Lecture 17

Reference: Judson, Chapters 9.1 & 5.2

Cayley theorem

Proposition 1

Let $f: G \to H$ be a group homomorphism. Then f is *injective* if and only if *kernel* of f is trivial, i.e.:

$$\mathrm{Ker}(f) = \{e_G\}.$$

Proof. Recall that

$$\mathrm{Ker}(f) = \{x \in G \mid f(x) = e_H\}.$$

We need to prove the statement in two directions.
1. If f is injective, then $\mathrm{Ker}(f) = \{e_G\}$. Indeed, for any homomorphism $e_G \in \mathrm{Ker}(f)$, since $f(e_G) = e_H$. On the other hand, since f is injective, there is at most one element in G which is mapped to e_H, thus $\mathrm{Ker}(f)$ must consist of a single element.
2. If $\mathrm{Ker}(f) = \{e_G\}$, then f is injective.
Take any two elements $x, y \in G$ such that $f(x) = f(y)$. We are about to prove that $x = y$. Consider $xy^{-1} \in G$. For this element we have

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e_H,$$

where in the first equality we used the defining property of a homomorphism, in the second equality we used the statement that $f(y)^{-1} = f(y^{-1})$ and the last equality follows from the assumptions $f(x) = f(y)$.
Thus $xy^{-1} \in \mathrm{Ker}(f)$. Since $\mathrm{Ker}(f)$ consists only of e_G this implies $x = y$. □

The above proposition gives a very efficient way to check whether a given homomorphism is injective or not.

Remark 1

If $f: G \to H$ is an injective homomorphism, then G is isomorphic to a subgroup $\mathrm{Im}(G) \subset H$, where

$$\mathrm{Im}(g) = \{f(x) \mid x \in G\} \subset H.$$

Indeed, f establishes a bijection between G and $\mathrm{Im}(G)$ and respects the group operations.

Theorem 1: Cayley theorem

Let G be a finite group of size n. Then G is isomorphic to a subgroup of S_n.

Proof. We will construct an injective homomorphism from G to S_n:

$$f: G \to S_n$$

Label all elements of G by $\{a_1, a_2, \dots a_n\}$. We will assign a permutation $\sigma \in S_n$ to every element $x \in G$ as follows.
Consider a string of elements in G:

$$xa_1, \dots, xa_n.$$

By the left cancellation property (or 'Sudoku' rule) this string contains all every element in $\{a_1, \dots, a_n\}$ exactly once. In other words, there is a permutation σ such that each xa_i equals $a_{\sigma(i)}$. Thus we define $f(x) = \sigma \in S_n$.
1. f is a homomorphism. Assume that $f(x) = \sigma$ and $f(y) = \mu$. Then, to compute $f(xy)$ we analyze the effect of multiplying $\{a_1, \dots, a_n\}$ with xy:

$$xya_1, \dots, xya_n$$

by definition of $f(y) = \mu$ is the same as

$$xa_{\mu(1)}, \dots xa_{\mu(n)}$$

which in its turn by definition of $f(x) = \sigma$ is the same as

$$a_{\sigma(\mu(1))}, \dots, a_{\sigma(\mu(n))}$$

Thus $f(xy) = \sigma \circ \mu = f(x) \circ f(y)$, proving that f is a homomorphism.
2. To prove that f is injective, we just observe that if $x \in G$ is not identity, then

$$xa_1 \neq a_1$$

thus $f(x)$ can not be the identity permutation. Thus $\mathrm{Ker}(f) = \{e_G\}$, implying that f is injective. □

This theorem shows that permutation group is in some sense 'universal', and understanding well-enough permutation group S_n we can derive statements about groups of size n.

Example 1

Consider $G = \mathbb{Z}_4$ and label its elements as

$$a_1 = 0, a_2 = 1, a_3 = 2, a_4 = 3.$$

We will follow the construction in the above proof and provide an injective homomorphism $f : \mathbb{Z}_4 \to S_4$. The Cayley table for this group looks like

$+$	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_3	a_4	a_1
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_1	a_2	a_3

Thus we can read off the map f by considering rows of this table:

$$f(a_1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathrm{i}d$$

which is not surprising as $a_1 = 0$ is the neutral element. Proceeding in the same way, we find

$$f(a_2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad f(a_3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad f(a_4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

In other words, f sends $a_2 = 1$ to the cycles (1234), and sends all other elements to its corresponding powers.

Dihedral group D_n

Definition 1: Dihedral groups

The group of rigid motions of a regular polygon with n vertices P_n ($n \geqslant 3$) is called the n-th dihedral group D_n.

Example 2

For $n = 3$ we get the group of rigid motions of an equilateral triangle, which consists of 3 axial symmetries, 2 rotations by $\pm 120°$ and the identity. We know that

$$D_3 \simeq S_3.$$

Remark 2

Let us label vertices of the polygon as $\{1, 2, \ldots, n\}$. Then any rigid motion of the polygon induces a permutation of $\{1, 2, \ldots, n\}$, since every rigid motion permutes the vertices. Thus we can think of D_n as a subgroup of S_n.

Proposition 2: Counting rigid motions

$|D_n| = 2n$.

Proof. To count the number of elements in D_n, we first observe that every rigid motion f of the polygon is completely determined by the images of two adjacent vertices 1 and 2.
For vertex 1 we have exactly n options for where to map it — any of the n vertices of the polygon. If we fix

$$f(1) = k$$

then for vertex 2 we have exactly two options to define $f(2)$:

$$f(2) = k - 1 \quad \text{or} \quad f(2) = k + 1.$$

Overall this gives $n \times 2$ options, and we have $|D_n| = 2n$. □

Proposition 3

Let $r \in D_n$ be a rotation by $2\pi/n$ clockwise, and denote by $s \in D_n$ the reflection in the axis going through vertex 1 and the center of the polygon. Then

$$D_n = \{r^0, r^1, \ldots, r^{n-1}, sr^0, sr^1, \ldots, sr^{n-1}\}.$$