Application of Groups to Word Problems

[1.] R. Sivaraman
Ph.D. Research Scholar in Mathematics
Sri Satya Sai University of Technology and Medical Sciences, Bhopal, Madhya Pradesh
National Awardee for Popularizing Mathematics among masses, Chennai – 600 094
Email: rsivaraman1729@yahoo.co.in
Contact Numbers: 9941914341/7845014341

[2.] Dr. Sonal Bharti
Head, Department of Mathematics
Sri Satya Sai University of Technology and Medical Sciences
Bhopal, Madhya Pradesh
Email: sbsonalbharti6@gmail.com

Abstract:- Using Combinatorial Group Theory an area of mathematics arising from Abstract Algebra, the so called Word Problems can be effectively understood. With the objective of finding applications of the elements of fundamental groups, an attempt has been made in this paper to discuss the word problem in the form of finding the generators in the English Alphabets. These ideas can be widely used in Cryptography, the science of secret codes.

*****

1. INTRODUCTION

The concept of Group presentation forms an indispensable and integral part of the manyapplications of group theory. The basic idea embodied is to form a group by giving a set of generators for the groups and certain equation or relations satisfied by the generators. In the theory of group presentations, the role that is played in analytic geometry by a coordinate system, is played by free groups.

The word problem in groups involves the case in which a group *G* is generated by a finite number of elements $a_1, a_2, a_3, \ldots, a_r$ and these satisfy a finite number of relations. In the group G is it possible to decide whether or not two different words w_1, w_2 represent the same element of G or equivalently, whether or not $w = w_1 w_2^{-1}$ is the identity?

One of the most interesting question about a group is deciding whether its word problems can be solvable? Lots of work has been done in the direction of answering this question and I will present some of the key ideas with my insights related to word problems in this paper.

2. GENERATORS OF ENGLISH ALPHABETS

Let $G = \{a, b, c, d, e, \ldots, x, y, z\}$ be any set. We may then think *G* as a set of English alphabets. We may also assume that any symbol of the form a^n with $n \in N, \forall a \in A$ is a syllable and a finite string of syllables written in juxtaposition shall be considered as a word.

Let the elements of *G* satisfy the relations $a = a^1, b = a^2, c = a^3, d = a^4, \ldots, z = a^{26}$ and $a^0 = a^{27} = \chi$ also be an element of *G*. Then $a^{35} = a^{35-27} = a^8 = h$.

Thus any element of *G* can be written as a^α for $0 \le \alpha \le 26$. So any word generated by *G* would also be some power of *a*. We now define a binary operation to combine any two words generated by G termed "Juxtaposition modulo 27" denoted by Δ as follows:

For $w_1 = a^{\alpha_1}, w_2 = a^{\alpha_2}$ we have: $w_1 \Delta w_2 = a^{\alpha_1} \Delta a^{\alpha_2} = a^{(\alpha_1 +_{27} \alpha_2)} \to (1)$, where $+_{27}$ denotes addition modulo 27 operation. I now show that G is a group under the binary operation defined in (1).

Theorem 1:

The set $G = \{a, b, c, d, e, ..., x, y, z\}$ form a group under the operation Δ defined above.

Proof: We will verify the Group axioms in order to establish this theorem.

(i) Closure Property: For any two words $w_1 = a^{\alpha_1}, w_2 = a^{\alpha_2}$ generated by *G*, we have $w_1 \Delta w_2 = a^{\alpha_1} \Delta a^{\alpha_2} = a^{(\alpha_1 +_{27} \alpha_2)} = a^{\alpha_3}$, where $0 \le \alpha_3 \le 26$. Since we consider modulo 27 operation, we get the desired range for α_3. Now for $0 \le \alpha_3 \le 26$, $a^{\alpha_3} \in G$. Thus for any two words $w_1 = a^{\alpha_1}, w_2 = a^{\alpha_2} \in G, w_1 \Delta w_2 = a^{\alpha_3} \in G$.

(ii) Associative Property: Since addition modulo 27 is associative, it follows that for any words w_1, w_2, w_3 generated by G, we have $(w_1 \Delta w_2) \Delta w_3 = w_1 \Delta (w_2 \Delta w_3)$.

(iii) Identity Element: For any word $w = a^{\alpha} \in G$, we have $w \Delta \chi = a^{\alpha} \Delta a^0 = a^{(\alpha +_{27} 0)} = a^{\alpha} = w$. Similarly, $\chi \Delta w = a^0 \Delta a^{\alpha} = a^{(0 +_{27} \alpha)} = a^{\alpha} = w$. Thus $w \Delta \chi = \chi \Delta w = w$ and so $\chi = a^0$ is the identity element of *G*.

(iv) Inverse Property: For any word $w = a^{\alpha} \in G$, $w^{-1} = a^{27-\alpha} \in G$ is the inverse of G, since

$w \Delta w^{-1} = a^{\alpha} \Delta a^{27-\alpha} = a^{(\alpha +_{27} 27-\alpha)} = a^0 = \chi$ and $w^{-1} \Delta w = a^{27-\alpha} \Delta a^{\alpha} = a^{(27-\alpha +_{27} \alpha)} = a^0 = \chi$

Thus all the four group axioms are satisfied and so *G* form a Group and the proof is complete.

3. CONGRUENCE RELATION FOR THE SET OF WORDS

We now try to define congruence relation modulo 27 for the set of words generated by *G*, and prove that such a relation is an "Equivalence Relation".

For any two words $w_1 = a^{\alpha_1}, w_2 = a^{\alpha_2}$ generated through *G*, we define the "Congruence modulo 27" relation between them as $w_1 \equiv w_2 (\bmod 27)$ if $\alpha_1 - \alpha_2$ is divisible by 27. We can now prove the following theorem.

