SciencePG
Science Publishing Group

Composition Series of the Solvable Multiplicative Abelian Groups over a Regular Even nth Roots of Unity: A Classical Approach

Alechenu Benard*, Babayo Muhammed Abdullahi, Daniel Eneojo Emmanuel

Department of Mathematics and Computer Science, Faculty of Science, Federal University of Kashere, Kashere, Nigeria

Email Address:

alechenu.benard@yahoo.com (A. Benard), baabaayo2014@gmail.com (B. M. Abdullahi), Emmytetra@yahoo.com (D. E. Emmanuel)
*Corresponding author

Abstract: Solubility of algebraic structures is what gleaned the introduction of group theory, which later stems the other realms of abstract algebra viz: rings, fields and semigroup theories. The nth roots of unity is found in the most sensitive texts ever in the history of abstract algebra: Cauchy's, Galois' and Cayley's. These three giant group theorists had the common ground of the roots of unity in even the title of their works. The idea is that if the nth roots of unity are solvable by radicals and so do the composition series approach, then all other products of the nth roots of unity – which the unity itself is part of – will automatically be solvable. Hence, all equations that dissolve to the least of the nth roots of unity are solvable by the composition series. This article penciled down how the congruence modulo of arithmetics due to Gauss and Leibnitz were used to break down the nth roots of unity, so that the recursive process can generate the composition series of normal subgroups between the unity and the group itself. Since they are P-Groups, they have normal P-Sylow Subgroups. The normality comes from the Index Theorem. Because they all have index 2 in their P-Groups, they are the maximal proper normal P-Sylow Subgroups and their factor groups are abelian accounting to the solubility of nth roots of unity by composition series. We combine the classical Euler Formula and the De Moivre Theorem to present the solvability of nth roots of unity. The P-Groups over nth roots of unity are multiplicative. nth roots of unity are subsequences of nth roots of unity and it converges to the limit point of the nth roots of unity.

Keywords: Cauchy Sequence, Rouche Theorem, Class Equation, Aleph Naught

1. Introduction

Galois [1] in 1831 first define group in an attempt to group some one-one functions and in an attempt to prove Abel [2] Proposition: There is no general formula that solves the linear quintic equations (see Buya [3]) and above. Galois proved Abel right using the group theory. The definition of group was followed by Cayley Theorem due to Cayley [4]. The Cayley Theorem was followed by the present definition of group by Henrish Weber [5] and Walter von Dyck [6] in 1852. The aim of Henrish Weber and Walter von Dick is that any algebraic structure that endured the present-day definition of group is embeddable in the Galois Group, now mostly called symmetric group.

Group is the father, father as in personification, of other algebraic structures viz: Ring (additive abelian group equipped with an associative multiplicative binary operation that is both left and right distributive over the addition), vector space(group acting on a set), module(ring acting on a set), field(both additive and multiplicative abelian groups), semigroup(a generalization of group, Christopher [13], that was born 87 years after group) and other consequences of group all under the universal algebra Stanley and Sankappanavar [14]. Group has analyzed very many regular shapes (symmetry groups) and numbers are partly regular shapes. Symmetry groups are embedded in the symmetric groups. We shall present the bottom line of construction of regular shapes using $x^n - a$ in the anal of this article. The p-groups of the aforementioned multiplicative solvable groups

all lie on the unit circle $|z| = 1$. There are uncountable infinitely many number of complex numbers on $|z| = 1$ as there are uncountable infinitely many number of real numbers in $(0, 1) \subseteq \mathbb{R}$.

Whenever there is a subgroup of a finite group, then the order of the subgroup divides the order of the group. This is the statement of Lagrange Theorem [7], first stated by Lagrange himself in 1771 almost 58 years before the definition of group by Galois. 30 years after the statement, Petro Abati [8] proved the theorem. See Richard [9]. Today, like many other decoded theorems, there are numerous alternative proofs of Lagrange Theorem. This brings us to: Proving a theorem is easier than stating it. The converse of the theorem is: Whenever there is a group of a finite order n, is there a subgroup of an order a divisor of n? The answer is yes if the group is abelian of a prime power order. Cauchy stated and proved that the group needs not to be abelian so far it is finite of prime order. The group is forced to equal its centre, the abelian subgroup of every group.

That is, Cauchy proved that every P-Group has a P-Subgroup; but his proof contained egregious error. Today, there is a simple proof of Cauchy Theorem via the Class Equation, Heinstein [10]. Sylow (John and Robertson [11]) narrowly states that there are $P^m r$-Group where r is a positive integer that does not divide P. It has the largest P-Subgroup, the P-Sylow Subgroup that forms a single conjugacy class of all the other P-non Sylow Subgroups. Sylow further gave $\equiv 1 \bmod p$, the formula that could find the number n of distinct P-Sylow Subgroups. That is, $\frac{n-1}{p} = m \in \mathbb{Z}$. That is, $1 + mp \backslash p^m r$.

