

# Mathematics

Robin Adams

April 6, 2024



# Contents

<b>I</b>	<b>Category Theory</b>	<b>7</b>
<b>1</b>	<b>Foundations</b>	<b>9</b>
<b>2</b>	<b>Categories</b>	<b>11</b>
2.1	Preorders . . . . .	12
2.2	Monomorphisms and Epimorphisms . . . . .	12
2.3	Sections and Retractions . . . . .	14
2.4	Isomorphisms . . . . .	15
2.5	Initial and Terminal Objects . . . . .	15
<b>3</b>	<b>Functors</b>	<b>17</b>
3.1	Comma Categories . . . . .	17
<b>II</b>	<b>Group Theory</b>	<b>19</b>
<b>4</b>	<b>Semigroups</b>	<b>21</b>
<b>5</b>	<b>Monoids</b>	<b>23</b>
<b>6</b>	<b>Groups</b>	<b>25</b>
6.1	Order of an Element . . . . .	28
6.2	Generators . . . . .	31
<b>7</b>	<b>Group Homomorphisms</b>	<b>33</b>
7.1	Subgroups . . . . .	35
7.2	Kernel . . . . .	36
7.3	Inner Automorphisms . . . . .	37
7.4	Direct Products . . . . .	38
7.5	Free Groups . . . . .	38
7.6	Normal Subgroups . . . . .	41
7.7	Quotient Groups . . . . .	42
7.8	Cosets . . . . .	46
7.9	Congruence . . . . .	50
7.10	Cyclic Groups . . . . .	51

7.11	Commutator Subgroup . . . . .	51
7.12	Presentations . . . . .	51
7.13	Index of a Subgroup . . . . .	52
7.14	Cokernels . . . . .	53
7.15	Cayley Graphs . . . . .	54
<b>8</b>	<b>Abelian Groups</b>	<b>55</b>
8.1	The Category of Abelian Groups . . . . .	59
8.2	Free Abelian Groups . . . . .	60
8.3	Cokernels . . . . .	63
<b>9</b>	<b>Group Actions</b>	<b>65</b>
9.1	Group Actions . . . . .	65
9.2	Category of $G$ -Sets . . . . .	68
<b>III</b>	<b>Ring Theory</b>	<b>71</b>
<b>10</b>	<b>Rngs</b>	<b>73</b>
10.1	Commutative Rngs . . . . .	75
10.2	Rng Homomorphisms . . . . .	75
10.3	Quaternions . . . . .	75
<b>11</b>	<b>Rings</b>	<b>77</b>
11.1	Units . . . . .	78
11.2	Euler's $\phi$ -function . . . . .	80
11.3	Nilpotent Elements . . . . .	82
<b>12</b>	<b>Ring Homomorphisms</b>	<b>83</b>
12.1	Products . . . . .	85
<b>13</b>	<b>Subrings</b>	<b>87</b>
13.1	Centralizer . . . . .	87
13.2	Center . . . . .	87
<b>14</b>	<b>Monoid Rings</b>	<b>89</b>
14.1	Polynomials . . . . .	89
14.2	Laurent Polynomials . . . . .	91
14.3	Power Series . . . . .	91
<b>15</b>	<b>Ideals</b>	<b>93</b>
15.1	Characteristic . . . . .	96
15.2	Nilradical . . . . .	96
15.3	Principal Ideals . . . . .	96
<b>16</b>	<b>Integral Domains</b>	<b>99</b>

<i>CONTENTS</i>	5
17 Unique Factorization Domains	101
18 Noetherian Rings	103
19 Principal Ideal Domains	105
20 Euclidean Domains	107
21 Division Rings	109
22 Simple Rings	111
23 Reduced Rings	113
24 Boolean Rings	115
IV Field Theory	117
25 Fields	119
V Linear Algebra	121



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

## Categories

**Definition 2.1** (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 2.2.** *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 2.3** (Category of Sets). The *category of sets* **Set** has objects all sets and morphisms all functions.

**Definition 2.4** (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 2.5** (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

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

## 2.1 Preorders

**Definition 2.6** (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 2.7.** For any ordinal  $\alpha$ , let  $\alpha$  be the preorder  $\{\beta : \beta < \alpha\}$  under  $\leq$ .

**Definition 2.8** (Discrete Preorder). We identify any set  $A$  with the *discrete* preorder  $(A, =)$ .

## 2.2 Monomorphisms and Epimorphisms

**Definition 2.9** (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 2.10** (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 2.11.** *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 2.12.** *The composite of two epimorphisms is epi.*

PROOF: Dual. □

**Proposition 2.13.** *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  $g \circ f \circ x = g \circ f \circ y$  and so  $x = y$ . □

**Proposition 2.14.** *Let  $f : A \rightarrow B$  and  $g : B \rightarrow C$ . If  $g \circ f$  is epi then  $g$  is epi.*

PROOF: Dual. □

**Proposition 2.15.** *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 2.16.** *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 2.17.** *In a preorder, every morphism is monic and epi.*

PROOF: Immediate from definitions.  $\square$

## 2.3 Sections and Retractions

**Definition 2.18** (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 2.19.** *Every identity morphism is a section and retraction of itself.*

PROOF: Immediate from definitions.  $\square$

**Proposition 2.20.** *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 2.21.** *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 2.22.** *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 2.23.** *Every retraction is epi.*

PROOF: Dual.  $\square$

**Proposition 2.24.** *In Set, every epimorphism has a retraction.*

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

**Example 2.25.** 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.

## 2.4 Isomorphisms

**Definition 2.26** (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 2.27.** *The inverse of an isomorphism is unique.*

PROOF: Proposition 2.20.  $\square$

**Proposition 2.28.** *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 2.29.** *If  $f : A \cong B$  then  $f^{-1} : B \cong A$  and  $(f^{-1})^{-1} = f$ .*

PROOF: Immediate from definitions.  $\square$

**Proposition 2.30.** *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 2.21.  $\square$

**Definition 2.31** (Groupoid). A *groupoid* is a category in which every morphism is an isomorphism.

## 2.5 Initial and Terminal Objects

**Definition 2.32** (Initial Object). An object  $I$  in a category is *initial* iff, for any object  $X$ , there is exactly one morphism  $I \rightarrow X$ .

