MATH 456 (Honours Algebra 3)

J. Han

September 17, 2024

The following notes are adapted and abridged from lectures given by Henri Darmon in Fall 2024. All errors in interpretation, reasoning, coherence, and articulation are my own.

This document's source code, located at `https://github.com/brunefig/math456/blob/main/notes.org`, can be converted into Anki flashcards with the `org-anki` package for GNU Emacs; just make sure to flush all lines containing an `:ANKI_NOTE_ID:` property first. Flashcard cloze deletions are typeset in magenta.

2024-08-28 groups and symmetries

definition and notation of groups

A group is a structure denoted by $(G, *, e)$, where G is a set equipped with a binary operation $*$, that satisfies

- $e \in G \land \forall a \in G : e * a = a * e = a$,
- $\forall a \in G : \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$, and
- $\forall a, b, c \in G : (a * b) * c = a * (b * c)$.

e, $a * b$, and $\underbrace{a * \cdots * a}_{n \text{ times}}$ are often expressed as 1, ab, and a^n respectively.

For commutative groups, e, $a * b$, and $\underbrace{a * \cdots * a}_{n \text{ times}}$ are often expressed as 0, $a + b$, and na respectively.

symmetry and automorphism groups

A symmetry of X is a function $X \to X$ that preserves the structure of X.

The set of symmetries of X, denoted by $\mathrm{Aut}(X)$, forms a group $(\mathrm{Aut}(X), \circ, \mathrm{id})$.

examples of automorphism groups

The permutation group for a finite set X is $\text{Aut}(X) = S_X := \{\text{bijections } X \to X\}$.

For a vector space V, $\text{Aut}(V) = \{\text{invertible linear transformations } V \to V\}$.

For a vector space V over a field $\mathbb{F}$, $V = \mathbb{F}^n$ if $n := \dim_{\mathbb{F}}(V) \in \mathbb{N}$, hence $\text{Aut}(X) = GL_n(\mathbb{F}) :=$ the group of invertible $n \times n$ matrices with entries in $\mathbb{F}$.

For a ring R, $(R, +, 0)$ is a commutative group.

The dihedral group on a square X is $\text{Aut}(X) = D_8 := \{1, r, r^2, r^3, V, H, D_1, D_2\}$, where r is a rotation by 90 degrees and V, H, D_1, D_2 are reflections over the vertical, horizontal, and diagonal axes respectively.

The orthogonal group of a Euclidean space V with $\dim_{\mathbb{R}}(V) \in \mathbb{N}$ is $\text{Aut}(V) = O(V) := \{T : V \to V \mid \forall u, v \in V : (Tu \cdot Tv) = uv\}$ with $e := \cdot$.

2024-08-30 isomorphisms and group actions

homomorphisms, isomorphisms, and automorphisms

For groups G and H, a homomorphism $\phi : G \to H$ is a function satisfying $\forall a, b \in G : \phi(ab) = \phi(a)\phi(b)$.

> *$\phi(1_G) = 1_H$ for a homomorphism $\phi : G \to H$.*

Proof. $\phi(1_G) = \phi(1_G)^{-1}\phi(1_G)^2 = \phi(1_G)^{-1}\phi(1_G^2) = \phi(1_G)^{-1}\phi(1_G) = 1_H$. □

> *$\phi(g^{-1}) = \phi(g)^{-1}$ for a homomorphism $\phi : G \to H$ and $g \in G$.*

Proof. $\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(1_G) = 1_H$. □

An isomorphism is a bijective homomorphism.

Groups G and H are isomorphic, denoted $G = H$, when a $G \to H$ isomorphism exists.

For a group G, $\mathrm{Aut}(G) = \{\text{isomorphisms } G \to G\}$.

cyclic groups

The cyclic group of order n is $\mathbb{Z}/n\mathbb{Z} := \{k \in \mathbb{N} \mid k < n\}$.

An isomorphism $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is uniquely determined by the value of $\phi(1)$.

$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$, since any $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ isomorphism ϕ must have $\phi(1) \in (\mathbb{Z}/n\mathbb{Z})^\times$ to ensure bijectivity.

group actions

A group action or action of a group G on an object X is $* : G \times X \to X$ such that, for $g, g' \in G$ and $x \in X$,

- $1_G * x = x$,
- $(g * g') * x = g * (g' * x)$, and
- $m_g : X \to X : x \mapsto g * x \in \mathrm{Aut}(X)$.