Every P-Group is nilpotent and every nilpotent group is solvable. Every group has a composition series which may be trivial or non trivial (interesting). The terms of the composition series of the group over $x^n - 1$ are P-Groups having P-Sylow Subgroups of Index 2. Hence, the factor group is abelian due to blending the following theorems Vasistha and Vasistha [12] and Heinstein [10].

Theorem 1.1. If H is a subgroup of index 2 in G, then H is a normal subgroup of G and G/H is a cyclic group of order 2.

Proof. Since the index of H in G is 2, there are only two right cosets of H in G. One of them is H and the other must be Hg, where g is an element of G that is not appearing in H for if $g \in H, g^{-1}hg \in H, \forall h \in H$. So let $g \notin H$ and let $g^{-1}hg \notin H$. Then $g^{-1}hg \in Hg$, the only other coset of G. But $h_1 g \in Hg$ for some $h_1 \in H$. That is $g^{-1}hg = h_1 g \in Hg$ which implies $g^{-1}h = h_1$ which implies $g = hh_1^{-1} \in H$. This contradicts $g \notin H$. Hence, $g^{-1}hg \in H, \forall g \in G$ and $h \in H$. H is a nomal subgroup of G.

G/H is a cyclic group of order 2 because of the Lagrange Theorem.

Theorem 1.2. If G is a group of prime order, then it is cyclic.

Proof. Let $|G| = p$, a prime number. Then every element of G has order 1 or p by Lagrange Theorem. But, the only element of order 1 is the identity. Therefore, all the other elements have order p and there is at least one because $|G| \geq 2$, the smallest prime. Thus, every non-identity element of G generates G. Hence, G is cyclic.

Theorem 1.3. Every cyclic group is abelian.

Proof. Let g^m and g^n be any two elements of the cyclic group $G = \{g^i : i > 0 \in \mathbb{Z}, g^{k-1} = g^1, k > 1\}$. Then $g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m$. This is from the fact that $n + m = m + n, \forall m, n \in \mathbb{Z}$. Hence G is abelian. Hence, G/H is an abelian group.

2. Preliminaries

Galois sought to solve a problem that had stymied mathematicians for centuries. Methods for solving linear and quadratic equations were known thousands of years ago. In the 16th century, Italian mathematician developed formulas involving only the operations of addition, subtraction, multiplication, division and extraction of roots (radicals). For example, the equation $x^3 + 0x^2 + bx + c = 0$ has the three solutions: $A + B, \frac{-(A+B)}{2} + \frac{(A-B)\sqrt{-3}}{2}, \frac{-(A+B)}{2} - \frac{(A-B)\sqrt{-3}}{2}$,

where $A = \sqrt[3]{\frac{-c}{2} + \sqrt{\frac{b^3}{27} + \frac{c^2}{4}}}$ and $B = \sqrt[3]{\frac{-c}{2} - \sqrt{\frac{b^3}{27} + \frac{c^2}{4}}}$.

The general formulas for the general cubics $x^3 + ax^2 + bx + c = 0$ and the quartics $x^4 + ax^3 + bx^2 + cx + d = 0$ are a little more complicated.

A polynomial over $F[x]$, a field, is solvable by radicals if we can obtain all its zeros by adjoining nth roots (for various n) to $F[x]$. In other words, each zero of the polynomial can be written as an expression involving elements of $F[x]$ combined by the operations of addition, subtraction, multiplication, division and extraction of roots.

Definition 2.1 (Solvable by Composition Series). We say that a group G is solvable if G has a series of subgroups $\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_k = G$, where for each $0 \leq i \leq k, H_i$ is normal in H_{i+1} and H_{i+1}/H_i is abelian.

Solvable groups have been investigated for over seventy years. Feit and Thompson [15] proved a long standing conjecture of Burnside [16] that every group of odd order is solvable. Burnside had shown this result to be true for groups of order less than 40,000. The proof of Feit-Thompson Proof extends to over 250 pages of deep mathematics.

Theorem 2.2 (Splitting Field of $x^n - a$). Let F be a field of characteristic 0 and let $a \in F$. If E is the splitting field of $x^n - a$ over F, then the Galois Group $\text{Gal}(E/F)$ is solvable.

