APPLICATIONS OF GROUP THEORY

Second Stage Lectures

By

Prof. Dr. Muna Abbas Ahmed

University of Baghdad\College of Science for Women\ Departement of Mathematics

Introduction

In these lectures, we study some applications of the group theory such as we study conjugate elements and conjugate groups, the converse of Lagrange theorem, P-group, Sylow P-group, Sylow theorem, Normalizer of subgroup, Nilpotent Group and solvable group. Moreover, some applications of Sylow theorems are considered.

THE CONVERSE OF LAGRANGE THEORY

Given a group G of order n, and integer m dividing n. One cannot be certain that G possesses a subgroup of order m. in fact, that is one of considerable difficulty. So in general, that is not true, for example, the subgroup A_4 of the permutation group S_4 is of order 12 and the number 6 divides 12 but A_4 hasn't subgroup of order 6. However, in this lecture, we discuss the case under which that thing is true. We begin the first case:

Theorem 1: If G is a finite abelian group of order n with a prime number p divided n, then G contains a subgroup of ordered p.

Theorem 2: Let G be a finite group with ordered n. for all prime numbers p divided n, there is a subgroup with order p.

CONJUGATE ELEMENTS

Definition 3: Let G be a group and x, y G. Then x and y is said to be **conjugate** if there is a G such that y = axa-1.

Remarks 4:

1. The conjugate relation is equivalent and hence it is made a partition on G.

2. We will refer to class of the element x by [x] = {y G| x = aya-1 }

2. The center of G is denotet by Z(G) where:

$$Z(G) = \{x\ G \mid ax = xa \text{ for all } a\ G\}$$

$$= \{x \in G \mid xa = ax \text{ for all } a \in G\}$$

3. $x \in Z(G)$ if and only if [x] contains only one element.

4. The set $C(y) = \{a \in G \mid ay = ya\}$ is said to be the **centre** of the element y.

5. C(y) is a subgroup of G.

6. There is an isomorphism between the right coset of the subgroup C(y) and the conjugate elements of y.

Remark 5: If G is a finite group, then:

$$|G| = |Z(G)| + \Sigma \text{ (where } y\ Z(G)\text{)}$$

is said to be a **conjugate class equation**.

P- Groups

Definition 6: Let p be a prime number. A group G is said to be a **P-group** if the order of each element of G is some power of p (not necessarily the same power).

Examples 7:

1. o(S3) = 6 = 2.3. It is not P-group, because S3 cannot be written as p^k for k = 0, 1, 2, …).

2. If O(G)=16, then G is P-group. Why?

3. G = {e}, then o(G)= p^0 for each prime number p.

Proposition 8:

1. Every subgroup of P-group is P-group.

Proof:

Let H be a subgroup of a P-group G. Then $o(G) = p^k$, $k = 1,2,3, \ldots$

By Lagrange's theorem, $o(H)/O(G)$. So, $O(H) = p^r$,$0 \leq r \leq k$. Hence, H is a P-group.

2. Let G be a P-group and f: G → G' be a homomorphism group. Then, f(G) is P-group.

Proof:

Since G is p- group, then G= p^k, k=0, 1, 2, 3, …) and kerf subgroup of G, then kerf is P-group, so that o(kerf) = p^r, $0 \leq r \leq k$). By 1^{st} iso th. , f(G) ≅ G\kerf . So, o(f(G)) = o(G)O(kerf) = P^{k-r} and cleary $0 \leq k\text{-}r \leq k$. This implies that f(G) is a P-group.

Corollary 9: Let H be a normal subgroup of G. If G is P-group, then both H and G/H are P-groups.

The converse of the previous proposition is
not true. The following proposition gives the necessary condition for the converse.

Proposition 10: If G is a finite group and H normal subgroup of G and both H and G\H are P-groups, then G is P-group.

Proof: Since O(G) = O(H). [G: H] = O(H) . O(G/H)
Assume that O(H)= p^r and O(G/H)= p^s. This implies that O(G) = p^{r+s} and r+s = 0, 1, 2, … . Then G is P-group.

From Corollary 9 and Proposition 10, we deduce the following.