For an object X and action of a group G on X, $m : G \to \mathrm{Aut}(X) : g \mapsto m_g$ is a group homomorphism.

Proof. $\forall g, g' \in G : \forall x \in X : m_{gg'}(x) = (gg')x = g(g'x) = (m_g \circ m_{g'})(x)$. □

Bijectivity of m_g follows from the definition of a group action.

Proof. $m_{g^{-1}} = m_g^{-1}$. □

2024-09-04 G-sets

definition and properties of G-sets

A G-set is a set X equipped with an action $*$ of a group G.

A G-set X is transitive when $\forall x, x' \in X : \exists g \in G : g * x = x'$.

A transitive G-subset of X is an equivalence class and is called an orbit of G on X.

Every G-set is a disjoint union of orbits.

Proof. Define a relation on X by $x \underset{G}{\sim} y$ if $\exists g \in G : gx = y$. Since $\underset{G}{\sim}$ is an equivalence relation, X can be expressed as a disjoint union of equivalence classes X/G for $\underset{G}{\sim}$. $\square$

examples of G-sets for an arbitary group G

For a group G, $X := \{1\}$ with $\forall g \in G : g * 1 = 1$ is a G-set with $\mathrm{Aut}(X) = \{\mathrm{id}\}$.

For a group G, $X := G$ with left multiplication is a G-set and produces an injective homomorphism $m : G \hookrightarrow S_G$.

(Cayley's theorem.) Every group is a subgroup of a group of permutations; in particular, if a group G is finite, then $G \subseteq S_G$.

For a group G, $X := G$ with $\forall (g, x) \in G \times X : g * x := xg^{-1}$ is a G-set.

Proof. Let $g, g', x \in G$. Then $1 * x = x1 = x$ and $g * (g'x) = g * (xg'^{-1}) = (xg'^{-1} *)g^{-1} = x(g'^{-1}g^{-1}) = x(gg')^{-1} = (gg') * x$. $\square$

For a group G, $X := G$ with the conjugation action $\forall g, g' \in G : \forall x \in X : (g', g) * x := g'xg^{-1}$ is a $(G \times G)$-set.

2024-09-06 isomorphic G-sets and cosets

Given an arbitrary group G, is it possible to classify all the G-sets up to isomorphism?

isomorphism between G-sets

An isomorphism between G-sets X and X' is a bijection $\phi : X \to X'$ such that $\forall (g, x) \in G \times X : \phi(g * x) = g * \phi(x)$.

cosets

For a subgroup $H \subseteq G$ and $g \in G$, $gH := \{gh \mid h \in H\}$ is called a left coset of H.

For a subgroup $H \subseteq G$, the orbits for the right action of H on G are $G/H := \{gH \mid g \in G\}$.

For a subgroup $H \subseteq G$, G/H with left multiplication is a G-set.

For a subgroup $H \subseteq G$, the orbits for the left action of H on G are $H \backslash G := \{Hg \mid g \in G\}$.

For a subgroup $H \subseteq G$, the sets G/H and $H \backslash G$ need not be identical; for example, $G := S_3$ and $H := \{\text{id}, (12)\}$ gives $G/H = \{\{\text{id}, (12)\}, \{(13), (123)\}, \{(23), (132)\}\}$ and $H \backslash G = \{\{\text{id}, (12)\}, \{(13), (132)\}, \{(23), (123)\}\}$.

For a finite subgroup $H \subseteq G$, $\forall g \in G : |gH| = |H|$.

Proof. Let $g \in G$. Then the map $H \to gH : h \mapsto gh$ has inverse $h \mapsto g^{-1}h$ and is therefore bijective. $\square$

(Lagrange's theorem.) Any subgroup $H \subseteq G$ satisfies $|H| \,\Big|\, |G|$.

For a transitive G-set X, $\exists\, H \subseteq G : X = G/H$ as a G-set.

Proof. Let $x \in X$, $H := \text{stab}_G(x) := \{g \in G \mid gx = x\}$, and $g, g' \in G$. $1x = x$ and $gx = x \wedge g'x = x \implies (gg')x = x$, so H is a subgroup.

$\phi : G/H \to X : gH \mapsto gx$ is well-defined; $gH = g'H \implies \exists h \in H : gx = (g'h)x = g'(hx) = g'x$. ϕ is also surjective by transitivity of X and injective since $g'x = gx \implies g^{-1}g'x = x \implies \exists h \in H : g^{-1}g' = h \implies g'H = gH$.

