Lecture 2 – Axioms

A set G along with a binary operation $*: G \times G \to G$ is called a group if

i) For all $u, v, w \in G$ the associativity property holds i.e.

$$u*(v*w) = (u*v)*w \quad \text{for all } u, v, w \in G$$

ii) $\exists$ an element e called the identity s.t. $u*e = e*u = u$ for all $u \in G$

iii) For all $u \in G$ $\exists$ an element u^{-1} (called inverse of u) such that

$$u*u^{-1} = u^{-1}*u = e$$

Examples of groups:

1. $(\mathbb{Z},+)$ – Integers under addition

   $(\mathbb{R},+)$ – Real numbers under addition

   $(\mathbb{C},+)$ – Complex numbers under addition

   $(\mathbb{R}^n,+), (\mathbb{C}^n,+)$ – are groups under component wise addition.

2. $M_n(\mathbb{C}), M_n(\mathbb{R})$ – $n\times n$ matrices with entries in the real numbers or complex numbers under usual matrix addition

3. $GL_n(\mathbb{R}), GL_n(\mathbb{C})$ – The set of invertible ($\det \neq 0$) matrices under matrix multiplication.

4. S_n – The set of permutations on n-letters under function composition

For eg. consider S_4

$e \equiv \begin{array}{c} 1\to 1 \\ 2\to 2 \\ 3\to 3 \\ 4\to 4 \end{array}$ is the identity permutation, $u \equiv \begin{array}{c} 1\to 2 \\ 2\to 3 \\ 3\to 4 \\ 4\to 1 \end{array}$ is $(1\,2\,3\,4)$ in cycle notation

$v \equiv \begin{array}{c} 1\to 2 \\ 2\to 1 \\ 3\to 4 \\ 4\to 3 \end{array}$ is $(1\,2)(3\,4)$

$u*v$ is also a permutation. In this notation permutation

v is applied first followed by u. Therefore

$u * v = (1234)\circ(12)(34)$. To compute and write the answer in cycle notation $1 \to 2$ in v and $2 \to 3$ in u so in the resultant permutation $1 \to 3$. Computing in this manner $2 \to 1$ in v and $1 \to 2$, so $2 \to 2$ in $u * v$. Next $3 \to 4$ in v and $4 \to 1$ in u so $3 \to 1$. And finally $4 \to 3$ in v and $3 \to 4$ in u so $4 \to 4$. Therefore the final permutation $w \equiv \begin{array}{l} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \\ 4 \to 4 \end{array}$ which in cycle notation is (13)

5. The group of rotational symmetries of a regular tetrahedron as was studied in the previous lecture

6. Let $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$. Let us define an operation $+_n$ on $\mathbb{Z}_n$

$$x +_n y = \begin{cases} x+y & \text{if } x+y < n \\ x+y-n & \text{if } x+y \geq n \end{cases}$$

Verify that this is a group! What is inverse of x

7. Is $(\mathbb{R}, \times)$, the set of real numbers a group under multiplication?
No! $x * 0 = 0$. So 0 does not have an inverse! But if we exclude 0 then everything looks ok! So $\mathbb{R} - \{0\}$ is a group under multiplication

8. $\{z : z^n = 1\}$, the n^{th} roots of unity. Check that this is a group under multiplication.

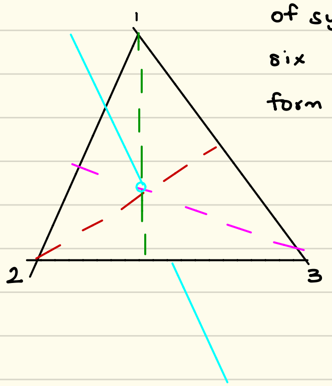
9. Consider $\mathbb{Z}_n^* = \mathbb{Z}_n - \{0\} = \{1, 2, \dots, n-1\}$ and operation $x *_n y = (xy) \bmod n$. Is this a group?

Consider $\mathbb{Z}_6^* = \{1, 2, 3, 4, 5\}$

$2 *_n 3 = (2 * 3) \bmod 6 = 0$, which does not belong to $\mathbb{Z}_n^*$. So $*_n$ is not

does not have closure property, so $\mathbb{Z}_6^*$ is not a group. What about $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$. You can verify that this indeed is a group.
Do you see any pattern?
In the future we will see that $\mathbb{Z}_p^*$ is a group. In a previous example we saw that by removing the element 0 we were able to form a group $\mathbb{R}-\{0\}$ under multiplication. Can something be done about $\mathbb{Z}_n^*$?

10. Finally consider the group of symmetries of a regular polygon D_n



Shown in the figure are the various axis of symmetry for a triangle. There are six symmetries of a triangle and they form a group under composition.