

# Group Theory Notes

Leon Lee

October 3, 2024

## Contents

<b>1</b>	<b>Recapping from previous courses</b>	<b>3</b>
1.1	Groups, Subgroups, Cosets, oh my! . . . . .	3
1.2	Group Homomorphisms . . . . .	6
1.3	something... . . . . .	7
1.4	First Isomorphism Theorem and stuff . . . . .	9
1.4.5	Recap of last time (which is not on the notes) . . . . .	10
<b>2</b>	<b>Group Actions</b>	<b>13</b>

# 1 Recapping from previous courses

## 1.1 Groups, Subgroups, Cosets, oh my!

### Definition 1.1.1: Group

A **group** consists of a set  $G$  together with a function  $G \times G \rightarrow G$  which maps an ordered pair  $(g, h) \in G \times G$  to an element  $g * h \in G$ . The following axioms must be satisfied:

1. **Associativity:**  $(g * h) * k = g * (h * k)$  for each triple  $(g, h, k) \in G \times G \times G$
2. **Identity:** There is an element  $e \in G$  s.t.  $e * g = g = g * e$  for each element  $g \in G$
3. **Inverse:** To each element  $g \in G$  there is an element  $h \in G$  s.t.  $gh = e = hg$

Every single course seems to have its own definition for a group, this one is a bit more compact than others. FPM had the **closure** axiom, but that is satisfied by the definition of the function  $G \times G \rightarrow G$

**Note on notation:** Usually just write  $gh$  instead of  $g * h$ . Additionally  $g^{-1}$  is the inverse of  $g$

### Definition 1.3.1: Subgroups

If  $H$  is a nonempty subset of  $G$ , then  $H$  is a **subgroup** provided that

1.  $hk \in H$  for all  $h, k \in H$
2.  $h^{-1} \in H$  for each  $h \in H$

Alternatively, we can say " $H$  is closed under the group operation"

#### Notation

- $H \leq G$  means  $H$  is a subgroup of  $G$ , whereas  $H \subseteq G$  means  $H$  is a subset of  $G$ .
- $H < G$  means that  $H$  is a subgroup of  $G$  and also  $H \neq G$ .
- A subgroup is **proper** if  $H \neq G$
- A subgroup is **non-trivial** if  $H \neq \{e\}$

**Note:**  $e \in H$  follows from the definition, and associativity follows from the fact that  $G$  is a group. Any subgroup  $H$  of  $G$  is a group using the same product as  $G$

### Definition 1.3.6: Cosets

Let  $H \leq G$  and let  $g \in G$ . Then the **left coset of  $H$  determined by  $g$**  is the set  $gH := \{gh : h \in H\}$ .  $Hg := \{hg : h \in H\}$  is the **right coset of  $H$  determined by  $g$**

#### Notation

- The set of left cosets of  $H$  is denoted  $G/H$ , the set of right cosets is denoted  $H \backslash G$ .
- The number of elements in a group  $G$  is denoted by  $\#G$  or  $|G|$ , and is known as the **order** of  $G$ . We will use  $|G|$  in this course.
- The number of left cosets of a subgroup  $H$  of  $G$  is the **index** of  $H$  in  $G$  and is denoted by  $|G : H|$  or  $[G : H]$  (That is,  $[G : H] = |G/H|$ ). We will use  $[G : H]$  in this course.

### Theorem 1.1.1: Coset Lemmas

If  $H$  is finite,  $|gH| = |H|$

If  $g_1H \cap g_2H \neq \emptyset$ , then  $g_1H = g_2H$

### Theorem 1.3.8: Lagrange's Theorem

Let  $H$  be a subgroup of a finite group  $G$ . Then

$$|G| = [G : H] \cdot |H|$$

#### Consequences and Results

- The order of a subgroup must divide the order of the group, e.g. A group of order 12 cannot have a subgroup of order 8
- The converse of Lagrange's Theorem is false, e.g. there is a group of order 12 that doesn't have a subgroup of order 6

