

# Mathematics

Robin Adams

February 12, 2024



# Contents

<b>I</b>	<b>Category Theory</b>	<b>5</b>
1	Foundations	7
2	Number Theory	9
2.1	Congruence . . . . .	9
2.2	Euler's $\phi$ -function . . . . .	10
3	Categories	11
3.1	Preorders . . . . .	12
3.2	Monomorphisms and Epimorphisms . . . . .	12
3.3	Sections and Retractions . . . . .	14
3.4	Isomorphisms . . . . .	15
3.5	Initial and Terminal Objects . . . . .	15
4	Functors	17
4.1	Comma Categories . . . . .	17
<b>II</b>	<b>Group Theory</b>	<b>19</b>
5	Groups	21
5.1	Order of an Element . . . . .	24
5.2	Generators . . . . .	26
6	Group Homomorphisms	29
7	Abelian Groups	31
<b>III</b>	<b>Linear Algebra</b>	<b>33</b>



Part I

Category Theory



# Chapter 1

## Foundations

This is a placeholder — I am not sure what foundation I want to use for this project yet. I will try to work in a way which is foundation-independent. What I do could be formalized in ZFC, ETCS, or some other system. I will assume the usual set theoretic constructions as needed. Sets will be defined up to bijection only.





## Chapter 2

# Number Theory

### 2.1 Congruence

**Definition 2.1** (Congruence). Let  $a, b, n$  be integers with  $n > 0$ . We say  $a$  is *congruent to  $b$  modulo  $n$* , and write  $a \equiv b \pmod{n}$ , iff  $n \mid b - a$ .

**Proposition 2.2.** *For  $n$  a positive integer, congruence modulo  $n$  is an equivalence relation.*

PROOF:

$\langle 1 \rangle 1$ . For any integer  $a$  we have  $a \equiv a \pmod{n}$ .

PROOF: Since  $n \mid 0 = a - a$ .

$\langle 1 \rangle 2$ . If  $a \equiv b \pmod{n}$  then  $b \equiv a \pmod{n}$ .

PROOF: If  $n \mid b - a$  then  $n \mid a - b = -(b - a)$ .

$\langle 1 \rangle 3$ . If  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$  then  $a \equiv c \pmod{n}$ .

PROOF: If  $n \mid b - a$  and  $n \mid c - b$  then  $n \mid c - a = (c - b) + (b - a)$ .

□

**Definition 2.3.** Let  $\mathbb{Z}/n\mathbb{Z}$  be the quotient set of  $\mathbb{Z}$  with respect to congruence modulo  $n$ .

**Proposition 2.4.**  $\mathbb{Z}/n\mathbb{Z}$  has exactly  $n$  elements.

PROOF: Every integer is congruent to one of  $0, 1, \dots, n - 1$  by the division algorithm, and no two of them are congruent to one another, since if  $0 \leq i < j < n$  then  $0 < j - i < n$ . □

**Proposition 2.5.** *If  $a \equiv a' \pmod{n}$  and  $b \equiv b' \pmod{n}$  then  $a + b \equiv a' + b' \pmod{n}$ .*

PROOF: If  $n \mid a' - a$  and  $n \mid b' - b$  then  $n \mid (a' + b') - (a + b)$ . □

**Proposition 2.6.** *If  $a \equiv a' \pmod{n}$  and  $b \equiv b' \pmod{n}$  then  $ab \equiv a'b' \pmod{n}$ .*

PROOF: If  $n \mid a' - a$  and  $n \mid b' - b$  then  $n \mid a'b' - ab = a'(b' - b) + (a' - a)b$ . □

## 2.2 Euler's $\phi$ -function

**Definition 2.7.** For  $n$  a positive integer, let  $(\mathbb{Z}/n\mathbb{Z})^* = \{m \in \mathbb{Z}/n\mathbb{Z} : \gcd(m, n) = 1\}$ .

PROOF: We prove this is well-defined.

$\langle 1 \rangle 1$ . If  $m \equiv m' \pmod{n}$  and  $\gcd(m, n) = 1$  then  $\gcd(m', n) = 1$ .

$\langle 2 \rangle 1$ . PICK integers  $a, b$  such that  $am + bn = 1$

$\langle 2 \rangle 2$ . PICK an integer  $c$  such that  $m' - m = cn$

$\langle 2 \rangle 3$ .  $am' + (b - ac)n = 1$

□

**Definition 2.8.** For  $n$  a positive integer, let  $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ .

**Proposition 2.9.** If  $n$  is an odd positive integer then  $\phi(2n) = \phi(n)$ .

PROOF:

$\langle 1 \rangle 1$ . LET:  $n$  be an odd positive integer.

$\langle 1 \rangle 2$ . For any integer  $m$ , if  $\gcd(m, n) = 1$  then  $\gcd(2m + n, 2n) = 1$

PROOF: For  $p$  a prime, if  $p \mid 2m + n$  and  $p \mid 2n$  then  $p \neq 2$  (since  $2m + n$  is odd) so  $p \mid n$  and hence  $p \mid m$ , which is a contradiction.

$\langle 1 \rangle 3$ . For any integer  $r$ , if  $\gcd(r, 2n) = 1$  then  $\gcd(\frac{r+n}{2}, n) = 1$

PROOF: If  $p \mid n$  and  $p \mid \frac{r+n}{2}$  then  $p \mid r + n$  so  $p \mid r$  which is a contradiction.

