# Group Theory III 

UW Math Circle - Advanced Group

Session 16 (7 February 2014)

A permutation of $\{1,2, \ldots, n\}$ is a bijection from $\{1,2, \ldots, n\}$ to itself. That is, it is a reordering of the numbers from 1 to $n$.

We can write a certain permutation of 8 elements as follows: $\sigma=\left(\begin{array}{llllllll}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 6 & 3 & 5 & 2 & 1 & 4\end{array}\right)$. This means: 1 goes to 7,2 goes to 8,3 goes to 6 , etc. Sometimes we drop the upper line and just write $\sigma=[78635214]$.

We define multiplication of permutations $a b$ to mean "first do $a$, then do $b$ ". ${ }^{1}$ For example, if $\sigma$ is as above and $\tau=\left(\begin{array}{cccccccc}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 4 & 2 & 3 & 8 & 5\end{array}\right)$, then we can compute $\sigma \tau$ as follows. 1 goes to 7, which goes to 8; 2 goes to 8, which goes to 5; etc. We find $\sigma \tau=\left(\begin{array}{cccccccc}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 3 & 1 & 2 & 7 & 5 & 4\end{array}\right)$.
Theorem 7. The set of permutations of $n$ elements forms a group, denoted $S_{n}$ or $\mathfrak{S}_{n}$, and $\left|\mathfrak{S}_{n}\right|=$ $n$ !. This group is called the symmetric group on $n$ elements.

A permutation can be decomposed into cycles, for example, $w=(17)(28436)(5)$. This means " 1 goes to 7,7 goes to $1 ; 2$ goes to 8,8 goes to 4,4 goes to 3,4 goes to 6,6 goes to $2 ; 5$ goes to itself".

Theorem 8. The order of an element $w \in \mathfrak{S}_{n}$ is the least common multiple of the lengths of the cycles of $w$.

A transposition is a permutation which reverses two elements and keeps all other elements fixed. An even permutation is one which can be written as a product of an even number of transpositions. A permutation that is not even is odd.

Theorem 9. The set of even permutations of $n$ elements forms a subgroup of $\mathfrak{S}_{n}$, denoted $A_{n}$, the alternating group, and $\left|A_{n}\right|=\frac{1}{2}\left|\mathfrak{S}_{n}\right|=\frac{n!}{2}$.

[^0]
[^0]:    ${ }^{1}$ In some other places you may see it written the other way: $a b$ means first $b$, then $a$.