**Example:** If  $G = S_3$  and  $H = \{e, (12)\}$ , what are the left cosets of  $H$ ?

$$H = eH = \{e, (12)\} \quad \{(23), (132)\} \quad \{(13), (123)\}$$

**Example:** If  $H \trianglelefteq G$  then the left cosets are right cosets

*Proof.*

$$gH = \{gh : h \in H\} = \{(ghg^{-1})g : h \in H\} \subseteq Hg$$

□

### Theorem 1.3.9: Cauchy's Theorem

If  $G$  is a finite group and  $p$  is a prime that divides the order of  $G$ , then  $G$  has a subgroup of order  $p$

### Definition 1.3.10: Order of an element

Let  $g \in G$ . The **order** of  $g$  is the least positive integer such that  $g^n = e$  or  $\infty$  if such  $n$  does not exist. We write the order of  $g$  as  $o(g)$ . Note that  $o(g) = |\langle g \rangle|$ .

It thus follows from Lagrange's Theorem that the order of an element of  $G$  must divide  $|G|$ , since if  $o(g) = n$  then  $\langle g \rangle = \{g, g^2, \dots, g^n = e\}$  is a subgroup of  $G$ . We also have:

**Corollary 1.3.11:** If  $|G|$  is prime, then  $G$  is cyclic

### Example A: Examples of Groups and Subgroups

- $\mathbb{Z}/n$  under addition, where  $a * b = a + b \pmod n$
- $(\mathbb{R} \setminus \{0\}, \times)$ , or  $K \setminus \{0\}$  for any field  $K$
- Alternating group:  $A_n \subset S_n$  - permutations from an even number of transpositions?

1.2.1  $S_n$ , the  **$n$ -th symmetric group** is the group of permutations of  $\{1, 2, \dots, n\}$ . The

group operation is composition of functions

1.2.6 A group  $(G, *)$  is **abelian** if  $g * h = h * g$  for all  $g, h \in G$

- Let  $F$  be a field
  - The **general linear group**  $GL(n, F)$  is the set of all invertible  $n \times n$  matrices
  - The **special linear group**  $SL(n, F)$  is the set of all invertible  $n \times n$  matrices with determinant equal to 1

1.3.5 Let  $G$  be a group and let  $g \in G$ . Then  $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$  is a subgroup of  $G$ . It is called the **subgroup generated by  $g$** . If  $G = \langle g \rangle$  for some  $g \in G$ , then  $G$  is referred to as **cyclic**

1.3.7 A subgroup  $H \leq G$  is **normal** if  $gH = Hg$  for all  $g \in G$ . In this case we write  $H \trianglelefteq G$

## 1.2 Group Homomorphisms

### Definition 1.4.1: Group Homomorphism

Let  $G, H$  be groups. A function  $\phi : G \rightarrow H$  such that

$$\phi(ab) = \phi(a)\phi(b)$$

for all  $a, b \in G$  is a **group homomorphism**

**Example:** If  $\phi$  is a group homomorphism then  $\phi(e) = e$

*Proof.*

$$\begin{aligned}\phi(e \cdot e) &= \phi(e)\phi(e) \\ \implies \phi(e) &= \phi(e)\phi(e) \\ \text{multiply by } \phi(e)^{-1} \quad e &= \phi(e)^{-1}\phi(e)\phi(e) = \phi(e)\end{aligned}$$

□

**Example:** Show  $\phi(g^{-1}) = \phi(g)^{-1}$

*Proof.*

$$\begin{aligned}\phi(g \cdot g^{-1}) &= \phi(g)\phi(g^{-1}) \\ \phi(e) &= \phi(g)\phi(g^{-1}) \\ \text{Multiply by } \phi(g)^{-1} \quad \phi(g)^{-1}\phi(e) &= \phi(g)^{-1}\phi(g)\phi(g^{-1}) \\ \phi(g)^{-1} &= \phi(g^{-1})\end{aligned}$$

□

### Example 1.4.2: Cyclic Group Homomorphisms

Let  $C_n$  be the **cyclic group of order  $n$** . We can think of  $C_n$  as the set of rotations of an equilateral  $n$ -gon. If  $g$  is a rotation of  $2\pi/n$  radians, then  $C_n = \{g, g^2, \dots, g^n = e\}$ . The group  $C_n$  is cyclic since all elements are powers of a single element  $g$ . Then

$$\begin{aligned}\phi : \mathbb{Z} &\rightarrow C_n \\ a &\mapsto g^a\end{aligned}$$

is a group homomorphism. (proof in lecture notes)

