

# MATH 250A: Groups, Rings, and Fields

Jad Damaj

Fall 2022

# Contents

<b>1</b>	<b>Groups</b>	<b>3</b>
1.1	August 25 . . . . .	3
1.1.1	Groups . . . . .	3
1.1.2	Review of homomorphisms, isomorphisms . . . . .	5
1.1.3	Classify all finite groups up to isomorphism . . . . .	6
1.2	August 30 . . . . .	6
1.2.1	Langrange's Theorem . . . . .	6
1.2.2	Normal Subgroups . . . . .	9
1.3	September 1 . . . . .	9
1.3.1	Semidirect Products . . . . .	9
1.3.2	Cauchy's Theorem . . . . .	10
1.3.3	Burnside's Lemma . . . . .	12
1.4	September 6 . . . . .	12
1.4.1	Burnside's Lemma . . . . .	12
1.4.2	Groups of order $p^2$ . . . . .	13
1.4.3	Dihedral Groups . . . . .	14

# 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  $X \rightarrow X$  with inverse that preserves “structure” (topology, order, binary operation, ...)

**Example 1.1.1.** The rectangle has 4 symmetries.

The icosaahedron has  $20 \times 3$  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  $G \times G \rightarrow G$  by  $(a, b) \mapsto ab, a \times, a + b, \dots$  with “Inverse” :  $G \rightarrow G$  by  $a \mapsto a^{-1}$  and “Identity”:  $1, 0, e, I, \dots$  satisfying 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 by “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) group action is a map  $G \times S \rightarrow S$  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  $G$  on  $G$ . There are 8 natural ways to do this.

First 4, we define  $G \times S \rightarrow S$  by

- $g(s) = s$  trivial action
- $g(s) = gs$  group product
- Try  $g(s) = sg$  Fails since  $G$  not necessarily 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 :  $S \times G \rightarrow S$  by  $(s, g) \mapsto (s)g, s^g$  satisfying  $(sg)h = s(gh), s1 = s$ .

We now define right group actions of  $G$  on  $G$ :  $S \times G \rightarrow G$  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 on the right on  $S$  (Structure of  $S$ )

Object  $S = S$  + right  $G$  action

What are the symmetries of this?

Bijection  $f : S \rightarrow S$  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  $G$

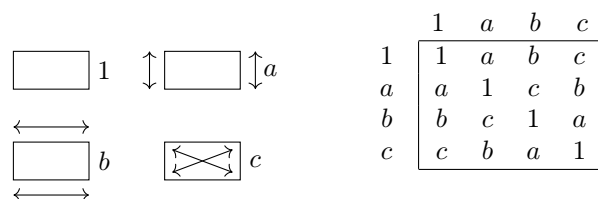
Check (1): For  $g \in G$  need  $(gs)h = g(sh)$ , follows by commutativity

Note: left  $G$ -action does not preserve right  $G$ -action:  $g(hs) \neq h(gs)$  in general

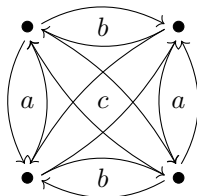
Check (2): Suppose  $f : S \rightarrow S$  preserves the right  $G$ -action,  $f(sh) = f(s)h$  for all  $h \in G$ . Need to find  $g \in G$  such that  $f(s) = gs$ . Take  $s = 1$ ,  $f(1) = g1 = g$  so  $g = f(1)$ . If  $g = f(1)$ , then  $f(s) = gs$  since  $gs = (f(1))s = f(1s) = f(s)$ .

So we have  $G =$  symmetries of (Set  $G$  + right  $G$  action)

**Example 1.1.5.**  $G$ =symmetries of rectangle, set  $S = G$



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, isomorphisms

**Definition 1.1.7.** A homomorphism is a map  $f : G \rightarrow H$  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.**  $\exp(x) = e^x : (\mathbb{R}, +) \rightarrow (\mathbb{R}, \times)$

$\exp(x + y) = \exp(x)\exp(y)$ ,  $\exp(0) = 1$ ,  $\exp(-x) = \exp(x)^{-1}$

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

**Example 1.1.10.**  $\mathbb{R} \rightarrow$  rotation in the plane by  $\theta \mapsto$  rotation by angle  $\theta$ .

nontrivial kernel : multiples of  $2\pi$ .

