

## 8. PERMUTATION GROUPS

A *permutation* of a sequence of symbols is a rearrangement of the order of the symbols. The things being permuted are called “letters” even though they are usually numbers. For example 3241 is a permutation of the “letters” 1234. The symbols need to be different. Permutations can be described algebraically in two different ways.

- (1) As a movement of the letters. (In 3241, 1 moves to position 4.)
- (2) As a transformation of the letters. (In 3241, 1 changes into 3.)

Our book takes the second interpretation. Thus the permutation given by 3241 is the function which transforms 1 into 3, 2 to 2, 3 to 4 and 4 to 1:

$$\sigma(1) = 3, \quad \sigma(2) = 2, \quad \sigma(3) = 4, \quad \sigma(4) = 1$$

In other words,  $\sigma$  is a bijection of the set  $\{1, 2, 3, 4\}$  to itself. One notation for this is the following.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

or in general:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Since permutations are functions, you can compose them. For example if  $\tau$  is the permutation

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

then  $\tau\sigma$  means do  $\sigma$  then do  $\tau$ . Permutations are composed *right to left*. If you remember that we are using the “transformation” interpretation (instead of the “movement” interpretation) then the composition is easy to calculate. In the example,  $\sigma$  gives 3241. Then  $\tau$  will transform 2 into 3 and 3 into two changing the first two symbols into 23. So  $\tau\sigma = 2341$  or:

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

The formula would be:

$$\begin{aligned} \tau\sigma(1) &= \tau(3) = 2, & \tau\sigma(2) &= \tau(2) = 3 \\ \tau\sigma(3) &= \tau(4) = 4, & \tau\sigma(4) &= \tau(1) = 1. \end{aligned}$$

A permutations of  $A = \{1, 2, 3, 4\}$  is therefore a bijection  $\sigma : A \rightarrow A$  and the set of all permutation of  $A$  forms a group under composition. (To be continued.)

### 8.1. symmetric group.

**Definition 8.1.** If  $A$  is any set then the **permutation group** of  $A$ , denoted  $S_A$ , is the group of bijections  $\sigma : A \rightarrow A$  under composition. Subgroups of  $S_A$  are also called permutation groups (or groups of permutations to avoid confusion).

This is both a definition and a theorem. It states that the set of all bijections  $A \rightarrow A$  forms a group under composition. Why is that?

A special case:

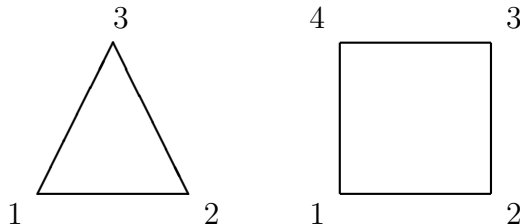
**Definition 8.2.** The permutation group of the set  $A = \{1, 2, \dots, n\}$  is called the **symmetric group** on  $n$  letters and is denoted  $S_n$ .

Problem: Show that  $S_n$  has order  $n!$ .

For example:  $|S_3| = 3! = 6$ .

### 8.2. dihedral groups.

**Definition 8.3.** The **dihedral group**  $D_n$  is the group of symmetries of the regular  $n$ -gon. These include  $n$  rotations and  $n$  reflections. So  $|D_n| = 2n$ .



If we represent these geometric symmetries as permutations then we see that  $D_n$  is isomorphic to a group of permutations of  $n$  letters. Composition of geometric movements corresponds to the second interpretation of permutation (the one we are using!) For example,

$$s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

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

This is given by doing the movement corresponding to  $s$  followed by the movement corresponding to  $t$ .

### 8.3. Cayley's theorem.

**Theorem 8.4** (Cayley). Every group is isomorphic to a group of permutations.

*Proof.* For any group  $G$  there is a mapping

$$\rho : G \rightarrow S_G$$

given by  $\rho(g) =$  left multiplication by  $g$ :

$$\rho(g)(h) = gh$$

I make the following claims:

- (1)  $\rho(g)$  is a permutation of  $G$ .
- (2)  $H = \{\rho(g) \mid g \in G\}$  is a subgroup of  $S_G$ .
- (3)  $\rho : G \rightarrow H$  is a bijection.
- (4)  $\rho$  satisfies the homomorphism property.

The first step is to understand that this list will complete the proof. (1) says that  $\rho$  is in fact a mapping from the set  $G$  to the set  $S_G$ . (2) says that  $H = \rho(G)$  is a subgroup of  $S_G$  and therefore  $\rho$  gives a surjective mapping

$$\rho : G \rightarrow H$$

The next two conditions say that this mapping is an isomorphism of groups.

Next we verify this one step at a time.

(1) To show that  $\rho(g)$  is a bijection, we just note that  $\rho(g^{-1})$  is the inverse of  $\rho(g)$ :

$$\rho(g^{-1})\rho(g)(h) = g^{-1}gh = eh = h$$

and similarly,  $\rho(g)\rho(g^{-1}) = id_G$ . This proves (1).

(4) Now let us go to (4). The homomorphism property is:

$$\rho(g)\rho(h) = \rho(gh)$$

This is obvious once we know what it says:

$$\rho(g)\rho(h)(k) = g(hk) = (gh)k = \rho(gh)(k)$$

(2) To show that  $H$  is a subgroup we need to show three things and we have already done two of them! The last one (the one that we should have done first is to show that it contains the identity of  $S_G$  which is the identity mapping  $\rho(e) = id_G$  since

$$\rho(e)(h) = eh = h.$$

We already know that  $H = \rho(G)$  has inverses:  $\rho(g)^{-1} = \rho(g^{-1}) \in H$  and is closed under composition since  $\rho(g)\rho(h) = \rho(gh)$ .

Finally, (3),  $\rho$  is a 1-1 by the cancellation property:

$$\rho(g) = \rho(h) \Rightarrow \rho(g)(x) = gx = hx = \rho(h)(x) \Rightarrow g = h$$

$\rho$  is onto by definition (since  $H$  is the image of  $\rho$ ). □

**8.4. example of Cayley's theorem.** The theorem is that every groups is isomorphic to a permutation group. The proof was that we have a monomorphism:

$$\rho : G \rightarrow S_G$$

called the regular representation which sends  $g \in G$  to  $\rho(g)$  which is multiplication on the left with  $g$ :

$$\rho(g)(h) = gh$$

Here is a simple example. Take  $G = \mathbb{Z}_3 = \{0, 1, 2\}$ . The binary operation is understood to be addition modulo 3. So, the regular representation is:

$$\rho(g)(h) = g +_3 h$$

So,  $\rho(0)$  is the identity mapping,  $\rho(1)$  adds 1:

$$\rho(1) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

and  $\rho(2) = \rho(1)^2$  adds 2:

$$\rho(2) = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$

Questions: Can you do the same for  $G = V$  and  $G = S_2$  using orbit notation (as explained in the next section)?