Finally, $\phi(g'(gH)) = \phi((g'g)H) = (gg')x = g'(gx) = g'\phi(gH)$. $\square$

2024-09-09 orbit stabilizer theorem

For a subgroup $H \subseteq G$, the index of H in G is $[G : H] = |G/H|$.

Group elements $a, b \subseteq G$ are called conjugate, or members of the same conjugacy class, when $\exists g \in G : a = gbg^{-1}$.

relationship between groups, G-sets, and stabilizers

For a transitive G-set X, all stabilizers of elements in X are isomorphic.

Let $x, x' \in X$, $g \in G : x' = gx$, and $h \in \text{stab}(x')$. Then $hx' = x' \iff hgx = gx \iff g^{-1}hgx = x \implies g^{-1}hg \in \text{stab}(x)$, so $\text{stab}(x')$ and $\text{stab}(x)$ are conjugate hence isomorphic.

For a finite group G with a transitive G-set X, $x \in X$, and $H := \text{stab}(x)$, $|G| = |X||H|$.

(Orbit stabilizer theorem.) For a group G, there exists a bijection between transitive G-sets (up to isomorphism) and subgroups of G (up to conjugacy). Thus the number of transitive G-sets of cardinality n is equal to the number of conjugacy classes of G of cardinality $\frac{|G|}{n}$.

examples using the orbit stabilizer theorem

For $n \in \mathbb{N}$, $G := S_n$, $X := [n]$, and $x \in X$, $\text{stab}(x) \cong S_{n-1} \subseteq G$.

For a regular tetrahedron $X := [4]$, a vertex $x \in X$, and $G := \text{Aut}(X) :=$ the group of rotations that preserve X's positions, $|G| = |X||\text{stab}(1)| = 12$ by the orbit stabilizer theorem. Since it is not possible to rotate a tetrahedron in a way that transposes exactly two vertices, $G \cong A_4$.

For a regular tetrahedron $X := [4]$, a vertex $x \in X$, and $G := \text{Aut}(X) :=$ the group of rotations and reflections that preserve X's positions, the rotations are isomorphic to A_4 and reflections are represented by transpositions, so $G \cong S_4$.

For a regular cube $X = [6]$, a face $x \in X$, and $G := \text{Aut}(X) :=$ the set of rotations that preserve X's positions, $\text{stab}_G(x) \cong \mathbb{Z}/4\mathbb{Z}$ Then $|G| = |X||\text{stab}_G(x)| = 24$ by the orbit stabilizer theorem. Furthermore, there are $\frac{|G|}{12} = 2$ and $\frac{|G|}{8} = 3$ rotations that fix a given edge and vertex respectively.

2024-09-11 kernels and injectivity

kernels

A normal subgroup $H \subseteq G$ is one for which $\forall g \in G : gHg^{-1} \subseteq H$; equivalently, $\forall g \in G : gH = Hg$, or G/H is a group.

The kernel of a group homomorphism $\phi : G \to H$ is $\ker(\phi) := \{g \in G \mid \phi(g) = 1_H\}$.

For a group homomorphism $\phi : G \to H$, $\ker(\phi)$ is a normal subgroup of G.

Proof. Let $g, g' \in G$. Then $\phi(1_G) = 1_H$, $\phi(g^{-1}) = \phi(g)^{-1} = 1_H^{-1} = 1_H$, and $\phi(gg') = \phi(g)\phi(g') = 1_H$ so $\ker(\phi) \subseteq G$. Furthermore, $\forall k \in \ker(\phi) : \phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)\phi(g^{-1}) = 1_H$. □

injective group homomorphisms

A group homomorphism $\phi : G \to H$ is injective if and only if $\ker(\phi) = \{1_G\}$.

Proof. Let $g, g' \in G$. Then $\phi(g') = \phi(g) \implies \phi(g)^{-1}\phi(g') = \phi(g^{-1}g') = 1_H \implies g^{-1}g' = 1_G$ holds if and only if $\ker(\phi) = \{1_G\}$. □

(Isomorphism theorem for groups.) A group homomorphism $\phi : G \to H$ induces an injective homomorphism $\tilde{\phi} : G/\ker(\phi) \hookrightarrow H$.

