Math 55a Lecture 1

<u>Remember</u>:
- Please wear masks at all times. This is really important.
- If sick or in isolation/quarantine, please don't come to class!
  If you give me a bit of advance notice, we'll arrange for you to be able to watch the lecture on Zoom. And/or ask a friend.

- Outside of lecture : → Office hours & discussion sections
  → Canvas (notes, assignments, ...)
  → Slack (please join + introduce yourself in #general)
  → e-mail

<u>Course staff</u>:  Prof. Denis AUROUX — office hours Mondays & Wednesdays
↳ not Sept 6 (holiday)
auroux@math.harvard.edu
TO BE CONFIRMED - tentatively 12:30-1:30 in Sc. Center 539?

<u>CAs</u>: Oliver Cheng  | Leo Fried  | Gaurav Goel  | Dora Woodruff  | Eric Yan 

- Office hours & sections : to be announced on Canvas.

- See course information & syllabus on Canvas (more logistics, policies, exams)
- Homework due Wednesdays on Canvas. HW 1 (due Sept 8) is posted.
  Handwritten submissions are fine, or try LaTeX / Overleaf
  Collaboration encouraged (but write your own solution!). Ask CAs for hints if needed!
  Use slack (#studygroups, #homework). List your collaborators.
- Feedback survey to be completed this weekend (after lecture 2, before lecture 3)
- What Math 55 is and isn't; reminder about community, respect, and inclusion.

<u>Course Content</u>:

1. Group theory (~ Artin chapter 2)
2. Fields and vector spaces, linear + multilinear algebra (Axler)
3. More group theory (Artin chapters 6-7)
4. Intro to Representation theory (Artin + Fulton-Harris)

<u>You should have</u>: { Artin, "Algebra" (2nd edition)
Axler, "Linear Algebra Done Right"

<u>Groups</u> = abstract structure that models the common features of concrete objects such as
{ - numbers
- permutations
- linear transformations
- symmetries

Definition: A <u>group</u> G consists of a set S together with a <u>law of composition</u>, ie. a map $m: S\times S \to S$
$(a,b) \mapsto a\cdot b$ (sometimes $a * b, \dots$)
satisfying the following axioms:

1) there exists an <u>identity element</u> $e \in S$ st. $\forall a \in S$, $ae = ea = a$.
"for all"

[note: e is unique! if e, e' both act as identity then $e = ee' = e'$].

2) <u>inverses</u> exist: $\forall a \in S$, $\exists b \in S$ st. $ab = ba = e$. <u>Write</u> $b = a^{-1}$.
"for all" "there exists"

3) <u>associativity</u>: $\forall a,b,c \in S$, $(ab)c = a(bc)$.
[so we can write just: abc].

Rmk:
- associativity implies the <u>cancellation law</u>: $\forall a,b,c \in S$, $ab = ac \Rightarrow b = c$.
  (<u>Pf</u>: $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \underset{\substack{\text{associativity}\\ +\text{inverse}}}{\Rightarrow} eb = ec \Rightarrow b = c$.)
- technically the group is the pair (S, m), but in real life we'll just write G for the set and talk of elements of G.

Variants:
- ⋆ if we omit the second axiom (inverses), we have a <u>semigroup</u>.
- ⋆ if we have a group whose law is <u>commutative</u>, ie. $ab = ba$ $\forall a, b$ we say that G is <u>abelian</u> (and may denote the operation $+$ instead)

Examples:

0) the trivial group $G = \{e\}$, $e\cdot e = e$.
(usually not an interesting example. Don't give this as answer to a HW problem asking for an example.).

1) number systems: $(\mathbb{Z}, +)$ or $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with addition. Identity: 0
integers — rationals, reals, complex — Inverse: $-x$.
but natural numbers $(\mathbb{N}, +)$ only form a semigroup!

2) a group with two elements? if $|G| = 2$, let e = identity, x = the other element, necessarily $e\cdot e = e$, $e\cdot x = x$, $x\cdot e = x$. What about $x \cdot x$?
Can think of
- $\{0,1\}$ or $\{\text{even}, \text{odd}\}$, with addition mod 2 $(1+1=0)$
- $\{+1, -1\}$ with multiplication.

<u>Q:</u>
- Come up with an example of a group with 8 elements. Convince yourself it is a group. Can you find another example?

Ex's continued:

3.) $\mathbb{Z}/n = \{0, 1, \dots, n-1\}$ with group law given by addition mod n:

$$(a,b) \mapsto \begin{cases} a+b & \text{if } a+b \le n-1 \\ a+b-n & \text{otherwise} \end{cases} \quad \text{(denote this by } +\text{)}$$

(finite group w/ n elements)

Similarly, $\mathbb{R}/\mathbb{Z}$: $S = [0,1) \subset \mathbb{R}$ with addition $(a,b) \mapsto \begin{cases} a+b & \text{if } a+b < 1 \\ a+b-1 & \text{otherwise.} \end{cases}$

4) nonzero numbers $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^*$, $\mathbb{C}^*$ with multiplication. Identity: 1, inverse: $1/x$.

