MATH 250A: Groups, Rings, and Fields

Jad Damaj

Fall 2022

Contents

Chapter 1

Groups

1.1 August 25

1.1.1 Groups

Two ways to define groups

- concrete: group = symmetries of an object X. Here a symmetry is a bijection $X \to X$ with inverse that preserves "structure" (topology, order, binary operation, ...)

Example 1.1.1. The rectangle has 4 symmetries.
The icossahedron has 20×3 symmetries since after fixing the first face there are 3 possible rotations.
Vector space $\mathbb{R}^k$: $n \times n$ matrices with $\det \neq 0$, denoted $GL_n(K)$

- abstract definition:

> **Definition 1.1.2.** A group is a set G with a binary operation $G \times G \to G$ by $(a, b) \mapsto ab, a\times, a+b, \ldots$ with "Inverse" : $G \to G$ by $a \mapsto a^{-1}$ and "Identity": $1, 0, e, I, \ldots$ satsifying the axioms:
> $1x = x1 = x \quad x(x^{-1}) = (x^{-1})x = 1 \quad (xy)z = x(yz)$

We can go from the concrete definition to the abstract one: the binary operation is composition, the identity is the trivial symmetry, inverses given y "undoing' a symmetry.

Is an abstract group the symmetries of something?

> **Theorem 1.1.3** (Cayley's Theorem)**.** Any abstract group is the group of symmetries of some mathematical object.

Recall group actions :

> **Definition 1.1.4.** Given a group G, a set S, a (left) gtroup action is a map $G \times S \to S$ by $(g, s) \mapsto g(s), gs$ satisfying $g(h(s)) = gh(s)$, $1s = s$.

To prove Cayley's theorem we need to find :

1. a set S acted on by G

2. structure on S so that $G =$ all symmetries.

What is S? Take $S = G$.

Need to define the action of $GonG$. There are 8 natural ways to do this.
First 4, we defin4 $G \times S \to S$ by

- $g(s) = s$ trivial action
- $g(s) = gs$ group product
- Try $g(s) = sg$ Fails since G not necesarily commutative: $g(h(s)) = (sh)g \neq s(gh) = gh(s)$
- $g(s) = sg^{-1}$ works since $g(h(s)) = g(sh^{-1}) = sh^{-1}g^{-1} = s(gh)^{-1} = gh(s)$
- $g(s) = gsg^{-1}$ adjoint action

The above group action is known as a left group action, We define a right group action in a similar way :
$S \times G \to S$ by$(s, g) \mapsto (s)g, s^g$ satisfying (sg)h = s(gh), $s1 = s$.

We now define right group actions of G on G: $S \times G \to G$ by

- $(s, g) \mapsto s$
- $(s, g) \mapsto sg$
- $(s, g) \mapsto g^{-1}s$
- $(s, g) \mapsto g^{-1}sg$

Now we have $S = G$, S=set acted on by G using left action $g(s) = gs$ - left translation. So we have shown $G \subseteq$ symmetries of S.

Want : G =symmetries of S + "structure". Let structure on S= right action of G on S.
We now have 3 copies of G:

1. set $S = G$
2. G acts on left on S (G = symmetries of S)
3. G acts o the right on S (Structure of S)

Object S = S + right G action

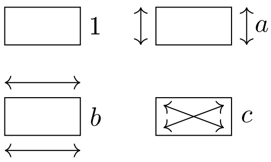
What are the symmetries of this?
Bijection $f : S \to S$ preserving the right G-action. eg. $f(sg) = f(s)g$
Need to check:

1. Left G-action of G preserves the right G-action
2. Anything that preserves the right G-action is given by left multiplication of an element of G

Check (1): For $g \in G$ need $(gs)h = g(sh)$, follows by commutativity
Note: left G-action does not preserve right G-action: $g(hs) \neq h(gs)$ in general

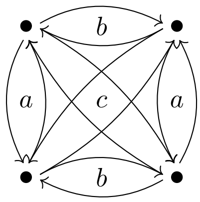
Check (2): Suppose $f : S \to S$ preserves the right G-action, $f(sh) = f(s)h$ for all $h \in G$. Need to find $g \in G$ such that $f(s) = gs$. Take $s = 1$, $f(1) = g1 = g$ so $g = f(1)$. If $g = f(1)$, then $f(s) = gs$ since $gs = (f(1))s = f(1s) = f(s)$.
So we have G = symmetries of (Set G + right G action)

Example 1.1.5. G=symmetries of rectange, set $S = G$



	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

We get the graph:



Cayley graph: Point for each $g \in G$ Draw a line from g to h with $gf = h$.

