

# MAT347 Lecture Notes

ARKY!! :3C

'25 Fall & '26 Winter Semester

## Contents

1	Day 1: Rubik's Cube (Sept. 3, 2025)	2
---	-------------------------------------	---

## §1 Day 1: Rubik's Cube (Sept. 3, 2025)

The first semester of this class will be taught by Dror Bar-Natan instead of Joe Repka. Since this was a last minute change, the Quercus, tutorials, textbook, homework policy, etc. are all unknown for now (until the rest of the week probably).

This will be today's **handout**. Let  $G = \langle g_1, \dots, g_\alpha \rangle$ , i.e., the group generated by  $g_1, \dots, g_\alpha$ , be a subgroup of  $S_n$ , with  $n = O(100)$ . To understand  $G$ , let us start by computing  $|G|$ . *insert long digression about Rubik's cubes that can be read elsewhere.*

**Definition 1.1.** A *group* is a set  $G$  along with a binary multiplication  $m : G \times G \rightarrow G$  usually written as  $(g_1, g_2) \mapsto g_1 \cdot g_2 = m(g_1, g_2)$  such that

- (i)  $m$  is associative, i.e., for all  $g_1, g_2, g_3 \in G$ , we have that  $(g_1 g_2) g_3 = g_1 (g_2 g_3)$ ,
- (ii)  $m$  has an identity, i.e., there exists some  $e \in G$  such that  $g \cdot e = e \cdot g = g$  for all  $g \in G$ ,
- (iii)  $m$  has an inverse, i.e., for all  $g \in G$ , there exists some  $h \in G$  such that  $g \cdot h = e = h \cdot g$ ,

We present a few examples of groups for intuition.

- (a)  $(\mathbb{Z}, m = +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ ,  $(F, +)$  are naturally all groups. We also have that  $(2\mathbb{Z}, +)$  is a group, even though it is not a field, because it does not admit inverses.
- (b)  $(\mathbb{Q} \setminus \{0\}, \times)$  has identity given by 1 and naturally admits inverses because all reciprocals are contained within  $\mathbb{Q} \setminus \{0\}$  itself. We commonly write the rationals without zero as  $\mathbb{Q}^\times$ .
- (c) If  $n \in \mathbb{Z}_{\geq 0}$ , then let  $S_n := \{\sigma : \underline{n} \rightarrow \underline{n} \mid \sigma \text{ is bijective}\}$ , where we define  $\underline{n} = \{1, \dots, n\}$ .<sup>1</sup> Let the group operation on  $S_n$  be given by composition. Here, Dror goes into a big digression on how composition should be written, and he suggests the following,<sup>2</sup>

$$\sigma \cdot \mu = \mu \circ \sigma = \sigma // \mu.$$

Indeed,  $S_n$  is a group, where its identity element  $e$  is given by the identity function on  $\underline{n}$ . We have that  $|S_n| = n!$ .

As a substantive example, consider  $S_2 = \{[1, 2], [2, 1]\}$ , where  $[1, 2]$  represents the identity function and  $[2, 1]$  represents the function mapping 1 to 2 and 2 to 1. Then we obtain the following possible compositions,

$$\begin{aligned} [1, 2][1, 2] &= [1, 2], \\ [1, 2][2, 1] &= [2, 1], \\ [2, 1][1, 2] &= [2, 1], \\ [2, 1][2, 1] &= [1, 2]. \end{aligned}$$

As for  $S_3$ , we have that  $S_3$  contains 6 functions, comprised of all the possible permutations possible on  $\{1, 2, 3\}$ . One such composition is given as follows,

$$[1, 3, 2][2, 1, 3] = [2, 3, 1], \quad [2, 1, 3][1, 3, 2] = [3, 1, 2],$$

<sup>1</sup>angry yapping incoming i am so used to seeing  $[n]$  when i saw that on the board i was like, watefak!!!

<sup>2</sup>also, plus one angry footnote for using  $//$  as a composition symbol

which confirms that  $S_3$  is indeed not abelian (i.e., non-commutative).

In the opposite direction,  $S_1$  consists of an identity function only; clearly,  $|S_1| = 1! = 1$ .  $S_0$  is the set of all permutations on  $\emptyset$ , which is clearly the empty set, meaning the “empty function” on the empty set is the only function in  $S_0$ ; similarly,  $|S_0| = 0! = 1$ .

(d) There are 24 rotational symmetries of a cube.

(e) The orthogonal transformations  $o(3) = \{A \in M_{3 \times 3}(\mathbb{R}) \mid A \cdot A^\top = I\}$  form a group.

**Theorem 1.2.** The identity element of a group is unique. If  $G$  is a group and  $e, e'$  are both identity elements, then for all  $g \in G$ , we have that  $eg = ge = g$  and  $e'g = ge' = g$ , and  $e = e'$ .

*Proof.* Observe that  $e' = e' \cdot e = e$ . □

**Theorem 1.3.** The inverse of an element in a group is unique. Let  $G$  be a group and  $g \in G$ ; if  $h, h'$  satisfy  $gh = hg = e = gh' = h'g$ , then  $h = h'$ .

*Proof.* Observe that  $h' = h' \cdot e = h'(gh) = (h'g)h = eh = h$ . □

From here on, the inverse of  $g$  will be denoted  $g^{-1}$ , i.e.,  $g^{-1}$  is the unique inverse of  $g$ .

**Theorem 1.4.** If  $ac = bc$  in a group then  $a = b$ .

*Proof.* Given that  $ac = bc$ , we have  $acc^{-1} = bcc^{-1}$ , implying  $a = b$ . □

**Theorem 1.5.**  $(ab)^{-1} = a^{-1}b^{-1}$ .

*Proof.* Observe that  $(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$ . □

**Definition 1.6.** A subset  $H \subset G$  of a group  $G$  is called a subgroup if  $H$  is closed under multiplication,  $e \in H$ , and admits inverses (i.e.,  $H$  is a group itself with the multiplication operation from  $G$ ). We write  $H < G$ .

As an example,  $(2\mathbb{Z}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ . The Rubik's cube group is also a subgroup of  $S_{54}$ .