Proof. We first handle the case where F contains a primitive nth root of unity w. Let b be a zero of $x^n - a$ in E. Then the zeros of $x^n - a$ are, wb, w^2b, ..., $w^{n-1}b$. Therefore, $E = F(b)$. Let $\text{Gal}(E/F)$ is abelian. Then it is solvable. To see this, observe that any automorphism in $\text{Gal}(E/F)$ is completely determined by its action on b. Since b is a zero of $x^n - a$; any element of $\text{Gal}(E/F)$ sends b to another zero of $x^n - a$. That is, any element of $\text{Gal}(E/F)$ takes b to $w^i b$ for some i. Let $\emptyset$ and σ be two elements of $\text{Gal}(E/F)$. Then, since $w \in F$, $\emptyset$ and σ fixes w and $\emptyset(b) = w^j b$ and $\emptyset(b) = w^k b$ for some j and k. Thus, $(\sigma(\emptyset))(b) = \sigma(\emptyset(b)) = \sigma(w^j b) = \sigma(w^j)\sigma(b) = w^j w^k b = w^{j+k} b$ and $(\emptyset(\sigma))(b) = (\emptyset(\sigma(b)) = \emptyset(w^k b) = \emptyset(w^k)\emptyset(b) =$

$w^k w^j b = w^{k+j} b$. So that $\sigma\emptyset$ and $\emptyset\sigma$ agree on b and fix the elements of F. This shows that $\sigma\emptyset = \emptyset\sigma$. Therefore, $Gal\left(\frac{E}{F}\right)$ is abelian. Now suppose that F does not contain a primitive nth root of unity. Let w be a primitive nth root of unity and let $b \neq 0$. Since wb is also a zero of $x^n - a$, both w and wb belong to E_1. Therefore, $w = \frac{wb}{b} \in E$. Thus, $F(w)$ is contained in E, and F(w) is the splitting field of $x^n - 1$ over F. Analogously, for any automorphism $\emptyset$ and σ in $Gal\left(\frac{F(w)}{F}\right)$, we have $\emptyset(w) = w^j$ for some j and $\sigma(w) = w^k$ for some k. Then, $(\sigma(\emptyset))(w) = (\sigma(\emptyset(w)) = \sigma(w^j) = (\sigma(w))^j = (w^k)^j = (w^j)^k = \emptyset(w)^k = \emptyset(w^k) = \emptyset(\sigma(w)) = (\emptyset\sigma)(w)$. Some elements of $Gal\left(\frac{F(w)}{F}\right)$ are completely determined by their action on w, this shows that $Gal\left(\frac{F(w)}{F}\right)$ is abelian. Because E is the splitting field of $x^n - a$ over F(w) and F(w) contains a primitive nth root of unity, $Gal\left(\frac{E}{F(w)}\right)$ is abelian, and the series $\{e\} \subseteq Gal\left(\frac{E}{F(w)}\right) \subseteq Gal\left(\frac{E}{F}\right)$ is a normal series. Since both

$Gal\left(\frac{E}{F(w)}\right)$ and $\frac{Gal\left(\frac{E}{F}\right)}{Gal\left(\frac{E}{F(w)}\right)} \simeq Gal\left(\frac{F(w)}{F}\right)$

are abelian; $Gal\left(\frac{E}{F}\right)$ is solvable. See Gallian [6] for the theorem and this accompanied proof.

We now take the following theorems that we will use in section 3.

Theorem 2.3 (Eisentein Criterion). Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0 \in \mathbb{Z}[x]$. If there exist some prime p in $\mathbb{Z}$ such that $p \nmid a_n, p \backslash a_i$ where $i = 0,1,\ldots,n-1$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. Refer to Heinstein [7] for the proof.

Theorem 2.4 (Rouche). Let $f(z)$ and $g(z)$ are analytic inside and on a simple closed curve C and let $|g(z)| < |f(z)|$ on C. Then $f(z) + g(z)$ and $f(z)$ have the same number of zeros inside C.

Proof. Refer to Seymour et al. [10] for the proof.

Example: Consider $g(x) = 3x^5 - 15x + 5$. By Einstein Criterion, $g(x)$ is irreducible over $\mathbb{Q}$. Since $g(x)$ is continuous and $g(-2) = -61$ and $g(-1) = 17$, we know that g(x) has a real zero between -2 and -1. A similar analysis shows that g(x) also has real zeros between 0 and 1 and between 1 and 2. Each of these real zeros has multiplicity 1. $G(x)$ has no more than three zeros, because of the Rouche Theorem. So far, $g(x)$ have no real zeros, $g'(x)$ would have to have three real zeros, and it does not. Thus, the other two zeros are non real complex numbers, say, $a + bi$ and $a - bi$.

Lemma 2.5. If $N \trianglelefteq G$ and both N and $\frac{G}{N}$ are solvable groups, then G is a solvable group.

Proof. Refer to Gallian [6] for the proof.

Theorem 2.6. Every p-Group G_P is solvable.

Proof. We will induct $|G|$, with the case $|G| = 1$ being trivial. Assume that the result is true for all p-Groups of order less than $|G|$. Since G is a nontrivial group, it contains a nontrivial centre $Z(G)$. If $Z(G) = p$, then G is abelian and therefore, it is solvable. If $Z(G) \neq p$, then both $Z(G)$ and

$\frac{G_P}{Z(G)}$ are p-groups of order less than $|G|$. By the induction hypothesis, both $Z(G)$ and $\frac{G_P}{Z(G)}$ are solvable. The result follows immediately from Lemma 2.5.

