# 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 $G = \langle g_1, \dots, g_\alpha \rangle$, 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 $m : G \times G \to G$ 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 $\underline{n} = \{1, \dots, n\}$.[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.** $(ab)^{-1} = b^{-1}a^{-1}$.

*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 $i$th sticker to the $j$th 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 $\sigma$ can be represented as a permutation of the form $[1, 2, \dots, i-1, j, *, \dots, *]$, i.e., $\sigma$ fixes the first $i-1$ entries, and the $i$th 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 $\sigma$, let the pivotal position be $i$ and let $j$ be given by $\sigma(i)$. If the box $(i, j)$ is empty, let us place $\sigma$ 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 $\sigma'$ 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.

# §3 Day 3: NCGE, Pt. 3 (Sep. 10, 2025)

Before we return to the discussion on the Rubik's cube, we have another property of inverses to discuss;

**Theorem 3.1.** Let $a \in G$. Then $(a^{-1})^{-1} = a$.

*Proof.* $(a^{-1})^{-1} = (a^{-1})^{-1} \cdot (a^{-1} \cdot a) = a$. □

The point of the twist is that we want to fill every box of our table that can be filled by the group; assuming that the twist hits everything, we would be able to work nicely with the group by just unfurling each permutation progressively. As an example, given $(\dot{z_1}, \dot{z_2}, \dots)$, we wish to find the index $k$ such that $\dot{z_k} = 1$. We may then apply $\sigma_{1,k}^{-1}$ to $(\dot{z_1}, \dot{z_2}, \dots)$ to obtain $(1, \dots)$, on which we may then recursively proceed. Inventing this gives us $(\dot{z_1}, \dot{z_2}, \dots)$ in terms of the generators.

**Lemma 3.2.** Every box $(i, j)$ of the table $T$ is in $G$.

*Proof.* We fed generators or elements of the table into the table, but each feed only performs group operations, which means inductively, we are done here. □

**Lemma 3.3.** Any $\sigma \in S_n$ fed into the table is a monotone product of elements of $T$. We have that $\sigma = \sigma_{1,j_1} \cdot \sigma_{2,\cdot j_2} \cdot \dots \cdot \sigma_{n,j_n}$, where our $\sigma_{i,j_i}$s are drawn from the table, and the box in the index $(i, j_i)$ is nonempty.

*Proof.* There are three possibilities;

(i) If $\sigma = e$, then it's just $\sigma_{1,1}\sigma_{2,2}\sigma_{3,3} \dots$.

(ii) If $\sigma$ is in the table, suppose its $\sigma_{i,j}$; then $\sigma = \sigma_{1,1} \dots \sigma_{i,j} \dots \sigma_{n,n}$.

(iii) If $\sigma$ is neither of these, then suppose $\sigma$ has pivot $i$, $\sigma(i) = j$, and $\sigma_{i,j}$ is full; then we just feed $\sigma' = \sigma_{i,j}^{-1}\sigma$. In other words, $\sigma = \sigma_{i,j}\sigma'$, and since you can only repeat this finitely many times, this is eventually $\sigma = \sigma_{1,1} \dots \sigma_{i,j} \dots \sigma_{n,j_n}$. □

The before holds for $\sigma \in S_n$ fed into the table, but we don't necessarily have that the table $T$ generates the group just yet[4]. If we feed in a generator $g_i$, we have that $g_i$ is in $\langle T \rangle$, meaning that by feeding our generators, we indeed have that $\langle T \rangle = G$. Therefore, feeding products of elements is to get everything in $G$ as a monotone product.

