

List of Theorems

Proposition 1	18
Proposition 2	Properties of S_n	20
Theorem 3	Cycle Decomposition Theorem	21
Proposition 4	Group Identity and Group Element Inverse	23
Proposition 5	26
Proposition 6	Cancellation Laws	29
Proposition 7	31
Proposition 8	Intersection of Subgroups is a Subgroup ..	35
Proposition 9	Finite Subgroup Test	35
Theorem 10	Parity Theorem	37
Theorem 11	Alternating Group	38
Proposition 12	Cyclic Group as A Subgroup	40
Proposition 13	Properties of Elements of Finite Order ...	41
Proposition 14	Property of Elements of Infinite Order ...	43
Proposition 15	Orders of Powers of the Element	43
Proposition 16	Cyclic Groups are Abelian	44
Proposition 17	Subgroups of Cyclic Groups are Cyclic ...	45
Proposition 18	Other generators in the same group	46
Theorem 19	Fundamental Theorem of Finite Cyclic Groups	47
Proposition 20	Properties of Homomorphism	50
Proposition 21	Isomorphism as an Equivalence Relation ..	51

ONE REASON that we are interested in the symmetric group is that they contain all finite groups.

Theorem (Cayley's Theorem)

If G is a finite group of order n , then G is isomorphic to a subgroup of S_n .

15 Lecture 15 Jun 04 2018

15.1 Group Action

15.1.1 Cayley's Theorem

Theorem 42 (Cayley's Theorem)

If G is a finite group of order n , then G is isomorphic to a subgroup of S_n .

Proof

Since G is finite, let $G = \{g_1, g_2, \dots, g_n\}$ and let S_G be the permutation group of G . By identifying g_i with i , where $1 \leq i \leq n$, we see that $S_G \cong S_n$ ¹. Therefore, it suffices to find an injective homomorphism² $\sigma : G \rightarrow S_G$.

Consider the function $\mu_a : G \rightarrow G$, where $a \in G$, such that $\mu_a(g) = ag$ for all $g \in G$. Clearly, μ_a is surjective. Suppose $\mu_a = \mu_b$, where $b \in G$. Then $a = \mu_a(1) = \mu_b(1) = b$. Thus μ_a is also injective. It follows that $\mu_a \in S_G$ by definition.

Now define the function $\sigma : G \rightarrow S_G$ such that $\sigma(a) = \mu_a$. Clearly, σ is injective, since $\sigma(a) = \sigma(b) \implies \mu_a = \mu_b$. Observe that $\sigma(ab) = \mu_{ab} = ab = \mu_a \mu_b$. Thus σ is a group homomorphism. Note that $\ker \sigma = \{1\}$, the trivial group. It follows from the First Isomorphism Theorem that $G \cong \text{Im } \sigma \leq S_G \cong S_n$.^{3 4} □

¹ S_G is the permutation group of G .

We can think of S_G as a group of permutations that permutes the index of the elements of G . Since there are n indices, there are $n!$ ways to permute the indices, and so $|S_G| = n! = |S_n|$. Then we can certainly find some isomorphism from S_G to S_n , and so $S_G \cong S_n$.

² **Why do we need injectivity?** We need homomorphicity in order to invoke the First Isomorphism Theorem so that we can get $G \cong \text{im } \sigma \leq S_G \cong S_n$.

³ We shall use $H \leq G$ to denote that H is a subgroup of G from here on.

⁴ This is a result from Proposition 36

Cayley's Theorem is, however, too strong at times. We can certainly find a smaller integer m such that G is contained in S_m . Consider the following example.