**Example 2.33.** The empty set is the initial object in **Set**.

**Definition 2.34** (Terminal Object). An object  $T$  in a category is *terminal* iff, for any object  $X$ , there is exactly one morphism  $X \rightarrow T$ .

**Example 2.35.** Every singleton is terminal in **Set**.

**Proposition 2.36.** *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 2.37.** *If  $S$  and  $T$  are terminal in a category, then there exists a unique isomorphism  $S \cong T$ .*

PROOF: Dual.  $\square$



## Chapter 3

# Functors

**Definition 3.1** (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 3.2** (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 3.3** (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

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

### 3.1 Comma Categories

**Definition 3.4** (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 3.5** (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 3.6** (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 3.7** (Pointed Sets). The *category of pointed sets*  $\mathbf{Set}_*$  is the coslice category  $\mathbf{Set} \backslash 1$ .

**Part II**

**Group Theory**



## Chapter 4

# Semigroups

**Definition 4.1** (Semigroup). A *semigroup* consists of a set  $S$  and an associative binary operation  $\cdot$  on  $S$ .



## Chapter 5

# Monoids

**Definition 5.1** (Monoid). A *monoid* consists of a semigroup  $M$  such that there exists  $e \in M$ , the *unit*, such that, for all  $x \in M$ , we have  $xe = ex = x$ .

We identify a monoid  $M$  with the category with one object whose morphisms are the elements of  $M$ , with composition given by  $\cdot$ .

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

PROOF: Proposition 2.2.





# Chapter 6

## Groups

**Definition 6.1** (Group). Let  $\mathcal{C}$  be a category with finite products. A *group (object)* in  $\mathcal{C}$  consists of an object  $G \in \mathcal{C}$  and morphisms

$$m : G^2 \rightarrow G, e : 1 \rightarrow G, i : G \rightarrow G$$

such that the following diagrams commute.

$$\begin{array}{ccc} G^3 & \xrightarrow{m \times \text{id}_G} & G^2 \\ \downarrow \text{id}_G \times m & & \downarrow m \\ G^2 & \xrightarrow{m} & G \end{array}$$
  

$$\begin{array}{ccc} 1 \times G & \xrightarrow{e \times \text{id}_G} & G^2 \\ & \searrow \cong & \downarrow m \\ & & G \end{array} \quad \begin{array}{ccc} G \times 1 & \xrightarrow{\text{id}_G \times e} & G^2 \\ & \searrow \cong & \downarrow m \\ & & G \end{array}$$
  

$$\begin{array}{ccccc} G & \xrightarrow{\Delta} & G^2 & \xrightarrow{\text{id}_G \times i} & G^2 \\ \downarrow & & & & \downarrow m \\ 1 & \xrightarrow{e} & G & & G \end{array} \quad \begin{array}{ccccc} G & \xrightarrow{\Delta} & G^2 & \xrightarrow{i \times \text{id}_G} & G^2 \\ \downarrow & & & & \downarrow m \\ 1 & \xrightarrow{e} & G & & G \end{array}$$

**Definition 6.2** (Group). We write just 'group' for 'group in **Set**'. Thus, 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  $xx^{-1} = x^{-1}x = e$ .

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 6.3.** *The inverse of an element is unique.*

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

**Example 6.4.** • 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
- 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.
- Let  $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$  under matrix multiplication.
- The quaternionic group  $Q_8$  is the group

$$\{1, -1, i, -i, j, -j, k, -k\}$$

with multiplication table

1	-1	i	-i	j	-j	k	-k
-1	1	-i	i	-j	j	-k	k
i	-i	-1	1	k	-k	-j	j
-i	i	1	-1	-k	k	j	-j
j	-j	-k	k	-1	1	i	-i
-j	j	k	-k	1	-1	-i	i
k	-k	j	-j	-i	i	-1	1
-k	k	-j	j	i	-i	1	-1

**Example 6.5.** • 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  $(a, b)(c, d) = (ac, bd)$ .

**Proposition 6.6** (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  $ga = ha$ .  $\square$

**Proposition 6.7.** *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 6.8.** 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 6.9.** *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:

$$g^{m+n-1}g = g^{m+n} \quad (\langle 1 \rangle 1)$$

$$= g^m g^n$$

$$\therefore g^{m+n-1} = g^m g^n g^{-1}$$

$$= g^m g^{n-1} \quad (\langle 1 \rangle 2)$$

□

**Proposition 6.10.** 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  $e$ .

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

PROOF:

$$(g^m)^{n+1} = (g^m)^n g^m \quad (\text{Proposition 6.9})$$

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

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

(Proposition 6.9)

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

PROOF:

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

$$\therefore (g^m)^{n-1} g^m = g^{mn-m} g^m \quad (\text{Proposition 6.9})$$

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

□

**Definition 6.11** (Commute). Let  $G$  be a group and  $g, h \in G$ . We say  $g$  and  $h$  *commute* iff  $gh = hg$ .

**Definition 6.12.** Let  $G$  be a group. Given  $g \in G$  and  $A \subseteq G$ , we define

$$gA = \{ga : a \in A\}, \quad Ag = \{ag : a \in A\} .$$

Given sets  $A, B \subseteq G$ , we define

$$AB = \{ab : a \in A, b \in B\} .$$

## 6.1 Order of an Element

**Definition 6.13** (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 6.14.** *Let  $G$  be a group. Let  $g \in G$  and  $n$  be a positive integer. If  $g^n = e$  then  $|g| \mid n$ .*

PROOF:

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

PROOF: Division Algorithm.

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

PROOF:

$$\begin{aligned} e &= g^n \\ &= g^{q|g|+d} \\ &= (g^{|g|})^q g^d && \text{(Propositions 6.9, 6.10)} \\ &= e^q g^d \\ &= g^d \end{aligned}$$

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

PROOF: By minimality of  $|g|$ .

