Group theory meets Number theory

Student: Narayanan S Advisor: Prof. A Satyanarayana Reddy

Department of Mathematics, Shiv Nadar Institute of Eminence

The characteristic that distinguishes finite group theory from other branches of algebra is the arithmetical nature of many important theorems. Indeed, proofs in finite group theory often amount to sophisticated counting; Lagrange's Theorem and the Sylow theorems are quintessential examples of the genre. An interesting question to ask in this regard is whether it is possible to characterize finite groups on the basis of natural numbers. For example, it is easy to see that if a group has one or two or three or four subgroups, then the group is cyclic.

P-numbers

In pursuit of achieving the previously stated goal, one can begin with the following question: Let P be a property observed in a certain finite group. What are the natural numbers n such that every group of order n has the property P? The natural numbers which fit into this category are referred to as P-numbers.

Cyclic numbers

When P is cyclic?: What are all natural numbers n such that every group of order n is cyclic? Those numbers are called cyclic numbers. By Lagrange's theorem, it is clear that every group of prime order is cyclic. That is all prime numbers are cyclic. One may notice that $\gcd(p, p-1) = 1$. One can observe that 15 is the smallest composite number such that $\gcd(n, \varphi(n)) = 1$ and 15 is also a cyclic number. It seems $\gcd(n, \varphi(n)) = 1$ is a necessary condition for a number to be cyclic. An interesting fact is that it is not only a necessary condition but also a sufficient condition.

n is cyclic if and only if $\gcd(n, \varphi(n)) = 1$.

1	2	3	5	7	11	13	15	17	19	23	29	31	33	35	37	41	43	
47	51	53	59	61	65	67	69	71	73	77	79	83	85	87	89	91	95	

Table 1. Cyclic numbers upto 95

Let $n = p_1^{a_1} p_1^{a_2} \dots p_k^{a_k}$. Then $\gcd(n, \varphi(n)) = 1$ if and only if $a_1 = a_2 = \dots = a_k = 1$ and for every i, j $\gcd(p_i, p_j - 1) = 1$.
Let $G(n)$ denote the number of groups of order n up to isomorphism. For example $G(4) = 2$ as there are only two groups of order 4, upto ismorphism $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$

$G(n) = 1$ if and only if n is a cyclic number.

Reference:"When are all groups of order n cyclic?"- Keith Conrad

---

A number n is an *abelian number* if every group of order n is abelian. It is clear that every cyclic number is an abelian number. If p is a prime number, then p^2 is a abelian number but not a cyclic number.
A number $n = p_1^{a_1} p_1^{a_2} \dots p_k^{a_k}$ is abelian number if and only if for every i, $a_i \leq 2$ and for every i, j $\gcd(p_i, p_j^2 - 1) = 1$.

Nilpotent numbers

- A finite group G is said to be nilpotent if it is the direct product of its sylow subgroups.
- A natural number $n = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$ is said to have nilpotent factorization if p_j does not divide $p_i^k - 1$ for any i, j, k such that $1 \leq k \leq a_i$.

A natural number is nilpotent if and only if it has nilpotent factorization.

Observing examples such as the non-abelian matrix group of order p^3(p prime) and $\mathbb{Z}_p \times \mathbb{Z}_p$, the following fact is easily deduced: **Abelian numbers are exactly nilpotent cube-free numbers and cyclic numbers are exactly nilpotent square-free numbers.**

Solvable numbers

A group G is said to be *solvable* if it has a subnormal series that is

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_k = G,$$

where G_{i+1}/G_i is abelian for every i such that $0 \leq i \leq k-1$.
The motivation for the definition of a solvable group is not very obvious. It stems from the desire to disprove the existence of solutions to equations of degree 5 or more by radicals(by addition, subtraction, multiplication, division or by taking n^{th}roots). Hence the very name!
The celebrated Abel-Ruffini theorem is a major application of solvable groups.

Polynomial equations of degree 5 or more are not solvable by radicals.

Upon using the classification result of minimal simple groups by J.G Thompson, solvable numbers can be classified entirely by demonstrating how it boils down to the problem of classification of minimally simple numbers.

A natural number is solvable if and only if it is not a multiple of any of the following numbers

1. $2^p(2^{2p} - 1)$; p is any prime
2. $3^p(3^{2p} - 1)/2$; p is any odd prime
3. $p(p^2 - 1)/2$; p is any prime greater than 3 such that $5|p^2 + 1$
4. $2^4.3^3.13$
5. $2^{2p}(2^{2p} + 1)(2^p - 1)$; p is any odd prime

References: Jonathan Pakianathan: Nilpotent and solvable numbers
Dummit and Foote: Abstract Algebra

Square-subgroup numbers

A beginner's exercise in group theory is asking if the squares of elements of a group always form a subgroup of the group, that is,

$$G^2 := \{g^2 | g \in G\} \leq G$$

. It can be verified that the alternating group A_4 does not have the property. It is thus natural to ask the following question in our context:
What are the natural numbers n such that every group of order n has the square-subgroup property?
With a little effort, one should be able to see that all odd numbers fit into this class of numbers. To see why? the function f from G to G taking g to g^2 is bijective. Thus, $G^2 = G$ which is more than what we need!
Viewing this problem modulo 4, one concludes that the only numbers left to be inspected are of the form $4k$ and $4k + 2$. With a more subtle, argument, it can be shown that numbers of the form $4k+2$ satisfy the conditions to be a square-subgroup number as well.
Collecting all the necessary counter-examples, we have the following result:

$n \in \mathbb{N}$ is a square-subgroup number if and only if $n \leq 8$ or $4 \nmid n$.

Reference: On groups whose squares are subgroups- H Chuah

Cube-subgroup numbers

Generalizing the previous problem, we may analogously define **cube-subgroup property** as $G^3 := \{g^3 | g \in G\} \leq G$. Arguments made for the claims on square-subgroup number are of great use here as well (For example, every non-cube subgroup number is a multiple of 3). Inspired by the same, it is possible to show how the problem boils down to merely odd multiples of 9. We have the following result on cube-subgroup numbers.

n is a cube-subgroup number if

1. $3 \nmid n$ or
2. $n = 3k$ where $\gcd(k, 6) = 1$.

n is not a cube-subgroup number if

1. $6|n$, or
2. $n = 9t$ where t is odd and there is a prime p such that $p|t$ and $3|p - 1$, or
3. $n = 9t$ where t is odd and there is a prime p such that $p^2|t$ and $3|p - 2$.

Reference: Finite Group Theory: Martin Isaacs