1 Symmetric Groups Continued

**Theorem 1 (Homework)** Suppose $\sigma \in S_n$ is written as a product of transposition in two different ways, say $\sigma = \beta_1 \beta_2 \cdots \beta_r$ and $\sigma = \gamma_1 \gamma_2 \cdots \gamma_s$. Then $r \equiv s \mod 2$.

**Definition.** If the parity of the number of transpositions in the above theorem (i.e. $r$ or $s$ in the above theorem) is even then we say $\sigma$ is an even permutation. Otherwise, $\sigma$ is an odd permutation.

**Proposition 2** The set of even permutations in $S_n$ is a subgroup of $S_n$. This group is called the alternating group of order $n$, and is denoted by $A_n$. Moreover, $|A_n| = \frac{n!}{2}$.

**Proof (Sketch)** If $\sigma, \tau \in A_n$ then they can be written as the product of an even number of transpositions, so $\sigma \tau$ can be as well (by concatenation). Moreover, since $\sigma$ and $\sigma^{-1}$ have the same number of cycles of the same lengths in their disjoint cycle decomposition, they can be written as the product of the same number of transposition so $\sigma \in A_n \implies \sigma^{-1} \in A_n$.

To see that $|A_n| = \frac{n!}{2}$, observe that the set map $T : A_n \to S_n \setminus A_n$ defined by $T(\sigma) = (1\ 2)\sigma$ is a bijection: $|A_n| = |S_n \setminus A_n|$, and the result follows.

2 Homomorphisms & Isomorphisms

**Definition.** Let $(G, \cdot)$ and $(G', \star)$ be groups. A homomorphism is a set map $\phi : G \to G'$ that preserves the group operation in the respective groups; that is,

$$\phi(a \cdot b) = \phi(a) \star \phi(b)$$

for all $a, b \in G$.

**Example.** 1. Consider the groups $(GL_2(\mathbb{R}), \text{matrix multiplication}), (\mathbb{R}\setminus\{0\}, \times)$. Define $\phi : GL_2(\mathbb{R}) \to \mathbb{R}\setminus\{0\}$ by

$$\phi(A) = \det(A).$$

Then $\phi(AB) = \det(AB) = \det(A) \det(B) = \phi(A)\phi(B)$.

2. If $V$ and $W$ are vector spaces, then $(V, +)$ and $(W, +)$ are groups. Let $T : V \to W$ be any linear transformation. Then $T$ is a group homomorphism. Indeed,

$$T(v_1 + v_2) = T(v_1) + T(v_2)$$

by linearity.
3. Consider the groups \((\mathbb{Z}, +)\) and \((\mathbb{Z}/n\mathbb{Z}, +)\). Define

\[ \phi(a) = [a]. \]

Then \(\phi(a + b) = [a + b] = [a] + [b] = \phi(a) + \phi(b)\).

4. Consider the groups \((\mathbb{R}, +)\) and \((\mathbb{R}_{>0}, \times)\). Define \(\phi : \mathbb{R} \to \mathbb{R}_{>0}\) by

\[ \phi(a) = 2^a. \]

Then \(\phi(a + b) = 2^{a+b} = 2^a \cdot 2^b = \phi(a) \cdot \phi(b)\).

5. For any group \((G, \cdot)\), we have an identity homomorphism \(I : G \to G\) given by

\[ I(g) = g \]

for all \(g \in G\).

6. Define \(\phi : S_n \to \mathbb{Z}/2\mathbb{Z}\) by:

\[ \phi(\sigma) = 1 \text{ if } \sigma \text{ is an odd permutation, } \phi(\sigma) = 0 \text{ if } \sigma \text{ is an even permutation.} \]

Exercise: \(\phi\) is a homomorphism.

**Definition.** Let \(\phi : G \to G'\) be a homomorphism. We say \(G\) is the *domain* of \(\phi\) and \(G'\) is the *codomain* of \(\phi\).

We now discuss some properties of homomorphisms.