Proof. $\tilde{\phi} : g\ker(\phi) \mapsto \phi(g)$ is clearly well-defined and a homomorphism. It is also injective because $\tilde{\phi}(g\ker(\phi)) = \phi(g) = 1 \implies g \in \ker(\phi) \implies g\ker(\phi) = \ker(\phi)$. □

By the isomorphism theorem for groups, $\mathrm{im}(\phi) \cong G/\ker(\phi)$.

cube rotations

A principal diagonal of a cube is a line containing two maximally distant vertices.

The group of structure-preserving rotations of a cube is isomorphic to S_4.

Proof. For the group homomorphism $\phi : G \to S_4$ associated with the action of rotations G on a cube's principal diagonals X,

$$\ker(\phi) = \{\sigma : X \to X \mid \forall x \in X : \sigma(x) = x\} = \bigcap_{x \in X} \operatorname{stab}_G(x).$$

$|\operatorname{stab}_G(x)| = \frac{|G|}{|X|} = 6$ by the orbit stabilizer theorem, and $\operatorname{stab}_G(x) \cong S_3$ by considering A_3 as the set of rotations about x and $S_3 - A_3$ as the set of nontrivial rotations about any line passing through an edge with vertices disjoint to x. The identity is only permutation common to all four stabilizers, so $\ker(\phi) = \{1\}$.

An injective homomorphism $\tilde{\phi} : G/\ker(\phi) \hookrightarrow S_4$ exists by the isomorphism theorem for groups; since $G \cong G/\ker(\phi)$ and $|G| = |S_4|$, this implies $G \cong S_4$. $\square$

2024-09-13 cube symmetries and conjugacy

The group $\tilde{G}$ of rotations and reflections of a cube is isomorphic to $S_4 \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Let X be the cube's principal diagonals and G the group of rotations. $\tilde{G} = \tilde{\operatorname{Aut}}(X)$ rotations and reflections on X Clearly $G \subseteq \tilde{G}$, so $|\tilde{G}| = |G|[\tilde{G} : G]$. Taking for granted that there are two orientations, collectively denoted by O, in $\mathbb{R}^3$, it can be seen that $\tilde{G}/G \cong \{1, \tau\}$ for some τ, hence $|\tilde{G}| = 48$.

A homomorphism $\eta : \tilde{G} \to \operatorname{Aut}(O) = S_2 = \mathbb{Z}/2\mathbb{Z} = \{1, \tau\}$ then exists with $\ker(\eta) = G$ and $\tau := v \mapsto -v$, which can thought of as the product of transpositions of each vertex with its opposite or the -1 matrix with the center of the cube considered as the origin. τ commutes with all of $\tilde{G}$, so $\tilde{G} = G \sqcup \tau G$.

Now $\phi : S_4 \times \mathbb{Z}/2\mathbb{Z} \to \tilde{G} : (g, j) \mapsto g\tau^j$ is clearly bijective, and since $\forall g, g' \in G : \forall j, j' \in \mathbb{Z}/2\mathbb{Z} : \phi(gg', jj') = (gg')\tau^{jj'} = (g\tau^j)(g\tau^{j'})$ it is a homomorphism. $\square$

center of a group

The center of a group G is $Z(G) := \{z \in G \mid \forall g \in G : zg = gz\}$.

$Z(S_4) = \{1\}$.

conjugation action

The conjugation action of G on itself is not transitive when $|G| > 1$, since $\forall g \in G : g1g^{-1} = 1$.

A conjugacy class is an orbit for the conjugation action.

(Class equation.) For a group G with conjugacy classes represented by elements $\{g_i\}$ disjoint from $Z(G)$, $|G| = |Z(G)| + \sum_i [G : Z_G(g_i)]$ where $Z_G(g)$ is the centralizer of g in G.

examples of conjugacy classes

A commutative group has only conjugacy classes of size 1::property.

The conjugacy classes of D_8 are $\{1\}$, $\{r^2\}$, $\{V, H\}$, $\{D_1, D_2\}$, and $\{r, r^3\}$.

The cycle shape of $\sigma \in S_n$ is the partition of $[n]$ that it determines.

The cycle shape of $1 \in S_n$ is $\underbrace{1 + \cdots + 1}_{n \text{ times}} = n$.

The cycle shape of $(1 \cdots n) \in S_n$ is $n = n$.

Conjugate permutations in S_n have the same cycle shape.

The conjugacy classes of S_4 are $\{1\}$, the transpositions, the 3-cycles, the compositions of disjoint transpositions, and the 4-cycles, which have cardinalities 1, $\binom{4}{2}$, $4 \cdot 2$, $\binom{4}{2}$, and $3!$ respectively.