Theorem 2:

The Congruence modulo 27 relation defined above between the words of *G* is an Equivalence relation with 27 equivalence classes.

Proof: We will prove the theorem by verifying the following three conditions for being Equivalence Relation.

(i) Reflexive Property: Any word $w = a^{\alpha}$ generated by *G* is related to itself because $\alpha - \alpha = 0$ and 0 is divisible by 27. Thus, $w \equiv w (\bmod 27)$.

(ii) Symmetric Property: For any two words $w_1 = a^{\alpha_1}, w_2 = a^{\alpha_2}$, if we assume that $w_1 \equiv w_2 (\bmod 27)$ then $\alpha_1 - \alpha_2$ is divisible by 27. But this means that $\alpha_2 - \alpha_1$ is also divisible by 27 and so we get $w_2 \equiv w_1 (\bmod 27)$.

(iii) Transitive Property: For any three words $w_1 = a^{\alpha_1}, w_2 = a^{\alpha_2}, w_3 = a^{\alpha_3}$, if we assume that $w_1 \equiv w_2 (\bmod 27)$ and $w_2 \equiv w_3 (\bmod 27)$ then $\alpha_1 - \alpha_2$ is divisible by 27 and $\alpha_2 - \alpha_3$ is divisible by 27. Therefore, their sum $(\alpha_1 - \alpha_2) + (\alpha_2 - \alpha_3) = \alpha_1 - \alpha_3$ is also divisible by 27. Thus $\alpha_1 - \alpha_3$ is divisible by 27. Hence $w_1 \equiv w_3 (\bmod 27)$.

Thus the “Congruence modulo 27” relation is an Equivalence relation for the words generated by *G*. So, if *W* is the set of all words generated by G, then the “Congruence modulo 27” relation induces a partition of *W* in to disjoint equivalence classes. Now we will try to find the equivalence classes generated by the above equivalence relation.

If $w = a^{\alpha} \in W$, then the equivalence class of *w* denoted by [*w*] is given by

$[w] = [a^{\alpha}] = \left\{ w = a^{\beta} \in W \right\}$ such that $\alpha - \beta$ is divisible by 27.

Thus if $w = a$, then its equivalence class is given by $[a] = \left\{ w = a^{\beta} \in W \right\}$ such that $1 - \beta$ is divisible by 27. Since $0 \le \beta \le 26$, it follows that $\beta = 1$ and so $[a] = \{a\}$. Thus equivalence class of *a* contain only one element namely *a*.

Similarly, if $w = b = a^2$, then its equivalence class is given by $[b] = \left\{ w = a^{\beta} \in W \right\}$ such that $2 - \beta$ is divisible by 27. But this happens only if $\beta = 2$ and so $[b] = \{b\}$. Continuing in the same fashion, we observe that the equivalence class of all 26 English alphabets contain only one element namely themselves and the equivalence class of the identity element is itself. Thus, the “Congruence modulo 27” relation gives rise to 27 disjoint equivalence classes of *W*. This completes the proof.

4. APPLICATION

The 27 equivalence classes found above forms an abelian Group of order 27 with respect to the operation juxtaposition of the equivalence classes. It is also evident that all possible word of English Language can be reduced to a form of a single letter of the alphabet, as we get only one element in all equivalence classes. This conversion has many applications in encryption and decryption process of Cryptography the Science of secret codes. It is also possible to consider any well-known global Language. If such language possesses*k* alphabets, then we can construct an abelian group of order *k* + 1 as discussed above. This group provides wonderful way to identify the words generated by that particular language.

5. GENESIS OF FREE GROUPS FOR ENGLISH ALPHABETS

We will consider an example to show the existence of Free Groups (through an example) which generates all words of English Language.

Let *X* be the generating set given by $X = \left\{ a, b, c, \ldots, k, l, m \right\}$. So, *X* contain the first 13 English alphabets and the remaining 13 alphabets can be considered as inverse of these elements and they are given by $z = a^{-1}, y = b^{-1}, w = c^{-1}, \ldots, n = m^{-1}$. Then the set of all reduced words formed from *X*will be called as “Free Group” denoted by $f(X)$ generated by *X*. By choosing different sets *X*we get different free groups and each has their own properties. These free groups have been widely used by engineers and scientists in identifying various categories for their investigations.

If we now consider $X = \{a, b\}$ and if these elements *a*, *b* satisfy the relations $a^2 = 1, b^2 = 1, ab = ba$. We can now construct a new group G_1, using the set *X* and the three relations stated above. Now any element in G_1 will be of the form $\left\{a^{\alpha_i} b^{\beta_j}\right\}$ where $0 \le \alpha_i \le 1, 0 \le \beta_j \le 1$. Since we see that every element of is one of the four basic forms given by $\{1, a, b, ab\}$. Thus using the idea of free groups we can generate words of desired nature and property. Needless to say that this facility of allowing to generate particular set of words from a specific language has wide applications in Literature and our great ancient Indian Mathematician and Sanskrit scholar Panini did the same work two millennium ago.

6. References

[1] J. Wang (1995) Average -case completeness of a word problem for groups.

[2] Joan S. Birman, Ki Hyoungko and Sang Jin Lee (1998) A new approach to the word and conjugacy problems in the braid groups, Advances in Mathematics, 139, 322-353.

[3] D. Garber, S. Kaplan & M. Teicher (2002), A new algorithm for solving theword problem in Braid groups, Ramat-Gan, Israel 52900.

[4] I.N. Herstein (2006) Topics in Algebra

[5] Hans Wussing (2007) The Genesis of the Abstract Group Concepts