UIT Report Vol. 14, No. 1, pp. 125~127, 1983 연구논문집 제14권 제1호 pp. 125~127, 1983

A Representation of the Symmetric Group

Keum, Byoung Joon
Dept. of Mathematics
(Received October 30, 1982)

〈**Abstract**〉

A new computational tool for symmetric groups is introduced, by generalizing graphs.

대칭군의 표현

琴 秉 俊
수 학 과
(1982. 10. 30 접수)

〈요 약〉

그래프를 일반화함으로써 대칭군의 새로운 계산방식을 제시한다.

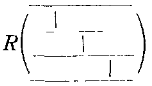
The symmetric group S_n plays a very important role in finite group theory, Galois theory, etc. In particular, Cayley's theorem implies that any finite group is a subgroup of a symmetric group. Hence it suffices to look into symmetric groups in order to study finite groups. But this logical advantage has not been fully exploited, because messy computations in S_n show the structural relationships only evasively.

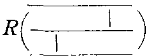
As matrices show the structure of linear transformations, there is an analogous representation of a permutation which shows the structure vividly and makes all manipulations effective and interesting. In elementary algebra it is taught that any element of S_n can be decomposed into transpositions, and this is our point of departure.

1. DEFINITION. We consider a sequence of horizontal line segments (called bases) in an array, and name these by writing a natural number at each right end of a base, which may be considered to be multiplication by an infinite column vector. Usually we assume the names are $1, 2, 3, \ldots$, in this order from the above, and in this case omit them.

Choose two bases a_1, a_2 of the sequence and represent this CHOICE by drawing a vertical line segment (called a bit) from a_1 to a_2, and call the resulting diagram the transposition of a_1 and a_2. Let S_0 be the free group generated by these transpositions, and write compositions as juxtapositions. The diagram with no bit will be called id and serve as the identity element of S_0, and the inverse of a diagram will be obtained from it by renaming the bases as negative integers. (This convention corresponds to reverse directions in diagram chasing.) It is clear that the elements of S_0 represent permutations. We naturally assume $S_1 \subset S_2 \subset \cdots \subset S_n \subset \cdots$ and let $S = \bigcup_{n=1}^{\infty} S_n$. Let R: $S_0 \to S$ be the representation map, and let $K = \ker R$. ***Every finite group is a subgroup of*** S_0/K, ***but our major interest will be in*** $M_n = R^{-1}(S_n)$, or $L_n = M_n/M_n \cap K$, ***and we usually omit bases not containing end points of bits.***

2. EXAMPLES. We adopt the notations of [1].

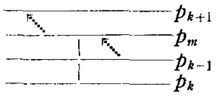
$(1234)=R$ 

$(132)=R$ 

3. REMARK. Let us call the number $0(d)$ of bits the order of the diagram d in S_0. Observe $(-1)^{0(d)}=\operatorname{sgn} R(d)$, and since d^{-1} can be obtained from d by reflection (in L_n), sgn R(d)=sgn $R(\mathrm{d}^{-1})$ follows. This simple and heuristic feature is noticeable.

4. PROPOSITION. $\min\{0(d):\ d\in R^{-1}(p_1,\ p_2,\ \ldots,p_n)\}=n-1$.

Proof. We may assume $n>4$. If $0(d)<n-1$, for d in $R^{-1}(p_1,\ p_2,\cdots,p_n)$, then any p_k $(k=1,2,\ldots,n)$ must contain at least one end point of a bit, and there are at most $2(n-2)-n=n-4$ of them containing more than one end points. In any way, there is a p_k containing end point of only one bit. If we write $p_{n+1}=p_1$, and if the other end point is at p_m, observe the following.

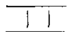


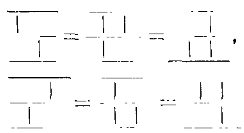
Hence we can efface p_k and its bit out and apply induction.

5. REMARK. If we collapse each base into a point, we get a graph in which the bits appear as edges, and proposition 4 will imply Denes' result requiring the graph be a tree. In other words, our diagrams generalize graphs by annexing time factor. In order to calculate effectively, we must know the structure of $M_n\cap K$, and we shall work in L_n, but use notations of M_n which will cause no confusion.

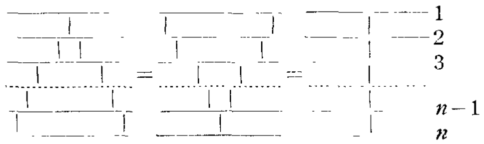
6. COROLLARY. Any d in L_n can be written in such a diagram that the associated graph (as in the Remark above) is a forest. This diagram, made into the form of disjoint union of descending steps, will be called the cannonical form of d. If $R(d)$ is of type $1^{b_1}\ 2^{b_2}\cdots n^{b_n}$, then $0(d)=\sum_{i=1}^{n}(i-1)b_i=n-\sum_{i=1}^{n}b_i$. (Here, a forest means a simple graph with no circuit.)