Theorem 11: Let G be a finite group and H is a normal subgroup of G then both H and G\H are P-groups if and only if G is P-group.

Remake 12: If G_1, G_2 are P-group, then so is $G_1 x G_2$.

Proof: It is obvious

Theorem 13: Let G be a finite group. Then G is P-group if and only if the order of each element of G is a power of p.

Proof: For the First direction, Let x∈G. Then o(x) = o((x)) ((x) = is the cyclic group generated by x).
Now, since (x) subgroup of G, then (x) is a P-group (by Remark *).

Each element of G is a power of p.
Conversely, Suppose that each element of G is a power of p, and to prove that G is P-group. Suppose G is not P-group. So, there is a prime number q, $q \neq p$; such that q divides o(G). By Cauchy theorem, G contains a subgroup of order q, and hence G contains an element of order $q \neq p$ C! (since each element of G is a power of p).

Examples 14:

1. If G = S3, then o(S3) = 6 = 2.3. So the order of each element is not power of p. Hence S3 is not P-group.

2. If G = 8. Then o(8)= 23. The subgroup of 8 is { }, { , }, { , }and 8. Hence each element of 8 is a power of 2.

Proposition 15: If G is a nontrivial P-group, then Z(G) is nontrivial and $o(Z(G)) = p^k$ for $k \geq 1$.

Proof: H.W

Corollary 16. Every P-group of ordered p^2 is abelian.

Proof: Let G be an abelian group with $o(G) = p^2$ and Z(G) be the centre of G. Since G is not trivial, then $Z(G) \neq \{e\}$. Then by Lagrange's theorem o(Z(G)) = p or p^2. If o(Z(G))= p2, then G = Z(G) and so G is an abelian group.

Corollary 17. If G is P-group with order p3 and G is not abelian, then o(Z(G)) = p.
Proof: Since G is not abelian group, then $G \neq Z(G)$ and hence $o(Z(G)) \neq$ p3. Now, by Lagrange's theorem, O(Z(G)) divides O(G). Hence either O(Z(G)) =1 or o(Z(G)) = p or $o(Z(G)) = p^2$.
If o(Z(G)) =1, then Z(G) = {e} C! since Z(G) is not a trivial subgroup.
If $o(Z(G)) = p^2$, then O(G/Z) = p. Hence is a cyclic group and so G is an abelian group C! (with hypothesis). Therefore, o(Z(G)) = p.

SYLOW GROUPS

Definition 18: Let G be a finite group with $o(G) = p^m$. such that p and the integer number $m \geq 1$. Then a subgroup H of G will be called **p-sylow subgroup** of order p^m.

Remark 19:

- The integer m is the largest positive integer such that pm divides the order of G.
- H is the maximize p-subgroup of G.

Definition 20: Let H and K be two subgroups of G such that H is **conjugate** to K if and only if there is a G such that $K = aHa^{-1}$.

Remark 21:

1. If H and K are conjugate, then O(H) = O(K).

Proof: Define f: $H \to K$ by : $f(h) = aha^{-1}$. Then f is 1-1 and onto. If H is (or K) is P-group with order p^n, then so is K (or H).

2. If H and K are conjugate and H is p-sylow subgroup, then K is p-sylow subgroup.

Definition 22: Let H be a subgroup of G. The set NG(H) = N(H) = {a G| $aHa^{-1} = H$}is said to be **normalize**r of H in G.

Remark 23: If H is normal subgroup of G, then N(H) = G and if N(H) = H, then H is normalizer subgroup of G.

Theorem 24:

i. N(H) is a subgroup of G and contain H.

ii. H is a normal subgroup of N(H).

iii. N(H) is the largest normal subgroup of G containing H.

Proposition 25: Let G be a group and H be a subgroup of G. Then, there is a 1-1 and onto map between the set of all subgroups conjugate of H and the set of all right coset (left) of N(H) in G.

Corollary 26: If G is a finite group and H subgroup of G, then the number of subgroups of G which conjugate to H are divided o(G).
Proposition. If G is a finite group, then the number of elements of the set [H]K = [K:NK(H)], then the number of elements in [H]K divides o(K) and hence the number of elements in [H]K divides o(G).