We get the short exact sequence:  $0 \rightarrow 2\pi\mathbb{Z} \rightarrow \mathbb{R} \rightarrow \text{rotations} \rightarrow 0$

**Definition 1.1.11.** A sequence of homomorphisms  $A \rightarrow B \rightarrow C$  is exact if  $\text{Image } A \rightarrow B = \text{Kernel } B \rightarrow C$

$0 \rightarrow A \rightarrow B$  means  $A \rightarrow B$  is injective

$A \rightarrow B \rightarrow 0$  means  $A \rightarrow B$  is surjective

**Definition 1.1.12.**  $f : A \rightarrow B$  is an isomorphism 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 multiplication:  $\{1, 2, 3, 4\}$  are isomorphic.

We map  $0 \rightarrow 1 = 2^0, 1 \rightarrow 2 = 2^1, 2 \rightarrow 4 = 2^2, 3 \rightarrow 3 = 2^3$  eg.  $x \mapsto 2^x$

### 1.1.3 Classify all finite groups up to isomorphism

**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 order 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 elements of  $G$   $1, g, \dots, g^{p-1}$  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 Lagrange’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 groups 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  $\cong \mathbb{Z}/n\mathbb{Z}$
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 some 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 groups,  $G \times H$  is a group 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  $f : \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ ,  $g : \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ . This gives  $h : \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ . If  $(m, n) = 1$ , then the map is injective since if  $h(k) = 0$ ,  $k \equiv 0 \pmod{m}$ ,  $k \equiv 0 \pmod{n}$

Infinite Products:  $G_1 \times G_2 \times G_3 \times \dots$ , set of all elements  $(g_1, g_2, g_3, \dots)$

Infinite Sums: Like infinite products but all but finitely many of  $g_i$  are 1.

**Example 1.2.2.** Roots of  $1 = e^{2\pi i q}$ ,  $q \in \mathbb{Q}$ .

Infinite sum  $G_2 + G_3 + G_5 + G_7 + G_11 + \dots$  ( $G_p$  = 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	$\rightarrow$ not a product
6	hexahedron (cube)	$24 = 6 \times 4$	48	} product $\mathbb{Z}/2\mathbb{Z} \times \text{rotations}$
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  $\begin{pmatrix} -1 & & \\ & -1 & \\ & & -1 \end{pmatrix}$  for 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 triangle is not abelian  
Permutation Notation:  $(5\ 2\ 1\ 3)$  = function sending  $5 \rightarrow 2, 2 \rightarrow 1, 1 \rightarrow 3, 3 \rightarrow 5$   
(Insert Figure)  
 $(12)(23) = (123)$  but  $(23)(12) = (132)$

**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  $g$ ,  $1, g, g^2, \dots, g^{n-1}$ ,  $|H| = |g|$

Construction of subgroups: 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 group  $G$ , subgroup  $H$ . We want to construct: a set  $S$  acted on by  $G$ .

Consider  $G$ =symmetries of triangle,  $H = \{(1)(2)(3), (23)\}$  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  $g(1) = 2$  ( $(12)H$ ),  $3 \leftrightarrow$  elements  $g$  with  $g(1) = 3$  ( $(13)H$ )

Left cosets of  $H$  are sets of the form  $aH$  (some fixed  $a \in G$ ).

Define  $g_1 \approx g_2$  if  $g_1 = g_2h$  for some  $h \in H$ . This is an equivalence relation:

Reflexivity:  $g_1 \approx g_1$  group identity, 1

Symmetry:  $g_1 \approx g_2 \rightarrow g_2 \approx g_1$  group inverses,  $h^{-1}$

Transitivity:  $g_1 \approx g_2, g_2 \approx g_3 \rightarrow g_1 \approx g_3$  group operation,  $h_1h_2$

$G$  = disjoint union of cosets (equivalence classes of  $\approx$ ) and any two cosets have the same size  $|H|$  since we have a bijection  $H \rightarrow aH$  by  $h \mapsto ah$  with inverse  $h \mapsto a^{-1}h$ .