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

□

**Corollary 6.14.1.** *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 6.15.** *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 6.16.** *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

$$g^{md} = e \Leftrightarrow |g| \mid md \quad (\text{Corollary 6.14.1})$$

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

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

□

and so  $|g^m| = \frac{\text{lcm}(m, |g|)}{m}$  by Corollary 6.14.1. □

**Corollary 6.16.1.** *If  $g$  has odd order then  $|g^2| = |g|$ .*

**Proposition 6.17.** *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  $(gh)^{\text{lcm}(|g|, |h|)} = g^{\text{lcm}(|g|, |h|)} h^{\text{lcm}(|g|, |h|)} = e$ .  $\square$

**Example 6.18.** 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 6.19.** *Let  $G$  be a group and  $g, h \in G$  have finite order. If  $gh = hg$  and  $\gcd(|g|, |h|) = 1$  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 6.17.

$\square$

**Proposition 6.20.** *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  $ef = f$ .  $\square$

**Proposition 6.21.** *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.  $\square$

**Corollary 6.21.1.** *If a finite group has even order, then it contains an element of order 2.*

**Proposition 6.22.** *Let  $G$  be a group and  $a, g \in G$ . Then  $|aga^{-1}| = |g|$ .*

PROOF: Since

$$\begin{aligned} (aga^{-1})^n = e &\Leftrightarrow ag^na^{-1} = e \\ &\Leftrightarrow g^n = e \end{aligned} \quad \square$$

**Proposition 6.23.** *Let  $G$  be a group and  $g, h \in G$ . Then  $|gh| = |hg|$ .*

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

**Proposition 6.24.** *Let  $G$  be a group of order  $n$ . Let  $k$  be relatively prime to  $n$ . Then every element in  $G$  has the form  $x^k$  for some  $x$ .*

$\langle 1 \rangle 1$ . PICK integers  $a$  and  $b$  such that  $an + bk = 1$ .

$\langle 1 \rangle 2$ . LET:  $g \in G$

$\langle 1 \rangle 3$ .  $g = (g^b)^k$

PROOF:

$$\begin{aligned} g &= g \cdot (g^n)^{-a} & (g^n = e) \\ &= g^{1-an} \\ &= g^{bk} \end{aligned}$$

$\square$

## 6.2 Generators

**Definition 6.25** (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  $x^n = a$ .

**Example 6.26.**  $\text{SL}_2(\mathbb{Z})$  is generated by

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $H = \langle s, t \rangle$

$\langle 1 \rangle 2$ . For all  $q \in \mathbb{Z}$  we have  $\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \in H$ .

PROOF: It is  $t^q$ .

$\langle 1 \rangle 3$ . For all  $q \in \mathbb{Z}$  we have  $\begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} \in H$ .

PROOF:

$$\begin{aligned} st^{-q}s^{-1} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} \end{aligned}$$

⟨1⟩4.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & qa+b \\ c & qc+d \end{pmatrix}$$

⟨1⟩5.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} = \begin{pmatrix} a+qb & b \\ c+qd & d \end{pmatrix}$$

⟨1⟩6. For any  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ , if  $c$  and  $d$  are both nonzero, then there exists  $N \in H$  such that the bottom row of  $MN$  has one entry the same as  $M$  and one entry with smaller absolute value.

PROOF: From ⟨1⟩4 and ⟨1⟩5 taking  $q = -1$ .

⟨1⟩7. For any  $M \in \text{SL}_2(\mathbb{Z})$ , there exists  $N \in H$  such that  $MN$  has a zero on the bottom row.

PROOF: Apply ⟨1⟩6 repeatedly.

⟨1⟩8. Any matrix in  $\text{SL}_2(\mathbb{Z})$  with a zero on the bottom row is in  $H$ .

⟨2⟩1.  $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H$

PROOF: ⟨1⟩2

⟨2⟩2.  $\begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} \in H$

PROOF: It is  $s^2 \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$  since  $s^2 = -I$ .

⟨2⟩3.  $\begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix} \in H$

PROOF: It is  $\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} s$ .

⟨2⟩4.  $\begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \in H$

PROOF: It is  $s^2 \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} s$ .

⟨1⟩9. Every matrix in  $\text{SL}_2(\mathbb{Z})$  is in  $H$ .

□



## Chapter 7

# Group Homomorphisms

**Definition 7.1** (Homomorphism). Let  $G$  and  $H$  be groups. A (group) homomorphism  $\phi : G \rightarrow H$  is a function such that, for all  $x, y \in G$ ,

$$\phi(xy) = \phi(x)\phi(y) \text{ .}$$

**Proposition 7.2.** 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 7.3.** 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 7.4.** 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

$$\psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\psi(\phi(y)) \text{ .}$$

**Proposition 7.5.** Let  $G$  be a group. Then  $\text{id}_G : G \rightarrow G$  is a group homomorphism.

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

**Proposition 7.6.** Let  $\phi : G \rightarrow H$  be a group homomorphism. Let  $g \in G$  have finite order. Then  $|\phi(g)|$  divides  $|g|$ .

PROOF: Since  $\phi(g)^{|g|} = \phi(g^{|g|}) = e$ .  $\square$

**Definition 7.7** (Category of Groups). Let **Grp** be the category of groups and group homomorphisms.

**Example 7.8.** There are 49487365402 groups of order 1024 up to isomorphism.

**Proposition 7.9.** *A group homomorphism  $\phi : G \rightarrow H$  is an isomorphism in **Grp** if and only if it is bijective.*

PROOF:

$\langle 1 \rangle 1.$  ASSUME:  $\phi$  is bijective.

PROVE:  $\phi^{-1}$  is a group homomorphism.

$\langle 1 \rangle 2.$  LET:  $h, h' \in H$

$\langle 1 \rangle 3.$   $\phi(\phi^{-1}(hh')) = \phi(\phi^{-1}(h)\phi^{-1}(h'))$

PROOF: Both are equal to  $hh'$ .

