International Journal of Mathematics and Statistics Invention (IJMSI)
E-ISSN: 2321 – 4767 P-ISSN: 2321 - 4759
www.ijmsi.org Volume 4 Issue 1 || January. 2016 || PP-30-38

On The Properties of Finite Nonabelian Groups with Perfect Square Roots Using the Centre

Jelten, B.Naphtali
Department of Remedial Sciences, University of Jos, P.M.B. 2084, Plateau State, Nigeria

ABSTRACT: *In this paper we determine some internal properties of non abelian groups where the centre Z(G) takes its maximum size. With this restriction we discover that the group G is necessarily a group with perfect square root as shown in our results. We also show that the property of Z(G) is inherited by direct product of groups. Furthermore groups whose centre is as large as possible were constructed.*
KEY WORDS: *centralizer, conjugacy class, direct product, non abelian, perfect square root,*

I. INTRODUCTION

Let G be a finite group and H the subset of G. We denote by |G| the order of G and Z(G) the centre of the group G. On finite non abelian group a bound for the size of the centre has been achieved. Previous work on groups with perfect square roots have been identified. Furthermore other works discussed the necessary conditions on groups having perfect square roots. In this paper we use the centre to determine some of the properties of finite non abelian groups with perfect square roots. In particular the group whose centre is of maximum size. Throughout this paper unless otherwise stated, G is finite and non abelian.

Definition 1.1

If a group G has the property that $rs = sr$ for every $r, s \in G$, we say that the group is abelian. A group is non-abelian if there exists some pairs of elements $r, s \in G$ such that $rs \neq sr$. This definition characterises abelian and non abelian groups.

Definition 1.2

Let G be a group and H < G. For q $\in$ G the subset Hq = {hq:h $\in$ H} of G is called a right coset of H in G. Distinct right cosets of H in G form a partition of G. Left coset is similarly defined. The number of distinct right cosets of H in G is written as |G:H| = |G/H| and is called the index of H in G. If G is finite so is H and G is partitioned into |G:H| cosets each of order |H|. We note that |H| and |G:H| divide |G|.

Next we define an important concept.

Definition 1.3

A subgroup N of G such that every left coset is a right coset and vice versa is called a normal subgroup of G. That is Nx = xN or $x^{-1}Nx \leq N$ and we write N $\triangleleft$ G. Normal subgroup is characterized by the fact that it does not possess any conjugate subgroup apart from itself. That is aH = Ha or $a^{-1}Ha = H$ for all a in G. If G is abelian then every subgroup of G is normal in G.

Definition 1.4

Let G be a non-abelian group and $N \triangleleft G$. Then the set $G / N = \{rN \mid r \in G\}$ is a group under the operation $(rN)(sN) = rsN$ called the factor or quotient group of G by N. It is the set of cosets of N in G.

Definition 1.5

The number of elements in a group G written |G| in called the order or cardinality of the group. If G is finite of order n we have |G| = n otherwise |G| = ∞ if G has infinite order. The least number n if it exists such that $a^n = 1$for a in G is called the order of a and we write o(a) = n. If no such n exists then o(a) = ∞. An element of order two is said to be an involution.

If a in G is such that o(a) = 2 then $a = a^{-1}$ so a, a^{-1} have the same order. However, if a, b $\in$ G such that $a = g^{-1}bg$ then o(a) = o(b). Furthermore the order of an element of G divides |G|. In particular $a^{|G|} = 1$ where G is finite. This naturally leads to an important theorem in group theory: The Lagrange's Theorem which is next.

Theorem 1.1

If G is a finite group and H is a subgroup of G then the order of H divides the order of G.

Proof

By Definition 1.2 we have that the right cosets of H form a partition of G. Thus each element of G belongs to at least one right coset of H in G and no element can belong to two distinct right cosets of H in G. Therefore every element of G belongs to exactly one right coset of H. Moreover each right coset of H in G contains |H| elements. Therefore if the number of right cosets of H in G is n, then |G| = n|H|. Hence the order of H divides the order of G.

