SEPTEMBER 7 NOTES

1. 1.2: Dihedral groups

Last time, we introduced the dihedral group of symmetries to the regular n-gon. If we denote by s the symmetry flipping the shape over through the axis of symmetry through vertex 1, and then denote by r the rotation clockwise by $2\pi/n$ radians, we showed that the dihedral group has $2n$ elements, given by:

$1, r, r^2, \ldots, r^{n-1}$ (the n rotations, including $1 =$ doing nothing), $s, sr, sr^2, \ldots, sr^{n-1}$ (the symmetries by first flipping the shape over and then rotating).

You should convince yourself of the following properties:

(1) $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$
(2) $|s| = 2$
(3) $s \neq r^i$ for any i, and further $sr^i \neq sr^j$ for $i \neq j$ with $0 \leq i, j \leq n-1$
(4) $rs = sr^{-1} = sr^{n-1}$
(5) $r^i s = sr^{n-i}$ for all $0 \leq i \leq n$

By (3), we may write each element of the dihedral group uniquely as $s^k r^i$ for $k \in \{0, 1\}$ and $i \in \{0, \ldots, n\}$:

$$D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$$

and by (4) and (5) we can determine the product of any two elements in D_{2n}.

In general, writing all of the elements of G in terms of powers of a fixed subset (in this case, r and s) is a way to present G in terms of *generators and relations*. We will come back to this in the future but introduce it here.

Definition 1.1. A subset S of a group G such that every element of G can be written as a finite product of elements in S and their inverses is called a set of **generators** for G. We will say that S **generates** G and write $G = \langle S \rangle$.

Any equations in G that the elements in S satisfy are called **relations**.

If G is generated by a subset S and there is a collection of relations $R_1, \ldots, R_m$ (where each R_i is an equation involving only elements of S and the identity element) such that any other relation in S can be deduced from these, we write

$$G = \langle S \mid R_1, \ldots, R_m \rangle$$

and call this a **presentation** of G.

Example 1.2. The set $S = \{1\}$ generates $\mathbb{Z}$, and there are no relations in S, so a presentation of $\mathbb{Z}$ is just $\mathbb{Z} = \langle 1 \rangle$.

Example 1.3. The set $S = \{r, s\}$ generates D_{2n}, and every relation can be derived from the relations $r^n = 1, s^2 = 1, rs = sr^{-1}$ (exercise!) so a presentation for the dihedral group is

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

2. 1.3: The symmetric group

In this section, we will define the symmetric group. This is a *permutation* group, i.e. a collection of all 'rearrangements' of a given set. Usually, we take our set to be $\{1, 2, \ldots, n\}$, but we can define a group of permutations on any set.

Definition 2.1. Let Ω be a non-empty set. A **permutation** σ of Ω is a bijection from Ω to itself, i.e. $\sigma : \Omega \to \Omega$ that is both injective and surjective. If $a \in \Omega$, we think of σ as a permutation by sending a to $\sigma(a)$.

Definition 2.2. Let Ω be any non-empty set, and let S_Ω be the set of all bijections from Ω to itself. This is a group with binary operation function composition $\circ$:

- Composition is associative;
- There is an identity function $1 : \Omega \to \Omega$ given by $1(a) = a$ for all $a \in \Omega$;
- For any function $\sigma \in S_\Omega$, σ is bijective, so has a bijective inverse function $\sigma^{-1} \in S_\Omega$ such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$.

This group S_Ω is called **the symmetric group on the set** Ω.

If $\Omega = \{1, 2, \ldots, n\}$, then we denote S_Ω by S_n.

We start with a basic fact.

Proposition 2.3. $|S_n| = n!$.

Proof. The elements of S_n are bijective functions (i.e. exact matchings) of the set $\{1, 2, \ldots, n\}$ with itself. To determine such a bijection σ, we need to know $\sigma(1), \sigma(2), \ldots, \sigma(n)$. Because $\sigma(1)$ can be any element in $\{1, 2, \ldots, n\}$, we have n choices for $\sigma(1)$, and then $\sigma(2)$ can be any element other than $\sigma(1)$, so we have $n-1$ choices for $\sigma(2)$, and then $\sigma(3)$ can be anything other than $\sigma(1)$ or $\sigma(2)$ so we have $n-2$ choices....continue this logic and we conclude we have $n(n-1)(n-2)\ldots 2 \cdot 1 = n!$ choices for σ. □

How do we denote elements of S_n? One method is called *two-line notation*, where we write the elements of $\{1, \ldots, n\}$ and below each element i write $\sigma(i)$, i.e. the permutation in S_3 of $\{1, 2, 3\}$ that switches 1 and 2 and keeps 3 where it is would be written as:

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

We can write all elements of S_3 this way:

$$S_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

This is quite cumbersome, so Dummit and Foote use what is known as *cycle notation*. Here, we imagine what the permutation does to each element moving things in a collection of cycles. In the example above, we know $1 \mapsto 2$, and then $2 \mapsto 1$, so we have a cycle $1 \mapsto 2 \mapsto 1$. Because 3 doesn't move, it is in its own cycle. We denote each cycle as strings of numbers in parentheses: (12)(3) where a closed parenthesis means the cycle goes back to the first element.