**Lemma 3.4.** Two monotone products are equal if and only if they are the same.

*Proof.* If they are the same, they are equal, so it suffices to check that if two monotone products are equal, they are the same. Suppose that $\sigma_{1,j_1} \dots \sigma_{n,j_n} = \sigma_{1,j_1'} \dots \sigma_{n,j_n'}$. Then

$$\sigma_{i,j_1} \dots \sigma_{n,j_n} = (\sigma_{i,j_1}^{-1}\sigma_{1,j_1'})\sigma_{2,j_2'} \dots \sigma_{n,j_n'},$$

meaning that

$$\sigma = \sigma_{n,j_n}^{-1}(\sigma_{n-1,j_{n-1}}^{-1}(\dots(\sigma_{1,j_1}^{-1}\sigma_{1,j_1})\dots)\sigma_{n-1,j_{n-1}'})\sigma_{n,j_n'} = e,$$

but then we have $\sigma(1) = 1$, so, since all but the middle are the identity on 1, we have that $\sigma(1) = \sigma_{1,j_1}^{-1}\sigma_{i,j_i}(1)$, meaning $j_1 = j_1'$, and so

$$\sigma = \sigma_{n,j_n}^{-1}(\dots(\sigma_{2,j_2}^{-1}\sigma_{2,j_2})\dots)\sigma_{n,j_n'} = e,$$

and so by an inductive process, we are done. □

[4] if we feed $\sigma \in G$, then we are essentially going to apply #2 until we reach the identity permutation; if we feed in $\sigma \notin G$, then we will arrive at an empty square in the table $T$

**Lemma 3.5.** $M = \{\sigma_{1,j_1}, \dots \sigma_{n,j_n} \mid j_i \in [n]; \sigma_{i,j_i} \in T\}$ is a group.

**Lemma 3.6.** $M_k = \{\sigma_{k,j_k} \dots \sigma_{n,j_n} \mid j_i \in [n]; \sigma_{i,j_i} \in T\}$ is a group.

*Proof.* $M_n$ is a group, because $M_n$ is just the identity. The proof is to be continued. □

Personal note; claims 3 and 4 from Dror's handout is used to establish a bijection between valid Rubik's cubes moves (i.e., elements of $G$), and elements in $M$ (monotone products of red boxes in $T$).

If we have $M_1 = G$, then we can solve the questions set out at the beginning of our course, namely,

(i) Compute $|G|$; we have that $|G| = |M_1|$.

(ii) Given $\sigma \in S_n$, decide if $\sigma \in G$; suppose we feed $\sigma$ into $T$. If it would change the table, then $\sigma$ is not in $G$.

(iii) Write a $\sigma \in G$ in terms of the generators $g_i$; by keeping track of the elements we feed in, we can find each of the boxes of $T$ in terms of the generators, so we can write each element as a monotone product in terms of the generators.

(iv) Product random elements $\sigma \in G$; for each $i \in [n]$, pick some $j_i$ randomly such that $\sigma_{i,j_i} \in T$. Then we may take the product of all such $\sigma_{i,j_i}$ to produce a random element of $G$.

In a random tangent, we now proceed to define cycle notation. Suppose

$$G = \langle (1\,2\,3), (1\,2)(3\,4) \rangle ;$$

we now proceed to fill in a $4 \times 4$ lower-triangular $T$, which Dror spent a lot of time trying to do. It also taught me that I am never going to even bother solving a Rubik's cube with this algorithm; this goes without saying but there is no chance in hell I'm typing all that shit down.

# §4 Day 4: NCGE, Pt. 4 (Sep. 12, 2025)

We do a review of the non-commutative Gaussian elimination process.

(i) We have that $T \subset G$. Recall the definition that

$$M_k = \{\sigma_{k,j_k} \dots \sigma_{n,j_n} \mid \sigma_{i,j_i} \in T\}.$$

(ii) Anything fed into the table is in $M_1$.

(iii) If two monotone products are equal as elements of $S_n$, then they are the same.

**Theorem 4.1.** For all $k$, $M_k \cdot M_k \subset M_k$; we note that in general, $A \cdot B = \{ab \mid a \in A, b \in B\}$.

