UNUSUAL WAY OF LOOKING AT A FINITE GROUP AS SUBGROUP OF A SPECIAL LINEAR GROUP

Gaurav Mittal#1, Kanika Singla#2

#1Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee, India;

#2Department of Mathematics, Indian Institute of Science Education and Research, Mohali, India;

ABSTRACT. In this paper we have proved that every group of finite order can be embedded in a normal subgroup of the group of invertible matrices over the field $\mathbb{R}$, i.e., $GL(n,\mathbb{R})$ for some n. The field we have taken, is $\mathbb{R}$. But, we can also take $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ or finite fields instead of $\mathbb{R}$. We have given the proof for embedding of A_n in $SL(n,\mathbb{R})$ which is stronger result than the embedding of A_n in $SL(n+1,\mathbb{R})$. We have also shown that any group of finite order can be embedded in a perfect group.

Keywords: Embedding, General linear group, Perfect group, Special linear group, Alternating group

1. INTRODUCTION

An embedding of some object R into a different or same object S is a map $F : R \to S$ which is injective and structure preserving, i.e., an injective homomorphism. We can then say that R is isomorphic to a subset of S having same structural properties as that of S. Example of such maps are injective group homomorphism, ring homomorphisms, field homomorphisms and many more. Homeomorphism between topological spaces is also one of the example of an embedding. But in this paper we confined ourselves to the injective group homomorphisms only. Our main aim is to define injective group homomorphims between the groups.

2. MAIN RESULT

Theorem 2.1. *Any group having finite order can be embedded in a normal subgroup of the general linear group of matrices i.e. $GL(k,\mathbb{R})$ for some positive integer k.*

For proving above theorem, we need few results. So, we first discuss them and then we will prove the Theorem.

Theorem 2.2. *Cayley Theorem: Any group G is isomorphic to a subgroup of a symmetric group S_G, where S_G is the permutation group of elements of G.*

Proof. For proof, see [1, p. 86, Th. 5.1]. □

Remark 2.1. *If G is of finite order, say n, then G will be isomorphic to a subgroup of S_n, where S_n is symmetric group on n symbols.*

Theorem 2.3. *The symmetric group S_n can be embedded in group of all even permutations on $n+2$ symbols $\{1, 2 \ldots, n+2\}$, i.e. Alternating group A_{n+2} for any positive integer n.*

Proof. To prove this, we use the following results about S_n which are already proved in [1], [2]:

(1) Any permutation $\zeta \in S_n$ can be written as product of even or odd number of transpositions and accordingly these permutations are coined as even or odd.

(2) Multiplying any odd (even) permutation with a $2-$ cycle, it becomes even (odd).

Now let us define a map $\psi : S_n \mapsto A_{n+2}$ as

$$\psi(\zeta) = \begin{cases} \zeta, & \text{if } \zeta \text{ is even} \\ \zeta(n+1, n+2), & \text{if } \zeta \text{ is odd} \end{cases}$$

where $(n+1, n+2)$ is a $2-$ cycle.

It is easy to prove that ψ is a group homomorphism. Further

$$\text{Kernel } \psi = \{\zeta \in S_n : \psi(\zeta) = (1)\}$$

$$= \{(1)\}$$

where (1) is identity permutation. Thus ψ is one-one and hence ψ is an embedding. □

Theorem 2.4. *The alternating group A_n can be embedded in $GL(n, \mathbb{R})$, where $GL(n, \mathbb{R})$ is general linear group of $(n \times n)$ matrices over reals for any positive integer n.*

Proof. For proving above result, again we have to define a one-one homomorphism between the two. So consider $F : A_n \mapsto GL(n, \mathbb{R})$ defined as

$$F(\zeta) = (A_\zeta)^t$$

where (A_ζ) is a matrix whose $(i, j)^{th}$ entry is 1 whenever $\zeta(i) = j$ and 0 elsewhere, i.e.,i^{th} row of (A_ζ) is e_j^t where e_j is the $(n \times 1)$ column vector with 1 at j^{th} position and 0 elsewhere . Now the main task is to prove that F is a group homomorphism, i.e.,

$$F(\zeta \circ \eta) = F(\zeta)F(\eta)$$

where $\zeta, \eta \in A_n$. For proving above, it is enough to prove that i^{th} column of both the matrices is same for each $i \leq n$. So, let $\zeta, \eta \in A_n$, and also consider

$$\zeta(j) = k \qquad \& \qquad \eta(i) = j \qquad 1 \leq i, j, k \leq n.$$

Then i^{th} column of $F(\zeta \circ \eta)$ is i^{th} row of the matrix $(A_{\zeta\circ\eta})$ which is the $(n \times 1)$ vector e_k.

Now i^{th} column of $F(\zeta)F(\eta)$ is obtained by multiplying $F(\zeta)$ with i^{th} column of $F(\eta)$ i.e., e_j. So, i^{th} column of $F(\zeta)F(\eta)$ will then be equal to j^{th} column of $F(\zeta)$ which is equal to e_k. Thus F is a homomorphism.