$\langle 1 \rangle 4.$   $\phi^{-1}(hh') = \phi^{-1}(h)\phi^{-1}(h')$

□

**Corollary 7.9.1.**

$$D_6 \cong C_3$$

PROOF: The canonical homomorphism  $D_6 \rightarrow C_3$  is bijective. □

**Corollary 7.9.2.**

$$(\mathbb{R}, +) \cong (\{x \in \mathbb{R} : x > 0\}, \cdot)$$

PROOF: The function that maps  $x$  to  $e^x$  is a bijective homomorphism. □

**Proposition 7.10.** *The trivial group is the zero object in **Grp**.*

PROOF: For any group  $G$ , the unique function  $G \rightarrow \{e\}$  is a group homomorphism, and the only group homomorphism  $\{e\} \rightarrow G$  maps  $e$  to  $e_G$ . □

**Proposition 7.11.** *For any groups  $G$  and  $H$ , the set  $G \times H$  under  $(g, h)(g', h') = (gg', hh')$  is the product of  $G$  and  $H$  in **Grp**.*

PROOF:

$\langle 1 \rangle 1.$   $G \times H$  is a group.

$\langle 2 \rangle 1.$  The multiplication is associative.

PROOF: Since  $(g_1, h_1)((g_2, h_2)(g_3, h_3)) = ((g_1, h_1)(g_2, h_2))(g_3, h_3) = (g_1g_2g_3, h_1h_2h_3)$ .

$\langle 2 \rangle 2.$   $(e_G, e_H)$  is the identity.

PROOF: Since  $(g, h)(e_G, e_H) = (e_G, e_H)(g, h) = (g, h)$ .

$\langle 2 \rangle 3.$  The inverse of  $(g, h)$  is  $(g^{-1}, h^{-1})$ .

PROOF: Since  $(g, h)(g^{-1}, h^{-1}) = (g^{-1}, h^{-1})(g, h) = (e_G, e_H)$ .

$\langle 1 \rangle 2.$   $\pi_1 : G \times H \rightarrow G$  is a group homomorphism.

PROOF: Immediate from definitions.

$\langle 1 \rangle 3.$   $\pi_2 : G \times H \rightarrow H$  is a group homomorphism.

PROOF: Immediate from definitions.

$\langle 1 \rangle 4.$  For any group homomorphism  $\phi : K \rightarrow G$  and  $\psi : K \rightarrow H$ , the function  $\langle \phi, \psi \rangle : K \rightarrow G \times H$  where  $\langle \phi, \psi \rangle(k) = (\phi(k), \psi(k))$  is a group homomorphism.

PROOF:

$$\begin{aligned} \langle \phi, \psi \rangle(kk') &= (\phi(kk'), \psi(kk')) \\ &= (\phi(k)\phi(k'), \psi(k)\psi(k')) \\ &= (\phi(k), \psi(k))(\phi(k'), \psi(k')) \\ &= \langle \phi, \psi \rangle(k)\langle \phi, \psi \rangle(k') \end{aligned}$$

□

## 7.1 Subgroups

**Definition 7.12** (Subgroup). Let  $(G, \cdot)$  and  $(H, *)$  be groups such that  $H$  is a subset of  $G$ . Then  $H$  is a *subgroup* of  $G$  iff the inclusion  $i : H \hookrightarrow G$  is a group homomorphism.

**Proposition 7.13.** *If  $(H, *)$  is a subgroup of  $(G, \cdot)$  then  $*$  is the restriction of  $\cdot$  to  $H$ .*

PROOF: Given  $x, y \in H$  we have

$$x * y = i(x * y) = i(x) \cdot i(y) = x \cdot y . \quad \square$$

**Example 7.14.** For any group  $G$  we have  $\{e\}$  is a subgroup of  $G$ .

**Proposition 7.15.** *Let  $G$  be a group. Let  $H$  be a subset of  $G$ . Then  $H$  is a subgroup of  $G$  iff  $H$  is nonempty and, for all  $x, y \in H$ , we have  $xy^{-1} \in H$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $H$  is a subgroup of  $G$  then  $H$  is nonempty.

PROOF: Since every group has an identity element and so is nonempty.

$\langle 1 \rangle 2$ . If  $H$  is a subgroup of  $G$  then, for all  $x, y \in H$ , we have  $xy^{-1} \in H$ .

PROOF: Easy.

$\langle 1 \rangle 3$ . If  $H$  is nonempty and, for all  $x, y \in H$ , we have  $xy^{-1} \in H$ , then  $H$  is a subgroup of  $G$ .

$\langle 2 \rangle 1$ . ASSUME:  $H$  is nonempty.

$\langle 2 \rangle 2$ . ASSUME:  $\forall x, y \in H. xy^{-1} \in H$

$\langle 2 \rangle 3$ .  $e \in H$

PROOF: Pick  $x \in H$ . We have  $e = xx^{-1} \in H$ .

$\langle 2 \rangle 4$ .  $\forall x \in H. x^{-1} \in H$

PROOF: Given  $x \in H$  we have  $x^{-1} = ex^{-1} \in H$ .

$\langle 2 \rangle 5$ .  $H$  is closed under the restriction of  $\cdot$

PROOF: Given  $x, y \in H$  we have  $xy = x(y^{-1})^{-1} \in H$ .

$\langle 2 \rangle 6$ .  $H$  is a group under the restriction of  $\cdot$

PROOF: Associativity is inherited from  $G$  and the existence of an identity element and inverses follows from  $\langle 2 \rangle 3$  and  $\langle 2 \rangle 4$ .

$\langle 2 \rangle 7$ . The inclusion  $H \hookrightarrow G$  is a group homomorphism.

PROOF: For  $x, y \in H$  we have  $i(xy) = i(x)i(y) = xy$ .

$\square$

**Corollary 7.15.1.** *The intersection of a set of subgroups of  $G$  is a subgroup of  $G$ .*

**Corollary 7.15.2.** *Let  $\phi : G \rightarrow H$  be a group homomorphism. Let  $K$  be a subgroup of  $H$ . Then  $\phi^{-1}(K)$  is a subgroup of  $G$ .*

PROOF:

$\langle 1 \rangle 1$ .  $\phi^{-1}(K)$  is nonempty.