**Corollary 4.2.** $M_1 \cdot M_1 \subset M_1$, meaning that $M_1 = G$.

*Proof.* To see this, $M_1 \subset G$ per its construction, as all the generators of $G$, $g_1, \dots, g_\alpha$, have been fed into $M_1$. Observe that by our previous claims, we have that products of elements in $M_1$ are in $M_1$. To check that $M_1$ is in fact a group (which requires $M_1$ to be closed under inverses and the group operation), we may first note that it is closed under multiplication, and observe the following;

$$e = g^0, g = g^1, g^2, g^3, \dots$$

is an infinite sequence, where each of the elements in said sequence are in $G$. However, $G$ is a finite group, meaning that there must be some sort of periodicity in the sequence. Without loss of generality, for all $n < m$ such that $g^n = g^m$, let us write $m = n + k$, where $k > 0$. Since $g^n = g^n g^k$, we must have that $e = g^k$, meaning that $g^{k-1}$ is indeed the inverse of $g$. Thus, we establish that if $G$ is finite and $M_1$ is a subset closed under multiplication, then $M_1$ is a subgroup of $G$. Thus, we conclude that $G = M_1$ by double inclusion. □

**Definition 4.3.** We define the *order* of $g \in G$ to be $\mathrm{ord}_G(g) = |g|$, i.e., the smallest possible $k$ such that $g^k = e$.

We now prove the theorem with backwards induction (from the maximum value of $k$ to the minimum value, i.e., $k = n$ to $k = 1$).

*Proof.* We start with the base case; $M_n \cdot M_n \subset M_n$ is trivially true, because $M_n$ contains only the identity, so $\{\mathrm{id}\}\{\mathrm{id}\} \subset \{\mathrm{id}\}$ is obviously true.

Since Dror doesn't want to work with some random $k$, we're going to assume $M_5 \cdot M_5 \subset M_5$, and show that $M_4 \cdot M_4 \subset M_4$ as a consequence.[5] Again, Dror doesn't like indices, so he's going to start by showing that $\sigma_{8,j} \cdot M_4 \subset M_4$. Observe that the set of all $\sigma_{8,j} M_4 \subset \bigcup_{j_4 \geq 4} \sigma_{8,j} (\sigma_{4,j_4} \cdot M_5)$; by associativity, we have that

$$\bigcup_{j_4 \geq 4} \sigma_{8,j} (\sigma_{4,j_4} \cdot M_5) = \bigcup_{j_4 \geq 4} (\sigma_{8,j} \sigma_{4,j_4}) M_5.$$

We have that $\sigma_{8,j}\sigma_{4,j_4}$ is a monotone product in $M_4$, meaning that the above is a subset of $M_4 \cdot M_5$, which is equal to $\bigcup_j \sigma_{4,j}(M_5 \cdot M_5)$, which, by our inductive hypothesis, we have that

$$\bigcup_j \sigma_{4,j}(M_5 \cdot M_5) \subset \bigcup_j \sigma_{4,j} M_5 \subset M_4,$$

[5] damn!!!! i hate indices!!!! rah!!!! grrr snarll growllll.... (bongos) BOMBS OVER BAGHDADDDdddd

since all $\sigma_{4,j}M_5$ is a monotone product in $M_4$. Moreover, observe that using our process above, we obtain

$$\sigma_{4,j_4} \dots \sigma_{n,j_n} M_4 \subset \sigma_{4,j_4} \dots \sigma_{n-1,j_{n-1}} M_4,$$

and so on, since we may note that $\sigma_{i,j_i}$ for $i \geq 4$ still fixes the pivot at 4. In the end, we have that any $\sigma \in M_4$ must satisfy $\sigma M_4 \subset M_4$, and so we are done with the inductive step. □

---

Recall that in math so far, we've seen linear functions $L : V \to W$ and continuous functions $F : X \to Y$ . We now discuss maps between groups.