### Definition 1.4.3: Group Isomorphism

If  $G$  and  $H$  are groups and  $\psi : G \rightarrow H$  is a bijective *group homomorphism*, we say that  $\psi$  is a **group isomorphism** and that  $G$  and  $H$  are **isomorphic**

### Definition 1.4.5: Kernel of a Homomorphism

Let  $\phi : G \rightarrow H$  be a group homomorphism. The **kernel** of  $\phi$  is  $\{g \in G : \phi(g) = e\}$

### Definition 1.4.6: Automorphisms

Let  $G$  be a group. The set of all isomorphisms  $\phi : G \rightarrow G$  is also a group. It is called the **automorphism group of  $G$** , and is written  $\text{Aut}(G)$ . The group operation is composition of functions

**Example:** What is  $\text{Aut}(C_3)$ ?

*Proof.*

$$C_3 = \{e, r, r^{-1}\}$$

□

### Definition 1.4.8: Direct Product

Let  $G, H$  be groups. The **product** (or **direct product**)  $G \times H$  is a group, with group operation  $*$  given by

$$(g, h) * (g', h') = (g *_G g', h *_H h')$$

**Note:** we usually just say that  $(g, h) * (g', h') = (gg', hh')$

## 1.3 something...

Let  $H \leq G$  ( $H$  a subgroup of  $G$ ). TFAE

1.  $\forall g \in G, h \in H, ghg^{-1} \in H$
2.  $gHg^{-1} = H, \forall g \in G$
3.  $gH = Hg, \forall g \in G$

*Proof.* Show conditions imply each other

- (2)  $\implies$  (1) immediately
- (1) says that  $gHg^{-1} \subseteq H, \forall g \in G$   
WTS:  $gHg^{-1} \supseteq H$

$$H = g^{-1}gHg^{-1}g \subseteq g^{-1}Hg, \forall g \in G$$

replacing  $g$  with  $g^{-1}$ :

$$H \subseteq gHg^{-1}, \forall g \in G$$

- (2)  $\implies$  (3): Multiply by  $g$  on right
- (3)  $\implies$  (2): Multiply by  $g^{-1}$  on left

□

### Theorem 1.3.1: lma

If  $\phi : G \rightarrow H$  is a group homomorphism, then  $\ker \phi \trianglelefteq G$

*Proof.* If  $\phi(x) = e$ , then

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g) = \phi(g)e\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e$$

□

**Theorem 1.3.2**

If  $N \leq G$ , then  $N \triangleleft G$  iff  $\exists \phi : G \rightarrow H$  s.t.  $N = \ker \phi$

*Proof.*  $\ker \phi$  is normal by the above lemma

Conversely, given  $N \triangleleft G$ , we can form **factor group**  $G/N$

$G/N$  is the set of left cosets, with:

- Identity  $N$
- Inverses  $(gN)^{-1} : g^{-1}N$
- Multiplication:  $(g_1N) \times (g_2N) := g_1g_2N$

Check that the group is well defined

1. If  $gN = g'N$ , then  $g' = gx$  for  $x \in N$

$$(g'N)^{-1} = (g')^{-1}N = (gx)^{-1}N = x^{-1}g^{-1}N$$

As  $N$  is normal,  $gx^{-1}g^{-1} \in N$

$$\implies x^{-1}g^{-1}N = g^{-1}(gx^{-1}g^{-1})N = g^{-1}N, \text{ as } gx^{-1}g^{-1} \in N$$

2. If  $g_1N = g'_1N$  and  $g_2N = g'_2N$ , then  $g'_1 = g_1x$  and  $g'_2 = g_2y$  for  $x, y \in N$

$$(g'_1N) \times (g'_2N) = g'_1g'_2N = g_1xg_2yN$$

$$yN = N, \text{ so } g_1xg_2yN = g_1xg_2N$$

$$N \text{ normal, so } g_2^{-1}xg_2 \in N \implies g_1g_2(g_2^{-1}xg_2)N = g_1g_2N$$

then prove the group axioms lol

Define  $\text{can} : G \rightarrow G/N$ ,  $g \mapsto gN$ . This is a group homomorphism

$$\text{can}(g_1g_2) = g_1g_2N = (g_1N) * (g_2N) = \text{can}(g_1) * \text{can}(g_2)$$

Kernel of  $\text{can}$

$$\ker(\text{can}) = \{g \in G : \text{can}(g) = N\} = \{g \in G : gN = N\} = N$$

□

**Example:** If  $G = \mathbb{Z}$ , (normal) subgroups are  $n\mathbb{Z} = \{ni : i \in \mathbb{Z}\}$ . What is  $\mathbb{Z}/n\mathbb{Z}$ ?