PROOF: Since  $e \in \phi^{-1}(K)$ .

$\langle 1 \rangle 2$ . LET:  $x, y \in \phi^{-1}(K)$

- $\langle 1 \rangle 3. \phi(x), \phi(y) \in K$
- $\langle 1 \rangle 4. \phi(x)\phi(y)^{-1} \in K$
- $\langle 1 \rangle 5. \phi(xy^{-1}) \in K$
- $\langle 1 \rangle 6. xy^{-1} \in \phi^{-1}(K)$

□

**Corollary 7.15.3.** *Let  $\phi : G \rightarrow H$  be a group homomorphism. Let  $K$  be a subgroup of  $G$ . Then  $\phi(K)$  is a subgroup of  $H$ .*

PROOF:

- $\langle 1 \rangle 1.$  LET:  $x, y \in \phi(K)$
- $\langle 1 \rangle 2.$  PICK  $a, b \in K$  such that  $x = \phi(a)$  and  $y = \phi(b)$
- $\langle 1 \rangle 3. xy^{-1} = \phi(ab^{-1})$
- $\langle 1 \rangle 4. xy^{-1} \in \phi(K)$

□

**Proposition 7.16.** *Let  $G$  be a subgroup of  $\mathbb{Z}$ . Then there exists  $d \geq 0$  such that  $G = d\mathbb{Z}$ .*

PROOF:

- $\langle 1 \rangle 1.$  ASSUME: w.l.o.g.  $G \neq \{0\}$

PROOF: Since  $\{0\} = 0\mathbb{Z}$ .

- $\langle 1 \rangle 2.$  LET:  $d$  be the least positive element of  $G$ .

PROVE:  $G = d\mathbb{Z}$

PROOF: If  $n \in G$  then  $-n \in G$  so  $G$  must contain a positive element.

- $\langle 1 \rangle 3. G \subseteq d\mathbb{Z}$

- $\langle 2 \rangle 1.$  LET:  $n \in G$

- $\langle 2 \rangle 2.$  LET:  $q$  and  $r$  be the integers such that  $n = qd + r$  and  $0 \leq r < d$ .

- $\langle 2 \rangle 3. r \in G$

PROOF: Since  $r = n - qd$ .

- $\langle 2 \rangle 4. r = 0$

PROOF: By minimality of  $d$ .

- $\langle 2 \rangle 5. n = qd \in d\mathbb{Z}$

- $\langle 1 \rangle 4. d\mathbb{Z} \subseteq G$

□

## 7.2 Kernel

**Definition 7.17** (Kernel). Let  $\phi : G \rightarrow H$  be a group homomorphism. The *kernel* of  $\phi$  is

$$\ker \phi = \{g \in G : \phi(g) = e\} .$$

**Proposition 7.18.** *Let  $\phi : G \rightarrow H$  be a group homomorphism. Then  $\ker \phi$  is a subgroup of  $G$ .*

PROOF: Corollary 7.15.2. □

**Proposition 7.19.** *Let  $\phi : G \rightarrow H$  be a group homomorphism. Then the inclusion  $i : \ker \phi \hookrightarrow G$  is terminal in the category of pairs  $(K, \alpha : K \rightarrow G)$  such that  $\phi \circ \alpha = 0$ .*

PROOF:

$\langle 1 \rangle 1.$   $\phi \circ i = 0$

$\langle 1 \rangle 2.$  For any group  $K$  and homomorphism  $\alpha : K \rightarrow G$  such that  $\phi \circ \alpha = 0$ , there exists a unique homomorphism  $\beta : K \rightarrow \ker \phi$  such that  $i \circ \beta = \alpha$ .

□

**Proposition 7.20.** *Let  $\phi : G \rightarrow H$  be a group homomorphism. Then the following are equivalent:*

1.  $\phi$  is monic.
2.  $\ker \phi = \{e\}$
3.  $\phi$  is injective.

PROOF:

$\langle 1 \rangle 1.$   $1 \Rightarrow 2$

$\langle 2 \rangle 1.$  ASSUME:  $\phi$  is monic.

$\langle 2 \rangle 2.$  LET:  $i : \ker \phi \hookrightarrow G, j : \{e\} \hookrightarrow \ker \phi \hookrightarrow G$  be the inclusions.

$\langle 2 \rangle 3.$   $\phi \circ i = \phi \circ j$

$\langle 2 \rangle 4.$   $i = j$

$\langle 1 \rangle 2.$   $2 \Rightarrow 3$

$\langle 2 \rangle 1.$  ASSUME:  $\ker \phi = \{e\}$

$\langle 2 \rangle 2.$  LET:  $x, y \in G$

$\langle 2 \rangle 3.$  ASSUME:  $\phi(x) = \phi(y)$

$\langle 2 \rangle 4.$   $\phi(xy^{-1}) = e$

$\langle 2 \rangle 5.$   $xy^{-1} \in \ker \phi$

$\langle 2 \rangle 6.$   $xy^{-1} = e$

$\langle 2 \rangle 7.$   $x = y$

$\langle 1 \rangle 3.$   $3 \Rightarrow 1$

PROOF: Easy.

□

**Proposition 7.21.** *A group homomorphism is an epimorphism if and only if it is surjective.*

## 7.3 Inner Automorphisms

**Proposition 7.22.** *Let  $G$  be a group and  $g \in G$ . The function  $\gamma_g : G \rightarrow G$  defined by  $\gamma_g(a) = gag^{-1}$  is an automorphism on  $G$ .*

PROOF:

$\langle 1 \rangle 1.$   $\gamma_g$  is a homomorphism.

PROOF:

$$\begin{aligned}\gamma_g(ab) &= gabg^{-1} \\ &= gag^{-1}gbg^{-1} \\ &= \gamma_g(a)\gamma_g(b)\end{aligned}$$

<1>2.  $\gamma_g$  is injective.

PROOF: By Cancellation.

<1>3.  $\gamma_g$  is surjective.

PROOF: Given  $b \in G$ , we have  $\gamma_g(g^{-1}bg) = b$ .