Goal of Group theory

1. Classify all groups
   - Hard but can do special cases: Groups of order 60, finite subgroups of rotations in $\mathbb{R}^3$, all finite simple groups, symmetries of crystals
2. Given a group G, classify all ways G can act on something (called a representation of G)
   - Permutation representation : G acts on a set S
   - Linear representation : G acts on a vector space

Example 1.1.6. Poncaire group = symmetries of space time
elementary particle: space of states = vector space acted on by G = linear group of G

1.1.2 Review of homomorphisms, isomorphims

Definition 1.1.7. A homomorphism is a map $f : G \to H$ that preserves structure
eg. $f(gh) = f(g)f(h)$, $f(1) = 1$, $f(g^{-1}) = f(g)^{-1}$

Note: last two properties can be derived from the first.

Example 1.1.8. $\exp(x) = e^x : (\mathbb{R}, +) \to (\mathbb{R}, \times)$
$\exp(x + y) = \exp(x)\exp(y)$, $\exp(0) = 1$, $\exp(-x) = \exp(x)^{-1}$

Definition 1.1.9. The kernel of a homomorphism f is the set of elements with image the identity.

Example 1.1.10. $\mathbb{R} \to$ rotation is the plane by $\theta \mapsto$ rotation by angle θ.
nontrivial kernel : multiples of 2π.
We get the short exact sequence: $0 \to 2\pi\mathbb{Z} \to \mathbb{R} \to \text{rotations} \to 0$

Definition 1.1.11. A sequence of homomorphisms $A \to B \to C$ is exact if Image $A \to B$ = Kernel $B \to C$

$0 \to A \to B$ means $A \to B$ is injective
$A \to B \to 0$ means $A \to B$ is surjective

Definition 1.1.12. $f : A \to B$ is an isomorphim if it is a homomorphism with an inverse. We say A, B are isomorphic. "basically the same"

Example 1.1.13. $2\pi\mathbb{Z}$ is isomorphic to $\mathbb{Z}$.

Example 1.1.14. $\mathbb{Z}/4\mathbb{Z}$, integers mod 4 with addition: $\{0, 1, 2, 3\}$ and $(\mathbb{Z}/5\mathbb{Z})^\times$, under multiplcation: $\{1, 2, 3, 4\}$ are isomorphic.
We map $0 \to 1 = 2^0$, $1 \to 2 = 2^1$, $2 \to 4 = 2^2$, $3 \to 3 = 2^3$ eg. $x \mapsto 2^x$

1.1.3 Classify all finite groups up to isomorphim

Definition 1.1.15. The order of a group G = number of elements in G

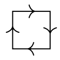
Order 1: $e \times e = e$ 1 group - trivial group
Order 2: 1 group - e, f with $f^2 = e \cong \mathbb{Z}/2\mathbb{Z}$
Order p for p prime: only one group $\mathbb{Z}/p\mathbb{Z}$ (integers modulo p)

Definition 1.1.16. For $g \in G$ the order of g is the smallest $n \geq 1$ with $g^n = 1$

Theorem 1.1.17 (Lagrange's Theorem)**.** If $g \in G$, the roder of g divides the order of G.

Example 1.1.18. Suppose $|G| = p$, (p prime). Pick $g \in G$ with $g \neq e$. Order of g divides $|G| = p$ so is either 1 or p. Can't be one since $g \neq e$. So elemenets of G $1, g, \ldots, g^{p-1}$ are all distinct since $g^p = 1$, $g^x \neq 1$ for $0 \leq x < p$ and if $g^i = g^j, g^{i-j} = 1$. Thus, these must be all elements of G.

Order 4:

- Ex : $\mathbb{Z}/4\mathbb{Z}$, symmetries of rectangle, $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/8\mathbb{Z})^\times$, symmetries of 
- only 2 groups of order 4

1.2 August 30

1.2.1 Langrange's Theorem

Order 4: $\mathbb{Z}/4\mathbb{Z}$, symmetries of rectangle
How to show not isomorphic?
Find some property (preserved by isomorphism) that one group has but the other does not.

