0 \notin S$
2. Given a finite subset $\{x_1, x_2, \ldots, x_n\}$of S with $x_i \neq x_j$, for $i \neq j$, $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0 \Rightarrow a_ix_i = 0\ \forall i$.

A subset which is not independent is called dependent.

Definition 9: A subset S of module M is called Linearly Independent if given a finite subset $\{x_1, x_2, \ldots, x_n\}$ of $S, x_i \neq x_j$, for $i \neq j$, $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0 \Rightarrow a_i = 0\ \forall i$. A subset S which is not linearly independent is called linearly dependent.

Definition 10: Let V be a vector space over a field K. A subset S of V is called a basis of V if it satisfies the following conditions:

1. S is a maximal linearly independent.
2. S is linearly independent and $\prec S \succ = V$.
3. Every element of V is a linear combination of elements of S and the representation of an element x as a linear combination of elements of S is unique in the sense that if

$$x = a_1x_1 + a_2x_2 + \ldots + a_nx_n = \beta_1y_1 + \beta_2y_2 + \ldots + \beta_my_m \quad (2)$$

where $x_1, x_2, \ldots, x_n$ are distinct members of S, $y_1, y_2, \ldots, y_m$ are also distinct members of S and a_i, β_j are all nonzero, then

1. $r = s$
2. After some rearrangement $a_i = \beta_i\ \forall i$
3. S is a minimal set of generators.

Definition 11: Let V be a finitely generated vector space over a field K. Then the number of elements in a basis of V is called Dimension of V over K. If V is not finitely generated then we say that it is infinite dimensional.

Definition 12: Let V be a vector space over a field F. A map $f: V \times V \to F$ is a bilinear form on V if f satisfies the following conditions:

1. $f(x + y, z) = f(x, z) + f(y, z)$
2. $f(x, y + z) = f(x, y) + f(x, z)$
3. $f(ax, y) = af(x, y) = f(x, ay)$

For all $x, y, z \in V$ and for all $a \in F$. Thus, if f is bilinear form on V, then $f(x, y)$is a scalar in F for each pair (x, y).

Proposition: Let f be a linear form on a vector space V over a field F.

1. For a fixed $x \in V$, the map $L_x: V \to F$ given by $L_x(y) = f(x, y)$, for all $y \in V$, is linear.
2. For a fixed $y \in V$, the map $L_y: V \to F$ given by $R_y(x) = f(x, y)$, for all $x \in V$, is linear.
3. For all $x \in V$, $f(0, x) = f(x, 0) = 0$.
4. If $g(x, y) = f(y, x)$ for $x, y \in V$, then g is a bilinear form on V.
5. For all $x, y, z, w \in V$, $f(x + y, z + w) = f(x, z) + f(x, w) + f(y, z) + f(y, w)$.

Example 3: In any vector space V over a field F, there is a trivial bilinear form given by $f(x, y) = 0$, where $0 \in F$ is the zero of the field F. We will refer to this form as the zero bilinear form on V which is identically zero.

Example 4: If $V = F^n$, the vector space of column vectors or $n \times 1$ matrices over F, then we can get a bilinear form f on V just like the dot product on R^n by $f(x, y) = x^ty$ for $x, y \in V$. The matrix product x^ty is a scalar in F.

Definition 13: Let L and R be the linear maps defined as: $L(x) = L_x$, $R(y) = R_y$. Then:

$$V^{\perp_R} = \{ x \in V \mid f(x, y) = 0 \in F \text{ for all } y \in V \}$$

$$V^{\perp_L} = \{ y \in V \mid f(x, y) = 0 \in F \text{ for all } v \in V \}.$$

Let f be a bilinear form on a vector space V. If $V^{\perp_R} = V^{\perp_L}$, then $V^{\perp} = V^{\perp_R} = V^{\perp_L}$ call radical of f.

Definition 14: A bilinear form f on a vector space V is said to be non-degenerate if $V^{\perp_L} = \{0\}$ or equivalently $V^{\perp_R} = \{0\}$.

Definition 15: A bilinear form f on a vector space V is symmetric if $f(x, y) = f(y, x)$ for all $x, y \in V$.