So  $G = \# \text{ cosets} \times \text{size of cosets} = \# \text{ elements of } S \times |\text{subgroup of elements fixing } s|$

Note: We assume  $S$  is transitive - if  $s_1, s_2 \in S$ .  $g(s_1) = s_2$  for some  $g$

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

Conways Group: has order 831555361308172000

Acting on Frames:  $\# 8252375$  Group fixing each frame: 1002795171840

Special Cases of Lagrange:

- Fermat:  $a^p \equiv a \pmod{p}$  ( $p$  prime),  $a^{p-1} \equiv 1 \pmod{p}$  ( $a, p$ ) = 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:  $a^{\varphi(m)} \equiv 1 \pmod{m}$  ( $a, m$ ) = 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  $a^4 \equiv 1 \pmod{8}$  ( $a$  odd) but we see  $a^2 \equiv 1 \pmod{8}$

Right Cosets:  $Ha \leftrightarrow$  elements of a set acted on, on the right by  $G$ .  $S \times G \rightarrow S$

Are left cosets the same as right cosets? sometimes

**Example 1.2.6.** Take  $G$  = symmetries of triangle.  $H = \{1, (23)\}$ . Find the left, right cosets of  $H$  in  $G$ .

Left:  $H = \{1(23)\}$ ,  $(31)H = \{(31), (321)\}$ ,  $(12)H = \{(12), (123)\}$

Right:  $H = \{1(23)\}$ ,  $(31)H = \{(31), (123)\}$ ,  $(12)H = \{(12), (321)\}$

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 general, right cosets  $\rightarrow$  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 define  $(g_1H) \times (g_2H)$ ?  $g_1g_2H$

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.  $H = \{(23), 1\}$ . Is  $H$  normal?

$(12)(23)(12)^{-1} = (13) \notin H$  so  $H$  is not normal

What about  $H = \{1, (123), (132)\}$ . 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 (Cauchy)

So  $G$  has elements  $a, b$  of order 2, 3 and subset  $\langle 1, b, b^2 \rangle$  has order 3 so it is normal.

## 1.3 September 1

### 1.3.1 Semidirect Products

#### Groups of Order 6:

2 subgroups  $A, B$  of order 2, 3  $|A| \cdot |B| = |G|$ ,  $A \cap B = \{e\}$

In general, suppose that for a group  $G$ , subgroups  $A, B$

1.  $|G| = |A| \cdot |B|$
2.  $A \cap B = \{e\}$

Want to reconstruct  $G$  from  $A, B$

$G = AB = \{ab \mid a \in A, b \in B\}$ ,  $\#$  pairs  $(a, b) = |G|$

If  $a_1b_1 = a_2b_2$ ,  $a_2^{-1}a_1 = b_2b_1^{-1} \in A \cap B = \{e\}$  so  $a_1 = a_2, b_1 = b_2$   
 Every element of  $G$  can be written uniquely as a product of  $a \in A, b \in B$

Problem: What is  $a_1b_1 \cdot a_2b_2$ ?  $= a_3b_3$

Easy case:  $ab = ba$  for all  $a \in A, b \in B$   $(a_1b_1)(a_2b_2) = (a_1a_2)(b_1b_2)$

We can view  $G$  as the product of  $A, B \rightarrow G = A \times B$

Slightly less easy case:  $A$  is a normal subgroup of  $G$ . We get an action of the group  $B$  on the group  $A$ .

Define the action of  $B$  on  $A$  by  $b(a) = bab^{-1} \in A$  ( $A$  normal)

This determines the product on  $G$ .  $(a_1b_1)(a_2b_2) = a_1(b_1a_2b_1^{-1})b_1b_2 = \underbrace{a_1b_1(a_2)}_{\in A} \times \underbrace{b_1b_2}_{\in B}$ .

Suppose given groups  $A, B$  action of  $B$  on  $A$ . We construct the semidirect product of  $A$  and  $B$ ,  $A \rtimes B$  on the set  $A \times B$  with the product given by  $(a_1, b_1)(a_2, b_2) = (a_1b_1(a_2), b_1b_2)$ . We can check this is a group.

### Order 6

So  $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$  defined by the action of  $\mathbb{Z}/2\mathbb{Z}$  on  $\mathbb{Z}/3\mathbb{Z}$ .