**Theorem 3** Let \(\phi : G \to G'\) be a homomorphism. For all \(a \in G, n \in \mathbb{Z}\), the following hold

1. \(\phi(e_G) = e_{G'}\)
2. \(\phi(a^{-1}) = \phi(a)^{-1}\)
3. \(\phi(a_1 \cdots a_n) = \phi(a_1) \cdots \phi(a_n)\)
4. \(\phi(a^n) = \phi(a)^n\)

**Proof.**
1. \(\phi(e_G) = \phi(e_G)\phi(e_G)\) so multiplying by \(\phi(e_G)^{-1}\) (on any side) implies \(\phi(e_G) = e_{G'}\)
2. \(e_{G'} = \phi(a \cdot a^{-1}) = \phi(a)\phi(a^{-1})\), so \(\phi(a^{-1}) = \phi(a)^{-1}\).
3. Induction on multiplicative definition.
4. Part 3) where \(a_i = a\) for all \(i\).

**Definition.** A group homomorphism \(\phi : G \to G'\) is an *isomorphism* if \(\phi\) is a bijection. If there is an isomorphism between \(G\) and \(G'\) we say \(G\) and \(G'\) are isomorphic. This is denoted by \(G \cong G'\).
Example. In the example with different groups, 4 and 5 are isomorphisms.

Remark. If $G$ is a group, the set of bijections $\{\phi : G \to G \mid \phi \text{ is a bijection} \}$ is a group under composition. Indeed, one can check that if $\phi : G \to G$ and $\psi : G \to G$ are isomorphisms, then $\phi \circ \psi$ is an isomorphism. The fact that $\phi \circ \psi$ is a bijection has nothing to do with the group structure. To see that $\phi \circ \psi$ is a homomorphism, observe

$$\phi(\psi(ab)) = \phi(\psi(a)\psi(b)) = \phi(\psi(a))\phi(\psi(b)).$$

Furthermore if $\phi : G \to G$ is a bijective homomorphism, and we define $\psi : G \to G$ by assigning $\psi(a)$ to the unique value $a' \in G$ such that $\phi(a') = a$, then by definition $\psi \circ \phi = \phi \circ \psi = I$, (where $I$ is the identity map, see Example 5 above). We need to justify that $\psi$, the candidate inverse for $\phi$, is indeed a homomorphism. In this light, if $a', b' \in G$ then there exist $a, b$ such that $\psi(a') = a$ and $\psi(b') = b$, and this means $\phi(a) = a'$ and $\phi(b) = b'$ and hence $\phi(ab) = a'b'$, so $\psi(a'b') = ab = \psi(a')\psi(b')$. Hence $\phi = \psi^{-1}$ is an isomorphism of $G$.

This group of isomorphisms from a group $G$ to itself is called the automorphism group of $G$, and is denoted $\text{Aut}(G)$.

Given a homorphism $\phi : G \to G'$ there are subgroups of each that can indicate to us whether $\phi$ is injective or surjective.

Definition. Let $\phi : G \to G'$ be a homomorphism. Define $\ker(\phi) = \{g \in G : \phi(g) = e_{G'}\}$. This is called the kernel of $\phi$. Define $\text{im}(\phi) = \{\phi(g) : g \in G\}$. This is called the image of $\phi$. We usually use the notation $\phi(G)$ for $\text{im}(G)$.

Example. If $\phi : \text{GL}_2(\mathbb{R}) \to \mathbb{R}\{0\}$ is given by $\phi(A) = \det(A)$ then $\ker(\phi(A)) = \text{SL}_2(\mathbb{R})$ and $\text{im}(\phi) = \mathbb{R}\{0\}$.

Theorem 4 Let $\phi : G \to G'$ be a homomorphism. Then

1. $\ker(\phi)$ is a subgroup of $G$, and $\phi$ is injective if and only if $\ker(\phi) = e_G$.
2. $\text{im}(\phi)$ is a subgroup of $G'$, and $\phi$ is surjective if and only if $\text{im}(\phi) = G'$ (or equivalently, $\phi(G) = G'$).

We shall prove this next time.