Property: Order of elements

- in $\mathbb{Z}/4\mathbb{Z}$, 0, 1, 2, 3 have orders 1, 4, 2, 4 respectively
- all nontrivial elements of the group of symmetries of the rectangle have order 2

Note: counting elements of each order works for small gorups but 2 groups of order 16 with same number of elements of each order

Classification: By Lagrange's theorem, each element has order 1, 2, or 4

1. Have an element of order 4: g, group $= \{1, g, g^2, g^3\} \cong \mathbb{Z}/4\mathbb{Z}$
   In general, if a group of n elements has an element of order n, it is $\cong \mathbb{Z}/4\mathbb{Z}$
2. All elements have order 1 or 2.
   Suppose G is finite and has this property. Then G commutes since $(gh)^2 = ghgh = 1 = g^2g^2$ so $gh = hg$.
   Note: only true for prime 2, there is a group of order 27 such that all elements have order 1 or 3 but is not commutative
   Write group operation as $+$. G is a vector space over $\mathbb{F}_2$ (field of 2 elements). So $G \cong \mathbb{F}_2^k$ for osme set $|G| = 2^k$. We get 1 group of order 4 with all elements of order 1 or 2.

Group of order 4 is product of 2 groups, $\mathbb{F}_2^2 = \mathbb{F}_2 \oplus \mathbb{F}_2$.
Suppose G, H are gorups, $G \times H$ is a gorup under operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1g_2, h_1h_2)$

Example 1.2.1. $\mathbb{C}^\times \cong \mathbb{R}_{\geq 0} \times S^1$, $z = |z| \cdot e^{i\theta}$

Chinese Remainder Theorem: (m, n) coprime, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
We have maps $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $g : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. This gives $h : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. If $(m, n) = 1$, then the map is injecitve since if $h(k) = 0$, $k \equiv 0 \mod m, \mod n$

Infinite Products: $G_1 \times G_2 \times G_3 \times \cdots$, set of all elements $(g_1, g_2, g_3, \ldots,)$
Infinite Sums: Like infinite products but all but finitely many of g_1 are 1.

Example 1.2.2. Roots of $1 = e^{2\pi q}$, $q \in \mathbb{Q}$.
Infinite sum $G_2 + G_3 + G_5 + G_7 + G_11 + \cdots$ (G_p = roots of order p^n for some $n \geq 1$)

Symmetry of Platonic Solids

Faces	Name	Rotations	Rotations + Reflections	
4	tetrahedron	$12 = 4 \times 3$	24	$\to$ not a product
6	hexahedron (cube)	$24 = 6 \times 4$	48	product $\mathbb{Z}/2\mathbb{Z} \times$ rotations
8	octahedron	$24 = 8 \times 3$	48	
12	dodecahedron	$60 = 12 \times 5$	120	
20	icosahedron	$60 = 20 \times 3$	120	

All except tetrahedron have symmetry $\begin{pmatrix} -1 & & \\ & -1 & \\ & & -1 \end{pmatrix}$ fo reflections in $\mathbb{R}^3$, so it commutes with everything

For the tetrahedron, we have $\begin{pmatrix} -1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$

Order 5: $\mathbb{Z}/5\mathbb{Z}$

Exercise 1.2.3. Find a graph as small as possible with symmetries $\mathbb{Z}/5\mathbb{Z}$

Order 6: 3 obvious examples: $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, symmetries of the triangle

- $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
- group of symmetries of the triange is not abelian
  Permutation Notation: $(5\,2\,1\,3)$ = function sending $5 \to 2$, $2 \to 1$, $1 \to 3$, $3 \to 5$
  (Insert Figure)
  $(1\,2)(2\,3) = (1\,2\,3)$ but $(2\,3)(1\,2) = (1\,3\,2)$

Definition 1.2.4. A subgroup of a group G, is a subset closed under group operations.

Theorem 1.2.5 (Lagrange's Theorem)**.** If H is a subgroup of G, $|H|$ divides $|G|$.

Special Case: If $H =$ powers of g, $1, g, g^2, \ldots, g^{n-1}$, $|H| = |g|$

Construction of subgorups: Pick a set S acted on by G, pick $s \in S$.
H: elements g with $gs = s$ (elements fixing s). Then H is a subgroup.
Lagrange (Converse to Cayley's Thm): If H is a subgroup of G we can find a set acted on by G, such that H=elements fixing $s \in S$.