□

**Definition 7.23** (Inner Automorphism). Let  $G$  be a group. An *inner automorphism* on  $G$  is a function of the form  $\gamma_g(a) = gag^{-1}$  for some  $g \in G$ .

We write  $\text{Inn}(G)$  for the set of inner automorphisms of  $G$ .

**Proposition 7.24.** Let  $G$  be a group. The function  $\gamma : G \rightarrow \text{Aut}_{\mathbf{Grp}}(G)$  that maps  $g$  to  $\gamma_g$  is a group homomorphism.

PROOF: Since  $\gamma_{gh}(a) = ghah^{-1}g^{-1} = \gamma_g(\gamma_h(a))$ . □

**Corollary 7.24.1.**  $\text{Inn}(G)$  is a subgroup of  $\text{Aut}_{\mathbf{Grp}}(G)$ .

## 7.4 Direct Products

**Definition 7.25** (Direct Product). The *direct product* of groups  $G$  and  $H$  is their product in  $\mathbf{Grp}$ .

## 7.5 Free Groups

**Proposition 7.26.** Let  $A$  be a set. Let  $\mathcal{F}^A$  be the category whose objects are pairs  $(G, j)$  where  $G$  is a group and  $j$  is a function  $A \rightarrow G$ , with morphisms  $f : (G, j) \rightarrow (H, k)$  the group homomorphisms  $f : G \rightarrow H$  such that  $f \circ j = k$ . Then  $\mathcal{F}^A$  has an initial object.

PROOF:

<1>1. LET:  $W(A)$  be the set of words in the alphabet whose elements are the elements of  $A$  together with  $\{a^{-1} : a \in A\}$ .

<1>2. LET:  $r : W(A) \rightarrow W(A)$  be the function that, given a word  $w$ , removes the first pair of letters of the form  $aa^{-1}$  or  $a^{-1}a$ ; if there is no such pair, then  $r(w) = w$ .

<1>3. Let us say that a word  $w$  is a *reduced word* iff  $r(w) = w$ .

<1>4. For any word  $w$  of length  $n$ , we have  $r^{\lceil \frac{n}{2} \rceil}(w)$  is a reduced word.

PROOF: Since we cannot remove more than  $n/2$  pairs of letters from  $w$ .

<1>5. LET:  $R : W(A) \rightarrow W(A)$  be the function  $R(w) = r^{\lceil \frac{n}{2} \rceil}(w)$ , where  $n$  is the length of  $w$ .

<1>6. LET:  $F(A)$  be the set of reduced words.

<1>7. Define  $\cdot : F(A)^2 \rightarrow F(A)$  by  $w \cdot w' = R(ww')$

(1)8.  $\cdot$  is associative.

PROOF: Both  $w_1 \cdot (w_2 \cdot w_3)$  and  $(w_1 \cdot w_2) \cdot w_3$  are equal to  $R(w_1 w_2 w_3)$ .

(1)9. The empty word is the identity element in  $F(A)$

(1)10. The inverse of  $a_1^{\pm 1} a_2^{\pm 1} \dots a_n^{\pm 1}$  is  $a_n^{\mp 1} \dots a_2^{\mp 1} a_1^{\mp 1}$ .

(1)11. LET:  $j : A \rightarrow F(A)$  be the function that maps  $a$  to the word  $a$  of length

(1)12. LET:  $G$  be any group and  $k : A \rightarrow G$  any function.

(1)13. The only morphism  $f : (F(A), j) \rightarrow (G, k)$  in  $\mathcal{F}^A$  is  $f(a_1^{\pm 1} a_2^{\pm 1} \dots a_n^{\pm 1}) = k(a_1)^{\pm 1} k(a_2)^{\pm 1} \dots k(a_n)^{\pm 1}$ .

□

**Definition 7.27** (Free Group). For any set  $A$ , the *free group* on  $A$  is the initial object  $(F(A), i)$  in  $\mathcal{F}^A$ .

**Proposition 7.28.**  $i : A \rightarrow F(A)$  is injective.

PROOF:

(1)1. LET:  $x, y \in A$

(1)2. ASSUME:  $x \neq y$

PROVE:  $i(x) \neq i(y)$

(1)3. LET:  $f : A \rightarrow C_2$  be the function that maps  $x$  to 0 and all other elements of  $A$  to 1.

(1)4. LET:  $\phi : F(A) \rightarrow C_2$  be the group homomorphism such that  $f = \phi \circ i$ .

(1)5.  $f(x) \neq f(y)$

(1)6.  $\phi(i(x)) \neq \phi(i(y))$

(1)7.  $i(x) \neq i(y)$

□

**Proposition 7.29.**

$$F(0) \cong \{e\}$$

PROOF: For any set  $A$ , the unique group homomorphism  $\{e\} \rightarrow A$  makes the following diagram commute.

$$\begin{array}{ccc} \{e\} & \longrightarrow & A \\ \uparrow & \nearrow & \\ \emptyset & & \end{array}$$

**Proposition 7.30.** The free group on 1 is  $\mathbb{Z}$  with the injection mapping 0 to 1.

PROOF: Given any group  $G$  and function  $a : 1 \rightarrow G$ , the required unique homomorphism  $\phi : \mathbb{Z} \rightarrow G$  is defined by  $\phi(n) = a(0)^n$ . □

**Proposition 7.31.** For any sets  $A$  and  $B$ , we have that  $F(A + B)$  is the coproduct of  $F(A)$  and  $F(B)$  in **Grp**.

$$\begin{array}{ccccc}
& & G & & \\
& f \nearrow & \uparrow k & \nwarrow g & \\
F(A) & \xrightarrow{\kappa_1} & F(A+B) & \xleftarrow{\kappa_2} & F(B) \\
i_A \uparrow & & j \uparrow & & i_B \uparrow \\
A & \xrightarrow{k_1} & A+B & \xleftarrow{k_2} & B
\end{array}$$

PROOF:

- (1)1. LET:  $i_A : A \rightarrow F(A)$ ,  $i_B : B \rightarrow F(B)$ ,  $j : A+B \rightarrow F(A+B)$  be the canonical injections.  
 (1)2. LET:  $\kappa_1, \kappa_2$  be the unique group homomorphisms that make the diagram above commute.  
 (1)3. LET:  $G$  be any group and  $f : F(A) \rightarrow G$ ,  $g : F(B) \rightarrow G$  any group homomorphisms.  
 (1)4. LET:  $h : A+B \rightarrow G$  be the unique function such that  $h \circ k_1 = f \circ i_A$  and  $h \circ k_2 = g \circ i_B$ .  
 (1)5. LET:  $k : F(A+B) \rightarrow G$  be the unique group homomorphism such that  $k \circ j = h$ .  
 (1)6.  $k$  is the unique group homomorphism such that  $k \circ \kappa_1 \circ i_A = f \circ i_A$  and  $k \circ \kappa_2 \circ i_B = g \circ i_B$ .  
 (1)7.  $k$  is the unique group homomorphism such that  $k \circ \kappa_1 = f$  and  $k \circ \kappa_2 = g$ .  
 □

**Definition 7.32** (Subgroup Generated by a Group). Let  $G$  be a group and  $A$  a subset of  $G$ . Let  $\phi : F(A) \rightarrow G$  be the unique group homomorphism such that  $\phi(a) = a$  for all  $a \in A$ . The subgroup *generated* by  $A$  is

$$\langle A \rangle := \text{im } \phi$$

$$\begin{array}{ccc}
F(A) & \xrightarrow{\phi} & G \\
\uparrow & \nearrow & \\
A & & 
\end{array}$$

**Proposition 7.33.** Let  $G$  be a group and  $A$  a subset of  $G$ . Then  $\langle A \rangle$  is the set of all elements of the form  $a_1^{\pm 1} a_2^{\pm 1} \cdots a_n^{\pm 1}$  (where  $n \geq 0$ ) such that  $a_1, \dots, a_n \in A$ .

PROOF: Immediate from definitions. □

**Corollary 7.33.1.** Let  $G$  be a group and  $g \in G$ . Then

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

**Proposition 7.34.** Let  $G$  be a group and  $A$  a subset of  $G$ . Then  $\langle A \rangle$  is the intersection of all the subgroups of  $G$  that include  $A$ .



PROOF: Easy.  $\square$

**Definition 7.35** (Finitely Generated). Let  $G$  be a group. Then  $G$  is *finitely generated* iff there exists a finite subset  $A$  of  $G$  such that  $G = \langle A \rangle$ .

**Proposition 7.36.** *Every subgroup of a finitely generated free group is free.*

PROOF: TODO.

**Proposition 7.37.**  *$F(2)$  includes subgroups isomorphic to the free group on arbitrarily many generators.*

PROOF: TODO

**Proposition 7.38.**

$$[F(2), F(2)] \cong F(\mathbb{Z})$$

PROOF: TODO

## 7.6 Normal Subgroups

**Definition 7.39** (Normal Subgroup). A subgroup  $N$  of  $G$  is *normal* iff, for all  $g \in G$  and  $n \in N$ , we have  $gng^{-1} \in N$ .

**Example 7.40.** Every subgroup of  $Q_8$  is normal.

**Proposition 7.41.** *Let  $G$  be a group and  $N$  a subgroup of  $G$ . Then the following are equivalent.*

1.  $N$  is normal.
2.  $\forall g \in G. gNg^{-1} \subseteq N$
3.  $\forall g \in G. gNg^{-1} = N$
4.  $\forall g \in G. gN \subseteq Ng$
5.  $\forall g \in G. gN = Ng$

PROOF:

$\langle 1 \rangle 1. 1 \Leftrightarrow 2$

PROOF: Immediate from definitions.

$\langle 1 \rangle 2. 2 \Rightarrow 3$

PROOF: If 2 holds then we have  $gNg^{-1} \subseteq N$  and  $g^{-1}Ng \subseteq N$  hence  $N = gNg^{-1}$ .

$\langle 1 \rangle 3. 3 \Rightarrow 2$

PROOF: Trivial.

$\langle 1 \rangle 4. 2 \Leftrightarrow 4$

PROOF: Easy.

$\langle 1 \rangle 5. 3 \Leftrightarrow 5$

PROOF: Easy.

□

**Proposition 7.42.** *Let  $\phi : G \rightarrow H$  be a group homomorphism. Then  $\ker \phi$  is a normal subgroup of  $G$ .*

PROOF: Given  $g \in G$  and  $n \in \ker \phi$  we have

$$\begin{aligned}\phi(gng^{-1}) &= \phi(g)\phi(n)\phi(g)^{-1} \\ &= \phi(g)\phi(g)^{-1} \\ &= e\end{aligned}$$

and so  $gng^{-1} \in \ker \phi$ . □

## 7.7 Quotient Groups

**Definition 7.43.** Let  $G$  be a group. Let  $\sim$  be an equivalence relation on  $G$ . Then we say that  $\sim$  is *compatible* with the group operation on  $G$  iff, for all  $a, a', g \in G$ , if  $a \sim a'$  then  $ga \sim ga'$  and  $ag \sim a'g$ .

**Proposition 7.44.** *Let  $G$  be a group. Let  $\sim$  be an equivalence relation on  $G$ . Then there exists an operation  $\cdot : (G/\sim)^2 \rightarrow G/\sim$  such that*

$$\forall a, b \in G. [a][b] = [ab]$$

*iff  $\sim$  is compatible with the group operation on  $G$ . In this case,  $G/\sim$  is a group under  $\cdot$  and the canonical function  $\pi : G \rightarrow G/\sim$  is a group homomorphism, and is universal with respect to group homomorphisms  $\phi : G \rightarrow G'$  such that if  $a \sim a'$  then  $\phi(a) = \phi(a')$ .*

PROOF: Easy. □

**Definition 7.45** (Quotient Group). Let  $G$  be a group. Let  $\sim$  be an equivalence relation on  $G$  that is compatible with the group operation on  $G$ . Then  $G/\sim$  is the *quotient group* of  $G$  by  $\sim$  under  $[a][b] = [ab]$ .