Example 5: In the (example 3.5.21) and the (example 3.5.22), the bilinear form is symmetric bilinear form.

Example 6: For the vector space $V = F^n$, any fixed matrix $A \in M_n(F)$, a bilinear form f_A on V is given by $f_A(x, y) = x^tAy$ for $x, y \in V$.A matrix $A \in M_n(F)$ is said to be symmetric if $A^t = A$. Now $(x^tAy)^t = y^tA^t(x^t)^t = y^tAx = f_A(y, x)$. On the other hand x^tAy being a scalar,

$(x^T Ay)^T = x^T Ay = f_A(x, y)$. It follows that $f_A(x, y) = f_A(y, x)$ for all for all $x, y \in F^n$. Thus, the symmetric matrix A forces the bilinear form f_A on F^n to be a symmetric form.

Definition 16: A bilinear form f on a vector space V is skew-symmetric if $f(x, y) = -f(y, x)$ for all $x, y \in V$.

Theorem 1: Let V be a finite dimensional vector space over a field F. Let $f: V \times V \longrightarrow F$ be a non-degenerate skew-symmetric bilinear form on V. Then $dim(V) = 2m$ for some $m \in N$ and there exists a basis $B=\{x_1, x_2, \ldots, x_n, y_1, y_2, \ldots y_n\}$ of V such that $f(x_i, y_i) = 1\ \forall i = 1,2, \ldots, n$ and $f(x_i, x_j) = f(y_i, y_j) = 0 \quad \forall i, j$, $f(x_i, y_j) = 0\ \forall i \neq j$.

III. EXTRA SPECIAL p-GROUP

Definition: A finite non-abelian group is called extra special p-group if $Z(G) = G' = \Phi(G)$.

A. Extra Special p-groups of order 8.

Here we have discussed extra special p-group of order 8. We have find that there are only two non-isomorphic extra special p-group of order 8, one is Q_8 and second is D_4.

Theorem 1: If G is a nonabelian group of order $2^3 = 8$ then it is isomorphic to either D_4 or Q_8.

Proof: Let G be a nonabelian group of. The non identity element in G have order 2 or 4. If all elements are of order 2, then $(ab)^2$=1 or $abab = 1$, $ba = a^2 bab^2 = aababb = a(abab)b = ab$. Thus the group is abelian. Hence there must be an element of order 4. Suppose $a \in G$ and the subgroup generated by a is of order 4. Since $< a >$ has index 2 in G, then it is a normal subgroup. Therefore $bab^{-1} \in < a >= \{1, a, a^2, a^3\}$. If $bab^{-1} = 1$ then a has order 1, so that cannot be. The same thing goes for $bab^{-1} = a^2$ since that implies that $ba^2b^{-1} = a^4$ =1, which would mean that a has order 2 so that cannot be either. If $b^{-1} = a$, then the group is abelian so this is also an impossibility. Therefore $b^{-1} = a^3 = a^{-1}$. The group $G/< a >$ has order 2, so $b^2 \in < a >=\{1, a, a^2, a^3\}$. Since b has order 2 or 4 , b^2 has order 1 or 2. Thus $b^2 = 1$ or $b^2 = a^2$. Putting this together, $G =< a, b >$ where either $a^4 = 1$, $b^2 = 1$, $bab^{-1} = a^{-1}$ or $a^4 = 1$, $b^2 = a^2$, $bab^{-1} = a^{-1}$. In the first case $G \cong D_4$ and in the second case $G \cong Q_8$.