Remark 1.1

If H, K are subsets of G then HK = {hk:h $\in$ H, k$\in$ K}. When K = {g}, we denote H{g} by Hg. In particular if H < G then Hg is called a right coset of H. This is the equivalence class of q in G. These equivalence classes yield a decomposition of G into disjoint subsets.

Definition 1.6

The subgroup G' or [G,G] of a group G generated by the elements of the form $sts^{-1}t^{-1}$, for all s, t $\in$ G is called the derived group or commutator subgroup of G. We write $[s,t] = sts^{-1}t^{-1}$ and call this the commutator of s and t. Thus:

$$G' = \{ [s,t] : s, t \in G \}.$$

The derived subgroup G' is normal in G and the quotient G/G' is called the abelianization of G which we denote by G_{ab}.

Definition 1.7

A group that is generated by its own commutators is called a perfect group. That is groups with the property that G'=G. The abelianization G_{ab} of such groups is trivial. That is $|G/G'| = 1$. Each element of such a group can be written as a product of commutators.

Abelian groups are generally perfect groups. We have that the quotient of perfect group by its centre is trivial.

Definition 1.8

Let a,q $\in$ G. Then a is conjugate to q in G if there exist an element g$\in$ G such that $q=g^{-1}ag$. The set of all elements of G that are conjugate to a in G is called the conjugacy class of a in G denoted by C(a). And as such:

$$C(a) =\{g^{-1} ag:g\in G\}$$

The order of the conjugacy class divides |G|. Subgroups belonging to the same conjugacy class are conjugates. Such subgroups are isomorphic. However conjugate elements lie in the same conjugacy class and have the same order.

Definition 1.9

The centre Z(G) of a group G is the set of all elements z in G that commute with every element q in G. We write:

$$Z(G)=\{z\in G:zq=qz, \text{ for all } q\in G\}$$

and note that Z(G) is a commutative normal subgroup of G and G modulo its centre Z(G) is isomorphic to the inner automorphism, inn(G) of G.

If Z(G) = {1} where 1 is the identity element of G, then G is said to have a trivial centre . The centre of a group G is its subgroup of largest order that commute with every element in the group.

Next we make an important remark

Remark 1.3

The centre Z(G) of G is maximum when G is abelian. In such case Z(G) = G and G/Z(G) = {1}. On the other hand the centre Z(G) is minimum when Z(G) = {1}. In this case G/Z(G) is equal to G itself. The centre of a group is the union of the conjugacy classes of size one. However in this work we are interested in non abelian groups. That is where $\{1\}<Z(G)<G$. An element $z \in Z(G)$ if and only if its conjugacy class has only one element which is z itself. We call the elements $x \in Z(G)$ central elements and $y \in G-Z(G)$ non central elements. Such elements do not commute with all elements $q \in G$. The divisors of |G| reveal a lot about the order of Z(G) and the conjugacy classes of G.

Definition 1.10

The centralizer $C_G(q)$ of an element q in G is the set of all elements $g \in G$ that commute with q. That is:

$$C_G(q) = \{g \in G : gq = qg, \text{ for some } q \in G\}.$$

This is a subgroup of G and the index of $C_G(q)$ in G is the size of the conjugacy class C(q) of q in G. That is

$$|C(q)| = |G : C_G(q)|.$$

In particular |C(q)| divides |G|. If q is a central element $q \in Z(G)$ then |C(q)|=1 and $q^{-1}gq=q$. So that $C_G(q) = G$.

The centralizer $C_G(q)$ of q in G is a subgroup of G but not a normal subgroup in general. Consequently the quotient of G by $C_G(q)$ is not a group.

From [1] we have a theorem on the size of the conjugacy class of an element of G.

Theorem 1.2

Let G be a finite group and $q \in G$, then the conjugacy class C(q) of q in G is given by:

$$|C(q)| = |G : C_G(q)| = |G| / |C_G(q)|.$$

Theorem 1.3

Let G be a finite group then

$$|G| = \sum |G : C_G(q_i)| \quad (1),$$

where the sum runs over the elements from each conjugacy class of G.