$\langle 1 \rangle 4$ . The function that maps  $m$  to  $2m + n$  is a bijection between  $(\mathbb{Z}/n\mathbb{Z})^*$  and  $(\mathbb{Z}/2n\mathbb{Z})^*$ .

□

# Chapter 3

## Categories

**Definition 3.1** (Category). A *category*  $\mathcal{C}$  consists of:

- A class  $|\mathcal{C}|$  of *objects*. We write  $A \in \mathcal{C}$  for  $A \in |\mathcal{C}|$ .
- For any objects  $A, B$ , a set  $\mathcal{C}[A, B]$  of *morphisms* from  $A$  to  $B$ . We write  $f : A \rightarrow B$  for  $f \in \mathcal{C}[A, B]$ .
- For any object  $A$ , a morphism  $\text{id}_A : A \rightarrow A$ , the *identity* morphism on  $A$ .
- For any morphisms  $f : A \rightarrow B$  and  $g : B \rightarrow C$ , a morphism  $g \circ f : A \rightarrow C$ , the *composite* of  $f$  and  $g$ .

such that:

**Associativity** Given  $f : A \rightarrow B$ ,  $g : B \rightarrow C$  and  $h : C \rightarrow D$ , we have

$$h \circ (g \circ f) = (h \circ g) \circ f$$

**Left Unit Law** For any morphism  $f : A \rightarrow B$ , we have  $\text{id}_B \circ f = f$ .

**Right Unit Law** For any morphism  $f : A \rightarrow B$ , we have  $f \circ \text{id}_A = f$ .

**Proposition 3.2.** *The identity morphism on an object is unique.*

PROOF: If  $i$  and  $j$  are identity morphisms on  $A$  then  $i = i \circ j = j$ .  $\square$

**Example 3.3** (Category of Sets). The *category of sets* **Set** has objects all sets and morphisms all functions.

**Definition 3.4** (Endomorphism). In a category  $\mathcal{C}$ , an *endomorphism* on an object  $A$  is a morphism  $A \rightarrow A$ . We write  $\text{End}_{\mathcal{C}}(A)$  for  $\mathcal{C}[A, A]$ .

**Definition 3.5** (Opposite Category). For any category  $\mathcal{C}$ , the *opposite* category  $\mathcal{C}^{\text{op}}$  is the category with the same objects as  $\mathcal{C}$  and

$$\mathcal{C}^{\text{op}}[A, B] = \mathcal{C}[B, A]$$

### 3.1 Preorders

**Definition 3.6** (Preorder). A *preorder* on a set  $A$  is a relation  $\leq$  on  $A$  that is reflexive and transitive.

A *preordered set* is a pair  $(A, \leq)$  such that  $\leq$  is a preorder on  $A$ . We usually write  $A$  for the preordered set  $(A, \leq)$ .

We identify any preordered set  $A$  with the category whose objects are the elements of  $A$ , with one morphism  $a \rightarrow b$  iff  $a \leq b$ , and no morphism  $a \rightarrow b$  otherwise.

**Example 3.7.** For any ordinal  $\alpha$ , let  $\alpha$  be the preorder  $\{\beta : \beta < \alpha\}$  under  $\leq$ .

**Definition 3.8** (Discrete Preorder). We identify any set  $A$  with the *discrete* preorder  $(A, =)$ .

### 3.2 Monomorphisms and Epimorphisms

**Definition 3.9** (Monomorphism). In a category, let  $f : A \rightarrow B$ . Then  $f$  is a *monomorphism* or *monic* iff, for every object  $X$  and morphism  $x, y : X \rightarrow A$ , if  $fx = fy$  then  $x = y$ .

**Definition 3.10** (Epimorphism). In a category, let  $f : A \rightarrow B$ . Then  $f$  is a *epimorphism* or *epi* iff, for every object  $X$  and morphism  $x, y : B \rightarrow X$ , if  $xf = yf$  then  $x = y$ .

**Proposition 3.11.** *The composite of two monomorphism is monic.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $f : A \rightarrow B$  and  $g : B \rightarrow C$  be monic.

$\langle 1 \rangle 2$ . LET:  $x, y : X \rightarrow A$

$\langle 1 \rangle 3$ . ASSUME:  $g \circ f \circ x = g \circ f \circ y$

$\langle 1 \rangle 4$ .  $f \circ x = f \circ y$

$\langle 1 \rangle 5$ .  $x = y$

□

**Proposition 3.12.** *The composite of two epimorphisms is epi.*

PROOF: Dual. □

**Proposition 3.13.** *Let  $f : A \rightarrow B$  and  $g : B \rightarrow C$ . If  $g \circ f$  is monic then  $f$  is monic.*

PROOF: If  $f \circ x = f \circ y$  then  $gfx = gfy$  and so  $x = y$ . □

**Proposition 3.14.** *Let  $f : A \rightarrow B$  and  $g : B \rightarrow C$ . If  $g \circ f$  is epi then  $g$  is epi.*

PROOF: Dual. □

**Proposition 3.15.** *A function is a monomorphism in **Set** iff it is injective.*

PROOF:

- ⟨1⟩1. LET:  $f : A \rightarrow B$
- ⟨1⟩2. If  $f$  is monic then  $f$  is injective.
  - ⟨2⟩1. ASSUME:  $f$  is monic.
  - ⟨2⟩2. LET:  $x, y \in A$
  - ⟨2⟩3. ASSUME:  $f(x) = f(y)$
  - ⟨2⟩4. LET:  $\bar{x}, \bar{y} : 1 \rightarrow A$  be the functions such that  $\bar{x}(*) = x$  and  $\bar{y}(*) = y$
  - ⟨2⟩5.  $f \circ \bar{x} = f \circ \bar{y}$
  - ⟨2⟩6.  $\bar{x} = \bar{y}$
  - PROOF: By ⟨2⟩1.
  - ⟨2⟩7.  $x = y$
- ⟨1⟩3. If  $f$  is injective then  $f$  is monic.
  - ⟨2⟩1. ASSUME:  $f$  is injective.
  - ⟨2⟩2. LET:  $X$  be a set and  $x, y : X \rightarrow A$ .
  - ⟨2⟩3. ASSUME:  $f \circ x = f \circ y$
  - PROVE:  $x = y$
  - ⟨2⟩4. LET:  $t \in X$
  - PROVE:  $x(t) = y(t)$
  - ⟨2⟩5.  $f(x(t)) = f(y(t))$
  - ⟨2⟩6.  $x(t) = y(t)$
  - PROOF: By ⟨2⟩1.

□

**Proposition 3.16.** *A function is an epimorphism in **Set** iff it is surjective.*

PROOF:

- ⟨1⟩1. LET:  $f : A \rightarrow B$
- ⟨1⟩2. If  $f$  is an epimorphism then  $f$  is surjective.
  - ⟨2⟩1. ASSUME:  $f$  is an epimorphism.
  - ⟨2⟩2. LET:  $b \in B$
  - ⟨2⟩3. LET:  $x, y : B \rightarrow 2$  be defined by  $x(b) = 1$  and  $x(t) = 0$  for all other  $t \in B$ ,  $y(t) = 0$  for all  $t \in B$ .
  - ⟨2⟩4.  $x \neq y$
  - ⟨2⟩5.  $x \circ f \neq y \circ f$
  - ⟨2⟩6. There exists  $a \in A$  such that  $f(a) = b$ .
- ⟨1⟩3. If  $f$  is surjective then  $f$  is an epimorphism.
  - ⟨2⟩1. ASSUME:  $f$  is surjective.
  - ⟨2⟩2. LET:  $x, y : B \rightarrow X$
  - ⟨2⟩3. ASSUME:  $x \circ f = y \circ f$
  - PROVE:  $x = y$
  - ⟨2⟩4. LET:  $b \in B$
  - PROVE:  $x(b) = y(b)$
  - ⟨2⟩5. PICK  $a \in A$  such that  $f(a) = b$
  - ⟨2⟩6.  $x(f(a)) = y(f(a))$
  - ⟨2⟩7.  $x(b) = y(b)$

□

**Proposition 3.17.** *In a preorder, every morphism is monic and epi.*

PROOF: Immediate from definitions.  $\square$

### 3.3 Sections and Retractions

**Definition 3.18** (Section, Retraction). In a category, let  $r : A \rightarrow B$  and  $s : B \rightarrow A$ . Then  $r$  is a *retraction* of  $s$ , and  $s$  is a *section* of  $r$ , iff  $r \circ s = \text{id}_B$ .

**Proposition 3.19.** *Every identity morphism is a section and retraction of itself.*

PROOF: Immediate from definitions.  $\square$

**Proposition 3.20.** *Let  $r, r' : A \rightarrow B$  and  $s : B \rightarrow A$ . If  $r$  is a retraction of  $s$  and  $r'$  is a section of  $s$  then  $r = r'$ .*

PROOF:

$$\begin{aligned} r &= r \circ \text{id}_A \\ &= r \circ s \circ r' \\ &= \text{id}_B \circ r' \\ &= r' \end{aligned} \quad \square$$

**Proposition 3.21.** *Let  $r_1 : A \rightarrow B$ ,  $r_2 : B \rightarrow C$ ,  $s_1 : B \rightarrow A$  and  $s_2 : C \rightarrow B$ . If  $r_1$  is a retraction of  $s_1$  and  $r_2$  is a retraction of  $s_2$  then  $r_2 \circ r_1$  is a retraction of  $s_1 \circ s_2$ .*

PROOF:

$$\begin{aligned} r_2 \circ r_1 \circ s_1 \circ s_2 &= r_2 \circ \text{id}_B \circ s_2 \\ &= r_2 \circ s_2 \\ &= \text{id}_C \end{aligned} \quad \square$$

**Proposition 3.22.** *Every section is monic.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $s : A \rightarrow B$  be a section of  $r : B \rightarrow A$ .

$\langle 1 \rangle 2$ . LET:  $x, y : X \rightarrow A$  satisfy  $sx = sy$ .

$\langle 1 \rangle 3$ .  $rsx = rsy$

$\langle 1 \rangle 4$ .  $x = y$

$\square$

**Proposition 3.23.** *Every retraction is epi.*

PROOF: Dual.  $\square$

**Proposition 3.24.** *In Set, every epimorphism has a retraction.*

PROOF: By the Axiom of Choice.  $\square$

**Example 3.25.** It is not true in general that every monomorphism in any category has a section. nor that every epimorphism in any category has a retraction.