3. Results and Discussion

This section presents the: Composition Series of the Solvable Group over $x^n \pm a$, Construction of Regular Shapes Using $x^n - a$, Discussion on $P -$ Sylow Subgroups of $x^{pq} - a, x^{pqr} \pm a, x^{p^2 q} \pm a$.

3.1. Composition Series of the Solvable Group over $x^n \pm a$

Euler Formula is given by $e^{i\theta} = cos\theta + i \sin\theta$ and De Moivre Theorem states that $z^m = r^m e^{im\theta} = r^m(\cos m\theta + i \sin m\theta)$. When $m = \frac{1}{n}$, we have: $z^{\frac{1}{n}} = r^{\frac{1}{n}}\left(cos\frac{\theta}{n} + i \sin\frac{\theta}{n}\right)$. For nth root of unity, $r^{\frac{1}{n}} = 1$, i.e. $|z| = 1$, the unit circle. Thus $\theta = 2\pi k$ and $(-1)^{\frac{1}{n}} = cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$. For $x^n - a$, we have $\sqrt{a}\left(cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}\right)$ or $\sqrt{a}w$, where $k = 0,1,2,\ldots,n-1$ or $k = 1,2,\ldots,n$. When $n = 1$ and $a = 1$; we have: $x = 1$. The group G over this is the group containing only the identity, the trivial group {1} since $G = (G,*)$ when * is known.

When $n = 2$ and $a = 1$; we have: $x^2 - 1 = (x - 1)(x + 1) \Rightarrow x = 1 \text{ or } x = -1$. The group over this is $\{1, -1\}$, a group isomorphic to the kernel group of absolute values and isomorphic to parity group {even, odd}. It is also a P-group since 2 is the oddest (even) prime.

When $n = 3$ and $a = 1$; we have: $e^0 = 1, e^{120} = \cos 120 + i \sin 120 = -0.5 + 0.9i, e^{240} = \cos 240 + i \sin 240 = -0.5 - 0.9i$. Thus, the multiplicative group is: $\{1, -0.5 + 0.9i, -0.5 - 0.9i\}$.

When $n = 4$ and $a = 1$, we have: $(x^2 - 1)(x^2 + 1)$. The group is $\{1, -1, i, -i\}$ which is a P-Group of the P-Sylow Subgroup $\{1, -1\}$ with index 2. Thus $\{-1, 1\}$ is normal in $\{1, -1, i, -i\}$. The factor group is $\{\{1, -1\}, \{i, -i\}\}$ and the canonical map is $\{1, -1, i, -i\} \to \{\{1, -1\}, \{i, -i\}\}$. Hence, it is abelian because of Theorem 1.1, 1.2 and 1.3.

When $n = 5$ and $a = 1$; we have: $e^0 = 1, e^{72} = \cos 72 + i \sin 72 = 0.3 + i, e^{144} = \cos 144 + i \sin 144 = -0.8 + 0.6i, e^{216} = cos216 + i \sin 216 = -0.8 - 0.6i, e^{299} = \cos 299 + i \sin 288 = 0.3 - i$. Thus, the multiplicative group is: $\{1, 0.3 + i, -0.8 + 0.6i, -0.8 - 0.6i, 0.3 - i\}$.

When $n = 6$ and $a = 1$; we have: $e^0 = \cos 0 + i \sin 0 = 1, e^{60} = cos60 + i \sin 60 = 0.5 + 0.9i, e^{120} = \cos 120 + i \sin120 = -0.5 + 0.9i, e^{180} = cos180 + i \sin 180 = -1, e^{240} = cos240 + i \sin 240 = -0.5 - 0.9i, e^{300} = cos300 + i sin300 = 0.5 - 0.9i$. The group with this underlying set has order $2p$. Hence we take the following theorem.

Theorem 3.2. If $|G| = 2p$, p an odd prime; then G has one and only one subgroup of order p and either G has exactly p subgroups of order 2 or it has exactly one subgroup of order 2.

The subgroup of order 3 is $\{1, -0.5 + 0.9i, -0.5 - 0.9i\}$.

It is a normal subgroup because of the Index Theorem. It is a P-Sylow Subgroup. The subgroup of order two is $\{1, -1\}$. It is normal because of the theorem that says any subgroup of an abelian group is normal. It is a P-Subgroup. $\{1, -0.5 + 0.9i, -0.5 - 0.9i\}$ is the conjugacy class of $\{1, -1\}$.