Inside $\mathbb{C}^*$, the unit circle $S^1 = \{z \in \mathbb{C} \,/\, |z| = 1\}$ is also a group for multiplication

These are still abelian (aside: nonzero quaternions form a nonabelian mult. group)

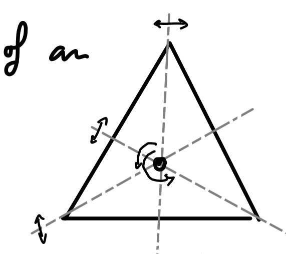
5) symmetries and permutations:

Recall $f : A \to B$ is
- injective (1-to-1) if $\forall x, y \in A$, $x \neq y \Rightarrow f(x) \neq f(y)$
- surjective (onto) if $\forall b \in B$ $\exists x \in A$ st. $f(x) = b$.
- bijective if injective and surjective.

A permutation of a set A is a bijection $f : A \to A$. The set of permutations of A, with operation = composition, is a group, $\mathrm{Perm}(A)$. (Why?)

The symmetric group on n elements: $S_n = \mathrm{Perm}(\{1, \dots, n\})$

- S_3 has a geometric interpretation if we think of symmetries of an equilateral triangle = rotations which preserve it (3 incl. identity) and reflections (3 of those).



Symmetries permute the vertices, and every permutation of the set of vertices arises from exactly one symmetry (+ composition laws agree).

So: S_3 also occurs as the group of symmetries of Δ.

(Other groups arise from symmetries of other geometric figures in $\mathbb{R}^2$ and $\mathbb{R}^3$).

6) Groups of matrices: $GL_n(\mathbb{R}) = \{$invertible $n \times n$ matrices with real coefficients$\}$ "general linear group" (with matrix multiplication)

also $SL_n(\mathbb{R}) = \{n \times n$ real matrices with determinant $1\}$ "special linear group".

also $GL_n(\mathbb{C})$, $SL_n(\mathbb{C})$ for matrices with complex coefficients... or $\mathbb{Q}$ or $\mathbb{Z}/n$ coeff's!

Products of groups:

- Given two groups G, H, the product group is $G \times H = \{(g,h) \,/\, g \in G, h \in H\}$ with composition law $(g,h) \cdot (g', h') = (gg', hh')$.

- If G, H are finite, of <u>order</u> $m = |G|$ and $n = |H|$, then $G \times H$ is a finite group of order mn.
- Similarly for product of n groups:
  <u>Ex:</u> $\mathbb{Z}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{Z}\}$, $(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$
  (similarly $\mathbb{Q}^n$, $\mathbb{R}^n$, $\mathbb{C}^n$ with componentwise addition)
  - Given infinitely many groups $G_1, G_2, G_3, \dots$ there are two different notions:
    → the direct product $\prod_{i=1}^{\infty} G_i = \{(a_1, a_2, a_3, \dots) \mid a_i \in G_i\}$
    → the direct sum $\bigoplus_{i=1}^{\infty} G_i = \{(a_1, a_2, a_3, \dots) \mid a_i \in G_i$, all but finitely many are identity$\}$

    <u>Ex:</u> consider $G_0 = G_1 = \dots = (\mathbb{R}, +)$, denote $(a_0, a_1, a_2, \dots)$ by $\sum a_i x^i$.
    Then $\prod_{i=0}^{\infty} \mathbb{R} = \mathbb{R}[[x]]$ formal power series $\sum_{i=0}^{\infty} a_i x^i$ (w/ addition)
    $\bigoplus_{i=0}^{\infty} \mathbb{R} = \mathbb{R}[x]$ polynomials $\sum_{\text{finite}} a_i x^i$.

★ <u>Subgroups & homomorphisms</u>:

<u>Def:</u> A <u>subgroup</u> H of a group G is a non-empty! subset $H \subset G$ which is closed under composition ($a, b \in H \Rightarrow ab \in H$) and inversion ($a \in H \Rightarrow a^{-1} \in H$).
Since $H \neq \emptyset$, these 2 conditions imply $e \in H$. So H (with same operation) is a group in its own right.

- say H is a <u>proper subgroup</u> if $H \subsetneq G$.

<u>Def:</u> Given two groups G, H, a <u>homomorphism</u> $\varphi: G \to H$ is a map which respects the composition law: $\forall a, b \in G$, $\varphi(ab) = \varphi(a)\varphi(b)$.
(This implies $\varphi(e_G) = e_H$, and $\varphi(a^{-1}) = \varphi(a)^{-1}$).

- an <u>isomorphism</u> is a bijective homomorphism
  (if G and H are isomorphic, then they are secretly the "same" group even if elements and law may have different names).

<u>Q:</u> among examples seen so far, which groups are isomorphic to each other? or to subgroups of other groups?

<u>Examples:</u>
- $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$
- $(\mathbb{Q}^*, \times) \subset (\mathbb{R}^*, \times) \subset (\mathbb{C}^*, \times) \supset (S^1, \times)$
- $\{e\} \subset G$ trivial subgroup
- $\mathbb{Z}/n$, $\mathbb{C}^*$, and $GL(2, \mathbb{R})$??
- $H_i \subset G_i \Rightarrow H_1 \times \dots \times H_n \subset G_1 \times \dots \times G_n$
- $\bigoplus G_i \subset \prod G_i$