Lecture 7

Reference: Judson, Chapter 3.3 & 4.1

Groups

Last time we have introduced a notion of a *group* $(G,*)$. In a certain sense which we make precise later in the course, the following example is an ultimate source of all groups.

Example 1

Let X be an arbitrary set. Consider
$$\mathcal{B}(X,X) \subset \mathcal{F}(X,X)$$
the set of all **bijections** from X to itself X.
Since the composition of bijections is a bijection, we have a set with a composition law:
$$(\mathcal{B}(X,X),\circ).$$

- This composition law is trivially associative, since the composition of functions is always associative
- $\mathcal{B}(X,X)$ also admits a neutral element with respect to $\circ$ — the identity map $\mathrm{id}_X \in \mathcal{B}(X,X)$.

Now, the point of considering only bijections among all maps $X \to X$, is that a bijection $f\colon X \to X$ always admits an inverse $f^{-1}\colon X \to X$ which makes $(\mathcal{B}(X,X),\circ)$ a group. Some of you might have seen this group under the disguise of *permutation group* of X.

Remark 1

The group of bijections is **not** commutative, unless the set X consists of $\leqslant 2$ elements.

Cayley tables

If G is finite set consisting of $|G|$ elements, and we want to specify a composition law on G, the most straightforward way is to use a *Cayley table*. This is a table of size $|G|\times|G|$, with rows and columns labeled by elements of G.

To fill out Cayley table, in the cell at the intersection of a row of element $x \in G$ and of a column of element $y \in G$ we record their composition $x*y$.

$$\begin{array}{c||ccc}
* & \dots & y & \dots \\
\hline\hline
\vdots & & \vdots & \\
x & \dots & x*y & \dots \\
\vdots & & \vdots &
\end{array}$$

Given a Cayley table of $(G,*)$ we can read off all the possible compositions of all the pairs of elements of G.

Problem 1: If $(G,*)$ is a group, then every column (resp. row) of its Cayley table contains every element exactly once.

Example 2

Let $X = \{A, B, C\}$ and consider the set of bijections $\mathcal{B}(X, X)$. Any bijection would permute elements A, B, C. To define a bijection we have to specify the image of A (3 choices), the image of B (only 2 choice left), and the image of C will be determined uniquely. Therefore we will have exactly $3 \times 2 = 6$ bijections. If $f : \{A, B, C\} \to \{A, B, C\}$ is a bijection, we will represent it as a 2×3 matrix:

$$f = \begin{pmatrix} A & B & C \\ f(A) & f(B) & f(C) \end{pmatrix}$$

We have the following 6 bijections:

$$\mathrm{id}_X = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$\tau_1 := \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \tau_2 := \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \tau_3 := \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

$$\mu_1 := \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \mu_2 := \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

So $G = \mathcal{B}(X, X)$ is

$$G = \{\mathrm{id}_X, \tau_1, \tau_2, \tau_3, \mu_1, \mu_2\}$$

To finish description of the group $(G, \circ)$ it remain to construct the (multiplication) Cayley table.

Since each of τ_1, τ_2, τ_3 just swaps two elements, we find that $\tau_i \circ \tau_i = \mathrm{id}_X$.

Also, it is easy to see that $\mu_1^2 = \mu_2$ and $\mu_1^3 = \mathrm{id}_X$. The latter implies that

$$\mu_2^{-1} = \mu_1$$

Therefore $\mu_2 = \mu_1^{-1}$, and since $(\mu_1^{-1})^3 = \mathrm{id}_X$, we see that

$$\mu_2^3 = \mathrm{id}_X$$

To see that group $(G, \circ)$ is not commutative, we consider

$$\tau_1 \circ \tau_2 \text{ and } \tau_2 \circ \tau_1.$$

Let us find out how map $\tau_1 \circ \tau_2 : X \to X$ acts on A, B, C:

$$(\tau_1 \circ \tau_2)(A) = \tau_1(\tau_2(A)) = \tau_1(C) = B$$

$$(\tau_1 \circ \tau_2)(B) = \tau_1(\tau_2(B)) = \tau_1(B) = C$$

$$(\tau_1 \circ \tau_2)(C) = \tau_1(\tau_2(C)) = \tau_1(A) = A$$

So we see that $\tau_1 \circ \tau_2 = \mu_1$.

Problem 2: Check hat $\tau_2 \circ \tau_1 = \mu_2 (\neq \mu_1)$. This is a manifestation of the fact that $(G, \circ)$ is not commutative.