B. Q_8 Hamiltonian Group:

One of the most famous finite groups is the quaternion group Q_8 . This group generated by the matrices

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad (3)$$

Using matrix multiplication, we have $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ and $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. Thus it is non-abelian group. Moreover 1 is the identity of Q_8 and -1 commutes with all elements of Q_8. Also, j, k have order 4 so any two of them generate the group. Therefore the presentation of Q_8 is:

$$< a, b \mid a^4 = b^4 = 1, bab^{-1} = a^{-1} >. \qquad (4)$$

Putting $i = a$, $j = b$, $k = ab$.Thus $(Q_8, .)$ is a group of order 8 called the Quaternion Group of degree 8 or Hamiltonian Group (after the name of Hamilton). $\{1, -1\}$,$\{1, -1, i, -i\}$,$\{1, -1, j, -j\}$ and $\{1, -1, k, -k\}$ are non trivial proper subgroups of Q_8. $Z(Q_8) =\{1, -1\}$,$Q_8' = \{1, -1\}$: $Q_8/\{1, -1\} \cong V_4$ is a group of order 4, therefore it is abelian. Thus $Q_8' \subseteq \{1, -1\}$. Further since Q_8 is nonabelian, $Q_8' \neq \{1\}$. Hence $Q_8' = \{1, -1\}$. $\Phi(Q_8) = \{1, -1\}$. Therefore $(Q_8) = Q_8' = \Phi(Q_8)$. Thus Q_8 is extra special group.

C. D_4 Dihedral group:

The dihedral group D_4 is one of the two non abelian groups of order 8. An example of D_4 is the symmetry group of the square. Rotating the square gives rise to four symmetries. We will label them as follows:

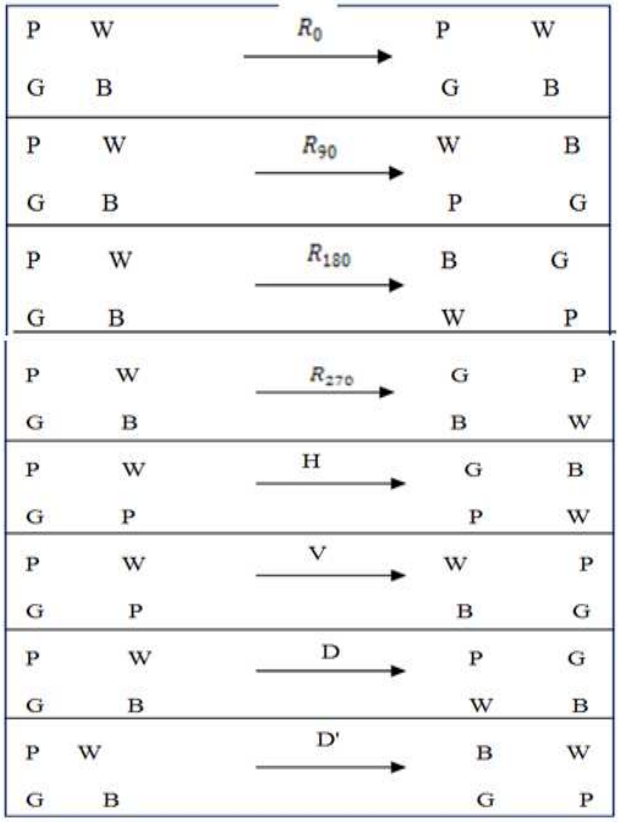

Fig 1: Symmetrics of rotation of D_4 Dihedral group

R_0 =Rotation of 0° (no change in position).
R_{90} =Rotation of 90° (counterclockwise).
R_{180} =Rotation of 180°.
R_{270} =Rotation of 270°.
H=Rotation of 180°about a horizontal axis.
V=Rotation of 180° about a vertical axis.
D=Rotation of 180° about the main diagonal.
D'=Rotation of 180° about the other diagonal.

The improper group of D_4 is $\{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$. The prober subgroups of D_4 is $\{R_0, R_{180}\}$, $\{R_0, R_{90}, R_{180}, R_{270}\}$, $\{R_0, R_{180}, H, V\}$ and $\{R_0, R_{180}, D, D'\}$. Since HD≠DH, thus D_4 is nonabelian group. The presentation of D_4 is:

$$\prec a, b \mid a^4 = b^2 = 1, bab^{-1} = a^{-1} \succ. \quad (5)$$

Also R_0 is the identity of D_4 and R_{180} commutes with all elements of D_4. The operation table for D_4 is:

TABLE 1: OPERATION TABLE FOR D_4

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D	D'	V	H
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}		D'	D	H	V
H	H	D'	V		R_0	R_{180}	R_{270}	R_{90}
V	V	D	H	D'	R_{180}	R_0	R_{90}	R_{270}