$\text{Sym}(\mathbb{Z}/3\mathbb{Z})$ : either  $f(1) = 1$  or  $f(1) = 2$  so only two possible homomorphisms  $\mathbb{Z}/2\mathbb{Z} \rightarrow \text{Sym}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ : identity and trivial homomorphisms

So groups of order 6:

- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  trivial action  $\cong \mathbb{Z}/6\mathbb{Z}$
- $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$  nontrivial action  $\cong S_3$

### 1.3.2 Cauchy's Theorem

**Theorem 1.3.1** (Cauchy's Theorem). If  $p \mid |G|$  ( $p$  prime),  $G$  has an element of order  $p$ .

**Proof.** We use induction on the size of the group: can assume true for any proper subgroups and quotient groups

$G$  abelian: pick  $g \in G$ . If  $p \mid |g|$ ,  $g$  has order  $pn$  so  $g^n$  has order  $p$ .

If  $p \nmid |g|$ , look at  $G/\langle g \rangle$ .  $\langle g \rangle$  normal since  $G$  is abelian,  $p$  divides  $|G/\langle g \rangle|$ . Pick  $h \in G/\langle g \rangle$ , order divisible by  $p$ . Lift  $h_1$  in  $G$ . Then  $p \mid |h_1|$ .

Standard Error: Can't always lift  $h$  to element of the same order

$G \cong \mathbb{Z}/4\mathbb{Z}$ ,  $g = 2$ .  $G/\langle g \rangle$  has order 2 so take nontrivial element. Its lift does not have order 2 in  $G$

**Definition 1.3.2.** The center of  $G$  is the elements that commute with all elements of  $G$ .

**Lemma 1.3.3.** Suppose  $G$  is nontrivial, all proper subgroups have index divisible by  $p$ . Then the center of  $G$  is divisible by  $p$ .

**Proof.** Look at left action of  $G$  on itself by conjugation.  $G =$  union of orbits where  $a, b$  in the same orbit if there is some  $g$  such that  $g(a) = b$ .  $|G| = \sum(\text{size of orbits})$

Size of orbit  $= |G|/\text{subgroup of elements fixing a point}$ . Either 1 or divisible by  $p$  so

$G = \underbrace{1 + 1 + 1}_{\text{size } 1} + \cdots + \underbrace{pn_1 + pn_2}_{\text{size } > 1} + \cdots$ . Since  $G$  divisible by  $p$  # orbits with one element is. Theorem follows

since Center of  $G$  = elements with orbit of size 1.

**Proof** (Cauchy's Theorem (Cont)). Case 1: Some proper subgroup has order divisible by  $p$ .

Such a subgroup has an element of order divisible by  $p$  by induction.

Case 2: All proper subgroups have index divisible by  $p$ . By lemma, center of  $G$  has order divisible by  $p$ .

Center of  $G$  is abelian so it has an element of order  $p$ .

**Order 7:**  $\mathbb{Z}/7\mathbb{Z}$

**Order 8:** Obvious examples: Product  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\mathbb{Z}/8\mathbb{Z}$ , symmetries of a square ( $D_8$ ) - dihedral group.

Orders of elements: 1, 2, 4, 8

- If element has order 8, group is cyclic
- If all elements have order 1 or 2, group is vector field over  $\mathbb{F}^2$  so is  $(\mathbb{Z}/2\mathbb{Z})^2$

So can assume  $G$  has an element  $a$ , of order 4.  $a^4 = 1$ . Subgroup  $A = \{1, a, a^2, a^3\}$  has index 2 so is normal.

Quotient group has order 2 so  $\cong \mathbb{Z}/2\mathbb{Z}$

We have an exact sequence  $1 \rightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow G \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 1$

Problem: Given  $1 \rightarrow A \rightarrow G \rightarrow B \rightarrow 1$  How to construct  $G$  from  $A, B$ ?