**Definition 4.4.** Let $G, H$ be groups. $\varphi : G \to H$ is called a *group homomorphism* (morphism) if its a set map and $\varphi(xy) = \varphi(x)\varphi(y)$, $\varphi(e_G) = e_H$, and $\varphi(x^{-1}) = \varphi(x)^{-1}$.

# §5 Day 5: Group Homomorphisms, Normal Subgroup (Sep. 17, 2025)

Recall the definition of a group homomorphism,

**Definition 5.1.** $\varphi : G \to H$ is said to be a group homomorphism (where $G, H$ are groups) if it is a structure-perserving group transformation, i.e.,

(i) $\varphi(xy) = \varphi(x)\varphi(y)$,

(ii) $\varphi(e_G) = e_H$,

(iii) $\varphi(x^{-1}) = \varphi(x)^{-1}$

for all $x, y \in G$.

In particular, the three properties above are equivalent to $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1}$; they are also equivalent to the implication that (i) implies (ii), (iii). Below are some examples of group homomorphisms,

(a) Let $\mathbb{Z}, \mathbb{R}$ both be equipped with addition; then the inclusion map $\mathbb{Z} \to \mathbb{R}$ is a group homomorphism.

(b) The function $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, x)$ is a group homomorphism ($e^{x+y} = e^x e^y$).

(c) $\mathbb{R} \ni t \mapsto e^{2\pi i t} \in \{z \in \mathbb{C} \mid |z| = 1\} = S^1 \subset \mathbb{C}$ is a group homomorphism.

(d) $\varphi : S_4 \to S_3$ given by mapping the faces of a tetrahedron to the three pairs arising from identifying its opposite edges is also a homomorphism.

As an aside, groups, together with their homomorphisms, form a category. In category theory terms, objects (groups) and maps (group homomorphisms) are seen as points and morphisms.

(i) The identity map $I : G \to G$ is a homomorphism.

(ii) If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms, then $\psi \circ \phi$ is a homomorphism.

A morphism is called an *isomorphism* if it has an inverse that is also a morphism, i.e., $\varphi : G \to H$ is an isomorphism if and only if it is bijective with $\varphi^{-1} : H \to G$ being a group homomorphism.

**Definition 5.2.** $\operatorname{Aut} G = \{\varphi : G \to G \mid G \text{ is an isomorphism}\}$; i.e., $\operatorname{Aut} G$ is the set of all group isomorphisms.

As an example, $\operatorname{Aut} \mathbb{Z}$ consists of the identity morphism and the "multiplication by $-1$" morphism, both of which we may readily check to satisfy isomorphism properties.

**Claim 5.3.** $\operatorname{Aut} G$ is a group under composition.

Given any group $G$, there is a map $C : G \to \operatorname{Aut} G$ called "conjugation", where $G \ni h \mapsto C_h \in \operatorname{Aut} G$; we have that $C_h(g) := h^{-1}gh = g^h$, i.e., "conjugation of $g$ by $h$", where $C_h : G \to G$.

(i) $C_h$ is a morphism, since $C_h(g_1 \cdot g_2) = C_h(g_1) \cdot C_h(g_2)$, since $(g_1 \cdot g_2)^h = g_1^h \cdot g_2^h$, i.e.,

$$g_1^h g_2^h = h^{-1}g_1 h h^{-1} g_2 h = h^{-1} g_2 g_2 h = (g_1 g_2)^h.$$

(ii) $C_h$ is an invertible map; in fact, $C_h \circ C_h^{-1} = I$. We see this by considering that $(g^{h_1})^{h_2} = g^{h_1 \circ h_2}$. In this way, $g \mapsto (g^{h^{-1}})^h = g^{h^{-1}h} = g^e = g$, and the same holds when we consider $g \mapsto (g^h)^{h^{-1}}$.