In the category **2**, the morphism  $0 \leq 1$  is monic and epi but has no retraction or section.

### 3.4 Isomorphisms

**Definition 3.26** (Isomorphism). In a category  $\mathcal{C}$ , a morphism  $f : A \rightarrow B$  is an *isomorphism*, denoted  $f : A \cong B$ , iff there exists a morphism  $f^{-1} : B \rightarrow A$ , the *inverse* of  $f$ , such that  $f^{-1} \circ f = \text{id}_A$  and  $f \circ f^{-1} = \text{id}_B$ .

An *automorphism* on an object  $A$  is an isomorphism between  $A$  and itself. We write  $\text{Aut}_{\mathcal{C}}(A)$  for the set of all automorphisms on  $A$ .

Objects  $A$  and  $B$  are *isomorphic*,  $A \cong B$ , iff there exists an isomorphism between them.

**Proposition 3.27.** *The inverse of an isomorphism is unique.*

PROOF: Proposition 3.20.  $\square$

**Proposition 3.28.** *For any object  $A$  we have  $\text{id}_A : A \cong A$  and  $\text{id}_A^{-1} = \text{id}_A$ .*

PROOF: Since  $\text{id}_A \circ \text{id}_A = \text{id}_A$  by the Unit Laws.  $\square$

**Proposition 3.29.** *If  $f : A \cong B$  then  $f^{-1} : B \cong A$  and  $(f^{-1})^{-1} = f$ .*

PROOF: Immediate from definitions.  $\square$

**Proposition 3.30.** *If  $f : A \cong B$  and  $g : B \cong C$  then  $g \circ f : A \cong C$  and  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .*

PROOF: From Proposition 3.21.  $\square$

**Definition 3.31** (Groupoid). A *groupoid* is a category in which every morphism is an isomorphism.

### 3.5 Initial and Terminal Objects

**Definition 3.32** (Initial Object). An object  $I$  in a category is *initial* iff, for any object  $X$ , there is exactly one morphism  $I \rightarrow X$ .

**Example 3.33.** The empty set is the initial object in **Set**.

**Definition 3.34** (Terminal Object). An object  $T$  in a category is *terminal* iff, for any object  $X$ , there is exactly one morphism  $X \rightarrow T$ .

**Example 3.35.** Every singleton is terminal in **Set**.

**Proposition 3.36.** *If  $I$  and  $J$  are initial in a category, then there exists a unique isomorphism  $I \cong J$ .*

PROOF:

- $\langle 1 \rangle 1$ . LET:  $i$  be the unique morphism  $I \rightarrow J$ .
- $\langle 1 \rangle 2$ . LET:  $i^{-1}$  be the unique morphism  $J \rightarrow I$ .
- $\langle 1 \rangle 3$ .  $i \circ i^{-1} = \text{id}_J$

PROOF: Since there is only one morphism  $J \rightarrow J$ .

- $\langle 1 \rangle 4$ .  $i^{-1} \circ i = \text{id}_I$

PROOF: Since there is only one morphism  $I \rightarrow I$ .  
 $\square$

**Proposition 3.37.** *If  $S$  and  $T$  are terminal in a category, then there exists a unique isomorphism  $S \cong T$ .*

PROOF: Dual.  $\square$



## Chapter 4

# Functors

**Definition 4.1** (Functor). Let  $\mathcal{C}$  and  $\mathcal{D}$  be categories. A *functor*  $F : \mathcal{C} \rightarrow \mathcal{D}$  consists of:

- for every object  $A \in \mathcal{C}$ , an object  $FA \in \mathcal{D}$
- for any morphism  $f : A \rightarrow B : \mathcal{C}$ , a morphism  $Ff : FA \rightarrow FB : \mathcal{D}$

such that:

- $F\text{id}_A = \text{id}_{FA}$
- $F(g \circ f) = Fg \circ Ff$

**Definition 4.2** (Identity Functor). For any category  $\mathcal{C}$ , the *identity functor*  $1_{\mathcal{C}} : \mathcal{C} \rightarrow \mathcal{C}$  is defined by

$$\begin{aligned} 1_{\mathcal{C}}A &= A \\ 1_{\mathcal{C}}f &= f \end{aligned}$$

**Definition 4.3** (Constant Functor). Given categories  $\mathcal{C}$ ,  $\mathcal{D}$  and an object  $D \in \mathcal{D}$ , the *constant functor*  $K^{\mathcal{C}}D : \mathcal{C} \rightarrow \mathcal{D}$  is the functor defined by

$$\begin{aligned} K^{\mathcal{C}}DC &= D \\ K^{\mathcal{C}}Df &= \text{id}_D \end{aligned}$$

### 4.1 Comma Categories

**Definition 4.4** (Comma Category). Let  $F : \mathcal{C} \rightarrow \mathcal{E}$  and  $G : \mathcal{D} \rightarrow \mathcal{E}$  be functors. The *comma category*  $F \downarrow G$  is the category with:

- objects all pairs  $(C, D, f)$  where  $C \in \mathcal{C}$ ,  $D \in \mathcal{D}$  and  $f : FC \rightarrow GD : \mathcal{E}$

- morphisms  $(u, v) : (C, D, f) \rightarrow (C', D', g)$  all pairs  $u : C \rightarrow C' : \mathcal{C}$  and  $v : D \rightarrow D' : \mathcal{D}$  such that the following diagram commutes:

$$\begin{array}{ccc} FC & \xrightarrow{f} & GD \\ \downarrow Fu & & \downarrow Gv \\ FC' & \xrightarrow{g} & GD' \end{array}$$

**Definition 4.5** (Slice Category). Let  $\mathcal{C}$  be a category and  $A \in \mathcal{C}$ . The *slice category* over  $A$ , denoted  $\mathcal{C}/A$ , is the comma category  $1_{\mathcal{C}} \downarrow K^1 A$ .