We note that from Theorem 1.2 equation (i) becomes

$$|G| = |Z(G)| + \sum |G : C_G(q_i)| \quad (2)$$

Here the sum in (ii) runs over q_i from each conjugacy class such that q_i is not an element of Z(G). From Theorem 1.2 and equation (ii) above we have:

$$|G| = |Z(G)| + \sum |C(q_i)| \quad (3)$$

Remark 1.4

In the abelian environment, the sum in equation (3) of Theorem 1.3 is zero. Consequently, the class equation is relevant only when we are in the non abelian environment. The fact that each element of Z(G) forms a conjugacy class containing just itself gives rise to the class equation. From Theorems .1.1 and .1.3 we have:

Corollary 1.1

For a finite non abelian group G and any element q in G:

(i) $|C_G(q)|=|Z(G)||C_G(q):Z(G)|$ and $|G|=|C_G(q)||G: C_G(q)|$.

(ii) Equivalently $|Z(G)|=|C_G(q)|/(|C_G(q):Z(G)|)$ and $|C_G(q)|=|G|/|G:C_G(q)|$.

Where $|C_G(q):Z(G)|\geq 2$ and $|G:C_G(q)|\geq 2$, since G is finite and non abelian.

We measure the maximum size of the centre of finite non abelian groups in the theorem that follows according to [1]

Theorem 1.4

If G is a finite non abelian group, then the maximum possible order of the centre of G is ¼|G|.That is, $|Z(G)| \leq 1/4|G|$.

Proof

Let $z \in Z(G)$. Since G is non abelian, $Z(G) \neq G$. Thus there exist an element $q \in G$ such that q is not in the centre. This imply that $C_G(q) \neq G$ and $C_G(q) \neq Z(G)$. Since $z \in Z(G)$ every element in G commute with z, so qz = zq. It follows that $z \in C_G(q)$. As $q \in C_G(q)$, we have that Z(G) is a proper subset of $C_G(q)$. Since a group that is a subset of a subgroup under the same operation is itself a subgroup of the subgroup, we find that Z(G) is a proper subgroup of $C_G(q)$. By Theorem .1.1 and Corollary 1.1, it follows that:

$$|Z(G)| \leq 1/2|C_G(q)|.$$

Now, since we assumed $C_G(q) \neq G$, then $C_G(q)$ is a proper subset of G. Therefore by Theorem 1.1 and the fact that the centralizer of any group element is a subgroup of G, we find that $|C_G(q)| \leq 1/2|G|$.That is:

$$\begin{aligned} |Z(G)| &\leq 1/2|C_G(q)| \\ &\leq 1/2(1/2|G|) \\ &= 1/4|G|. \end{aligned}$$

Next is a lemma in which we measure the size of the centralizer as in [1]

Lemma 1.1 $|C_G(t)| = |G|/2$.

Proof

Since $|Z(G)|=|G|/4$, the number of centralizers of t such that $C_G(t) = G$ is |G|/4. We claim that the remaining ¾ elements of G each has order equal to |G|/2 as (G:Z(G)) =4. Suppose t is an element of G such that $t \notin Z(G)$ we have that

$$|G : Z(G)| = |G : C_G(t)|\,|C_G(t) : Z(G)| .$$

From theorem 1.1 we also have that $C_G(t) \neq G$ and $C_G(t) \neq Z(G)$ .since $t \neq Z(G)$ and $t \in C_G(t)$, then:

$$|C_G(t) : Z(G)| = 2 .$$

We conclude that $|G : C_G(t)| = 2$ implying that $|C_G(t)| = |G|/2$.

Definition 1.11

Let $G_1, G_2, \ldots G_r$ be a collection of groups. The external direct products of the $G_i, 1 \leq i \leq r$ written $G_1 \times G_2 \times \ldots \times G_r$ is the set of all the r- tupples for which the i^{th} component is an element of G_i with a component wise operation.