**Claim 5.4.** $C$ is an anti-homomorphism, i.e. $\varphi(ab) = \varphi(b)\varphi(a)$. Specifically, $C_{h_1 \circ h_2}(g) = C_{h_2} \circ C_{h_1}(g)$, which we see from expanding both sides to obtain $g^{h_1 \cdot h_2} = (g^{h_1})^{h_2}$.

**Claim 5.5.** Let $\varphi : G \to H$ is a morphism. Then $\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}$ is a subgroup of $G$. We write $\ker \varphi < G$. Also, $\operatorname{im} \varphi = \{\varphi(g) \mid g \in G\} < H$, meaning that $\operatorname{im} \varphi$ is a subgroup too.

As an example, let $t \mapsto e^{2\pi i t}$ from $\mathbb{R} \to S^1$; we have that

$$\ker t = \{t \mid e^{2\pi i t} = 1\} = \{t \mid \cos 2\pi t + i \sin 2\pi t = 1\} = \mathbb{Z}.$$

We also have that if $\varphi : S_4 \to S_3$, then $\ker \varphi = \{I, (12)(34), (14)(23), (13)(24)\}$, and $\operatorname{im} \varphi = S_3$. In general, if $H < G$, then $H$ is always in the image of $\varphi$ for some $\varphi$; we may immediately see this to be true by considering the inclusion $H \hookrightarrow G$.

**Claim 5.6.** If $\varphi : G \to S^1$ and $g \in \ker \varphi$, then for any $h \in G$, $g^h \in \ker \varphi$.

*Proof.* $\varphi(g^h) = \varphi(h^{-1}gh) = \varphi(h^{-1})\varphi(g)\varphi(h) = \varphi(h^{-1})\varphi(h) = e$, meaning that $g^h \in \ker \varphi$. □

Yet, if we consider the example where $S_3 < S_4$, is there $\varphi : S_3 \to S_n$ such that $\ker \varphi = S_3$? We observe that $(23) \in S_3$, and $(23)^{3\,4} = (34)(23)(34) = [1432] \notin S_3$, meaning that $S_3$ is not a kernel in $S_n$.

**Definition 5.7.** $N < G$ is called *normal* in $G$ and denoted $N \lhd G$ if $n \in N$, $h \in G$, then $n^h \in N$ if and only if $h^{-1}Nh \subset N$.[6]

**Claim 5.8.** $\varphi : G \to H$ has $\ker \varphi \lhd G$.

Suppose $N \lhd G$. Is there a morphism $\varphi : G \to H$ such that $N = \ker \varphi$?

[6] we're going to use lhd for normal subgroup and see if it works, like "left hand delta" ig

# §6 Day 6: Normal Subgroup as Kernel of Homomorphism (Sep. 19, 2025)

Term test 1 has been moved a week earlier to Nov. 4; homework 1 is due at 11:59pm today, and homework 2 is online now.

We now recap last class' definitions,

**Definition 6.1.** We say that $N \lhd G$ if $N < G$ and for all $h \in G$, we have that $N^h = h^{-1}Nh = N$. We say that $N$ is *normal.*

**Claim 6.2.** If $\varphi : G \to H$, then $\ker \varphi \lhd G$.

Given $N \lhd G$, there exists a unique $\varphi : G \twoheadrightarrow H$ (we denote surjections with double headed arrows, $\twoheadrightarrow$) with $\ker \varphi = N$. As an aside, surjections are the same as equivalence relations. This is a general set theoretic fact, and we should be aware of it.

Let us discuss in terms of sets, for now. We say that a relation $\sim: X \times X \to \{T, F\}$ (i.e., true or false) on a set $X$ is called an *equivalence relation*, where $a \sim b$ if $\sim (a, b) = T$, if it satisfies the following axioms,

(i) (*Reflexivity*) For all $x \in X$, we have that $x \sim x$.

(ii) (*Symmetry*) For all $x, y \in X$, we have that $x \sim y$ if and only if $y \sim x$.