Elements of  $\mathbb{Z}/n\mathbb{Z}$  are cosets,  $i + n\mathbb{Z}$  (fixed  $i$ ), or  $\{x \in \mathbb{Z} : x \equiv i \pmod{n}\}$

Group operation:  $(i + n\mathbb{Z}) * (j + n\mathbb{Z}) = i + j + n\mathbb{Z} = i + j \pmod{n}$

soooo...  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n$ , where elements are  $n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, n-1 + n\mathbb{Z}$

lol !



## 1.4 First Isomorphism Theorem and stuff

### Theorem 1.4.1: First Isomorphism Theorem

If  $\theta : G \rightarrow H$  a group homomorphism, then:

- $\text{im}(\theta)$  is a subgroup of  $H$
- $\ker(\theta) \triangleleft G$
- $\exists$  a group homomorphism  $\bar{\theta} : G/\ker \theta \rightarrow \text{im}(\theta)$

*Proof.* Prove all 3

- If  $\theta(a), \theta(b) \in \text{im}(\theta)$ , then  $\theta(a)\theta(b) = \theta(ab) \in \text{im}(\theta)$   
 $\theta(a)^{-1} = \theta(a^{-1}) \in \text{im}(\theta)$  therefore  $\text{im}(\theta) \leq H$
- Already  $\ker(\theta) \triangleleft G$
- Let  $N = \ker(\theta)$ . Then  $gN \in G/N$ . Define  $\bar{\theta}(gN) := \theta(g)$ .  
 Well defined: If  $gN = g'N$ , then  $g' = gx$  for some  $x \in N$ . Then  $\bar{\theta}(g'N) = \theta(g') = \theta(g)\theta(x) = \theta(g)e$  as  $x \in \ker(\theta) = \theta(g)$

□

Ex 1:  $\theta : \mathbb{C} \rightarrow \mathbb{C} \setminus \{0\}$

### Theorem 1.4.2: Property of Finite Groups

If  $N \triangleleft G$ , then for any homomorphism  $\psi : G \rightarrow H$  with  $N \subseteq \ker \psi$ .  $\exists$  a group homomorphism  $\bar{\psi} : G/N \rightarrow H$  s.t.  $\psi = \bar{\psi} \circ \text{can}$

If  $\psi : G \rightarrow K$  surjective...?  $\psi : G \rightarrow H$  with  $\ker \phi \subseteq \ker \psi$ , then  $\exists \bar{\psi} : K \rightarrow H$  s.t.  $\psi = \bar{\psi} \circ \psi$

### Theorem 1.4.3

Let  $N \triangleleft G$ ,  $\text{can} : G \rightarrow G/N$  and  $K \leq G/N$

1.  $\text{can}^{-1}(K) \leq G$  with  $\text{can}^{-1}(K) \geq N$
2.  $\text{can}^{-1}(K) \triangleleft G \iff K \triangleleft G/N$

### Theorem 1.4.4: Correspondence Theorem

If we have  $N \triangleleft G$ ,  $\text{can} : G \rightarrow G/N$ , then:

- $H \rightarrow \text{can}(H)$  gives a bijection between subgroups of  $G/N$  and subgroups of  $G$  containing  $N$
- Normal subgroups of  $G$  containing  $N \iff$  normal subgroups of  $G/N$
- If  $A, B \leq G$  with  $N \subseteq A, N \subseteq B$ , then:  $A \subseteq B$  iff  $\text{can}(A) \subseteq \text{can}(B)$

