

A Primer on Cayley's Theorem

Peter Stalin

September 18, 2008

1 Introduction

Cayley's Theorem has its foremost importance in its theoretic ability as a classification theorem. All finite groups are permutation groups, and thus items that are useful in combinatorics become useful in group theory, and thus can be immediately generalized to the whole of algebra. From then on it may be used for our simplification needs, structure identification, or to be used in conjunction with the other natural operations induced by the progress of group theory. A lot of the older theorems in group theory that predate its actual known existence, were about because they were theorems about permutations: Lagrange's theorem is a good example of this (see the Wikipedia page of Lagrange's Theorem about that).

Of course, the theorem goes both ways. What is good with permutations is good with groups and vis a vis. It's because of this that, somewhat ironically, group theory has done more for permutation groups than the other way around.

Either way, we set up to examine the main proof of Cayley's Theorem. The core aspect of which, is that somewhere in the proof the group induces a permutation. I looked through multiple books about this, and all essentially have the same theorem. Some actually explain to the reader that the crucial concept involved is that we are collecting what is known as a 'group action', while still others let this fact slide by the less advanced reader. Before we get to group actions though, we'll start-up with bijections, and go through and create the line of thought that connects bijections, group actions, and permutations in order to understand Cayley's Theorem.

2 The Bijection Set

We define a 'bijection set'. The idea of bijections is crucial behind understanding Cayley's Theorem, since bijections are essentially permutations of the set. This

is why two sets having the same cardinality is defined as being two sets that have a bijection between each other.

Def: Given a set $T \neq \emptyset$, let its bijection set $B(T) := \{f_T : T \rightarrow T \mid f \text{ is a bijective map}\}$.

Remark: Specifically, for an arbitrary finite set $T = \{x_1, x_2, \dots, x_n\}$, notice that $B(T) \cong B(J_n)$ where $J_n = \{1, 2, \dots, n\}$, since T is just a renaming of the elements in J_n . Furthermore, by definition $B(J_n) = S_n$.

3 A Crash Course on Group Actions

In general, a group action is defined as the following.

Def: $g \cdot a : G \times A \rightarrow A$ is a group action iff:

$$\text{i) } g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a \forall g_1, g_2 \in G, a \in A$$

$$\text{ii) } 1 \cdot a = a \forall a \in A$$

In a sense, by studying this mapping, we can impose some of the structure of G onto A , most of which is beyond the scope of this primer (and parts a little bit beyond myself). However, notice that if we fix a $g \in G$ with a given group action, then we are creating a permutation of the set A , since $\phi_g(a) = g \cdot a : A \rightarrow A$. To check that this is a permutation, we need to check that ϕ_g has a two-sided inverse. Which we do as follows with $\phi_{g^{-1}}$:

$$(\phi_{g^{-1}} \circ \phi_g)(a) = \phi_{g^{-1}}(\phi_g(a))$$

Definition:

$$= g^{-1} \cdot (g \cdot a)$$

Property (i):

$$= (g^{-1}g) \cdot a$$

$$= 1 \cdot a$$

Property (ii):

$$= a$$

□

The other side may be done similarly by interchanging g^{-1} and g .

4 Permutation Representation of a Group

Furthermore, as an extension of this, notice that every g creates a ϕ_g . From this it is natural to consider the mapping from G to some set of permutations over A which we call $S_A \subseteq B(A)$ by $\psi : G \rightarrow S_A, \psi(g) = \phi_g(a)$. It is easy to show that this is a homomorphism to S_A .

Thm: G is homomorphic to S_A

Pf:

We check group operation preservation:

$$\psi(g_1g_2) = \phi_{g_1g_2}(a) = (g_1g_2) \cdot a$$

(i):

$$= g_1(g_2 \cdot a) = \phi_{g_1} \circ \phi_{g_2} = \psi(g_1)\psi(g_2)$$

□

Remark: It is also via this mapping that we can check that S_A is a group. That is, we have that group actions help induce subgroups of permutation groups.

Now, let's consider the permutation representation if $A = G$, with the mapping $G \times G \rightarrow G$ defined to be the regular operation over G . With this, if we show that the permutation representation is in fact an isomorphism between G and $A(G)$. Then we note, by the section on the bijection set, that $A(G) \cong A(|G|)$, and then we are done.

5 The Proof of Cayley's Theorem

Thm: $G \cong A(G)$

Pf: We wish to show that ψ is an isomorphism, since group operation preservation has been shown, this means we ought to check injectivity and surjectivity.

Injectivity:

Let $\psi(g_1) = \psi(g_2)$, we show that $g_1 = g_2$

By definition:

$$\psi(g_1) = \phi_{g_1}(g) = \phi_{g_2}(g) = \psi(g_2) \forall g \in G.$$

In particular, let $g = 1$, then by definition:

$$\phi_{g_1}(e) = g_1 \cdot e = g_1 = g_2 = g_2 \cdot e = \phi_{g_2}(e)$$

Done.

Surjectivity:

Given $\phi_g, \exists g \ni \psi(g) = \phi_g$, which is true by construction.

Done.

Thus we have that $G \cong A(G)$.

□

6 Conclusion

That pretty much sums up Cayley's Theorem. The main idea is that groups induce actions, these actions induce bijections, and bijections are synonymous with permutations.