Further, $Z(D_4) = \{R_0, R_{180}\}$. $D_4' = \{R_0, R_{180}\}$: $D_4/\{R_0, R_{180}\} \cong V_4$ is a group of order 4, therefore it is abelian. Thus $D_4' \subseteq \{R_0, R_{180}\}$. Further since D_4 is nonabelian, $D_4' \neq \{R_0\}$. Hence $D_4' = \{R_0, R_{180}\}$. $\Phi(D_4) = \{R_0, R_{180}\}$. Therefore $Z(D_4) = D_4' = \Phi(D_4)$. Thus D_4 is extra special group.

IV. GROUPS OF ORDER p^3

For any prime p, there are five groups of order p^3 up to isomorphism**.** From the fundamental theorem of abelian groups there are three different abelian non-isomorphic groups of order p^3, namely Z_{p^3}, $Z_{p^2} \times Z_p$ and $Z_p \times Z_p \times Z_p$. These are non isomorphic since they have different maximal orders for their elements. The two nonabelian groups of order p^3 have different descriptions for $p = 2$ and $p \neq 2$. So will treat these cases separately.

Theorem 1: If G is nonabelian group of order p^3, then $Z(G)$ has order p.

Proof: Let G be nonabelian group of order p^3, p is prime. Since the center is a subgroup of G. Therefore it has orders $1, p, p^2$ or p^3. For $p-groups$, the center never be trivial, so it is cannot be of order 1, thus $Z(G) \neq \{e\}$. Since G is not abelian group, therefore $Z(G) \neq p^3$. If $Z(G) = p^2$, then $|G/Z(G)| = p$. Thus $G/Z(G)$ is cyclic. But by G is abelian. Contradiction with G is not abelian group. Thus $|Z(G)| = p$ and $|G/Z(G)| = p^2$.

Theorem 2: If G is nonabelian group of order p^3, then the commutator subgroup, $G' = [G, G] = \prec (a, b) \mid a, b \in G \succ$, has order p. .

Proof: $Z(G)$ is normal subgroup of G. In a group of order p^3, $|G/Z(G)| = p^2$. Thus $G/Z(G)$ is abelian. Thus $G' \subseteq Z(G)$. Since G is nonabelian, then G' is nontrivial. Thus G' must be proper subgroup of G. Therefore the only possibility is $G' = Z(G)$. Since the Frattini subgroup contained in the center of a group. Hence $\Phi(G) = Z(G)$.

Corollary: Every group of order p^3 is extra special p-group.

A. Extra Special p-group of order p^{2m+1}

A group G is said to be the Central product of it's normal subgroups $G_1, G_2, \ldots, G_r$ if :

1. $G = G_1 G_2 \ldots G_r$.
2. $Z(G) \subseteq G_i \ \forall i$ and $G/Z(G)$ is direct product of $G_1/Z(G), G_2/Z(G), \ldots, G_r/Z(G)$.
3. $[G_i, G_j] = e \ \forall i \neq j$.

Theorem 1: A finite abelian $p-group$ which every element (non-identity) having order p, which is defined as elementary abelian group, can be treated as a vector space over a field Z_p.

Proof: Let G be elementary abelian $p-group$. Define a map from $Z_p \times G$ to G such that: $\cdot(\bar{c}, a) = \bar{c} \cdot a = a^c$.

$$(\bar{\alpha} + \bar{\beta}) \cdot x = (\overline{\alpha + \beta}) \cdot x = x^{\alpha+\beta} = \underbrace{x + x + \cdots + x}_{\alpha-times} + \underbrace{x + x + \cdots + x}_{\beta-times}$$

$$= x^{\alpha} + x^{\beta} = \bar{\alpha} \cdot x + \bar{\beta} \cdot x \quad (6)$$