When $n = 7$ and $a = 1$; we have the following group: $\{e^0 = cos0 + i\,sin0 = 1, e^{51.4} = cos51.4 + isin51.4 = 0.6 + 0.8i, e^{102.9} = cos102.9 + isin102.9 = -0.2 + i, e^{154.3} = cos154.3 + i\,sin154.3 = -0.9 + 0.4i, e^{205.7} = cos205.7 + isin205.7 = -0.9 - 0.4i, e^{257.1} = cos257.1 + i\,sin257.1 = -0.2 - i, e^{308.6} = cos308.6 + isin308.6 = 0.6 - 0.8i\}$

When $n = 8$ and $a = 1$, we have the following group: $\{e^0 = cos0 + isin0 = 1, e^{45} = cos45 + isin45 = 0.7 + 0.7i, e^{90} = cos90 + isin90 = i, e^{135} = cos135 + isin135 = -0.7 + 0.7i, e^{180} = cos180 + isin180 = -1, e^{225} = cos225 + isin225 = -0.7 - 0.7i, e^{270} = cos270 + isin270 = -i, e^{315} = cos315 + isin315 = 0.7 - 0.7i\}$. This is a P-Group because it is of order $2^3 \times 1$, it is of the form $p^m r$. It has at least a P-Sylow Subgroup $\{1, -1, i, -i\}$. The index theorem applies. This 8-Group is the identity of the coset classes of the Factor 16-Group by 8-Normal Subgroup. The canonical map is natural.

Theorem 3.3. This works in general.

Proof. We prove this by the Induction Hypothesis. Case I: When $a = 1$. For $n = 1$, we got $e^0 = cos0 + i\,sin0$. Assume that it is true for $n = k$. Then: $e^{ki\theta} = cosk\theta + isnk\theta$. Now $e^{ki\theta}e^{i\theta} = (cosk\theta + isink\theta)(cos\theta + isin\theta) = cosk\theta cos\theta + icosk\theta sin\theta + isink\theta cos\theta - sink\theta sin\theta = [cosk\theta cos\theta - sink\theta sin\theta] + i[cosk\theta sin\theta + sink\theta cos\theta] = cos(k+1)\theta + isin(k+1)\theta = e^{(k+1)i\theta}$. Whence, it is true for $n = k + 1$.

Case II: When $a \neq 1$, for $n = 1$, we have: $ae^0 = a(cos0 + i\,sin0) = a$. Assume that it is true for $n = k$. Then: $a^k e^{ki\theta} = a^k(cosk\theta + isnk\theta)$. Now $a^k e^{ki\theta}ae^{i\theta} = a^k a(cosk\theta + isink\theta)(cos\theta + isin\theta) = a^k a(cosk\theta cos\theta + icosk\theta sin\theta + isink\theta cos\theta - sink\theta sin\theta) = a^{k+1}\{cosk\theta cos\theta - sink\theta sin\theta + i[cosk\theta sin\theta + sink\theta cos\theta]\} = a^{k+1}[cos(k+1)\theta + isin(k+1)\theta] = a^{k+1}e^{(k+1)i\theta}$. Hence, it is true for $n = k + 1$
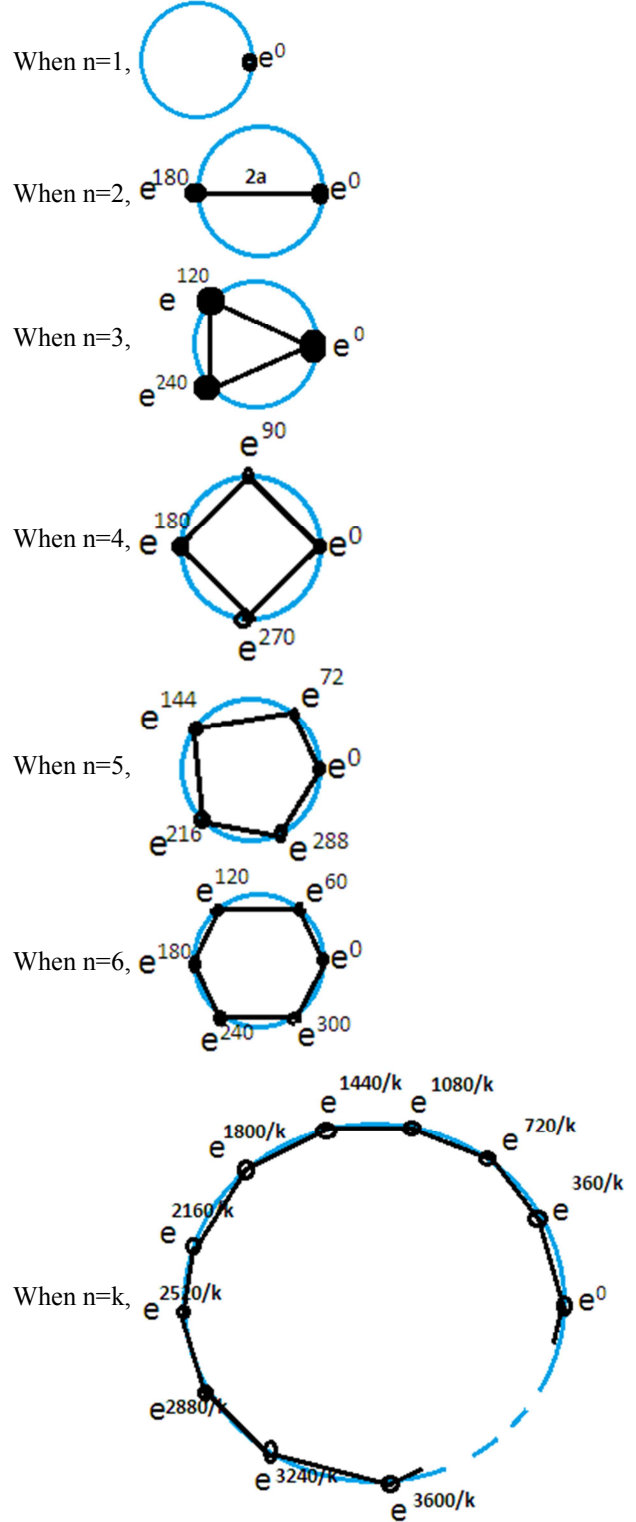
Let $z = ae^{i\theta} = a(cos\theta + isin\theta)$. Then $z^n = a^n e^{in\theta} = a^n(cosn\theta + isinn\theta)$, for all n, by the induction hypothesis.