*Proof.* Given  $K < G/N$ ,  $\text{can}^{-1}K \leq G$  and  $N \leq \text{can}^{-1}K$  since  $\text{can}^{-1}\{e\} = N$   
 Last prop says:  $\text{can}^{-1}\text{can}(H) = H$  when  $N \subseteq H$

$$\text{can}(\text{can}^{-1}K) \subseteq K$$

Since  $\text{can}$  is surjective,  $\forall x \in K$ ,  $\exists y \in G$  s.t.  $\text{can}(y) = x$ . Then  $y \in \text{can}^{-1}K$  so  $x \in \text{can}(\text{can}^{-1}K)$   
 So,  $\text{can}(\text{can}^{-1}K) = K$  since  $\text{can}$  is surjective. Therefore  $\text{can}$  &  $\text{can}^{-1}$  give a bijection

$$\{\text{subgroups of } G \text{ containing } N\} \rightsquigarrow \{\text{subgroups of } G/N\}$$

□

#### 1.4.5 Recap of last time (which is not on the notes)

- $\text{can}(H) \triangleleft G/N \iff H \triangleleft G$
- If  $A \subseteq B$  then  $\text{can}(A) \subseteq \text{can}(B)$   
 Conversely, if  $\text{can}(A) \subseteq \text{can}(B)$  then  $\text{can}^{-1}\underbrace{\text{can}(A)}_{=A} \subseteq \text{can}^{-1}\underbrace{\text{can}(B)}_{=B}$

#### Definition 1.4.6: Random notation

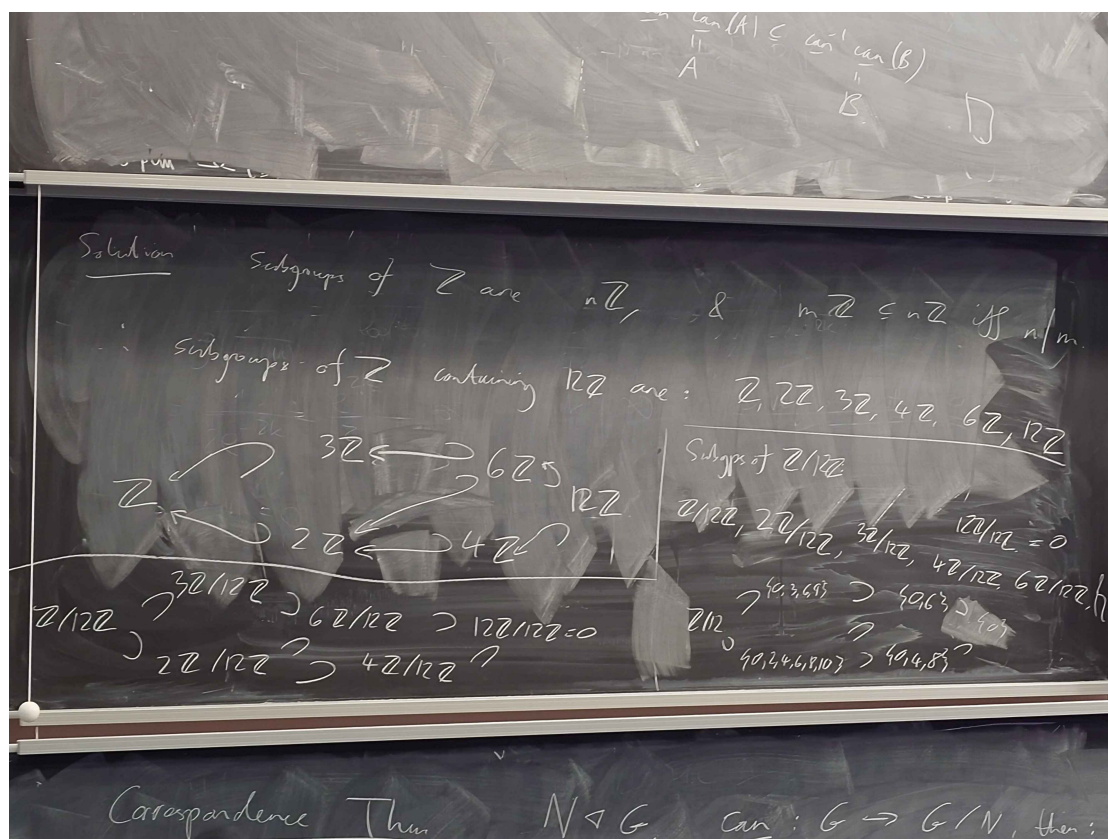
- $\exists$ : There exists
- $\exists!$ : There exists unique
- $\nexists$ : there does not exist