Given a gorup G, subgroup H. We want to construct: a set S acted on by G.
Consider G=symmetries of triangle, $H = \{(1)(2)(3), (2\,3)\}$ fixing 1.
How do we write 1, 2, 3 in terms of G, H?
Left cosets of H: $1 \leftrightarrow$ elements g with $g(1) = 1$ (H), $2 \leftrightarrow$ elements g with $g(1) = 2$ ($(1\,2)H$), $3 \leftrightarrow$ elements g with $g(1) = 3$ ($(1\,3)H$)

Left cosets of H are sets of the from aH (some fixed $a \in G$).
Define $g_1 \approx g_2$ if $g_1 = g_2 h$ for some $h \in H$. This is an equivalence relation:
Reflexivity: $g_1 \approx g_1$ group identity, 1
Symmetry: $g_1 \approx g_2 \to g_2 \approx g_1$ group inverses, h^{-1}
Transitivity: $g_1 \approx g_2, g_2 \approx g_3 \to g_1 \approx g_3$ group operation, $h_1 h_2$
$G =$ disjoint union of cosets (equivalence classes of $\approx$) and any two cosets have the same same $|H|$ since we have a bijection $H \to aH$ byb $h \mapsto ah$ with inverse $h \mapsto a^{-1}h$.
So $G = \#$ cosets $\times$ size of cosets $= \#$ elements of S $\times$ |subgroup of elements fixing s|
Note: We assume S is transisitve - if $s_1, s_2 \in S$. $g(s_1) = s_2$ for some g

Rotations of a dodecahedron: 12 (faces) $\times$ 5 = 20 (vertices) $\times$ 3 = 30 (edges) $\times$ 2 = 60

Conways Group: has order 8315553613086720000
Acting on Frames: # 8252375 Group fixing each frame: 1002795171840

Special Cases of Lagrange:

- Fermat: $a^p \equiv a \mod p$ (p prime), $a^{p-1} \equiv 1 \mod p$ $(a, p) = 1$
  Group $(\mathbb{Z}/p\mathbb{Z})^\times$ integers modulo p under $\times$ has order $p - 1$.
  Lagrange: order of a divides $p - 1$ so $a^{p-1} \equiv 1$

- Euler: $a^{\varphi(m)} \equiv 1 \mod n$ $(a, m) = 1$
  $(\mathbb{Z}/m\mathbb{Z})^\times$= group of elements coprime to m, mod m, order $= \varphi(m)$

$m = 8$: $\varphi(m) = 4$, $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$. Euler $a^4 \equiv 1 \mod 8$ (a odd) but we see $a^2 \equiv 1 \mod 8$

Right Cosets: $Ha \leftrightarrow$ elements of a set acted on, on the right by G. $S \times G \to S$
Are left cosets the same as right cosets? sometimes

Example 1.2.6. Take $G =$ symmetries of triangle. $H = \{1, (2\,3)\}$. Find the left, right costs of H in G.
Left: $H = \{1(2\,3)\}, (3\,1)H = \{(3\,1), (3\,2\,1)\}, (1\,2)H = \{(1\,2), (1\,2\,3)\}$
Right: $H = \{1(2\,3)\}, (3\,1)H = \{(3\,1), (1\,2\,3)\}, (1\,2)H = \{(1\,2), (3\,2\,1)\}$
so left cosets $\neq$ right cosets

Definition 1.2.7. Index of H in G, $[G : H]$= # cosets of H in G.

Left or right cosets? $[G : H][H] = |G|$ when G finite so # left cosets = # right cosets.
In gernal, right cosets $\to$ left cosets by $Ha \mapsto a^{-1}H$ so # left cosets = # right cosets

1.2.2 Normal Subgroups

G/H = set of left coset of G. Is G/H a group?
How to definte $(g_1H) \times (g_2H)$? g_1g_2H
Problem: not well defined - suppose we have g_1, g_2, g_1h_1, g_2h_2. Want $g_1g_2H = g_1h_1g_2h_2H$
Is $h_1g_2 = g_2(h \in H)$? not in general
Want: $ghg^{-1} \in H$ for all $g \in G$. If this holds, then we can turn G/H into a group.

Definition 1.2.8. If H satisfies the above property, H is called a normal subgroup of G.

Example 1.2.9. G = symmetries of triangle. $H = \{(2\,3), 1\}$. Is H normal?
$(1\,2)(2\,3)(1\,2)^{-1} = (1\,3) \notin H$ so H is not normal

What about $H = \{1, (1\,2\,3), (1\,3\,2)\}$. Is H normal?
H has index 2 in G. $[G : H] = \frac{|G|}{|H|} = 2$. We claim any subset of order 2 is normal.
There are only 2 left cosets: H, things not in H. Similarly for right cosets. So right cosets = left cosets. So H is normal.

Classifying Groups of Order 6

- orders of elements 1, 2, 3, 6
- If element of order 6, group must be cyclic
- Want element of order 3

Lagrange: order of element divides order of group
Converse: If n divides $|G|$, does G have a subgroup of order n?
No: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has no element of order 4
Yes: if n is prime (Cayley)
So G has elements a, b of order 2,3 and subset $(1, b, b^2)$ has order 2 so it is normal.