Transactions of the Nigerian Association of Mathematical Physics
***Volume 9,* (*March and May, 2019*), pp1 – 4**
© Trans. of NAMP

DETERMINATION OF NORMAL SUBGROUPS OF GROUPS OF PRIME ORDERS $p^{\alpha}q^{\beta}, \alpha, \beta \in \{0, 1, 2\}$

Ademola L. A., Bimwarit R. and Hosea G. G.

Department of Mathematics, University of Jos, Jos, Nigeria.

Abstract

Ademola and Anghosh in 2018, published a paper on the subgroups of Cyclic groups of order p^2, with an extra condition $p \neq 2$. The extra condition $p \neq 2$, uncovered the possibility of obtaining several other results in group theory by adjusting the values of the order of the group under consideration. Thus, in this paper is presented the interesting results obtained on the determination of normal subgroups of groups of prime orders $p^{\alpha}q^{\beta}, \alpha, \beta \in \{0, 1, 2\}$ when some specific conditions are imposed. For example groups of order p^2q can only have a normal subgroup of order p^2, if $p < q$, $p \nmid (q-1)$.

Keywords: Group, Subgroup, Order, Normal subgroup, Lagrange's theorem, Sylow's theorem.

1. DEFINITIONS AND NOTATIONS

This section gives some basic definitions and relevant results needed for the verification of the solubility of the groups under consideration. The reader can refer to [1] for definitions and relevant results that are not listed here.

Definition 1.1

A set is a collection of objects. If X is a set we write $x \in X$ to mean that x is an element of set X. similarly, $x \notin X$ mean that X is not an element of X (which only really makes sense if both x and the elements of X are elements of some common larger set.

Definition 1.2

A set X is finite if X has only a finite number of elements and it is infinite otherwise.

Definition 1.3

If X is a finite set then the order of X denoted by $|X|$ is the number of elements it has.

Definition 1.4

A group is a non-empty set G together with a binary operation $*$ which satisfies the following conditions.

i. G is closed under the operation *. That is for every$x, y \in G$, there exists a unique element $x * y$ such that, $x * y \in G$.
ii. The binary operation * is associative; that is $(x * y) * Z = x * (y * Z)$ for all $x, y, z \in G$.
iii. There exist an element e called the identity in G such that for all a in G, $a * e = e * a = a$.
iv. To each $a \in$ G, there exists an element $a^{-1} \in$ G called the inverse of a such that $a * a^{-1} = a^{-1} * a = e$.

Definition 1.5

A subset H of group G is said to be a subgroup of Gwritten $H \leq G$, if H is also a group with respect to the binary operation of G.

Definition 1.6

Let G be a group. If there exist a positive integer n such that G has exactly n elements, we say that G has finite order. The order of G is said to be n and we write $|G| = n$.

Correspondence Author: Ademola L.A., Email: ademolal@unijos.edu.ng, Tel: +2348163833611

By convention, if G does not have a finite number of elements we write $|G| = \infty$ and we say that G has infinite order.

Definition 1.7

Let G be a group and suppose that $H \leq G$. If $a \in G$, we define the right coset Ha of H as

$Ha = \{ha | h \in H\}$.

Similarly, we define the left coset aH of H as

$aH = \{ah | h \in H\}$.

Definition 1.8

A group G is said to be abelian (after *N.H.* Abel a Norwegian) or commutative if $ab = ba \ \forall a, b \in G$.

Definition 1.9

A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all a in G. That is every left coset is a right coset. We denote this by $H \trianglelefteq G$

Definition 1.10

A finite group G is said to be a p-group if its order is a power of p, where p is a fixed prime number.

Definition 1.11

Let G be a group, if $T \leq G$ and $|T| = p^r$, where p is a prime and r t is any integer. Then T is called a p-subgroup of G.

Definition 1.12

If G is finite and $|G| = p^r m$, $r \geq 1$ and p does not divide m and $H \leq G$ such that $|H| = p^r$, we say that it is a Sylow p-subgroup of G.

Clearly, a Syl p-subgroup is maximal among p-subgroup of G.

Definition 1.13

Cyclic group is a group that is generated by a single element.

2 BASIC PROPERTIES AND KNOWN RESULTS

Lemma 2.1 Lagrange's Theorem

The order of a subgroup of a finite group is a quotient of the order of the group. [2]

Lemma 2.2 Sylow's Theorem

Let p be a prime number, G is a finite group and $|G|$ the order of G

1. There is atleast one sylow p-subgroup H of G.
2. If K is any sylow p-subgroup of G, then $K = g^{-1}H g$ for some $g \in G$.
3. If n_p is the number of Sylow p-subgroups of G, then $n_p \equiv 1 \mod p$.[1]

Lemma 2.3 Cauchy's Theorem

Any group G of finite order whose order is divisible by a prime p contains an element of order p . [1]

Lemma 2.4

In a finite group G, the order of an element $g \in G$ divides the order of G itself. [4]

Lemma 2.5

A group whose order is prime is said to be cyclic. [3]

MAIN WORK

Theorem 3.1

Let G be a group of prime order p, then for any $m, n \in G$, $mn = nm$ for all $m, n \in G$.