We can formalize this process into an algorithm:

(1) Given a permutation, to start a new cycle, pick the smallest element a of $\{1, 2, \ldots, n\}$ that has not yet appeared in a cycle. Begin a new cycle with a: $(a$
(2) Find $b = \sigma(a)$. If $b = a$, close the cycle with a right parenthesis and go back to step 1. If $b \neq a$, continue the cycle: $(ab$
(3) Find $c = \sigma(b)$. If $c = a$, close the cycle and return to step 1. If $c \neq 1$, write c next to b: $(abc$. Repeat until the cycle closes.

Example 2.4. Write the permutation

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

in cycle notation.

Let's start with 1: we see $1 \mapsto 4$, and then $4 \mapsto 1$, so we have our first cycle (14). Then, we see $2 \mapsto 3$, $3 \mapsto 5$, $5 \mapsto 7$, and $7 \mapsto 2$, so we have our next cycle (2357). Then, we see $6 \mapsto 6$, so we obtain the cycle decomposition (14)(2357)(6).

By convention, we usually do not write the cycles of length 1, so we actually would write the previous permutation as (14)(2357). In general, any numbers that do not appear in the cycle notation are assumed to be fixed by σ. The algorithm will have you write cycles in a prescribed order, but these disjoint cycles (cycles with no elements in common) *commute* (because the permutation is moving elements in disjoint sets). Therefore, you can rearrange the order you write them as desired.

Example 2.5. The elements of S_3 in cycle notation (in the same order as above) are:

$$1, (23), (12), (123), (132), (13).$$

We compute the composition of elements in S_n using the cycle notation by working our way from the right-most cycle to the left-most cycle. For example:

$$(12)(13) = (132)$$

because the right cycle says $1 \mapsto 3$, and the left cycle doesn't move 3, so we know the composition sends $1 \mapsto 3$; then, $3 \mapsto 1$ in the first cycle and $1 \mapsto 2$ in the second, so $3 \mapsto 2$ in the composition; finally, 2 is fixed by the right cycle and $2 \mapsto 1$ by the left, so we know $2 \mapsto 1$.

Similarly,

$$(13)(12) = (123).$$

This shows that $(12)(13) \neq (13)(12)$, and by considering these as permutations in S_n for any $n \geq 3$, we have proven the following:

Proposition 2.6. *For $n \geq 3$, S_n is not abelian.*

On your homework, you will practice more with S_n: composing elements, computing orders of elements, etc.

3. 1.4: Matrix Groups

To define matrices in general, we first need to define fields.

Definition 3.1. A **field** is a set F together with two binary operations $+$ and $\times$ such that:

(1) $(F, +)$ is an abelian group with identity $0 \in F$;
(2) denoting by $F^\times = F - \{0\}$, $(F^\times, \times)$ is an abelian group;
(3) $+$ and $\times$ satisfy the distributive law: for any $a, b, c \in F$,

$$a \times (b + c) = (a \times b) + (a \times c).$$

For now, the only fields that we will encounter are: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{F}_p$, where $\mathbb{F}_p = \mathbb{Z}_p$ for p a prime number and $+ = + \pmod p$ and $\times = \times \pmod p$. (You can go ahead and prove $\mathbb{F}_p$ is a field on your own, or reference Section 0 of Dummit and Foote.)

Everything you learned about matrices in linear algebra can be done over arbitrary fields, not just $\mathbb{R}$. Given an $n \times n$ matrix A with entries in F, we compute the determinant by the same formula as you would over $\mathbb{R}$, using the appropriate + and × from the field F. Because $F^\times$ is a group, there is an identity element 1, and the identity matrix is still the matrix with 1's along the diagonal and 0's elsewhere.

Furthermore, it is still true that A is invertible (meaning, there exists an $n \times n$ matrix A^{-1} with $AA^{-1} = A^{-1}A = I$) if and only if $\det A \neq 0$.

Thus, we define the matrix group:

Definition 3.2. If F is a field, the **general linear group** $\mathrm{GL}_n(F)$ is the set of all $n \times n$ invertible matrices with entries in F. It is a group with binary operation multiplication.

It is a *fun* exercise to compute the number of elements of $GL_2(\mathbb{F}_p)$!

On your homework, you will prove that if $n \geq 2$, then $GL_n(F)$ is never abelian.

4. 1.5: The Quaternion Group

Imagine the four complex numbers $\{1, -1, i, -i\}$. These form a group under multiplication because the product of any two elements in this set is still in the set, multiplication is associative, 1 is in this set, and the multiplicative inverse of any element is in this set.

The quaternion group is a (non-abelian) generalization of this!

Definition 4.1. Let $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ be the group with multiplication defined by:

$$1 \cdot a = a \cdot 1 = a \quad \text{for all } a \in Q_8 \text{ (so 1 will be the identity)}$$
$$(-1) \cdot (-1) = 1, \quad (-1) \cdot a = a \cdot (-1) = -a \quad \text{for all } a \in Q_8$$
$$i^2 = j^2 = k^2 = 1$$
$$ij = k, \quad ji = -k, \quad jk = i, \quad kj = -i, \quad ki = j, \quad ik = -j$$[1]

Note that we did not verify that this multiplication is associative. It is indeed true, but painful to verify, so we will do it in the future in a better way. Some facts that you should be able to verify now:

Proposition 4.2. *(1) 1 is the identity element*
(2) Q_8 is not abelian
(3) $\pm i, j, k$ all have order 4
(4) The inverse of i, j, k is $-i, -j, -k$.

[1] This is just the 'right hand rule' for vector cross products, if you'd like to remember it this way.