So far we have essentially computed the following entries of the Cayley table (see below)

(The first row and column just reflect the fact that id_X is a neutral element)

$\circ$	id_X	τ_1	τ_2	τ_3	μ_1	μ_2
id_X	id_X	τ_1	τ_2	τ_3	μ_1	μ_2
τ_1	τ_1	id_X	μ_1			
τ_2	τ_2	μ_2	id_X			
τ_3	τ_3			id_X		
μ_1	μ_1				μ_2	id_X
μ_2	μ_2				id_X	μ_1

Part of the Cayley table of $\mathcal{B}(X, X)$, $X = \{A, B, C\}$

Remark 2

From the known compositions, we can formally find, for example, $\mu_2 \circ \tau_1$:

$$\tau_2 \circ \tau_1 = \mu_2 \Rightarrow \tau_2 \circ \tau_1 \circ \tau_1 = \mu_2 \circ \tau_1 \Rightarrow \tau_2 = \mu_2 \circ \tau_1.$$

Problem 3: Fill in the remaining entries of the table. Check that the product of two τ's is either identity of μ, and the product of a τ and a μ is always a μ.

Subgroups

Let $(G,*)$ be a group. Often we would like to understand G by considering subsets which themselves are groups with respect to $*$. To this end we need the following definition.

Definition 1: S

bset $H \subset G$ is called a *subgroup* if it satisfies the following properties:

- $e \in H$;
- if $x, y \in H$, then $x * y \in H$;
- if $x \in H$, then $x^{-1} \in H$.

Clearly $(H,*)$ is itself a group.

Problem 4: Prove that a subset $H \subset G$ satisfying

- if $x, y \in H$, then $(x^{-1}) * y \in H$,

is a subgroup.

Example 3: Obvious subgroups

Any group $(G,*)$ has two obvious subgroups:

1. $H = \{e\}$ (trivial subgroup)
2. $H = G$.

If subgroup H is neither of the above, we will say that $H \subset G$ is a *proper* subgroup.

Example 4

Group $(\mathbb{Z}_3,+)$ does not have any subgroups besides $\{0\}$ and $\mathbb{Z}_3$.
Indeed, we have $\mathbb{Z}_3 = \{[0],[1],[2]\}$. If $H \in \mathbb{Z}_3$ is a nontrivial subgroup, then either $[1] \in H$ or $[2] \in H$. If $[1] \in H$, then by the second property $-[1] = [2] \in H$ and $H = \mathbb{Z}_3$.

Remark 3

If $H \subset G$ is a subgroup, and $h \in H$ is an element in H, then for any integer $m \in H$ we also have $h^m \in H$.

Example 5

Let $(\mathbb{Z}_7^\times, \times)$ be the set of units (i.e., elements admitting multiplicative inverse) in $\mathbb{Z}_7$ under multiplication operation. In this group we have a subgroup

$$H = \{[1], [6]\}.$$

Indeed, since $[6] \times [6] = [36] = [1]$, this subset satisfies all the properties of a subgroup.
There is another proper subgroup in $(\mathbb{Z}_7^\times, \times)$:

$$K = \{[1], [2], [4]\}.$$

Problem 5: Prove that subset $K \subset \mathbb{Z}_7^\times$ satisfies all the properties of a subgroup.

Example 6

Consider group $(\mathbb{Z}, +)$. Then for any fixed nonzero $m \in \mathbb{Z}$ there is a subgroup of elements divisible by m

$$m\mathbb{Z} := \{k \cdot m \mid k \in \mathbb{Z}\} \subset \mathbb{Z}.$$

It turns out that the above example provides an exhaustive list of subgroups of $(\mathbb{Z}, +)$. Specifically, we have the following theorem:

Theorem 1

Let $H \subset \mathbb{Z}$ be a subgroup with respect to addition. Then either H is trivial:

$$H = \{0\}$$

or H is of the form

$$H = m\mathbb{Z}$$

for some fixed nonzero $m \in \mathbb{Z}$.

Proof. Assume that H is nontrivial. Then we have some nonzero integer $a \in H$. By subgroup property, we also have $-a \in H$, hence there is at least one positive integer in H.
Let m be the smallest positive integer in H. We claim that $H = m\mathbb{Z}$.
1. $m\mathbb{Z} \subset H$**:** Since $m \in H$, by subgroup properties, we have $-m \in H$, $2m = m + m \in H$, and, more generally, for any $k \in \mathbb{Z}$ we have $k \cdot m \in H$. This proves $m\mathbb{Z} \subset H$.
2. $H \subset m\mathbb{Z}$. Let us take any element $a \in H$. We claim that a is divisible by m without remainder.
Indeed, let us divide a by m with remainder:

$$a = m \cdot q + r, \quad r \in \{0, 1, \dots, m-1\}.$$

Since $a \in H$ and $m \in H$, by subgroup properties we have

$$a - k \cdot m \in H$$

for any $k \in \mathbb{Z}$. In particular taking $k = q$ we conclude that

$$r \in H.$$

But m is the smallest positive element of H, therefore r must be 0. □