**Definition 4.6** (Coslice Category). Let  $\mathcal{C}$  be a category and  $A \in \mathcal{C}$ . The *coslice category* over  $A$ , denoted  $\mathcal{C} \backslash A$ , is the comma category  $K^1 A \downarrow 1_{\mathcal{C}}$ .

**Definition 4.7** (Pointed Sets). The *category of pointed sets*  $\mathbf{Set}_*$  is the coslice category  $\mathbf{Set} \backslash 1$ .

**Part II**

**Group Theory**



# Chapter 5

## Groups

**Definition 5.1** (Group). A *group*  $G$  consists of a set  $G$  and a binary operation  $\cdot : G^2 \rightarrow G$  such that  $\cdot$  is associative, and there exists  $e \in G$ , the *identity* element of the group, such that:

- For all  $x \in G$  we have  $xe = ex = x$
- For all  $x \in G$ , there exists  $x^{-1} \in G$ , the *inverse* of  $x$ , such that  $xx^{-1} = x^{-1}x = e$ .

We identify a group  $G$  with the category  $G$  with one object and morphisms the elements of  $G$ , with composition given by  $\cdot$ .

The *order* of a group  $G$ , denoted  $|G|$ , is the number of elements in  $G$  if  $G$  is finite; otherwise we write  $|G| = \infty$ .

**Proposition 5.2.** *The identity in a group is unique.*

PROOF: Proposition 3.2.

**Proposition 5.3.** *The inverse of an element is unique.*

PROOF: If  $i$  and  $j$  are inverses of  $x$  then  $i = ixj = j$ .  $\square$

**Example 5.4.** • The *trivial* group is  $\{e\}$  under  $ee = e$ .

- $\mathbb{Z}$  is a group under addition
- $\mathbb{Q}$  is a group under addition
- $\mathbb{Q} - \{0\}$  is a group under multiplication
- $\mathbb{R}$  is a group under addition
- $\mathbb{R} - \{0\}$  is a group under multiplication
- $\mathbb{C}$  is a group under addition
- $\mathbb{C} - \{0\}$  is a group under multiplication

- $\{-1, 1\}$  is a group under multiplication
- The set of  $2 \times 2$  real matrices with non-zero determinant is a group under matrix multiplication.
- For any positive integer  $n$ , the set  $\mathbb{Z}/n\mathbb{Z}$  of integers modulo  $n$  under addition is a group. We call this set the *cyclic* group of order  $n$ , denoted  $C_n$ .
- For any category  $\mathcal{C}$  and object  $A \in \mathcal{C}$ , we have  $\text{Aut}_{\mathcal{C}}(A)$  is a group under  $gf = f \circ g$ .  
For  $A$  a set, we call  $S_A = \text{Aut}_{\text{Set}}(A)$  the *symmetric group* or *group of permutations* of  $A$ .
- For  $n \geq 3$ , the *dihedral group*  $D_{2n}$  consists of the set of rigid motions that map the regular  $n$ -gon onto itself under composition.

**Example 5.5.** • The only group of order 1 is the trivial group.

- The only group of order 2 is  $\mathbb{Z}_2$ .
- The only group of order 3 is  $\mathbb{Z}_3$ .
- There are exactly two groups of order 4:  $\mathbb{Z}_4$  and  $\mathbb{Z}_2 \times \mathbb{Z}_2$  under  $(a, b)(c, d) = (ac, bd)$ .

**Example 5.6.** For any positive integer  $n$ , the set

$$(\mathbb{Z}/n\mathbb{Z})^* = \{m \in \mathbb{Z}/n\mathbb{Z} : \gcd(m, n) = 1\}$$

is a group under multiplication.

PROOF:

- <1>1. If  $\gcd(m_1, n) = \gcd(m_2, n) = 1$  then  $\gcd(m_1 m_2, n) = 1$
- <2>1. PICK integers  $a, b, c, d$  such that  $am_1 + bn = cm_2 + dn = 1$
- <2>2.  $acm_1 m_2 + (bcm_2 + d)n = 1$
- <1>2. Multiplication is associative.
- <1>3. 1 is the identity element.
- <1>4. Every element has an inverse.
- <2>1. LET:  $a \in (\mathbb{Z}/n\mathbb{Z})^*$
- <2>2. PICK integers  $b, c$  such that  $ab + cn = 1$
- <2>3.  $ab = 1$  in  $(\mathbb{Z}/n\mathbb{Z})^*$

□

**Proposition 5.7** (Cancellation). *Let  $G$  be a group. Let  $a, g, h \in G$ . If  $ag = ah$  or  $ga = ha$  then  $g = h$ .*