Proof:

Assume that the order of G is the prime p, then by Lemma(2.5), G is cyclic. Thus since G is cyclic, it follows that for any $m, n \in G$, $mn = nm$ for all $m, n \in G$. Thus, G is normal.

Theorem 3.2

Let G be a group of order pq such that $p \neq q$. Then there exists normal subgroups of order p and q in G.

Proof;

Let G be a group of order pq such that $p \neq q$, then by Lemma(2.2), there exist P and Q such that P is a sylow p-subgroup of orders p and Q is a sylow q-subgroup of order q. Now since $|P|=p$ and $|Q|= q$, it follows by Lemma(2.2) and Theorem(3.1), that P and Q are both normal.

Theorem 3.3

Let G be a group of order p^2q where p and q are prime and $p < q$, $p \nmid (q-1)$. Then there exist a normal subgroup of p^2 and a normal subgroup of order q in G.

Proof:

Let G be a group of order p^2q, then by Lemma (2.2), there exist a Sylow p-subgroup P of order p^2 and a Sylow q-subgroup Q of order q.

Let n_p be the number of Sylow p-subgroup in G. Then by Lemma (2.2), $n_p \equiv 1(modp)$. Thus by Lemma (2.1), $n_p = 1, q$.

If $n_p = q$, then $q \equiv 1(modp)$, i.e $q = 1 + kp, k \in$ Z. Hence $q - 1 = kp$, meaning $p|q-1$. This contradicts the statement of the Theorem , so $n_p = 1$. So by Lemma (2.2), P is a normal subgroup of order p^2 in G.

Next let n_q be number of Sylow q-subgroup in G. Then by Lemma (2.2), $n_q \equiv 1(modq)$. Thus by Lagranges theorem, $n_p = 1, p, p^2$.

If $n_p = p$, then $p \equiv 1(modq)$, i.e $p = 1 + kq, k \in$ Z. Hence $p - 1 = kq$, meaning $q|p-1$. This contradicts the statement of the Theorem as p and q are prime and $p < q$.

So $n_p = p^2$, then $p^2 \equiv 1(modq)$, i.e $p^2 = 1 + kq, k \in$ Z. Hence $p^2 - 1 = kq \Rightarrow (p-1)(p+1) = kq$, meaning $q|p-1$ or $q|p+1$. This contradicts the statement of the Theorem as p and q are prime and $p < q$.

So $n_q = 1$. So by Theorem (3.1), Q is a normal subgroup of order q in G.

Theorem 3.6

Let G be a group of order p^2q^2 where p and q are prime and $p < q$, $p \nmid (q-1)$. Then G has normal subgroup of order q^2 and a normal subgroup of order p^2 only if $p \neq 2$.

Proof

Let G be a group of order p^2q^2, then by Lemma (2.2), there exist a Sylow p-subgroup P of order p^2 and a Sylow q-subgroup Q of order q^2.

Let n_p be number of Sylow p-subgroup in G. Then by Lemma (2.2), $n_p \equiv 1(modp)$. Thus by Lagranges theorem, $n_p = 1, q, q^2$.

If $n_p = q$, then $q \equiv 1(modp)$, i.e $q = 1 + kp, k \in$ Z. Hence $q - 1 = kp$, meaning $p|q-1$. This contradicts the statement of the Theorem, so $n_p = 1$.

So $n_p = q^2$, then $q^2 \equiv 1(modp)$, i.e $q^2 = 1 + kp, k \in$ Z. Hence $q^2 - 1 = kp \Rightarrow (q-1)(q+1) = kp$, meaning $p|q-1$ or $p|q+1$. Thus $n_p \neq 1$, as if $p = 2, q = 3 \Rightarrow 2|3+1$. Thus if $p \neq 2$ it follows that $n_p = 1$, and by Lemma (2.2), P is a normal subgroup of order p^2 in G.

Next let n_q be number of Sylow q-subgroup in G. Then by Lemma (2.2), $n_q \equiv 1(modq)$. Thus by Lagranges theorem, $n_p = 1, p, p^2$.

If $n_p = p$, then $p \equiv 1(modq)$, i.e $p = 1 + kq, k \in$ Z. Hence $p - 1 = kq$, meaning $q|p-1$. This contradicts the statement of the Theorem as p and q are prime and $p < q$.

So $n_p = p^2$, then $p^2 \equiv 1(modq)$, i.e $p^2 = 1 + kq, k \in$ Z. Hence $p^2 - 1 = kq \Rightarrow (p-1)(p+1) = kq$, meaning $q|p-1$ or $q|p+1$. This contradicts the statement of the Theorem as p and q are prime and $p < q$.

So $n_q = 1$. So by Lemma (2.2), Q is a normal subgroup of order q^2 in G.

References

[1] Fraleigh, J. E. 7Ed (2003). *A First Course In Abstract Algebra, Addison Wesley. IBSN 0-201-76390-7.*
[2] Benjamin, B., & Bruce, C. (1968). *Schaum's Outline: Theory and Problems of Group Theory*. (New York): *Schaum Publishing Co.*
[3] James, S. (2016). *Lecture Notes for Abstract Algebra I: Liberty University, Department of Mathematics*.
[4] Ademola L. A, & Anghosh, N. L. (2018). *Subgroups of Cyclic Groups of Order* p^2, $p \neq 2$. *Benue Journal of Mathematics and Mathematics Education 2(7).*