Since $z^n = a^n e^{in\theta} = a^n(cosn\theta + isinn\theta), \forall n$, $z^{\frac{1}{m}} = a^{\frac{1}{m}}e^{i\frac{\theta}{m}} = a^{\frac{1}{m}}\left(cos\frac{\theta}{m} + isin\frac{\theta}{m}\right)$, where $m = \frac{1}{n}$.

Remark 3.4. Do not go to nth degree and conclude the proof mathematics theorem. Induction is embedding an assertion in an extended set of natural numbers that includes aleph naught in this regards.

3.2. Construction of Regular Shapes Using $x^n - a$

We are aware that group theory that gleaned 85 years before the introduction of ring and 87 years before the introduction of semigroup has seemingly and apparently no number analysis: Semigroup analyzes natural numbers, ring analyzes integers, field analyzes rational and real numbers, vector space analyzes complex numbers. Group, the mother of algebraic structures, analyzes any regular shapes which

includes numbers. Any regular shape is constructible using $x^n - a$:

3.3. The P −Sylow Subgroups of the Group over $x^{pq} - a, x^{pqr} \pm a, x^{p^2q} \pm a$

Any group over $x^p - a$ having order p is a normal subgroup of the group over $x^{pq} - a$. Any integer p is either a prime or a composite. If it is a prime, it is a P-Group as well as a P-Sylow Subgroup. If it is a composite, it has a P-Sylow

Subgroup because of the following theorems (Heinstein and Fraleigh [17]):

Theorem 3.5. If $|G| = pq$, where p,q are distinct primes such that $q \not\equiv 1 \bmod p$; then G has a normal Sylow Subgroup.

Proof. The number of n distinct sylow p-subgroups of G is a divisor of q and $n \equiv 1 \bmod p$. Since q is prime, n is either 1 or q. Since $q \not\equiv 1 \bmod p$, $n = 1$. That is, G has a unique sylow p-sylow subgroup. It is normal in G.

Corollary 3.6. If $|G| = pq$ where p,q are distinct primes, then G has a proper normal subgroup.

Proof. We may assume without loss of generality that $p > q$. Then $q - 1$ cannot be divisible by p, and so by Theorem 3.7, G has a normal sylow p-subgroup.

The group over $x^n - a$ may be of small or big order. It duo two composition series $x^{2n} - a$ and $x^{2n+1} - a$. The groups over $x^{2n} - a$ are forming p-Groups and normal p-sylow subgroups of index 2. Thus, they are nilpotent and every nilpotent group is solvable. Besides, we presented the theorem that states that every p-group is solvable. The groups over $x^{2n+1} - a$ are solvable because of the Burnside Lemma.