Possibilities:  $G = A \times B$ , or  $A \rtimes B$ , not always the case:

- $1 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 1$  not a semidirect product
- $1 \rightarrow \mathbb{Z}/3\mathbb{Z} \rightarrow S_3 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 1$   $S_3 = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

We get an action of  $B$  on  $A$  by conjugation so considering  $1 \rightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow G \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 1$  we can take the nontrivial element  $b$  of  $\mathbb{Z}/2\mathbb{Z}$ . Can't say  $b^2 = 1$ , but  $b^2 \in A$ . Also  $B$  acts on  $A$  by conjugation.

So we have  $\mathbb{Z}/4\mathbb{Z} = \{1, a, a^2, a^3\}$   $a \mapsto bab^{-1}$ :  $a \mapsto a$  or  $a \mapsto a^{-1}$

Possibilities:

	$bab^{-1} = a$	$bab^{-1} = a^{-1}$	
$b^2 = 1$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$D_8$	Semidirect Products $a = b^2, ab = ba \rightarrow a^2 = 1$
$b^2 = a, b^2 = a^3$	$\mathbb{Z}/8\mathbb{Z} (a = 1, b = 2)$	Impossible	
$b^2 = a^2$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	Quaternions	

Quaternion group: generated by  $a, b$  with  $a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1}$

Does it exist? Yes: have been viewed in  $M_2(\mathbb{C})$ -  $a = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Usually denote elements:  $I = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}, J = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, K = IJ = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

Quaternions  $Q_8 = \{i, I, J, J, -1, -I, -J, -K\}$  satisfying  $I^2 = J^2 = K^2 = 1, IJ = K, JK = 1, KI = J$

Hamilton's Quaternions ( $H$ ) = all numbers  $a + bi + cj + dk$   $a, b, c, d$  real

Nonzero elements of  $H$  form a group. Problem: Show inverses exist.

$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2 > 0$  so

$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$

Can also look at  $S^3 \subset H = \{a + bi + cj + dk \mid a^2 + b^2 + c^2 + d^2 = 1\}$

For  $z = a + bi + cj + dk, \bar{z} = a - bi - cj - dk$  let  $z\bar{z} = N(z)$

We see  $N(z_1 z_2) = N(z_1)N(z_2)$  so if  $N(z) = 1$  closed under  $\times$  so is a group.

Only spheres that are a group are  $S^0, S^1, S^3$ . Elements of  $\mathbb{R}, \mathbb{C}, H$  with absolute value 1.

Note:  $Q_8 \subseteq S^3$

### 1.3.3 Burnside's Lemma

Problem: How many ways to arrange 8 rooks on a chess board so that no 2 attack each other?

8 ways for first row, 7 for second,  $\dots$ , so  $8! = 40320$  total

Suppose we want to count them up to symmetry:

- For  $3 \times 3$ : (Insert Figure)  
can only have 2

Approximate number =  $\frac{\text{total \# of elements}}{\text{order of group}} = \frac{8!}{8} = 7! = 5050$

General problem: Suppose we have a group  $G$  acting on a set  $S$ . How many orbits?  $\geq \frac{|S|}{|G|}$

Answer:

**Lemma 1.3.4** (Burnside's Lemma). # of orbits = average number of fixed points of  $g \in G$ , eg.  $s \in S$  with  $g(s) = s$

**Proof.** Count number of pairs  $(g, s) \in G \times S$  with  $g(s) = s$  in 2 ways:

1. Sum over  $G$ :  $\sum_{g \in G} (\# \text{ fixed by } g)$
2. Sum over  $S$ : Each orbit contributes (size of orbit)  $\times$  (# of elements fixing a point) =  $|G|$   
so sum =  $|G| \times \# \text{ of orbits}$

So # of orbits =  $\frac{1}{|G|} \sum_g \# \text{ fixed points} = \text{avg } \# \text{ fixed points}$

## 1.4 September 6

### 1.4.1 Burnside's Lemma

**Example 1.4.1.** Find the number of ways to arrange 8 nonattacking rooks on a chessboard up to symmetry.

Recall - # of orbits of a set = average number of fixed points =  $\frac{1}{|G|} \sum_{g \in G} \# \text{ fixed points of } g$ .

