MATH 456 (Honours Algebra 3)

J. Han

September 8, 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

- $e \in G \wedge \forall a \in G : e * a = a * e = a$,
- $\forall a \in G : \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$, 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 $\mathrm{Aut}(X) = S_X \coloneqq \{\text{bijections } X \to X\}$.

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

For a vector space V over a field $\mathbb{F}$, $V = \mathbb{F}^n$ if $n \coloneqq \dim_{\mathbb{F}}(V) \in \mathbb{N}$, hence $\mathrm{Aut}(X) = GL_n(\mathbb{F}) \coloneqq$ 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 $\mathrm{Aut}(X) = D_8 \coloneqq \{1, r, r^2, r^3, V, H, D_1, D_2\}$, 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 $\mathrm{Aut}(V) = O(V) \coloneqq \{T : V \to V \mid \forall u, v \in V : (Tu \cdot Tv) = uv\}$ with $e \coloneqq \cdot$.

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 $\underset{G}{\sim}$. □

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 $m : G \to S_G$.

(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 $\forall g, g' \in G : \forall x \in X : (g', g) * x := g'xg^{-1}$ 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 $x \in X$, $H := \mathrm{stab}_G(x) := \{g \in G \mid gx = x\}$, 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, $\phi(g'(gH)) = \phi((g'g)H) = (gg')x = g'(gx) = g'\phi(gH)$. $\square$

For a finite group G with a transitive G-set X, $|X| \, \big| \, |G|$.