Math 375
Week 5

5.1 Symmetric Groups

The Group S_X

Now let X be any non-empty set. Let

$$S_X = \{\phi |\ \phi : X \to X \text{ and } f \text{ is both surjective and injective}\}.$$

Notice that if $\phi, \lambda \in S_X$, then $\phi\lambda : X \to X$ and is surjective and injective by previous arguments. That is, the composition $\phi\lambda \in S_X$. Thus composition is a binary operation on S_X.

THEOREM 1 *S_X is a group under composition. (S_X is called the **Symmteric Group on** X).*

PROOF (i) We just checked closure. (ii) Associativity: mentioned last time (see text Chapter 0). (iii) The identity in S_X is i_X because $\phi\_X(x) = \phi(i_X(x)) = \phi(x)$, that is, $\phi i_X = \phi$. Similarly $i_X\phi = \phi$. (iv) Evidently the inverse of ϕ is ϕ^{-1} which we know exists because ϕ is injective and surjective and $\phi\phi^{-1}(x) = x = i_X(x)$ and $\phi^{-1}\phi(x) = x = i_X x$. ∎

This last example shows just how general the group concept is. Symmetric groups are extraordinarily important. Arthur Cayley (as in Cayley table) showed that every group is the subgroup of some symmetric group. So if you understand symmetric groups completely, then you understand all groups! We can examine S_X for any set X. For example if $X = \mathbf{R}$, then examples of of elements in $S_{\mathbf{R}}$ are $i_{\mathbf{R}}$, $f : \mathbf{R} \to \mathbf{R}$ by $a \to a + 1$, $g : \mathbf{R} \to \mathbf{R}$ by $a \to a/2$, and so on. It is clear that $S_{\mathbf{R}}$ is infinite.

The individual elements of S_X are often called **permutations** of the elements of X. This will be the next big topic we cover.

The Symmetric Group on n Elements: S_n

To make matters simpler, we will study symmetric groups of finite sets. For example, if X is a set of n elements, then we may as well label the elements of X as $\{1, 2, \ldots, n\}$. We usually denote the **symmetric group on n elements** by S_n.

Now any element or **permutation** ϕ in S_n is an injective and surjective function from the set of the first n integers to itself. It merely shuffles these elements around. Consequently it can be represented as a two row matrix in which the first row represents the input and the second represents the corresponding output.

Example 1 List all the elements of S_3.

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \beta\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

It should be clear what the identity element is. How do we get the inverse of any element? (Merely exchange rows, and re-order.) How do we take the product or composition of two such elements in S_n? In composing functions always remember to *work from the right to the left* which is backwards from what we read. This is a hold over from composition of functions, which is what we implicitly are doing here.

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Notice that order matters:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Clearly S_1 is abelian, since it consits of only the identity element. We'll see that S_2 is abelian (in fact it's cyclic) since it has only two elements. However, we have seen that S_3 is not abelian and in general:

Theorem 2 *If $n \geq 3$ then S_n is non-abelian.*

PROOF Let α and β be the following two elements in S_n:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \dots & n \\ 3 & 2 & 1 & 4 \dots & n \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \dots & n \\ 2 & 1 & 3 & 4 \dots & n \end{pmatrix}.$$

Then

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \dots & n \\ 3 & 1 & 2 & 4 \dots & n \end{pmatrix} \quad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \dots & n \\ 2 & 3 & 1 & 4 \dots & n \end{pmatrix}. \ \square$$

EXAMPLE 2 Find the following inverse:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

THEOREM 3 $|S_n| = n!$.

PROOF $|S_n|$ is just the number of ways the integers 1 through n can arranged. In other words in how many different ways can we fill in the blanks:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ - & - & \dots & - \end{pmatrix}$$

Well we have n choices for the first entry, and then $n-1$ choices for the next entry, and so on yielding a total of

$$n \cdot (n-1) \cdots 1 = n!$$

total choices. ∎

For example $|S_3| = 3! = 6$ as we have already seen. $|S_2| = 2! = 2$. If we write out the Cayley table for S_2 we see that it is abelian. (Note that the square of every element is the identity.)

$\circ$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

EXAMPLE 3 Compare the symmetries of an equilateral triangle to S_3. Write each element in D_3 as a permutation.

EXAMPLE 4 Compare D_4 to S_4. Are they the same group?