$G$  = dihedral group  $D_8$ , acting on  $8! = 40320$  ways to arrange 8 rooks

Elements of  $D_8$ :

- Trivial (Insert Figure):  $8! = 40320$
- $180^\circ$  rotation (Insert Figure) : 8 options for 1rst, 6 options for 2cnd,  $\dots$  so  $8 \times 6 \times 4 \times 2$
- $90^\circ$  rotation (Insert Figure): 6 options for 1rst, 2 options for 2cnd so  $6 \times 2$

2 elements  $g_1, g_2$  are called conjugate if  $g_1 = gg_2g^{-1}$  for some  $g$  (Formalizes notion of "looks the same")

$g_1$  = (Insert Figure)  $g_2$  = (Insert Figure)  $g$  = (Insert Figure) exchanging  $g_1, g_2$ .

If two elements are conjugate then they have the same number of fixed points.

$g_1(s) = s \rightarrow g_2(gs) = gg_1g^{-1}gs = gs$

- (Insert Figure): conjugate with  $90^\circ$  rotation so  $6 \times 2$

- (Insert Figure): conjugate and have 0 since rotates rook to the same column/row
- (Insert Figure): conjugate.  $C_n = \#$  ways to place rooks on  $n \times n$  chessboard invariant under transformation.  $c_0 = 1, c_1 = 1$ .  
Case 1 : (Insert Figure) Case 2: (Insert Figure)  
so  $c_n = c_{n-1} + (n-1)c_{n-2}$  and  $c_n = 1, 1, 2, 4, 10, 26, 76, 232, 764$

So # of ways to place rooks =  $\frac{1}{8}(1 \times 8! + 1 \times 384 + 2 \times 12 + 2 \times 0 + 2 \times 764) = 5282$   
Slightly more than original guess  $\frac{40320}{8} = 5040$

**Example 1.4.2.** Find the number of ways to color a cube with  $n$  different colors up to symmetry.

### 1.4.2 Groups of order $p^2$

**Order 9:** Obvious examples =  $\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Classify all groups of order  $p^2$  ( $p$  prime): only ex are  $\mathbb{Z}/p^2\mathbb{Z}, (\mathbb{Z}/p\mathbb{Z})^2$

(1): Every group of order  $p^n$  ( $p$  prime,  $n > 0$ ) has nontrivial center

*Proof.* Recall, if all proper subgroups have index divisible by  $p$ ,  $p \mid |G|$  then  $G$  has nontrivial center. So if  $|G| = p^n$ ,  $n > 0$ , we see  $G$  has nontrivial center.  $\square$

Implies that if  $|G| = p^n$ ,  $G$  is nilpotent. ie. repeatedly modding out by the center gives you the trivial group.  $G_0 = G, G_1 = G_0/Z(G_0), G_2 = G_1/Z(G_1), \dots$  If  $G_n$  is trivial for some  $n$ ,  $G$  is called nilpotent.

This gives an exact sequence:  $1 \rightarrow Z(G_i) \rightarrow G_i \rightarrow G_{i+1} \rightarrow 1$

Note: A group may still have nontrivial center even after modding out by the original center:  $G = D_8, G/Z(G) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

$S_3$  (order 6) is not nilpotent

(2): If  $G/Z(G)$  is cyclic then  $G$  is abelian.

*Proof.* Consider  $1 \rightarrow Z(G) \rightarrow G/Z(G) \rightarrow 1$ .  $Z/(G)$  is powers of  $g_1$ , lift  $g_1$  to  $g$  in  $G$ .

Every element in  $G$  is of the form  $zg^n$  ( $z \in \text{center}$ ) so all commute  $z_1g^{n_1}, z_2g^{n_2}$ :

$z_1$  commutes with  $z_2g^{n_2}$ ,  $g^{n_1}$  commutes with  $z_2$ , and  $g^{n_1}$  commutes with  $g^{n_2}$   $\square$

(3): Every group of order  $p^2$  is abelian.