Further we can easily prove that Kernel $F = \{(1)\}$ which implies that F is one-one and hence an embedding. □

Theorem 2.5. *The general linear group of $k \times k$ matrices i.e. $GL(k, \mathbb{R})$ can be embedded in special linear group of $(k+1) \times (k+1)$ matrices over reals having determinant 1 i.e. $SL(k+1, \mathbb{R})$ for any positive integer k.*

Proof. Let us consider the following map $\phi : GL(k,\mathbb{R}) \mapsto SL(k+1,\mathbb{R})$ defined by

$$\phi(G) = \begin{bmatrix} \frac{1}{det(G)} & 0 \\ 0 & G \end{bmatrix}$$

Since G is an invertible $k \times k$ matrix, clearly $\phi(G)$ is a well defined $(k+1)\times(k+1)$ matrix. Moreover,

$$det(\phi(G)) = \frac{1}{det(G)} \times det(G) = 1$$

and thus $\phi(G) \in SL(k+1,\mathbb{R})$.

To prove ϕ is injective homomorphism.

For homomorphism, take $G_1, G_2 \in GL(k,\mathbb{R})$, we have

$$\begin{aligned} \phi(G_1G_2) = \begin{bmatrix} \frac{1}{det(G_1G_2)} & 0 \\ 0 & G_1G_2 \end{bmatrix} &= \begin{bmatrix} \frac{1}{det(G_1)det(G_2)} & 0 \\ 0 & G_1G_2 \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{det(G_1)} & 0 \\ 0 & G_1 \end{bmatrix} \times \begin{bmatrix} \frac{1}{det(G_2)} & 0 \\ 0 & G_2 \end{bmatrix} \\ &= \phi(G_1)\phi(G_2). \end{aligned}$$

It is easy to check that ϕ is injective. □

Above two theorems combinely say that an Alternating group of degree n , i.e., A_n can be embedded in the special linear group , $SL(n+1,\mathbb{R})$. Infact we can also prove a slightly stronger result.

Theorem 2.6. *The alternating group A_n can be embedded in $SL(n,\mathbb{R})$, where $SL(n,\mathbb{R})$ is general linear group of $(n \times n)$ matrices over reals.*

Proof. We begin with the same mapping $F : A_n \to SL(n,\mathbb{R})$, as taken in Theorem 2.4, and we prove that $F(\zeta) \in SL(n,\mathbb{R})$ for all $\zeta \in A_n$. For that, we have to prove that determinant of $F(\zeta) = 1$ for all $\zeta \in A_n$, i.e., to prove that $det(F(\zeta)) = 1$ for all $\zeta \in A_n$. Let $\sigma = (i,j) \in S_n$, where $i < j$,

$$F(\sigma) = \begin{bmatrix} R_1 \\ . \\ . \\ . \\ R_n \end{bmatrix}$$

where $R_k = e_k^t$ for $k \neq i,j$; $R_i = e_j^t$ and $R_j = e_i^t$. By interchanging R_i and R_j, we get the identity matrix I. Thus, from $([1], p.51, \mathrm{Cor.}5.2)$

$$det(F(\sigma)) = -det(I) = -1$$

Now, any $\zeta \in A_n$ can be written as product of even number of transpositions and as F is a homomorphism, we get

$$det(F(\zeta)) = (-1)^k$$

where ζ is product of k number of transpositions. Further we know that k is even, and so,

$$det(F(\zeta)) = 1$$

and hence the result. □

Theorem 2.7. *$SL(k, \mathbb{R})$ is a normal subgroup of $GL(k, \mathbb{R})$ for every positive integer k.*

Proof. We know that Kernel of any group homomorphism is a normal subgroup of the group. So we will use this result to prove above stated theorem. Now define a map $f : GL(k, \mathbb{R}) \mapsto R^*$ given by

$$f(A) = det(A)$$

where R^* is a multiplicative group of non zero reals. So, f is an onto homomorphism having kernel $SL(k, \mathbb{R})$, and hence the result. □

Now we are ready to give the proof of theorem 2.1.

Proof. (theorem-2.1) Using theorems 2.2 to 2.7, we conclude that any group of finite order can be embedded in a normal subgroup of a matrix group. □

3. Embedding of any finite group into a Perfect group

Definition 3.1. *Commutator subgroup of a Group G :- It is the subgroup generated by all the commutators of G. It is denoted by $G^{'}$ and is defined by $G^{'} = \langle ghg^{-1}h^{-1} | g, h \in G \rangle$. It is also known as derived subgroup of the group G.*

Definition 3.2. *Perfect Group :- A group G for which the commutator subgroup, G' is the whole group G, is called perfect group.*

Theorem 3.1. *Every finite group can be embedded in a simple group.*

Proof. If the order of G is finite, then clearly G can be embedded in S_n for n = order of G and from theorem 2.3, S_n can be embedded in A_{n+2}. So any group of order n can be embedded in A_{n+2} , and further we know that A_n can be embedded inside A_k for all $k \geq n$. Now as we know that A_n is simple for $n \geq 5$,$(cf.[1], p.135, \text{Thm.3.3})$ we have the result. □

Corollary 3.1. *Every group of finite order can be embedded inside a perfect group.*

Proof. We have the result that commutator subgroup of a group G is a normal subgroup of G, $(cf.[1], p.93, \text{Thm.1.4})$, and hence $A_n^{'} \trianglelefteq A_n$, but as we know that the alternating group A_n is simple for $n \geq 5$, so either $A_n^{'} = (1)$ or ${A_n}' = A_n$, but if $A_n^{'} = (1)$, this would imply that A_n is abelian which is not true for $n \geq 4$, and so ${A_n}' = A_n$ for $n \geq 5$, so A_n is perfect for $n \geq 5$, and hence the result. □

References

[1] Basic Abstract Algebra, 2nd ed, P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul, Cambridge University Press, 1994.

[2] Contemporary Abstract Algebra, 8^{th} ed, Joseph A. Gallian, Thomson Brooks/Cole, 2012.