$$\bar{\alpha} \cdot (x + y) = (x + y)^{\alpha} = \underbrace{(x+y) + (x+y) + \cdots + (x+y)}_{\alpha-times} = \underbrace{x + x + \cdots + x}_{\alpha-times} + \underbrace{y + y + \cdots + y}_{\alpha-times} = x^{\alpha} + y^{\alpha} = \bar{\alpha} \cdot x + \bar{\alpha} \cdot y \quad (7)$$

$$(\overline{\alpha \cdot \beta}) \cdot x = (\overline{\alpha \cdot \beta}) \cdot x = (\overline{\beta \cdot \alpha}) \cdot x = x^{\beta \cdot \alpha} = \underbrace{x + x + \cdots + x}_{\alpha\beta-times}$$

$$= \underbrace{x^{\alpha} + x^{\alpha} + \cdots + x^{\alpha}}_{\beta-times} = \bar{\alpha} \cdot (\bar{\beta} \cdot x) \quad (8)$$

$$\bar{1}.x = x^1 = x \qquad (9)$$

Theorem 2: Let G be a finite extra special group. Then it is central product of non-abelian groups of order p^3. In particular G is of order p^{2m+1} for some m.

Proof: Since $G' = Z(G)$. Let $a_1, a_2 \in G$ and $x \in G$. Then $x, a_1a_2) = xa_1a_2x^{-1}(a_1a_2)^{-1} = xa_1a_2x^{-1}a_2^{-1}a_1^{-1} = xa_1x^{-1}a_1^{-1}a_1xa_2x^{-1}a_2^{-1}a_1^{-1}$. Since (x, a_1), $(x, a_2) \in Z(G)$. Thus $(x, a_1)\, a_1\, (x, a_2)\, a_1^{-1} = (x, a_1)\, (x, a_2)$. If $a_1 = a_2 = a$, then we have $(x, a^2) = (x, aa) = (x, a)\, (x, a) = (x, a)^2$. Thus by induction, we have $(x, a^k) = (x, a)^k \ \forall k \in N$. In particular $(x, a^p) = (x, a)^p = e \ \forall x \in G$. Hence $a^p \in Z(G) = G' \ \forall a \in G$. Thus $G/Z(G)$ is an elementary abelian $p-group$ and so it is a vector space over the field Z_p. Since $(x, a) \in G' = Z(G)$ and $|Z(G)| = p$. Therefore $Z(G)$ is cyclic group. Let c be a generator of $Z(G)$ such that $Z(G) = \langle c \rangle = \{ e, c, c^2, \ldots, c^{p-1} \}$. Let $x, y \in G$ and $u, v \in Z(G)$. Then $u = c^i$, $v = c^j$ for some i, j. Now $(xu, yv) = xuyv\ (xu)^{-1}(yv)^{-1} = xuyv\, u^{-1}x^{-1}\, v^{-1}y^{-1} = xyx^{-1}y^{-1} = (x, y)$. Thus we have a map $f: G/Z(G) \times G/Z(G) \longrightarrow Z(G)$ defined by $f(xZ(G), yZ(G)) = (x, y) = c^j$ for some j. Also we have a map $\theta: Z(G) \longrightarrow Z_p$ defined by $\theta(c^i) = \bar{i}$. Let $\hat{f} = \theta \circ f$. So $\hat{f}: G/Z(G) \times G/Z(G) \longrightarrow Z_p$ which satisfies $c^{\hat{f}(xZ(G), yZ(G))} = f(xZ(G), yZ(G)) = (x, y)$. Since $G/Z(G)$ is an elementary abelian $p-group$ so $\hat{f}$ is bilinear form on a vector space $G/Z(G)$. Since $(x, y) = (y, x)^{-1}$, so if $(x, y) = c^i$, then $(y, x) = c^{-i}$. Then $\hat{f}(xZ(G), yZ(G)) = -\hat{f}(yZ(G), xZ(G))$. So $\hat{f}$ is skew symmetric bilinear form. Next assume that $x \in G$ such that $\hat{f}(xZ(G), yZ(G)) = 0 \ \ \forall y \in G$. Then $\hat{f}(xZ(G), yZ(G)) = (x, y) = c^0 = e \ \ \forall y \in G$. But $(x, y) = e \ \ \forall y \in G$ implies that $x \in Z(G)$. $xZ(G) = Z(G)$ the identity element of $G/Z(G)$. Hence $\hat{f}$ is non-degenerate. Then $dim(G/Z(G)) = 2m$ for some $m \in N$ and there is a basis $B = \{x_1Z(G), x_2Z(G), \ldots, x_mZ(G), y_1Z(G), y_2Z(G), \ldots y_mZ(G)\}$ such that $\hat{f}(x_iZ(G), y_iZ(G)) = 1 \ \ \forall i, \ \ \hat{f}(x_iZ(G), y_jZ(G)) = 0 \ \ \forall i \neq j$. Also $\hat{f}(x_iZ(G), x_jZ(G)) = 0 = \hat{f}(y_iZ(G), y_jZ(G)) \ \ \forall i, j$. Let $G_i = \langle x_i, y_i \rangle$. Then each $G_i (1 \leq i \leq m)$ is a non-abelian group of order p^3. Since $|Z(G)| = p$ and $|Z(G_i)| = p$, so $Z(G) = Z(G_i) \ \forall i$. So $G = \langle x_1, x_2, \ldots, x_m, y_1, y_2, \ldots y_m \rangle$. Thus $G = G_1 \cdot G_2 \cdot \ldots \cdot G_m$. which is central product.