PROOF: If  $ag = ah$  then  $g = a^{-1}ag = a^{-1}ah = h$ . Similarly if  $ga = ha$ . □

**Proposition 5.8.** *Let  $G$  be a group and  $g, h \in G$ . Then  $(gh)^{-1} = h^{-1}g^{-1}$ .*

PROOF: Since  $ghh^{-1}g^{-1} = e$ .  $\square$

**Definition 5.9.** Let  $G$  be a group. Let  $g \in G$ . We define  $g^n \in G$  for all  $n \in \mathbb{Z}$  as follows:

$$\begin{aligned} g^0 &= e \\ g^{n+1} &= g^n g & (n \geq 0) \\ g^{-n} &= (g^{-1})^n & (n > 0) \end{aligned}$$

**Proposition 5.10.** Let  $G$  be a group. Let  $g \in G$  and  $m, n \in \mathbb{Z}$ . Then

$$g^{m+n} = g^m g^n .$$

PROOF:

$\langle 1 \rangle 1$ . For all  $k \in \mathbb{Z}$  we have  $g^{k+1} = g^k g$

$\langle 2 \rangle 1$ . For all  $k \geq 0$  we have  $g^{k+1} = g^k g$

PROOF: Immediate from definition.

$\langle 2 \rangle 2$ .  $g^{-1+1} = g^{-1} g$

PROOF: Both are equal to  $e$ .

$\langle 2 \rangle 3$ . For all  $k > 1$  we have  $g^{-k+1} = g^{-k} g$

PROOF:

$$\begin{aligned} g^{-k+1} &= (g^{-1})^{k-1} \\ &= (g^{-1})^{k-1} g^{-1} g \\ &= (g^{-1})^k g \\ &= g^{-k} g \end{aligned}$$

$\langle 1 \rangle 2$ . For all  $k \in \mathbb{Z}$  we have  $g^{k-1} = g^k g^{-1}$

PROOF: Substitute  $k = k - 1$  above and multiply by  $g^{-1}$ .

$\langle 1 \rangle 3$ .  $g^{m+0} = g^m g^0$

PROOF: Since  $g^m g^0 = g^m e = g^m$ .

$\langle 1 \rangle 4$ . If  $g^{m+n} = g^m g^n$  then  $g^{m+n+1} = g^m g^{n+1}$

PROOF:

$$\begin{aligned} g^{m+n+1} &= g^{m+n} g & (\langle 1 \rangle 1) \\ &= g^m g^n g \\ &= g^m g^{n+1} & (\langle 1 \rangle 1) \end{aligned}$$

$\langle 1 \rangle 5$ . If  $g^{m+n} = g^m g^n$  then  $g^{m+n-1} = g^m g^{n-1}$

PROOF:

$$\begin{aligned} g^{m+n-1} g &= g^{m+n} & (\langle 1 \rangle 1) \\ &= g^m g^n \\ \therefore g^{m+n-1} &= g^m g^n g^{-1} \\ &= g^m g^{n-1} & (\langle 1 \rangle 2) \end{aligned}$$

$\square$

**Proposition 5.11.** Let  $G$  be a group. Let  $g \in G$  and  $m, n \in \mathbb{Z}$ . Then

$$(g^m)^n = g^{mn} .$$

PROOF:

$$\langle 1 \rangle 1. (g^m)^0 = g^0$$

PROOF: Both sides are equal to  $e$ .

$$\langle 1 \rangle 2. \text{ If } (g^m)^n = g^{mn} \text{ then } (g^m)^{n+1} = g^{m(n+1)}.$$

PROOF:

$$(g^m)^{n+1} = (g^m)^n g^m \quad (\text{Proposition 5.10})$$

$$= g^{mn} g^m$$

$$= g^{mn+m} \quad (\text{Proposition 5.10})$$

$$\langle 1 \rangle 3. \text{ If } (g^m)^n = g^{mn} \text{ then } (g^m)^{n-1} = g^{m(n-1)}.$$

PROOF:

$$(g^m)^n = g^{mn}$$

$$\therefore (g^m)^{n-1} g^m = g^{mn-m} g^m \quad (\text{Proposition 5.10})$$

$$\therefore (g^m)^{n-1} = g^{mn-m} \quad (\text{Cancellation})$$

□

**Definition 5.12** (Commute). Let  $G$  be a group and  $g, h \in G$ . We say  $g$  and  $h$  *commute* iff  $gh = hg$ .

## 5.1 Order of an Element

**Definition 5.13** (Order). Let  $G$  be a group. Let  $g \in G$ . Then  $g$  has *finite order* iff there exists a positive integer  $n$  such that  $g^n = e$ . In this case, the *order* of  $g$ , denoted  $|g|$ , is the least positive integer  $n$  such that  $g^n = e$ .

If  $g$  does not have finite order, we write  $|g| = \infty$ .

**Proposition 5.14.** Let  $G$  be a group. Let  $g \in G$  and  $n$  be a positive integer. If  $g^n = e$  then  $|g| \mid n$ .