Cycle Notation

It will prove much more convenient to use a differnt type of notation to denote the individual permutations of S_n. This **cycle notation** is useful because it reveals the structure of individual elements in the group, much as powers of a generator indicate the nature of a cyclic group. Here's how it works.

Consider the following elements of S_5:

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \qquad \lambda = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$$

Notice that ϕ breaks quite naturally into two parts:

$$1 \to 2 \to 3 \to 1 \quad \text{and} \quad 4 \to 5 \to 4$$

Each of these pieces is called a **cycle**. The first is a three-cycle because it contains three different elements, the second is a two-cycle. Each of these cycles can be represented more compactly without the arrows:

$$(1,2,3) \quad \text{and} \quad (4,5)$$

Let's look at λ. This time the cycles are:

$$1 \to 4 \to 1 \quad \text{and} \quad 2 \to 3 \to 5 \to 2$$

or

$$(1,4) \quad \text{and} \quad (2,3,5)$$

When using cycles we adopt the convention that if an element is missing from the cycle, then it is mapped to itself.

Example 5 What permutation does the cycle $(2,4,3)$ represent in S_6?

$$(2,4,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$$

Example 6 Let $\alpha = (1,3,6)(2,4,5)$ and $\beta = (1,2,3)(4,5)$ in S_6. Then $\alpha\beta = (4,2,6,1)(5)(3) = (4,2,6,1)$. Do some more.

Example 7 What is the inverse of a single cycle: $\alpha = (4,2,3,5)$? This is easy to spot in matrix form. If

$$\alpha = (4,2,3,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix},$$

then

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix} = (5,3,2,4).$$

More generally:

THEOREM 4 *The inverse of a cycle is the cycle in inverse (reverse) order. Further the inverse of a product of cycles is the product of the inverse cycles in reverse order.*

REMARK The second part of the theorem is the usual statement about inverses of products being the product of the inverses in reverse order.

DEFINITION 5 *Two cycles are called* ***disjoint*** *if they contain no term in common.*

For example $(1,2,6)$ and $(3,4)$ are disjoint but $(1,2,4)$ and $(3,4,5)$ are not. One of the basic facts about permutations is that

THEOREM 6 *Any permutation can be written as a product of disjoint cycles.*

The details of the proof are presented in the text, but note that this is how we first got started on looking at cycles. Given an individual example of a permutation it is easy to see how to split it into disjoint cycles. Consider

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 3 & 8 & 6 & 1 & 4 & 7 & 2 \end{pmatrix}.$$

We simply start the first cycle with 1, continue back until we get 1. Then start the second cycle with the smallest remaining unused number until we get back to it and so on. In this case the cycles are: $(1,5,6)(2,9)(3)(4,8,7)$.

THEOREM 7 *Disjoint cycles commute.*

PROOF Let the disjoint cycles be $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, \beta_n)$, where α and β have no entries in common. Let the full set S be given by

$$S = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, \beta_n, c_1, \ldots, c_k\}.$$

We want to prove that $\alpha\beta = \beta\alpha$. To do this, we must show that $a(\alpha\beta) = x(\beta\alpha)$ for all $x \in S$. There are three cases: x is either an a, b, or c.

Suppose that $x = a_i$. Then

$$(\beta\alpha)(x) = (\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1 \bmod m}) = a_{i+1 \bmod m}.$$

while

$$(\alpha\beta)(x) = (\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1 \bmod m}.$$

Hence the permutations agree on the a's. A similar argument works for the b's. The c's are the easiest of all. If $x = c_i$, then

$$(\alpha\beta)(x) = (\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i$$

while

$$(\beta\alpha)x = (\beta\alpha)(c_i) = \beta(\alpha(c_i) = \beta(c_i) = c_i.$$

Again the permutations are the same. ∎

5.2 More about S_n

The Order of a k-cycle

Example 8 Consider the following elements of S_5: $\alpha = (2,3)$ and $\beta = (1,2,4)$, and $\beta = (1,3,4,2)$ Find the orders of each of these elements.