(iii) (*Transitivity*) For all $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

As an example of an equivalence relation, let $f : X \to Y$ be a function, and define $a \sim b$ for $a, b \in X$ if $f(a) = f(b)$.

**Definition 6.3.** Let $(X, \sim)$ be a set equipped with an equivalence relation $\sim$; given some $x \in X$, we say $[x]_\sim = \{y \in X \mid x \sim y\}$. The subscript $\sim$ denoting which equivalence class it belongs to is dropped if it is evident from context.

**Claim 6.4.** Equivalence classes are either equal or disjoint, i.e., let $[x], [y]$ be equivalence classes; we have that $[x] \cap [y]$ is either $\emptyset$ or $[x] = [y]$. The former occurs if $x \not\sim y$, and the latter occurs if $x \sim y$.

**Definition 6.5.** We say that $X/\sim = \{[x] \mid x \in X\}$ is the set of equivalence classes on $X$.

**Definition 6.6.** $\phi : X \to X/\sim$ is the quotient map $\phi : X \ni x \mapsto [x]$. We have that $\phi$ is surjective. Specifically, $\phi : X \twoheadrightarrow Y \implies a \sim b$ if $\phi(a) = \phi(b)$, and $\sim$ induces the $\phi : X \to X/\sim$ map.

We now look to construct the surjection $\varphi : G \twoheadrightarrow H$ with $\ker \varphi = N \lhd G$. Given $N \lhd G$, we define $g_1 \sim g_2$ if and only if $g_1^{-1}g_2 \in N$. This comes from the train of thought where we want $\varphi(g_1) = \varphi(g_2) \implies \varphi(g_1)^{-1}\varphi(g_2) = \varphi(g_1^{-1}g_2) = e$, i.e., we're constructing $\varphi$ such that $N$ is the kernel of $\varphi$. Clearly, we can see that $\sim$ is an equivalence relation when defined as earlier; reflexivity and symmetry are immediate, and for transitivity, we see that if $a, b, c \in G$ are such that $a^{-1}b, b^{-1}c \in N$, then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in N$, since $N$ is a subgroup and is closed.

In this manner, let us write $G/\sim = \{[g] \mid g \in G\}$. We write this group as $G/N = \{gN \mid g \in G\}$, and $[g] = g \cdot N = \{g \cdot n \mid n \in N\}$. Indeed, we have that $\phi : G \to G/N$ by $\varphi(g) = g \cdot N$. It remains to check that $\phi$ is a group homomorphism and $\ker \phi = N$. Let us define a group structure on $G/N$ by including the operation $[g_1] \cdot [g_2] = [g_1 g_2]$. To check

that $\cdot$ is well-defined, observe that for any $g_1 \sim g_1'$ and $g_2 \sim g_2'$, we have that $g_1 g_2 \sim g_1' g_2'$, since by definition, there exists $n_1, n_2 \in N$ where $g_1' = g_1 \cdot n_1$, and $g_2' = g_2 \cdot n_2$, so

$$g_1' g_2' = g_1 n_1 g_2 n_2 = g_1 g_2 g_2^{-1} n_1 g_2 n_2 = g_1 g_2 n_1^{g_2} n_2 \in g_1 g_2 N,$$

where we use the fact that $N$ is normal to see that $n_1^{g_2} \in N$. We note that this is the only place that we've used the fact that $N$ is normal.

**Theorem 6.7.** Let $G/N$ be a group, and let $\phi : G \to G/N$ be a morphism (recall that we let $g \mapsto gN$). Then $\ker \phi = N$.[7]

*Proof.* Since we already established that $\phi$ is a well-defined morphism, we have that $\ker \phi = \{g \in G \mid \phi(g) = gN = N\} = N$, since $gN = N$ if and only if $g \in N$ (which is true in general for any subgroup, not just normal $N$). □

[7] we call this the natural homomorphism iirc? and its surj