SYLOW'S THEOREMS

First Sylow Theorem: Let G be a finite group with o(G) = n and a prime number p \n , then G contains a Sylow P-group.

Example 27: If o(G)=36=$3^2.2^2$, then there exists a 3-Sylow subgroup H, with O(H)=3^2=9.

Second Sylow Theorem: Let G be a finite group, with o(G) = n and p be a prime number then:

1. All Sylow P-groups are conjugate.
2. If t is the number of Sylow P-group , then there exist s≥ 0, ; t = 1 +s p .
3. t divides O(G).

Proposition 28: A Sylow P-group H is a normal subgroup if and only if H is a unique P-group.

Remark 29: Any group G is said to be simple if it has no non-trivial normal subgroup.
(i.e. if H Δ G, then either H = {e} or H = G).

SOME APPLICATIONS OF SYLOW THEOREMS

Example 30: There is no simple group with order 200.

Proof: Let G be a group with $o(G) = 200 = 5^2.2^3$.

G contains a Sylow 5-group say H and o(H) = 52 = 25 (by First Sylow Theorem).

Let t be the number of Sylow 5-group, then $t = 1 + 5k$ for $k \geq 0$.
Also, t | 200 (by Second Sylow Theorem). Now,
There exists a unique Sylow 5-group H and hence H is normal.
so G is not simple.
Now, The group G contains a Sylow 2-group with o(K) = 23 = 8 (by First Sylow Theorem) and if r is the number of Sylow 2-group, then $r = 1 + 2k$ for $k \geq 0$. Also, r \ 200 (by Second Sylow Theorem). Now,
r= {1, 5, 25}, this means there exists a three Sylow 2-group K and hence we cannot know if K is unique or not.
We cannot know if K is normal or not.

Remark: In the previous example if group G is abelian, then K is normal and hence K is unique (by Second Sylow Theorem). 12

Example 31: There is no simple group with order 30.

Proof: H.W

Definition 32. (Decomposable)
Let H and K be normal subgroups of the group G. Then G is said to be the internal direct product of H and K if :

1. $H \Delta G$ and $K \Delta G$
2. $G = HK$
3. $H \cap K = \{e\}$, then $G \approx H \times K$

Example 33: Every group G with order 35 is decomposable and cyclic.

Proof: Let G be a group with o(G) = 35. By Sylow Theorem, G contains a normal subgroup H with o(H) = 5 and normal subgroup K with o(K) = 7. In the same way of the previous example, G H × K.

o(H) = 5 and o(K) = 7 (prime numbers), then each of H and K is cyclic.
Let H = (x) and K = (y) for x H and y K. Hence x5 = e and y7 = e.
Claim that H × K **=** (x, y). For that:
Since each of 5 and 7 is a prime number, then there is t and s such that 5t +7s = 1.
Let (xi, yj) H ×K ; $0 \leq i \leq 6$, $0 \leq j \leq 4$.
Since i – j = (5t + 7s)(i - j) ⟶ 5t(i - j) + j = 7s(j – i) + i = m.
xm = xst(i - j) + j= (x5)6-j × j = exi = xi and ym = yi.
(xi, yj) = (xm, ym) = (x, y)m ⟶ H ×K = (x, y) and hence H ×K is cyclic.

Remark 34: Let G be a finite group with order pn and n = 1, 2, 3, … then:

1. $o(Z(G)) \neq p^{n-1}$
2. Every subgroup H with $o(H) = p^{n-1}$ is normal.

Exercises

1. Every group of order 45 is not simple, abelian and decomposable.
2. Every group of order 63 is not simple.
3. Every group of order 77 is cyclic, abelian and decomposable.
4. Show that the group order 30 is not simple.

FINITE NILPOTENT GROUPS AND SOLVABLE GROUPS

First: FINITE NILPOTENT GROUPS

Definition 35: Let G be a finite group, then G is said to be **a Nilpotent group** if every Sylow group of G is a normal subgroup of G.
Examples.

Proposition 36: Every finite abelian group is Nilpotent.