Taking β first, $\beta^2 = (1,4,2)$, every entry is moved two places down the cycle. So if we have a k-cycle, moving each entry k places down the cycle takes the entry back to its starting point, i.e., the k^{th} power of a k-cycle yields the identity and no smaller power will. It is clear that $\alpha^2 = e$, $\beta^3 = e$, and $\phi^4 = e$. In fact, this proves the general theorem:

Theorem 8 *If α is a k-cycle in S_n, then $|\alpha| = k$.*

Theorem 9 *The order of the product of disjoint cycles is the least common mutliple of their lengths (orders).*

PROOF Asume that $|\alpha| = m$ and $|\beta| = n$. Let $k = \text{lcm}(m,n)$. Then it follows that $\alpha^k = e = \beta^k$ since $|\alpha| \mid k$ and $|\beta| \mid k$. Since the cycles are disjoint, they commute, so $(\alpha\beta)^k = \alpha^k\beta^k = ee = e$. Consequently $|\alpha\beta| \mid k$.

But is k the smallest positive power with this property? Suppose instead that it were t. Then $(\alpha\beta)^t = \alpha^t\beta^t = e$ implies that $\alpha^t = \beta^{-t}$. But α^t and β^{-t} are disjoint. The only way two disjoint cycles can be the same is if both are empty. That is, $\alpha^t = \beta^{-t} = e$ (remember fixed symbols are not included in the cycles.) But now it follows that both m and n divide t. That is, t is a common multiple of m and n so $k = \text{lcm}(m,n) \leq t$. Therefore, $k = t$. ∎

Example 9 Give some. If the cycles are not disjoint, simply rewrite them as disjoint, and then apply the theorem.

Disjoint cycles are especially helpful for order calculations as we have seen. But permutations can be written as a different sort of product as the follwing discussion shows.

Two Cycles or Transpositions

The simplest sort of permutation is the one that shuffles two elements, that is, a two-cycle. In fact two-cycles are the building blocks of the entire permutation group. Two-cycles are also called **transpositions**.

Example 10 Consider the permutation $(1,2,3)$. It can be written as a product of two-cycles:

$$(1,2,3) = (1,3)(1,2).$$

Notice that it can be written as a different product of two-cycles:

$$(1,2,3) = (2,3)(1,3).$$

In fact, this is a particular example of

Theorem 10 *Any k-cycle in S_n can be written as a product of transpositions (two-cycles). (Here $n > 1$ or else we have $S_1 = \{e\}$.)*

PROOF If we have a 1-cycle, then it is the identity element which can be written as $(1,2)^2 = (,2)(1,2) = e$. Now if we have a k-cycle were $k \geq 2$ then we can work out the product just as we did in the example above:

$$(a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_1, a_3) \ldots (a_1, a_k). \blacksquare$$

Example 11 $(5,3,1,2) = (5,2)(5,1)(5,3)$

Corollary 11 *Any element of S_n can be written as a product of transpositions.*

PROOF Any element in S_n can be written as a product of disjoint cycles, each of which can be written as a product of two-cycles. So every element can be broken down eventually into a product of transpositions. $\blacksquare$

Example 12

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 6 & 3 & 4 \end{pmatrix} = (1,2,5,3)(4,6) = (1,3)(1,5)(1,2)(4,6).$$

It is also the case that

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 6 & 3 & 4 \end{pmatrix} = (4,6)(2,5,3,1) = (4,6)(2,1)(2,3)(2,5). \blacksquare$$

But notice that even though the number of transpositions in each decomposition is different, in both cases the number of transpositions is even.

Definition 12 *A permutation is **even** if it can be written as the product of an even number of permuatations. It is **odd** if it can be written as a product of an odd number of transpositions.*

For this distinction to be useful, it is necessary that no odd permutation be even. That is, either a permutation should always decompose into an odd number of transpositions or always into an even number (even though the actual number of transpositions in the decomposition can vary). In fact, this is the case:

THEOREM 13 *No permuatation is both odd and even.*

PROOF The proof is in the text; read through it. The main idea is that the identity permutation can *only* be written as an even product of transpositions. The general result easily follows from this. For if a permutation was both even and odd, then its inverse would be both even and odd. Take the permutation in its *even* representation and multiply by its inverse in its *odd* representation. The reuslt is product with an odd number of transpositions, but the result is also the identity which is supposed to be even. ∎

COROLLARY 14 *A k-cycle is even if k is odd; a k-cycle is odd if k is even.*

PROOF This follows immediately from the the method we use to break a k-cycle into transpositions. A k-cycle can always be written as the product of $k-1$ transpositions (see the factors in Examples 17.3 and 4).

EXAMPLE 13 Let A_n = the set of even permutations in S_n. Show that A_n is a subgroup of S_n. A_n is called the **alternating group** of degree n.

CLOSURE The product of two even permutations will again have an even number of factors, so A_n is closed.