PROOF:

$$\langle 1 \rangle 1. \text{ LET: } n = q|g| + d \text{ where } 0 \leq d < |g|$$

PROOF: Division Algorithm.

$$\langle 1 \rangle 2. g^d = e$$

PROOF:

$$e = g^n$$

$$= g^{q|g|+d}$$

$$= (g^{|g|})^q g^d \quad (\text{Propositions 5.10, 5.11})$$

$$= e^q g^d$$

$$= g^d$$

$$\langle 1 \rangle 3. d = 0$$

PROOF: By minimality of  $|g|$ .

$$\langle 1 \rangle 4. n = q|g|$$

□



**Corollary 5.14.1.** *Let  $G$  be a group. Let  $g \in G$  have finite order and  $n \in \mathbb{Z}$ . Then  $g^n = e$  if and only if  $|g| \mid n$ .*

**Proposition 5.15.** *Let  $G$  be a group and  $g \in G$ . Then  $|g| \leq |G|$ .*

PROOF:

$\langle 1 \rangle 1$ . ASSUME: w.l.o.g.  $G$  is finite.

$\langle 1 \rangle 2$ . PICK  $i, j$  with  $0 \leq i < j \leq |G|$  such that  $g^i = g^j$ .

PROOF: Otherwise  $g^0, g^1, \dots, g^{|G|}$  would be  $|G| + 1$  distinct elements of  $G$ .

$\langle 1 \rangle 3$ .  $g^{j-i} = e$

$\langle 1 \rangle 4$ .  $g$  has finite order and  $|g| \leq |G|$

PROOF: Since  $|g| \leq j - i \leq j \leq |G|$ .

□

**Proposition 5.16.** *Let  $G$  be a group. Let  $g \in G$  have finite order. Let  $m \in \mathbb{N}$ . Then*

$$|g^m| = \frac{\text{lcm}(m, |g|)}{m} = \frac{|g|}{\text{gcd}(m, |g|)}$$

PROOF: Since for any integer  $d$  we have

$$g^{md} = e \Leftrightarrow |g| \mid md \quad (\text{Corollary 5.14.1})$$

$$\Leftrightarrow \text{lcm}(m, |g|) \mid md$$

$$\Leftrightarrow \frac{\text{lcm}(m, |g|)}{m} \mid d \quad \square$$

and so  $|g^m| = \frac{\text{lcm}(m, |g|)}{m}$  by Corollary 5.14.1. □

**Corollary 5.16.1.** *If  $g$  has odd order then  $|g^2| = |g|$ .*

**Corollary 5.16.2.** *Let  $m$  and  $n$  be integers with  $n > 0$ . The order of  $m$  in  $\mathbb{Z}/n\mathbb{Z}$  is  $\frac{n}{\text{gcd}(m, n)}$ .*

PROOF: Since the order of 1 is  $n$ . □

**Proposition 5.17.** *Let  $G$  be a group. Let  $g, h \in G$  have finite order. Assume  $gh = hg$ . Then  $|gh|$  has finite order and*

$$|gh| \mid \text{lcm}(|g|, |h|)$$

PROOF: Since  $(gh)^{\text{lcm}(|g|, |h|)} = g^{\text{lcm}(|g|, |h|)} h^{\text{lcm}(|g|, |h|)} = e$ . □

**Example 5.18.** This example shows that we cannot remove the hypothesis that  $gh = hg$ .

In  $\text{GL}_2(\mathbb{R})$ , take

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Then  $|g| = 4$ ,  $|h| = 3$  and  $|gh| = \infty$ .

**Proposition 5.19.** *Let  $G$  be a group and  $g, h \in G$  have finite order. If  $gh = hg$  and  $\text{gcd}(|g|, |h|) = 1$  then  $|gh| = |g||h|$ .*

PROOF:

$$\langle 1 \rangle 1. \text{ LET: } N = |gh|$$

$$\langle 1 \rangle 2. g^N = (h^{-1})^N$$

$$\langle 1 \rangle 3. g^{N|g|} = e$$

$$\langle 1 \rangle 4. |g^N| \mid |g|$$

$$\langle 1 \rangle 5. h^{-N|h|} = e$$

$$\langle 1 \rangle 6. |g^N| \mid |h|$$

$$\langle 1 \rangle 7. |g^N| = 1$$

PROOF: Since  $\gcd(|g|, |h|) = 1$ .

$$\langle 1 \rangle 8. g^N = e$$

$$\langle 1 \rangle 9. |g| \mid N$$

$$\langle 1 \rangle 10. h^{-N} = e$$

$$\langle 1 \rangle 11. |h| \mid N$$

$$\langle 1 \rangle 12. N = |g||h|$$

PROOF: Using Proposition 5.17.