Remark 1.5

In an abelian group, $C_G(t) = G$ for all t in G but $C_G(t) \leq G$ if G is non abelian. In this case, $C_G(t) < G$. The number of the centralizers that are equal to G is |Z(G)|.

From [1] we have:

Theorem 1.4

There are no groups of order $4 \bmod 8$ such that $Z(G) \leq |G|/4$.

Proof

Let $|G| = 4 \bmod 8$ and $Z(G) \leq |G|/4$, t an arbitrary element , then

$$|G| = \sum |G : C_G(t)|$$

where the sum runs over an element t from each conjugacy class of G. From theorem 1.3:

$$|G| = Z(G) + \sum |G : C_G(t)|.$$

Here the sum runs over element t from each conjugacy class of non central elements. Since, the centralizer of the element t in G satisfying $t \notin Z(G)$ can be atmost $|G|/2$, lemma 1.1. The element t commutes with itself as well as with the $\frac{1}{4}|G|$ elements of Z(G). This implies that $|C_G(t)| > \frac{1}{4}|G|$. By assumption G is even. So 3 does not divide |G| in general. Hence $|C_G(t)| = |G|/2$ (G is non abelian and t is non central). Also $C_G(t) \neq G$. By the choice of t, $C_G(t) = \frac{1}{2}|G|$ for all $t \in G, t \notin Z(G)$. This implies that:

$$|G : C_G(t)| = \frac{|G|}{|G|/2} = 2 \cdot$$

By this we have that $\sum |G : C_G(t)|$ is even. However since $|G| = 4 \bmod 8$, $Z(G) = \frac{1}{4}|G|$ is odd. The sum of the $\sum |G : C_G(t)|$ which is even and $|Z(G)|$ which is odd cannot be |G|. Here we arrive at a contradiction and so the theorem holds.

The next definition, theorem and corollary that follow are from [2] and [3]

Definition 1.12

The subset H of a finite group G of order n^2 is a perfect square root of G if :

(i) $H^2 = G$

(ii) $|H|^2 = |G|$

This implies that each element of G occurs exactly once in the multiplication table for H and we have that no two elements of a perfect square root commute. Equivalently there are no repeated products in H^2 and we have

Theorem 1.5

(i) If G has a perfect square root then G is non abelian;

(ii) If G has a perfect square root H then H contains no element of Z(G);

(iii) Let $r, s \in H$, then r is not in the centralizer of s if $r \neq s$.

From theorem 1.5 (iii) we have the following corollary

Corollary 1.2

The intersection of H with the centre of G is trivial, particularly, the identity element is not in H

If $r, r^{-1} \in H$, then $r = r^{-1}$

H contains a unique involution

The following proposition is from [2]

Proposition 1.1

If G has a perfect square root H then 4 divides |G|.

Proof

The identity element of G must be the product of two elements of H. As inverse pairs always commute and distinct elements of H do not commute we must have that $h^2 = 1$ for some h in H. Since $1 \in Z(G)$ there does not exist $1 = h \in H$. Hence h must have order 2 and so G has an even order. It follows that |G| with G having a perfect square root is a multiple of 4.

We are now equipped to proof:

Theorem 1.6

If H is a perfect square root of G, then H contains a unique involution.

Proof

Since $1 \in H^2$, there exists $r, s \in H$, such that rs=1. That is $r = s^{-1}$. From corollary 1.1(b) r=s so r is and involution. If H contains two involutions r and s then H^2 contains repeated products, rr = ss

Next is a corollary from [3]

Corollary 1.3

If G is a group with a perfect square root then 36 divides the order of G.

In proposition 1.2 we have a necessary condition on groups having perfect square roots where the size of the centre places a lower bound on the square root of the order of G as contained in [2]

Proposition 1.2

If G has a perfect square root then $|Z(G)|^2 < |G|$

Proof

Let H be the perfect square root of G . Since elements of H do not commute no two elements of H are in the same coset of Z(G). For if $z_1, z_2 \in Z(G)$, then $(tz_1)(tz_2) = (tz_2)(tz_1)$. Let $|G| = n^2$ so that there are at least n cosets of Z(G) from which to choose as elements of H. That is we have:

$$|G : Z(G)| = \frac{|G|}{|Z(G)|} \geq n \text{ or } n \geq |Z(G)|.$$

Accordingly we have $|Z(G)|^2 < |G|$ as H contains no element of Z(G).