INVERSES Notice that $(a\ b)^{-1} = (a\ b)$. Thus the inverse of a product of even permutation (using the general formula for the inverse of a product) is the product of the same transpositions in reverse order, hence is even again. ∎

EXAMPLE 14 Do the odd permutations form a subgroup of S_n?

Example 15 We can easily write out the elements of A_3 and A_4 because we know that the length of a cycle determines whether it is odd or even.

Here are the 6 elements of S_3, let's pick out the elements of A_3:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e \in A_3 \qquad \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (2\ \ 3) \notin A_3$$
$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1\ \ 2) \notin A_3 \qquad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1\ \ 2\ \ 3) \in A_3$$
$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1\ \ 3\ \ 2) \in A_3 \qquad \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (1\ \ 3) \notin A_3$$

For S_4 and A_4 the situation is similar. S_4 has 24 elements:

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = e \in A_4 \qquad \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix} = (2\ \ 3) \notin A_4$$
$$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} = (1\ \ 2) \notin A_4 \qquad \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix} = (1\ \ 2\ \ 3) \in A_4$$
$$\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = (1\ \ 3\ \ 2) \in A_4 \qquad \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} = (1\ \ 3) \notin A_4$$
$$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix} = (3\ \ 4) \notin A_4 \qquad \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix} = (2\ \ 3\ \ 4) \in A_4$$
$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = (1\ \ 2)(3\ \ 4) \in A_4 \qquad \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = (1\ \ 2\ \ 3\ \ 4) \notin A_4$$
$$\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix} = (1\ \ 3\ \ 4\ \ 2) \notin A_4 \qquad \begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix} = (1\ \ 3\ \ 4) \in A_4$$
$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix} = (2\ \ 4\ \ 3) \in A_4 \qquad \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix} = (2\ \ 4) \notin A_4$$
$$\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix} = (1\ \ 2\ \ 4\ \ 3) \notin A_4 \qquad \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix} = (1\ \ 2\ \ 4) \in A_4$$
$$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = (1\ \ 3)(2\ \ 4) \in A_4 \qquad \begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix} = (1\ \ 3\ \ 2\ \ 4) \notin A_4$$
$$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = (1\ \ 4\ \ 3\ \ 2) \notin A_4 \qquad \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix} = (1\ \ 4\ \ 2) \in A_4$$
$$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix} = (1\ \ 4\ \ 3) \in A_4 \qquad \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix} = (1\ \ 4) \notin A_4$$
$$\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix} = (1\ \ 4\ \ 2\ \ 3) \notin A_4 \qquad \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = (1\ \ 4)(2\ \ 3) \in A_4$$

There are two important observations. First, we see that S_3 is a subset and hence a subgroup of S_4 (just take a look at the first elements of S_4). In general we can always view S_m as a subgroup of S_n if $m < n$. Second, half the elements in S_3 are even; the same is true for S_4. In fact,

Theorem 15 $|A_n| = |S_n|/2 = n!/2$.

PROOF We need to show that half the elements of S_n are even. Let α be any two-cycle of S_n (say $\alpha = (1\ 2)$). Consider the mapping $f : S_n \to S_n$ by $f(\beta) = \alpha\beta$. Notice that f is both surjective and injective.

SURJECTIVE Let $\gamma \in S_n$. We must find $\beta \in S_n$ so that $f(\beta = \gamma$. But

$$f(\beta) = \gamma \iff \alpha\beta = \gamma \iff \beta = \alpha^{-1}\gamma.$$

INJECTIVE $\phi(\beta_1) = \phi(\beta_2) \iff \alpha\beta_1 = \alpha\beta_2 \iff \beta_1 = \beta_2$.

Notice that f maps the even permutations to the odd ones and vice versa (since it adds one transposition to the permutation) in a one-to-one, onto fashion. Hence there must be the same number of even and odd permutations, that is half of S_n is even. ∎

Some Examples

Example 16 Do Gallian page 110 #50.