V. CONCLUSION

We have solved extra Special p-group of order p^3, where p is even prime discussed, we have find that one is Q_8 and second is D_4. We have proved that every non-abelian group of order p^3 is extra special p-group. We have proved that G be a finite extra special group, then it is central product of non-abelian groups of order p^3. In particular G is of order p^{2m+1} for some m.

VI. REFERENCES

[1] A. Mahalanobis, the Diffie-Hellman Key Exchange Protocol and Non-Abelian Nilpotent Groups, Israel J. Math., 165 (2008), 161 - 187.

[2] A.M. Tripathi, N. Mathu and S. Srivastav, A Study Of Nilpotent Groups Through Right Transversals Iranian Journal Of Mathematical Sciences And Informatics Vol. 4, No. 2 (2009), Pp. 49-54.

[3] Adrien Deloro, P-Rank and P-Groups in Algebraic Groups, Turk J Math 36 (2012), 578 – 582.

[4] Ahmad M. Alghamdi, Dade's Projective Conjecture For P-Block With An Extra-Special Defect Group, International Journal Of Algebra, Vol. 4, 2010, No. 11, 525 –534.

[5] Ahmad M. Alghamdi, Ordinary Weight Conjecture Implies Brauer's K(B)-Conjecture, International Journal Of Algebra, Vol. 4, 2010, No. 13, 615 – 618.

[6] Alexander Moret´O, an Answer To Two Questions Of Brewster And Yeh On M-Groups, 2009, Mathematics Department University Of Wisconsin 480 Lincoln Drive Madison WI 53706 USA.

[7] Andreas Distler, Finite Nilpotent Semigroups Of Small Coclass, Arxiv: 1205.2817v1 [Math.RA] 12 May 2012.

[8] Artur Schäfer, Masters Thesis, Two Sided and Abelian Group Ring Codes, October 2012, Aachen, Germany.

[9] C. Hopkins, Non-Abelian Groups Whose Groups Of Isomorphisms Are Abelian, The Annals Of Mathematics, 2nd Ser., 29, No. 1/4. (1927 - 1928), 508-520.

[10] C. J. E. Pinnock, Supersolubility And Some Characterizations Of Finite Supersoluble Groups, 2nd Edition, January 1998.

[11] Charles Hobby, The Frattini Subgroup Of A P-Group, 2001.

[12] Cody Clifton, Commutativity In Non-Abelian Groups, May 6, 2010.

[13] Craig Gentry, A FULLY HOMOMORPHIC ENCRYPTION SCHEME, September 2009.

[14] D. Jonah, M. Konvisser, Some Non-Abelian P-Groups With Abelian Automorphism Groups, Arch. Math. (Basel) 26 (1975), 131 - 133.

[15] David A. Craven, the Theory Of P-Groups, Hilary Term, 2008.