Proof: let G be a finite abelian group and H be a subgroup of G.
H Δ G (every subgroup of an abelian group is normal)
Every Sylow subgroup of an abelian group is normal.
G is a Nilpotent group (by definition of a Nilpotent group).

Remark 37: Every P-group G is Nilpotent (In fact G contains only one Sylow group G and hence G Δ G).

Exercise:

- 10 is Nilpotent group.
- S3 is not Nilpotent group.

Proposition 38: A finite group G is Nilpotent iff for all prime number p \ o(G), then G contains a unique Sylow P-group.

Proposition 39: Every Nilpotent group can be represented as an internal direct product of its Sylow P-group.
(i.e. if S1, S2, …, Sn are Sylow P-group of the group G, then G = S1 S2 … Sn).

Remarks 40:

1. If both G1 and G2 are P-group, then G1 x G2 is Nilpotent group.

2. The center of Nilpotent group is not trivial.

3. Every subgroup of the Nilpotent group is Nilpotent.

4. If G is the Nilpotent group and H Δ G, then is the Nilpotent group.

Definition 41: Let G be a group and H be a subgroup of G. then H is said to be **maximal** subgroup if whenever $H \leq K \leq G$, then either $H = K$ or $G = K$.

Remark 42:

- If G is a finite group, then G contains a maximal subgroup
- 2. Every subgroup contained in one (or more one) maximal subgroup.

Proposition 43: Let G be a finite group and S Sylow P-group. Let N0(S) = N. If H is a subgroup of H such that $N \leq H \leq G$, then NG(H) = H.

Proof: Let x G such that x NG(H). So xHx-1 = H. since each of S and xSx-1 is a Sylow subgroup of H, then by the second Sylow theorem, S and xSx-1 are a conjugate group. Hence there is h H such that h-1x-1Sxh = S. That implies xh $N(S) \leq H$, then xh H. Hence x H.

Proposition 44: Let G be a finite group. If every maximal subgroup of G is normal, then G is the Nilpotent group.

Remark 45: If G is a finite Nilpotent group, then every maximal subgroup of G is normal.

Second: SOLVABLE GROUPS

Definition46: Let G be a group. Then G is said to be **a solvable group** if there exists a finite set {G0, G1, G2, …, Gr}of subgroups of G that satisfy the following conditions:

a) $G = G_0, G_1, G_2, \ldots, G_r = \{e\}$

b) Every subgroup G_i is a normal subgroup in Gi-1

c) A quotient group is an abelian group for all i, $0 \leq i \leq r - 1$.

Examples 47:

- Every abelian group is solvable.
- Every P-group is solvable.

Proposition 48: Every subgroup of a solvable group is solvable.

Proof: Let H be a subgroup of a solvable group G and let $\{G = G_0, G_1, G_{2'} \ldots, G_r = \{e\}\}$ be a set of subgroups of G satisfying the conditions of solvable group. Put $H_i = G_i \cap H$. then the set $\{ H = H_0, H_1, H_2, \ldots, H_r = \{e\}\}$satisfy the following conditions

1. $H = H_0\ H_1\ H_2 \ldots H_n = \{e\}$
2. Since $H \Delta H$ and $G_i \Delta G_{i-1}$, then $Hi \Delta H_{i-1}$
3. H.W.

Proposition 49: Every finite Nilpotent group is solvable.

Remark 50: The group S_3 is solvable not Nilpotent group.

REFERENCES

[1] Chase J. and Brigitte S., Group Theory in Chemistry, Amajor Qualifying Project, Worcester Polytechnic institute, 2008 .

[2] D.M. Burton, Abstract and Linear Algebra , 1972.

[3] Joseph J.Rotman, “Afirst Course in Abstract Algebra with Applications”, 2006 .

[4] John B.Fraleigh, AFirst Course in Abstract Algebra, Seventh Edition, 2002.

[5] Joseph A.Gallian, “Contemporary Abstract Algebra”, 2010.

[**6**] Thomas W.Judson, "Abstract Algebra", Theory and Applications, 2009.
[**7**] M.S.Dresselhous, Applications of Group Theory to The Physics of Solid**.**