SOLUTION If we let α denote the shuffle in question, then we are given that

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & J & Q & K \\ 10 & 9 & Q & 8 & K & 3 & 4 & A & 5 & j & 6 & 2 & 7 \end{pmatrix}$$
$$= (1 \quad 10 \quad J \quad 6 \quad 3 \quad Q \quad 2 \quad 9 \quad 5 \quad 13 \quad 7 \quad 4 \quad 8).$$

Notice that α must have been a 13-cycle since α^2 is. (If we expressed the original α as a product of disjoint cycles, powers of α simply permute the elements of those cycles among themselves.) Thus, $|\alpha| = 13$. So

$$(\alpha^2)^7 = \alpha^{14} = \alpha^{13}\alpha = \alpha.$$

But

$$(\alpha^2)^7 = (1 \quad 9 \quad 10 \quad 5 \quad J \quad K \quad 6 \quad 7 \quad 3 \quad 4 \quad Q \quad 8 \quad 2).$$

Example 17 Do Gallian page 109 #28.

SOLUTION $\beta = (123)(145) = (14523)$, so $\beta^{99} = \beta^{-1} = (32541)$.

Example 18 Do Gallian page 109 #37.

SOLUTION Let β be a 10-cycle. Do you see that there are powers so that β^k is not a 10-cycle? Those powers share a divisor with 10. So β^k is a 10-cycle iff $\gcd(10, k) = 1 \iff <\beta> = <\beta^k>$.

5.3 Dihedral Groups and Symmetric Groups

$D_3 \cong S_3$

Let us now reconsider thte rigid motions of an equilateral triangle with vertices labelled 1, 2, 3. Then every motion of the the triangle can be thought of as a permutation in S_3. Specifically, we can set up the following correspondence:

$$r_0 \to (1) \quad r_{120} \to (1,2,3) \quad r_{240} \to (1,3,2)$$

$$v \to (2,3) \quad d \to (1,3) \quad d' \to (1,2).$$

If we denote this correspondence or mapping by ϕ, then we see that $\phi : D_3 \to S_3$ is one-to-one and onto. Further, one can check that ϕ respects the group operations involved. That is: if $x, y \in D_3$, then

$$(xy)\phi = (x\phi)(y\phi).$$

Notice the group operation on the left takes place in D_3 and the operation on the right takes place in S_3. For example:

$$(vr_{240})\phi = d'\phi = (1,2) \text{ and} (a\phi)(r_{240}\phi) = (2,3)(1,3,2) = (1,2).$$

This is an example of an **group isomorphism**, that is, a one-to-one, onto map between groups that respects the group operations. We will study such maps in great detail later.

Notice that the elements of D_3 can be listed in another way. If we let $\rho = r_{120}$ then the following six elements are distinct:

$$\{e, \rho, \rho^2, h, h\rho, h\rho^2\} \subseteq D_3.$$

But since $|D_3| = 6$ these six elements must comprise all of D_3. In other words D_3, while it is not cyclic, it is *generated by two elements.*

D_4 and S_4

We can construct a similar correspondence between D_4 and some of the elements of S_4. Label the vertices of a square as 1, 2, 3, 4. As with the motions of a triangle, the particualr righid motion in D_4 is determined

by whether the square is face up or face down and by where the vertex 1 ends up. Hence $|D_4| = 2 \cdot 4 = 8$. this time the rotations are

$$r_0 = (1) \quad r_{90} = (1,2,3,4) \quad r_{180} = (1,3)(2,4) \quad r_{270} = (1,4,3,2)$$

$$h = (1,4)(2,3) \quad v = (1,2)(3,4) \quad d = (1,3) \quad d' = (2,4).$$

Let $\rho = r_{90}$. Now $|D_4| = 8$ and the following 8 elements are distinct and in D_4:

$$\{e, \rho, \rho^2, \rho^3, h, h\rho, h\rho^2, h\rho^3\} \subseteq D_4.$$

Therefore this must be the entire group.

We know now two different subgroups of S_4, namely A_4 and D_4. Are there others? (All the cyclic groups, S_3, and there are others (see text).)

This same process that we have carried out with D_4 and S_4 can be done with D_n and S_n, where D_n represents the motions of a regular n-sided polygon. This lime let

$$\rho = (1,2,\ldots,n) \quad \text{and} \quad h = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n-1 & n \\ 1 & n & n-1 & n-2 & \ldots & 3 & 2 \end{pmatrix}$$

Here ρ represents a rotation of $\frac{360}{n}$ and h represents the reflection across the line through vertex 1.

You should be able to show that

$$D_n = \{e, \rho, \rho^2, \ldots, \rho^{n-1}, h, h\rho, h\rho^2, \ldots, h\rho^{n-1}\}.$$

That is D_n is generated by two elements: its smallest rotation and any flip. See the optional exercise on Problem Set #11.