[16] David Bornand, Elementary Abelian Subgroups In P-Groups Of Class 2, 23 July 2009.

[17] David John Green and Pham Anh Minh, Almost All Extraspecial P-Groups Are Swan Groups, Ath/9911083v1 [Math.AT] 12 Nov 1999.

[18] Doron Hai-Reuven, Non-Solvable Graph Of A Finite Group And Solvabilizers, Rxiv: 1307.2924v1 [Math.GR] 10 Jul 2013.

[19] G. A. Miller, A Non-Abelian Group Whose Group Of Isomorphism Is Abelian, Mess. Of Math. 43 (1913-1914), 124 - 125.

[20] Geir T. Helleloid And Ursula Martin, The Automorphism Group Of A Finite P-Group Is Almost Always A P-Group, Nankai University, Tianjin, China, 2007.

[21] Geir T. Helleloid, Automorphism Groups Of Finite P-Groups: Structure and Applications, Arxiv: 0711.2816v1 [Math.GR] 18 Nov 2007.

[22] H. Heineken, H. Liebeck, The Occurrence Of Finite Groups In The Automorphism Group Of Nilpotent Groups Of Class 2, Arch. Math. (Basel) 25 (1974), 8 - 16. (1979/80), 497 - 503.

[23] H. Hilton, an Introduction To The Theory Of Groups Of Finite Order, Oxford, Clarendon Press (1908).

[24] I. M. Isaacs, the Fitting and Frattini Subgroups, 2002.

[25] J. E. Adney, T. Yen, Automorphisms Of A P-Group, Illinois J. Math. 9 (1965), 137 - 143.

[26] James Clark Beidleman And Tae Kun Seo, Generalized Frattini Subgroups Of Finite Groups, Pacific Journal Of Mathematics, Vol. 23, No. 3, 1967.

[27] Javier Otal, the Frattini Subgroup Of A Group, Spain, 2001.

[28] John C. Lennox, Finite Frattini Factors In Finitely Generated Soluble Groups1, Proceedings Of The American Mathematical Society Volume 41, Number 2, December 1973.

[29] John Cossey and Alice Whittemore1, On the Frattini Subgroup, 2001.

[30] Katrin E. Gehles, Ordinary Characters Of Finite Special Linear Groups, M.Sc. Dissertation August 2002.

[31] M. H. Jafari, Elementary Abelian P-Groups as Central Automorphism Groups, Comm. Algebra 34 (2006), 601 - 607.

[32] M. Morigi, On The Minimal Number Of Generators Of Finite Non-Abelian P-Groups Having An Abelian Automor- Phism Group, Comm. Algebra 23 (1995), 2045 - 2065.

[33] Mohammad K. Azarian, Conjectures And Questions Regarding Near Frattini Subgroups Of Generalized Free Products Of Groups, International Journal Of Algebra, Vol. 5, 2011, No. 1, 1 – 15.

[34] P. Hegarty, Minimal Abelian Automorphism Groups Of Finite Groups, Rend. Sem. Mat. Univ. Padova 94 (1995), 121 - 135.

[35] Pham Anh Minh, the Modp Cohomology Group Of Extra-Special P-Group Of Order P5 And Of Exponent P2, Math. Proc. Camb. Phil. Soc. (1996), Printed In Great Britain.

[36] Ryan J. Wisnesky, Solvable Groups, May 2005.

[37] Stuart Hendren, Extra Special Defect Groups, September 2003, A Thesis Submitted To The University Of Birmingham For The Degree Of Doctor Of Philosophy.

[38] V. K. Jain, M. K. Yadav, On Finite P-Groups Who's Automorphisms Are All Central, Israel J. Math. 189 (2012),225 - 236.

[39] Wojciech A. Trybulec, Lattice Of Subgroups Of A Group. Frattini Subgroup, Formalized Mathematics Vol.2, No.1, January–February 1991.

[40] Y. Berkovich, Z. Janko, Groups Of Prime Power Order - Volume 2, Walter De Gruyter, Berlin, New York (2008).

[41] Yark, Frattini Subgroup Of A Finite Group Is Nilpotent, 2013-03-21.