Note: not true for  $p^3$ , consider  $D_8, Q_8$  of order  $2^3$

*Proof.* Center is nontrivial so has order  $\geq p$ .  $G/Z(G)$  has order 1 or  $p$  so it is cyclic so  $G$  is abelian.  $\square$

(4): Every group of order  $p^2$  is  $(\mathbb{Z}/p^2\mathbb{Z})$  or  $(\mathbb{Z}/p\mathbb{Z})^2$

*Proof.* Case 1 : elements of order  $p^2 \rightarrow G$  is cyclic  $\cong \mathbb{Z}/p^2\mathbb{Z}$

Case 2: all elements have order  $p$  or 1  $\rightarrow G$  abelian.  $G$  is really a vector field over  $\mathbb{F}_p$  the field with  $p$  elements so  $G = \mathbb{F}_p \oplus \mathbb{F}_p$ .  $\square$

### 1.4.3 Dihedral Groups

**Order 10:**  $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ,  $D_{10} = (\mathbb{Z}/5\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$

Groups of Order  $2p$ :  $G$  has a subgroup of order  $p$ , index 2 so is normal.  $G$  has a subgroup of order 2 so  $G \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ , determined by action of  $\mathbb{Z}/2\mathbb{Z}$  on  $\mathbb{Z}/p\mathbb{Z}$ .

Symmetries of  $\mathbb{Z}/p\mathbb{Z}$ : map generator  $1 \rightarrow$  element of order  $p$ .  $n \mapsto na \pmod{p}$

Symmetries =  $(\mathbb{Z}/p\mathbb{Z})^\times$  nonzero integers mod  $p$  under  $\times$ . Only elements of order 2 are  $\pm a \pmod{p}$

$G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  (trivial action of  $\mathbb{Z}/2\mathbb{Z}$  on  $\mathbb{Z}/p\mathbb{Z}$ )

$G \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$  ( $\mathbb{Z}/2\mathbb{Z}$  acting by  $-1$  on  $\mathbb{Z}/p\mathbb{Z}$ ) = dihedral group.

Dihedral Groups: symmetries of a regular  $n$ -gon ( $n \geq 3$ ). Order  $2n$

(Insert Figure)

What is the center of  $D_{2n}$ ? ( $n \geq 2$ )? Order 2 if even, order 1 if odd.

Why does  $D_{12}$  split as a product?

(Insert Figure)  $D_{12} = D_6 \times \mathbb{Z}/2\mathbb{Z}$  = symmetries of triangles  $\times$   $180^\circ$  rotation commutes with elements and flips the two triangles

$D_{10}$  (Insert Figure) Problem:  $180^\circ$  does not flip two squares.

$D_{2n}$  can be split  $D_{2n} \times \mathbb{Z}/2\mathbb{Z}$  for  $D_4, D_{12}, D_{20}, D_{28} \pmod{4}$

Involutions in dihedral groups (elements of order 2)

$D_{2n}$  (Insert Figure)

Reflection Groups (generated by relations)

(Insert Figure) Suppose  $g$  and  $h$  are relations. If  $g^2 = 1, h^2 = 1, (gh)^n = 1$

- Fid property of all finite groups that doesn't hold for all infinite groups, in the language of groups.

Property: If  $g, h$  are involutions, either  $g, h$  are conjugates or some involution commutes with  $g, h$

$g^2 = 1, h^2 = 1, (gh)^n = 1$  for some  $n$  (since group finite)

$n$  even:  $D_{2n}$  has nontrivial element in center

$n$  odd: All involutions commute

Fails for  $\infty$  dihedral group  $g^2 = 1, h^2 = 1$  (Insert Figure)

**Order 12:**  $\mathbb{Z}/12\mathbb{Z}$ , products -  $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ,  $S_3 \times \mathbb{Z}/2\mathbb{Z}$ , rotations of tetrahedrons, semidirect products-  $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ ,  $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/4\mathbb{Z}$ .

Binary Dihedral:  $S^3$  (= unit quaternions) is a group acting on  $\mathbb{R}^3 = bi + cj + dk$  - rotations in  $\mathbb{R}^3$

$1 \rightarrow \pm 1 \rightarrow S^3 \rightarrow$  rotations on  $\mathbb{R}^3 \rightarrow 1$  where  $\pm 1$  act trivially on  $\mathbb{R}^3$

$1 \rightarrow \pm 1 \rightarrow \hat{G} \rightarrow G =$  finite reflection group. Ex: group over  $D_{2n}$

Binary dihedral groups of order  $4n$  so binary dihedral group of order 12. ( $Q_8$  binary dihedral group of order 8) 5 groups of order 12.