Now since $x^n - 1$ works out well, then $x^n - a$ works: The group over this is the group containing only the identity, the trivial group $\{1\}$ since $G = (G, *)$ when $*$ is known. When $= 2$, we have: $\{\sqrt{a}, -\sqrt{a}\}$. When $n = 3$, we have: $\sqrt[3]{a}\{1, -0.5 + 0.9i, -0.5 - 0.9i\}$. When $= 4$, we have: $\{\sqrt[4]{a}, -1\sqrt[4]{a}, i\sqrt[4]{a}, -i\sqrt[4]{a}\}$. When $n = 5$; we have: $\sqrt[5]{a}\{1, 0.3 + i, -0.8 + 0.6i, -0.8 - 0.6i, 0.3 - i\}$. When $n = 6$; we have: $\sqrt[6]{a}\{e^0 = \cos 0 + i \sin 0 = 1, e^{60} = \cos 60 + i \sin 60 = 0.5 + 0.9i, e^{120} = \cos 120 + i \sin 120 = -0.5 + 0.9i, e^{180} = \cos 180 + i \sin 180 = -1, e^{240} = \cos 240 + i \sin 240 = -0.5 - 0.9i, e^{300} = \cos 300 + i \sin 300 = 0.5 - 0.9i\}$. When $n = 7$, we have the following group: $\sqrt[7]{a}\{e^0 = \cos 0 + i \sin 0 = 1, e^{51.4} = \cos 51.4 + i \sin 51.4 = 0.6 + 0.8i, e^{102.9} = \cos 102.9 + i \sin 102.9 = -0.2 + i, e^{154.3} = \cos 154.3 + i \sin 154.3 = -0.9 + 0.4i, e^{205.7} = \cos 205.7 + i \sin 205.7 = -0.9 - 0.4i, e^{257.1} = \cos 257.1 + i \sin 257.1 = -0.2 - i, e^{308.6} = \cos 308.6 + i \sin 308.6 = 0.6 - 0.8i\}$. When $n = 8$, we have the following group: $\sqrt[8]{a}\{e^0 = \cos 0 + i \sin 0 = 1, e^{45} = \cos 45 + i \sin 45 = 0.7 + 0.7i, e^{90} = \cos 90 + i \sin 90 = i, e^{135} = \cos 135 + i \sin 135 = -0.7 + 0.7i, e^{180} = \cos 180 + i \sin 180 = -1, e^{225} = \cos 225 + i \sin 225 = -0.7 - 0.7i, e^{270} = \cos 270 + i \sin 270 = -i, e^{315} = \cos 315 + i \sin 315 = 0.7 - 0.7i\}$.

If $x^n - a$ works out well, nothing can deny $x^n - (-a) = x^n + a$ to work out. This is the reason for the prior assumption. $x^{2n} \pm a$ and $x^{2n+1} \pm a$ are partitions of $x^n \pm a$ under modulo 2. $x^{2n} \pm a$ are subsequences of $x^n \pm a$ that converges to the limit point of $x^n \pm a$ due to the following theorem.

Theorem 3.7. A subsequence converges to the limit point of its super sequence.

Proof. Let x^{2n} be a subsequences of x^n. Since every Cauchy Sequence Converges, $|x^n - x^{2n}| < \frac{\varepsilon}{2}, \forall n \geq N$. x^n converges l means: Given $\varepsilon > 0, \exists N > 0$(N is no matter how large) such that $|x^n - l| < \frac{\varepsilon}{2}, \forall n \geq N$. Hence, we have $|x^n - x^{2n}| < \frac{\varepsilon}{2}$ and $|x^n - l| < \frac{\varepsilon}{2}, \forall n \geq N$. From Triangular Inequality,

$\frac{\varepsilon}{2} + \frac{\varepsilon}{2} > |x^n - x^{2n}| + |x^n - l| > |x^{2n} - x^n + x^n - l|, \forall n \geq N$. That is $x^{2n} - l < \varepsilon, \forall n \geq N$. Hence, x^{2n} converges to l, the limit point of x^n.

Theorem 3.8. If $|G| = p^2 q$, where p and q are distinct primes, then G has either a normal sylow p-subgroup or a normal sylow q-subgroup and G is not simple.

Proof. Let n_p and n_q be respectively the number of sylow p-subgroups and the number of sylow q-subgroups of G. Suppose on the contrary, $n_p > 1$ and $n_q > 1$. By sylow 3rd theorem, n_p divides q which is a prime. Hence, $n_p = q$. Also $n_p \equiv 1 \bmod p$ implies $q > p$. Again, by sylow 3rd theorem, n_q divides p^2, so n_q is either p or p^2. Any element of order q in G generates a subgroup of order q which is a sylow q-subgroup of G. Any two distinct sylow q-subgroup of G of order q intersect in 1 and so there are in G, $n_q(q - 1)$ distinct elements of order q. Hence, if $n_q = p^2$, there are in G just $p^2 - q - p^2(q - 1) = p^2$ element which are not of order q. Since no element of a sylow p- subgroup of G has order q and since $|P| = p^2$. P must be a unique sylow p-subgroup of G in contradiction to $n_q > 1$. Therefore, $n_q = p$. Since, $n_q \equiv 1 \bmod q, p > q$. This is a contradiction.

Theorem 3.9. If $|G| = pqr$, where p, q, r are distinct primes, then G is not simple.

