The symmetric group

The symmetric groups are some of the most useful and versatile groups. In some sense, which we will see later, every group can be thought of as a subgroup of a symmetric group. So the symmetric groups contain a lot of interesting structure.

Definition. The *symmetric group of degree n*, denoted S_n, is the group whose elements are the permutations on the set $\{1, \ldots, n\}$, and the binary operation is function composition $\circ$. Note that $|S_n| = n!$. p.29

There are different conventions for writing down permutations. We will use the *cycle decomposition* notation most of the time. First, notice that permutations consist of disjoint cycles of the form $a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_k \mapsto a_1$. We write these cycles, starting at their minimum element first. Then we order the cycles by their first element. Finally, we don't write down cycles of length 1 (fixed points), for simplicity of notation. You can find an explicit algorithm and examples on pages 30-31 of D&F.

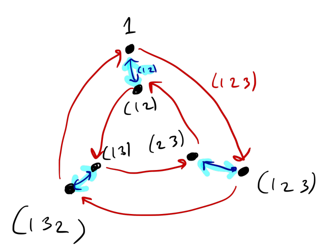
Example. The group S_3 has 3! elements:

$$\begin{aligned}&1\\&(1\ 2)\\&(1\ 3)\\&(2\ 3)\\&(1\ 2\ 3)\\&(1\ 3\ 2).\end{aligned}$$

We see that we can generate this group using elements (1 2) and (1 2 3), such that

$$\begin{aligned}&1\\&(1\ 2)\\&(1\ 3) = (1\ 2)(1\ 2\ 3)^2\\&(2\ 3) = (1\ 2)(1\ 2\ 3)\\&(1\ 2\ 3)\\&(1\ 3\ 2) = (1\ 2\ 3)^2.\end{aligned}$$

So, we can draw Cayley diagram:



Compare this to D_6!

Homomorphisms and isomorphisms

In class, we have seen some groups that seem to have a "similar structure", such as C_n and $\mathbb{Z}/n\mathbb{Z}$, as well as D_6 and S_3.

Definition. Let $(G, *)$ and $(H, \diamond)$ be two group. The map $\phi : G \to H$ is a *homomorphism* if p.36

$$\phi(a * b) = \phi(a) \diamond \phi(b), \text{ for all } a, b \in G.$$

A bijective homomorphism is called an *isomorphism*.

Some useful facts about isomorphisms are given in the following proposition. As an exercise, prove them.

Proposition. *If $\phi : G \to H$ is an isomorphism, then $|G| = |H|$, G is abelian if and only if H is abelian, and $|x| = |\phi(x)|$ for all $x \in G$.* p.38

It is possible for all three of these statements to be true about two groups G, H even though they are not isomorphic. They serve as quick ways to show that two groups are not isomorphic. Showing that two groups are isomoprhic, on the other hand, usually involves finding an explicit map. None of these hold for homomorphisms, but we do have one that is close to the last one. (Proof is left as an exercise.)

Proposition. *If $\phi : G \to H$ is a homomorphism, then $|x| = k$ implies that $|\phi(x)|$ divides k.*

Quaternion Group

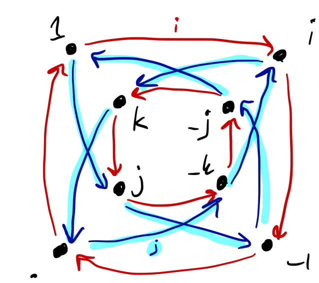
The quaternion group Q_8 is a non-abelian group on 8 elements with a structure that is slightly different from D_8. Q_8 has elements $\{1, -1, i, -i, j, -j, k, -k\}$, and it can be generated by any two of i, j, k. for example: p.36

$$Q_8 = \langle i, j \mid i^4 = 1,\ i^2 = j^2,\ j^{-1}ij = i^{-1} \rangle.$$

Deducing the full set of rules from this is not so easy. It will be more helpful to write out a larger set of them. Let $|-1| = 2$ and $(-1) \cdot a = a \cdot (-1) = -a$ for all $a \in Q_8$. Furthermore:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ i \cdot j = k,\ j \cdot i &= -k \\ j \cdot k = i,\ k \cdot j &= -i \\ k \cdot i = j,\ i \cdot k &= -j. \end{aligned}$$

