MAT347 Lecture Notes

Arky!! :3c

'25 Fall & '26 Winter Semester

Contents

§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 $G = \langle g_1, \ldots, g_\alpha \rangle$, i.e., the group generated by $g_1, \ldots, g_\alpha$, 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 $m : G \times G \to G$ 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 $S_n := \{\sigma : \underline{n} \to \underline{n} \mid \sigma \text{ is bijective}\}$, where we define $\underline{n} = \{1, \ldots, n\}$.[1] 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,[2]

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

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,

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

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

[2] 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 $\underline{0}$, 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}.

§2 Day 2: More Non-commutative Gaussian Elimination (Sep. 5, 2025)

The syllabus is not yet public, but you should check this link next Wednesday for more information. Our TAs are Jacob and Matt. The course code for this class is "MAT347", and it carries the iconic '7', meaning this class will be "hard as shit".

The permutation product is the usual composition $\sigma \cdot \tau = \sigma \circ \tau$.[3] Today's goal is to understand $G = \langle g_1, \dots, g_\alpha \rangle \in S_n$, where we wish to answer the questions: (i) what size is $|G|$? (ii) what does it mean to say $\sigma \in G$? (iii) if $\sigma \in G$, how do we write it in terms of the g_i's? (iv) what does a random $\sigma \in G$ look like?

Let us construct a lower-triangular table of size $n \times n$, where each box (i, j) describes an operation on how to move the ith sticker to the jth sticker. In particular, we have that if $i = j$, the operation is simply the identity. We start with an empty such table, and we will proceed to fill it in with permutations. For any $\sigma \in S_n$, we have that σ can be represented as a permutation of the form $[1, 2, \dots, i-1, j, *, \dots, *]$, i.e., σ fixes the first $i-1$ entries, and the ith entry contains j. We label such a permutation as $\sigma_{i,j} \in S_n$, and we call i the *pivot*.

We proceed to "feed $g_1, \dots, g_\alpha$" in order; to feed a non-identity σ, let the pivotal position be i and let j be given by $\sigma(i)$. If the box (i, j) is empty, let us place σ there; otherwise, if it already contains some $\sigma_{i,j}$, let us place $\sigma' := \sigma_{i,j}^{-1}\sigma$ in there instead. Notice that this makes it so that σ' is indeed the identity for the first i entries, instead of the first $i-1$ entries, meaning we have fixed an additional sticker. After this step, for each pair of occupied boxes (i, j) and (k, l), let us feed $\sigma_{i,j}\sigma_{k,l}$ and perform the steps above again, until the table no longer changes for any such pair of $(i, j), (k, l)$.

Claim 2.1. This process stops in $O(n^6)$ time; call the resulting table T.

We obtain n^6 from observing that there is approximately n operations per permutation, and hence n per inverse permutation; since computing $\sigma' = \sigma_{i,j}^{-1}\sigma$ potentially requires n inverses, we note that each feeding operation takes at worst n^2 operations. For the (i, j), (k, l) pairs, the table is of $O(n^2)$ size, meaning there are a total of $O(n^4)$ possible foods. Combining these figures we have $O(n^6)$, which is much less than $O(n!)$.

Claim 2.2. Every $\sigma_{i,j} \in T$ is indeed in G.

[3] so we're going to be changing the notation conventions every lecture from now on.