Proof. Let $p > q > r$. Suppose on the contrary, G is simple. Let n_p, n_q and n_r be respectively the number of sylow p subgroups, sylow q subgroups and sylow r subgroups of G. Then $n_p > 1, n_q > 1$ and $n_r > 1$. Any two distinct sylow p-subgroup of G intersect in 1. Hence, n_p sylow p subgroup of G contains $n_p(p - 1)$ distinct element of order p. Similarly, n_q sylow q-subgroups of G contains $n_p(p - 1)$ distinct elements of order p. The n_q sylow q-subgroups of G contains $n_q (q - 1)$ distinct elements of order q and n_r sylow r subgroup of G contains $n_r(r - 1)$ distinct elements of order r. Therefore,

$$|G| = pqr \geq 1 + n_p(p - 1) + n_q(q - 1) + n_r(r - 1)$$

By the 3rd sylow theorem, n_p divides qr and $n_q \equiv 1 \bmod p$. Since $n_p > 1$ and $p > q > r$, it follows that $n_p = qr$. Also, n_q divides pq. So that $n_r \geq q$. Thus,

$$pqr \geq 1 + qr(p - 1) + p(q - 1) + q(r - 1)$$

$$pqr \geq 1 + pqr - qr + pq - p - qr - q \text{ or}$$

$$0 \geq 1 + pq - q - p$$

$0 \geq (p - 1)(q - 1)$, the contradiction.
The proofs are gotten from Heinstein and Fraleigh.

4. Conclusion

There are infinitely many elements on the circle $\{a + ib : a^2 + b^2 = 1\}$, and $\{a + ib : a^2 + b^2 = 1\} \equiv |z| = 1$ as there are infinitely many elements of $(0, 1) \subseteq \mathbb{R}$. Every group, including the symmetry group, is embedded in a symmetric group and every symmetric group is constructible

with at least $x^n - a$. To this end, the existence of composition series of every solvable group are the consequences of the construction of any regular shape using $x^n - a$. Solubility of algebraic structures is what gleaned the introduction of group theory. The $x^n + a$ is solvable by radicals since $x^n - a$ is. Hence $x^n \pm a$ is solvable by composition series despite $S_n, n \geq 5$ – the symmetric groups of length 5 and above – are not soluble, not even by the radical. When $a = 1$, all the solvable groups are multiplicative and are P-Groups. They all lie on the unit circle $\{a + ib: a^2 + b^2 = 1\}$. Since they are P-Groups, they have normal P-Sylow Subgroups. The normality comes from the Index Theorem. Because they all have index 2 in their P-Groups, they are the maximal proper normal P-Sylow Subgroups and their factor groups are abelian accounting to the solubility of $x^n \pm 1$ by composition series. We combine the classical Euler Formula and the De Moivre Theorem to present the solvability of $x^n \pm a$. The P-Groups over $x^{2n} \pm a$ and $x^{2n+1} \pm a$ are multiplicative. $x^{2n} \pm a$ are subsequences of $x^n \pm a$ and it converges to the limit point of the $x^n \pm a$. The inherent methodology is the intertwine of the works of Cauchy [18].

References

[1] Galois E, *Oueveres Mathematiques*, Journal de Liouville, Converted to Djvu format by Prof. Antoine Chambert – Loir at the University of Reines, 1846.

[2] Abel N H, Ouevres Completes de Neils Henrik Abel, Norway 1829.

[3] Buya S B, The Bring-Jerrad Quintic Equation, Its Solvability by Factorization into Cubic and Quadratic Factors, *Journal of Applied Science and Innovations,* 1 (2017): 16-21.

[4] Cayley A, *On the Theory of Groups, as Depending on the Symbolic Equation* $\theta^n = 1$, Philosophical Magazine, 4th Series, 7 (42): 40-47.

[5] Weber H, Lehbuch der Algebra, Braunschweig, Robert Fricke, 1924.

[6] Dyck WV, Gruppen theoretische Studien, Methematische Annalen, 20 (1) (1882): 1-44.

[7] Richard L R, A History of Lagrange Theorem on Groups, *Mathematics Magazine*, 74 (2) (2001): 99 - 108.

[8] Abbati P M, Dizionario Biografico degli Italiani, Vol. I, 1960.

[9] Richard D, *Essays on the Theory of Numbers.* Open Court Publishing Company, Chicago, 1901.

[10] Heinstein I N, *Topics in Algebra*, John Wiley & Sons, 2nd Edition, 1975.

[11] John J O', Robertson E F, *Mac Tutor History of Mathematics,* University of St Andrews, Scotland, UK, 2017.

[12] Vasistha A R, Vasistha A K, *Modern Algebra (Abstract Algebra),* Krishna Parakashan Media (P) Ltd, Meerut, Delhi, 2006.

[13] Christopher H, The Early Development of the Algebraic Theory of Semigroups, *Archive for History of Exact Sciences*, 63 (5) (2009): 497-536.

[14] Stanley B and Sankappanavar H P, *A Course in Universal Algebra*, Springer-Varlag, United States of America, 1981.

[15] Feit W, Thompson G J, Solvability of Groups of Odd Order, *Pacific J. Math*, 13 (3) (1963): 775-1029.

[16] Burnside W, *Theory of Groups of Finite Order,* Cambridge University Press, 1897.

[17] Fraleigh J B, A First Course in Abstract Algebra, Waterstines, 7Ed, 2003.

[18] Seymour L, Murray R S, John J S, Dennis S, *Complex Variables*, McGraw-Hill Companies, United States of America, 2nd Edition, 2009.