The next proposition gives relationship between the elements of Z(G) and H according to [2]

Proposition 1.3

Let G be finite with perfect square root H. Then for each $z \in Z(G)$ there is some h in H such that $h^2 = z$. In other words each element of Z(G) occurs in the main diagonal of the multiplication table of G.

Proof

Each $z \in Z(G)$ there is a product of some $h_1, h_2 \in H$ .Since z is in the $Z(G)$ and the pairs h_1h_2 and h_2h_1 are conjugates. It follows that $h_1h_2 = h_2h_1$. This is a contradiction of the fact that no two elements of a perfect square root commute, definition 1.12. Hence $h_1 = h_2$ and $z = h_1^2$.

Theorem 1.7

The number of elements of order 4 in G is odd if G is finite group with a square root.

Proof

Consider $I = \{t \in G \mid t^2 = 1\}$. Then I has even order since |G| is even and $|G - I|$ is even. The latter holds because each element may be paired with its distinct inverse for all $r, s \in H, rs \in I$. This implies that $sr \in I$, since rs and sr have the same order there is exactly one element of order 2 in H and the square of this element is an element in I . So we have that all $r, s \in H$ yields either 0 or 2 elements of I when $r \neq s$. Therefore there must be an odd number of elements $u \in H$ such that $u^2 \in I$. Each of these elements has order 4.

From [3] we have:

Lemma 1.2

If G has a perfect square root H then it has at least |H| perfect square roots;

Let H be a subset of a group G such that $|H| > \frac{|G|}{2}$ then $H^2 = G$;

G has subset of size $\frac{1}{2}|G|$ such that $H^2 \neq G$ if and only if the graph of G associated with some $t \in G$ has only even length cycles.

Next is a corollary on direct products from [3].

Corollary 1.4

If G and K have perfect square roots, then $G \times K$ has a perfect root.

Proof

Let M and N be perfect square roots of G and K respectively. Then $M \times N$ is a perfect square root of $G \times K$ such that $(M \times N)^2 = M^2 \times N^2 = G \times K$ and hence $|G \times K| = |M \times N|^2$.

II. OUR RESULTS

Our results show that having a maximum size of Z(G) is a condition for G to have a perfect square root. We construct groups of order 8n where n is an integer.

Theorem 2.1

(a) A group G such that the number of elements in its centre is at most $\frac{1}{4}|G|$ contains a perfect square root.

(b) Let H be a subset of a group G. If $H^2 = G$ implies that $|H|^2 = |G|$, then H cannot be normal in G.

(c) A group G is non abelian with perfect square root if $|Z(G)| \geq 2$.

Proof

If $Z(G)$ takes at most the given value then we have that G is non abelian from theorem 1.5(i) and so $\{1\} < Z(G) < G$. Hence there exists a subset H say of G such that for any $r \in H$, $r \notin Z(G)$ and $r^2 = 1 \in Z(G)$. That is $H^2 = G$ and hence $|H|^2 = |G|$. From definition 1.12 and proposition 1.1, H has a perfect square root.

$H \subset G$, $H^2 = G$ implies that $|H|^2 = |G|$, then we have that there is an element $r \in H$ such that $r^2 = 1$ with the property that $r \notin Z(G)$.

Now $r^2 \in Z(G)$ for all $r \in H$ and $r \neq 1$. We observe that with $H \subset G$ and $1 \notin H$, it is obvious that H cannot be normal in G.

Given that $2 \leq |Z(G)|$, we need to show that G is divisible by 4.

We have that $4 \leq |Z(G)|^2$. So that $4 \leq |Z(G)|^2 < |G|$, from proposition 1.2.

This implies that $4Z(G) < |G|$ and $|Z(G)| < \frac{1}{4}|G|$.