**Example:** Let  $G = \mathbb{Z}$ ,  $N = 12\mathbb{Z}$ .

- Find all subgroups of  $G$  containing  $N$  and all inclusions between them
- Find all subgroups of  $\mathbb{Z}/12$

**Solution:** Subgroups of  $\mathbb{Z}$  are of the form  $n\mathbb{Z}$ .  $m\mathbb{Z} \subseteq n\mathbb{Z}$  iff  $n/m$   
 Therefore, subgroups of  $\mathbb{Z}$  containing  $12\mathbb{Z}$  are:

$$\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 12\mathbb{Z}$$



Subgroups of  $\mathbb{Z}/12\mathbb{Z}$ :

$$12\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, 2\mathbb{Z}/12\mathbb{Z}, 3\mathbb{Z}/12\mathbb{Z}, 4\mathbb{Z}/12\mathbb{Z}, 6\mathbb{Z}/12\mathbb{Z}$$

some working out

### Theorem 1.4.7: Third Isomorphism Theorem

If  $N, H \triangleleft G$ , with  $N \leq H$ , then

$$(G/N)/(H/N) \cong G/H$$

*Proof.*  $N \leq \ker(\text{can}_H) = H$ , so  $\exists! \pi$  by universal property of finite groups

$\pi$  is surjective, because  $\text{can}_H$  is isomorphic

Explicitly,

$$\pi(gN) = gH = \pi(\text{can}_N(g)) = \text{can}_H(g)$$

$$\ker(\pi) = \{gN : g \in H\} = H/N$$

By the first isomorphism theorem,

$$G/H \cong (G/N)/\ker \pi = (G/N)/(H/N)$$

□

**Theorem 1.4.8: Second Isomorphism Theorem**

Let  $N \triangleleft G$  and  $H \leq G$ . Then:

1.  $HN \leq G$
2.  $N \triangleleft HN$
3.  $H \cap N \triangleleft H$
4.  $HN/N \cong H/H \cap N$

*Proof.* Let  $h_1h_2 \in H$ ,  $n_1n_2 \in N$

1.

$$h_1n_1h_2n_2 = \underbrace{h_1h_2}_{\in H} \underbrace{(h_2^{-1}n_1h_2)n_2}_{\in N}$$

$$(hn)^{-1} = n^{-1}h^{-1} = \underbrace{h^{-1}}_{\in H} \underbrace{(hn^{-1}h^{-1})}_{\in N}$$

2. If  $g \in HN$  and  $n \in N$ , then  $g \cap g^{-1} \in n$  since  $g \in G$

3. If  $x \in H \cap N$  and  $h \in H$ , then  $\underbrace{h x h^{-1}}_{N \triangleleft G} \in N$  and  $\underbrace{h x h^{-1}}_{x \in H} \in H$

4. Need  $\theta : H \rightarrow HN/N$  surjective with kernel  $H \cap N$

Let  $\theta(h) = hN$  i.e.  $\theta = \text{can}_N|_H$ ,  $(\text{can}_N G \rightarrow G/N)$

Surjective: cosets of  $HN/N$  are cosets  $xN$  for  $x \in HN$  but  $x = hn$ ,  $h \in H$ ,  $n \in N$  and  $xN = hN = \theta(h)$  (wtf?)

Kernel: If  $\theta(h) = e$ ,  $hN = N$ , so  $h \in N$ , so  $\ker \theta = H \cap N$ , so by the correspondence theorem,

$$H/H \cap N \subseteq HN/N$$

□

## 2 Group Actions

### Definition 2.0.1: Free Group

The **free group on generators**  $x_1, \dots, x_m$  is the group whose elements are words in the symbols  $x_1, \dots, x_m, x_1^{-1}, \dots, x_m^{-1}$ , subject to the group axioms and all logical consequences. The group operation is concatenation. The free group is written

$$\langle x_1, \dots, x_m \rangle$$

**Example:** Find presentations for:

- $\mathbb{Z}^2 = \langle x, y \mid xy = yx \rangle = \langle x, y \mid xyx^{-1}y^{-1} = e \rangle \cong \{x^i y^j = i, j \in \mathbb{Z}\}$