□

**Proposition 5.20.** *Let  $G$  be a finite group. Assume there is exactly one element  $f \in G$  of order 2. Then the product of all the elements of  $G$  is  $f$ .*

PROOF: Let the elements of  $G$  be  $g_1, g_2, \dots, g_n$ . Apart from  $e$  and  $f$ , every element and its inverse are distinct elements of the list. Hence the product of the list is  $ef = f$ . □

**Proposition 5.21.** *Let  $G$  be a finite group of order  $n$ . Let  $m$  be the number of elements of  $G$  of order 2. Then  $n - m$  is odd.*

PROOF: In the list of all elements that are not of order 2, every element and its inverse are distinct except for  $e$ . Hence the list has odd length. □

**Corollary 5.21.1.** *If a finite group has even order, then it contains an element of order 2.*

**Proposition 5.22.** *Let  $G$  be a group and  $a, g \in G$ . Then  $|aga^{-1}| = |g|$ .*

PROOF: Since

$$(aga^{-1})^n = e \Leftrightarrow ag^na^{-1} = e$$

$$\Leftrightarrow g^n = e$$

□

**Proposition 5.23.** *Let  $G$  be a group and  $g, h \in G$ . Then  $|gh| = |hg|$ .*

PROOF: Since  $|gh| = |ghgg^{-1}| = |hg|$ . □

## 5.2 Generators

**Definition 5.24** (Generator). Let  $G$  be a group and  $a \in G$ . We say  $a$  *generates* the group iff, for all  $x \in G$ , there exists an integer  $n$  such that  $x^n = a$ .

**Proposition 5.25.** *The integer  $m$  generates  $\mathbb{Z}/n\mathbb{Z}$  if and only if  $\gcd(m, n) = 1$ .*

PROOF: By Corollary 5.16.2.  $\square$

**Corollary 5.25.1.** *If  $p$  is prime then every non-zero element in  $\mathbb{Z}/p\mathbb{Z}$  is a generator.*



## Chapter 6

# Group Homomorphisms

**Definition 6.1** (Homomorphism). Let  $G$  and  $H$  be groups. A (group) *homomorphism*  $\phi : G \rightarrow H$  is a function such that, for all  $x, y \in G$ ,

$$\phi(xy) = \phi(x)\phi(y) \ .$$

**Proposition 6.2.** Let  $G$  and  $H$  be groups with identities  $e_G$  and  $e_H$ . Let  $\phi : G \rightarrow H$  be a group homomorphism. Then  $\phi(e_G) = e_H$ .

PROOF: Since  $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$  and so  $\phi(e_G) = e_H$  by Cancellation.  $\square$

**Proposition 6.3.** Let  $\phi : G \rightarrow H$  be a group homomorphism. For all  $x \in G$  we have  $\phi(x^{-1}) = \phi(x)^{-1}$ .

PROOF: Since  $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(e_G) = e_H$ .  $\square$

**Proposition 6.4.** Let  $G, H$  and  $K$  be groups. If  $\phi : G \rightarrow H$  and  $\psi : H \rightarrow K$  are homomorphisms then  $\psi \circ \phi : G \rightarrow K$  is a homomorphism.

PROOF: For  $x, y \in G$  we have

$$\psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\psi(\phi(y)) \ .$$

**Proposition 6.5.** Let  $G$  be a group. Then  $\text{id}_G : G \rightarrow G$  is a group homomorphism.

PROOF: For  $x, y \in G$  we have  $\text{id}_G(xy) = xy = \text{id}_G(x)\text{id}_G(y)$ .  $\square$

**Definition 6.6** (Category of Groups). Let **Grp** be the category of groups and group homomorphisms.



## Chapter 7

# Abelian Groups

**Definition 7.1** (Abelian Group). A group is *Abelian* iff any two elements commute.

In an Abelian group  $G$ , we often denote the group operation by  $+$ , the identity element by  $0$  and the inverse of an element  $g$  by  $-g$ . We write  $ng$  for  $g^n$  ( $g \in G, n \in \mathbb{Z}$ ).

**Example 7.2.** Every group of order  $\leq 4$  is Abelian.

**Example 7.3.** For any positive integer  $n$ , we have  $\mathbb{Z}/n\mathbb{Z}$  is an Abelian group under addition.

**Example 7.4.**  $S_n$  is not Abelian for  $n \geq 3$ . If  $x = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$  and  $y = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$  then  $xy = \begin{pmatrix} 2 & 3 \end{pmatrix}$  and  $yx = \begin{pmatrix} 1 & 3 \end{pmatrix}$ .

**Proposition 7.5.** Let  $G$  be a group. If  $g^2 = e$  for all  $g \in G$  then  $G$  is Abelian.

PROOF: For any  $g, h \in G$  we have

$$ghgh = e$$

$$\therefore hgh = g \quad (\text{multiplying on the left by } g)$$

$$\therefore hg = gh \quad (\text{multiplying on the right by } h) \square$$

**Proposition 7.6.** Let  $G$  be an Abelian group. Let  $g, h \in G$ . If  $g$  has maximal finite order in  $G$ , and  $h$  has finite order, then  $|h| \mid |g|$ .

PROOF:

$\langle 1 \rangle 1$ . ASSUME: for a contradiction  $|h| \nmid |g|$ .

$\langle 1 \rangle 2$ . PICK a prime  $p$  such that  $|g| = p^m r$ ,  $|h| = p^n s$  where  $p \nmid r$ ,  $p \nmid s$  and  $m < n$ .

$\langle 1 \rangle 3$ .  $|g^{p^m} h^s| = p^n r$

PROOF: Proposition 5.19.

$\langle 1 \rangle 4$ .  $|g| < |g^{p^m} h^s|$

$\langle 1 \rangle 5$ . Q.E.D.

PROOF: This contradicts the maximality of  $|g|$ .

$\square$





## Part III

# Linear Algebra



**Definition 7.7.** Let  $\text{GL}_n(\mathbb{R})$  be the group of invertible  $n \times n$  real matrices.