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

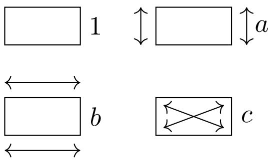
What are the symmetries of this?
Bijection $f : S \to S$ preserving the right G-action. eg. $f(sg) = f(s)g$
Need to check:

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

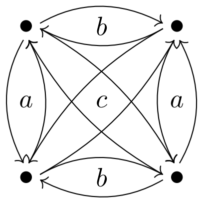
Check (2): Suppose $f : S \to S$ preserves the right G-action, $f(sh) = f(s)h$ for all $h \in G$. Need to find $g \in G$ such that $f(s) = gs$. Take $s = 1$, $f(1) = g1 = g$ so $g = f(1)$. If $g = f(1)$, then $f(s) = gs$ since $gs = (f(1))s = f(1s) = f(s)$.
So we have G = symmetries of (Set G + right 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 (Insert Figure)
- only 2 groups of order 4