Hence, we have that $|G|$ is even and it is divisible by 4 and the theorem follows since G is non abelian.

Remark 2.1

In theorem 2.1(b) we observe that in a non abelian group with the central property discussed G has a subset H which is not a subgroup. So that neither $H \leq Z(G)$ nor $Z(G) \leq H$. In (b) of the same theorem we set a lower bound for the size of the centre of the group, if it must contain a perfect square root. The centre has a lower bound of 2 where the group is non abelian.

In theorem 2.3 we construct new groups whose centres are as large as possible, motivated by definition 1.11 and [1]

Theorm 2.3

The property $Z(G) = |G|/4$ is preserved by direct products of groups.

Proof

Let $G = \{t_1, t_2, \ldots, t_n\}$ be a finte abelian group. Consider a non abelian group D_4. We wish to show that $D_4 \times G$ is non abelian with the stated property of Z(G). Let $(d_i, t_x) \in D_4 \times G$ where $d_i \in D_4$, $t_x \in G$. Suppose that $(d_i, t_x).(d_j, t_y) \in D_4 \times G$. Then:

$$(d_i, t_x).(d_j, t_y) = (d_i d_j, t_x t_y).$$

Now when $d_i d_j = d_j d_i$ we have:

$$(d_i, t_x).(d_j, t_y) = (d_j d_i, t_y t_x) = (d_j, t_y).(d_i, t_x)$$

We also have that $t_x t_y = t_y t_x$ by the choice of G. However, $(d_i, t_x).(d_j, t_y) \neq (d_j, t_y).(d_i, t_x)$ whenever $d_i d_j \neq d_j d_i$.

Thus as $|G| = n$ was arbitrarily chosen $|D_4 \times G| = 8n$ in which $Z(G) \leq |G|/4$. We have constructed groups of order 8n which satisfy the property on the size of Z(G).

In the next result we have that the property of groups with perfect square root is inherited by direct products of groups.

Theorem 2.4

A non abelian group that is a direct product of two groups has a perfect square root.

Proof

Let G be an abelian group. We chose a non abelian group D_4 the dihedral group of order 8. Let K and H be subgroup such that $K \leq D_4$, $H \leq G$. We consider the direct products $D_4 \times G$ and $K \times H$.

Clearly $K \times H \leq D_4 \times G$. Let $x, y \in D_4 \times G$, where $x \in D_4$, $y \in G$. Then $xy \in K \times H$ such that $xy \neq 1$ and $xy \notin Z(N)$ where $N = D_4 \times G$. N has the property that $(xy)^2 = 1$. That is $(xy)^2 \in Z(N)$. By this we have that the elements of $K \times H$ are involutions and so N is even. That is for any $r, s \in K \times H$ such that:

$$r^2 s^2 = (rs)^2 \in N$$

then $(K \times H)^2 = N$ and $|K \times H|^2 = |N|$. From, Corollary 1.2(c) and Corollary 1.3 we conclude the proof.

III. CONCLUSION

The results show that for a non abelian group to have a perfect square root the size of the centre must be at most $1/4\,|G|$. Such a group possesses a subset H say. This subset is not a subgroup of G and it does not contain the centre. Our results hold mostly in p – groups. Our choice of D_4 in the result is because it is the lowest group for which we have $Z(G) \leq |G|/4$. The sizes of the centres of the groups in this paper have a lower bound of 2 and an upper bound of $1/4\,|G|$.

REFERENCES

[1] Cody, C Commutativity in non abelian groups. www.whitman.edu/mathematics/.../2010/seniorproject.codyclifton. (2010) pp1-18

[2] Kashi, A and Daniel, G Square roots of finite groups. A technical Report MSTR 94-03. Rose- Hulman Institute of Technology, Terre Haute.(1994) pp 1-8

[3] Matthew , D; David, M and Rebecca Square roots of finite groups II. A technical report MSTR 94- 06. Rose- Hulman Institute of Technology Terre Haute.(1994) pp 1-7