7. FUNDAMENTAL IDENTITIES.

(1)  $=id$

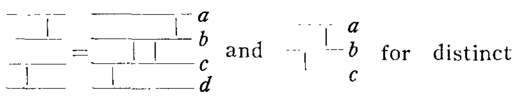
(2) 

(3)



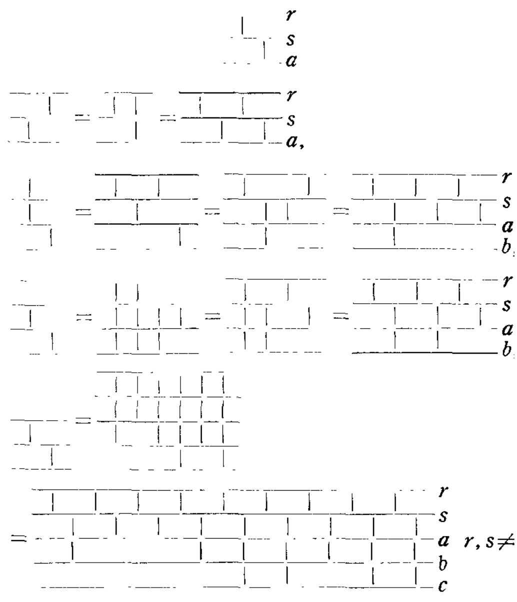
8. ILLUSTRATION. Observe how our machinery makes the following well-known but rather *troublesome proof elegant: the alternating group* A_n is simple if $n\geq 5$.

Proof Since A_n is generated by

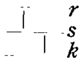


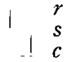
a, b, c, d, in $\{1,2,\ \cdots,n\}$, A_n must be generated by the set of three cycles.

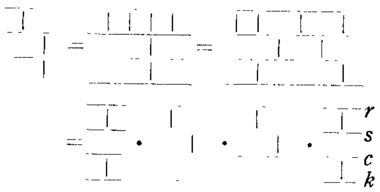
Choose distinct r,s in $\{1,2,\cdots n\}$. Then any *three cycle is of one of the following forms:*



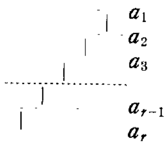
$a, b, c,$ distinct. Hence A_n is generated by

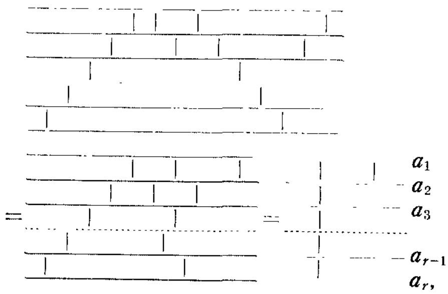
 $1 \leq k \leq n,\ k \neq r, s.$

If  $\in N$, for $N \lhd A_n$, then for $k \neq r$, s, c, N contains

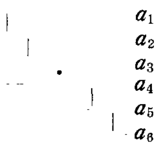


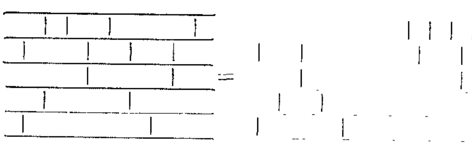
Hence $N = A_n$.

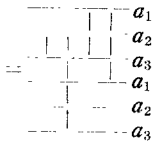
If N contains $s=$  $\cdot$ t, where the product is disjoint and $r \geq 4$, then N contains

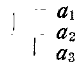
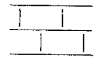


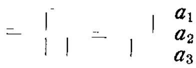
and hence $N = A_n$.

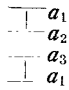
If N contains $s=$  $\cdot\, t$. where the product is disjoint, then N contains

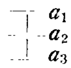


 and hence $N = A_n$.

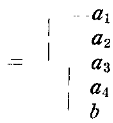
If N contains $s=$  $\cdot\, t$, where the product is disjoint and t is a product of disjoint transpositions, then N contains $s^2=$ 

 and hence $N = A_n$.

If every element of N is the product of disjoint transpositions, let $s=$  $\cdot\, t \in N$,

$u=$  $\in A_n$. Then N contains

Since $n \geq 5$, we can choose $b \in \{1, 2, \cdots, n\} - \{a_1, a_2, a_3, a_4\}$. But, N contains



Hence $N = A_n$.

Now, we can conclude that A_n is simple.

Reference

[1] M. Aigner, Combinatorial Theory, New York, Springer-Verlag, 1979.