This group has Cayley Diagram (when generated by i, j):



Group actions

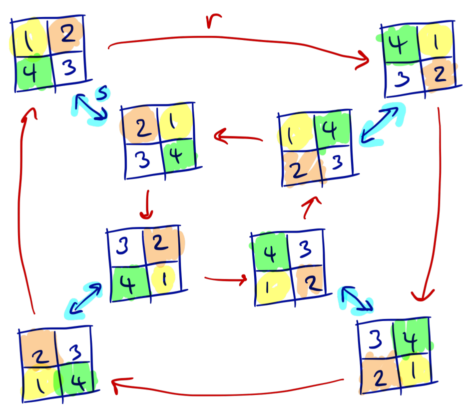
Often we think of groups in terms of actions on other objects. For example, the symmetric group shuffles a set, the cyclic and dihedral groups describe rigid motions of objects that possess symmetry. In this section we make this idea more precise, and we'll use group actions as a powerful tool that helps us use groups to uncover structure of other types of objects, as well as let groups act on themselves or other groups.

Definition. A *group action* of a group G on a set A is a map $\cdot : G \times A \to A$, satisfying the following properties: Sec. 1.7 p.41

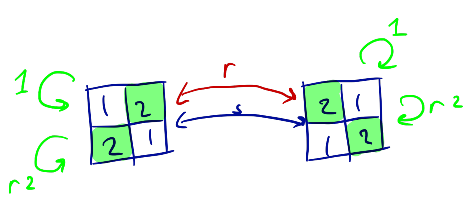
(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G$ and $a \in A$,

(2) $1 \cdot a = a$ for all $a \in A$.

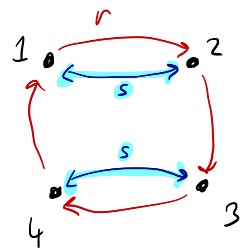
Example. We are already familiar with the dihedral group D_8 acting on a square via rotations and reflections. We can now let the set A be the set of all 8 states of the square, for example. We can depict this action in a diagram that is somewhat like a Cayley diagram. For example, if we only write arrows for a set of generators, all other actions can be derived (by item (1) in the definition of group actions). However, this diagram is not a Cayley diagram since the elements of the set are not the elements of the group.



Example. The previous example makes the diagram of the group action look a lot like the Cayley diagram of the group itself. This has to do with the fact that if we define a starting state, then each state of the square corresponds to exactly one element of the group that gets us there from the starting state. Instead, consider the states of a square with a checkerboard coloring (same on both sides). In this case, we only keep track of opposite pairs of corners but don't distinguish between the corners within an opposite pair. Now, we can depict the group action as follows. Not all elements of D_8 are depicted here (they can be deduced from the generators r, s), but we did draw r^2 to show that there are non-trivial elements that act trivially on the set in this case.



Example. Finally, we can also think of the group D_8 as simply acting on the set of corners of the square, which we can label 1,2,3,4 going clockwise around the square. Then the action can be depicted like this.



Exercises

Exercise 1. Prove that if σ is the m-cycle $(a_1\ a_2\ \dots\ a_m)$, then for all $1 \leq i \leq m$, $\sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least positive residue $\pmod{m}$. Deduce that $|\sigma| = m$. 1.3.10

Exercise 2. Find the orders of the elements of S_3, as well as a few of the elements of S_4 or S_5. Phrase a conjecture about the relationship between the cycle decomposition of a permutation and its order. 1.3.4

Exercise 3. Let $\phi : G \to H$ be a homomorphism. Prove that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}$. 1.6.1

Exercise 4. Show that if $\phi : G \to H$ is a homomorphism, then $|x| = k$ implies that $|\phi(x)|$ divides k. 1.6.2

Exercise 5. Show that D_{24} and S_4 are not isomorphic. 1.6.9

Exercise 6. Find a set of generators and relations for Q_8. 1.5.3