**Proposition 7.46.** *Let  $G$  be a group and  $H$  a subgroup of  $G$ . Then  $H$  is normal if and only if there exists a group  $K$  and homomorphism  $\phi : G \rightarrow K$  such that  $H = \ker \phi$ .*

PROOF: One direction is given by Proposition 7.42. For the other direction, take  $K = G/H$  and  $\phi$  to be the canonical map  $G \rightarrow G/H$ . □

**Definition 7.47** (Modular Group). The *modular group*  $\text{PSL}_2(\mathbb{Z})$  is  $\text{SL}_2(\mathbb{Z})/\{I, -I\}$ .

**Proposition 7.48.**  $\text{PSL}_2(\mathbb{Z})$  is generated by  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  and  $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ .

PROOF: By Example 6.26.

**Proposition 7.49** (Roger Alperin).  $\text{PSL}_2(\mathbb{Z})$  is presented by  $(x, y | x^2, y^3)$ .

PROOF:

$\langle 1 \rangle 1.$  LET:  $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$\langle 1 \rangle 2.$  LET:  $y = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$

$\langle 1 \rangle 3.$  Define an action of  $\text{PSL}_2(\mathbb{Z})$  on  $\mathbb{R} - \mathbb{Q}$  by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} r = \frac{ar + b}{cr + d}.$$

$\langle 2 \rangle 1.$  Given  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PSL}_2(\mathbb{Z})$  and  $r$  irrational we have  $\frac{ar+b}{cr+d}$  is irrational.

$\langle 3 \rangle 1.$  ASSUME: for a contradiction  $\frac{ar+b}{cr+d} = \frac{p}{q}$  where  $p$  and  $q$  are integers with  $q > 0$ .

$\langle 3 \rangle 2.$   $aqr + bq = cpr + dp$

$\langle 3 \rangle 3.$   $(aq - cp)r = dp - bq$

$\langle 3 \rangle 4.$   $aq = cp = dp - bq = 0$

$\langle 3 \rangle 5.$   $adq - cdp = 0$

$\langle 3 \rangle 6.$   $cdp - cbq = 0$

$\langle 3 \rangle 7.$   $(ad - cb)q = 0$

PROOF: Since  $ad - cb = 1$ .

$\langle 3 \rangle 8.$   $q = 0$

$\langle 3 \rangle 9.$  Q.E.D.

PROOF: This contradicts  $\langle 3 \rangle 1$ .

$\langle 2 \rangle 2.$   $-Ir = r$

PROOF: Since  $-Ir = \frac{-r}{-1} = r$ .

$\langle 2 \rangle 3.$  Given  $A, B \in \text{PSL}_2(\mathbb{Z})$  we have  $A(Br) = (AB)r$ .

PROOF:

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \left[ \begin{pmatrix} e & f \\ g & h \end{pmatrix} r \right] &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{er + f}{gr + h} \\ &= \frac{a \frac{er+f}{gr+h} + b}{c \frac{er+f}{gr+h} + d} \\ &= \frac{a(er + f) + b(gr + h)}{c(er + f) + d(gr + h)} \\ &= \frac{(ae + bg)r + (af + bh)}{(ce + dg)r + (cf + dh)} \\ &= \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} r \\ &= \left[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] r \end{aligned}$$

$\langle 1 \rangle 4.$

$$yr = 1 - \frac{1}{r}$$

$\langle 1 \rangle 5.$

$$y^{-1}r = \frac{1}{1 - r}$$

PROOF: Since  $y^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$

(1)6.

PROOF: Since  $yx = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$ .  $yxr = 1 + r$

(1)7.

$$y^{-1}xr = \frac{r}{1+r}$$

PROOF: Since  $y^{-1}x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ .

(1)8. If  $r > -1$  is positive then  $yxr$  is positive.

(1)9. If  $r$  is positive then  $y^{-1}xr$  is positive.

(1)10. If  $r < -1$  then  $y^{-1}xr$  is positive.

(1)11. If  $r$  is negative then  $yr$  is positive.

(1)12. If  $r$  is negative then  $y^{-1}r$  is positive.

(1)13. No product of the form

$$(y^{\pm 1}x)(y^{\pm 1}x) \cdots (y^{\pm 1}x)$$

with one or more factors can equal the identity.

PROOF: If the last factor is  $(yx)$ , then the product maps numbers in  $(-1, 0)$  to positive numbers. If the last factor is  $(y^{-1}x)$ , then the product maps numbers  $< -1$  to positive numbers.

(1)14. No product of the form

$$(y^{\pm 1}x)(y^{\pm 1}x) \cdots (y^{\pm 1}x)y^{\pm 1}$$

with one or more factors can equal the identity.

PROOF: The product maps negative numbers to positive numbers.

(1)15.  $\text{PSL}_2(\mathbb{Z})$  is presented by  $(x, y|x^2, y^3)$ .

□

**Corollary 7.49.1.**  $\text{PSL}_2(\mathbb{Z})$  is the coproduct of  $C_2$  and  $C_3$  in **Grp**.

**Theorem 7.50.** Every group homomorphism  $\phi : G \rightarrow H$  may be decomposed as

$$G \longrightarrow G/\ker \phi \xrightarrow{\cong} \text{im } \phi \longrightarrow H$$

PROOF: Easy. □

**Corollary 7.50.1** (First Isomorphism Theorem). Let  $\phi : G \rightarrow H$  be a surjective group homomorphism. Then  $H \cong G/\ker \phi$ .

**Proposition 7.51.** Let  $H_1$  be a normal subgroup of  $G_1$  and  $H_2$  a normal subgroup of  $G_2$ . Then  $H_1 \times H_2$  is a normal subgroup of  $G_1 \times G_2$ , and

$$\frac{G_1 \times G_2}{H_1 \times H_2} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2}.$$

PROOF:  $\pi \times \pi : G_1 \times G_2 \twoheadrightarrow G_1/H_1 \times G_2/H_2$  is a surjective homomorphism with kernel  $H_1 \times H_2$ . □

**Example 7.52.**

$$\mathbb{R}/\mathbb{Z} \cong S^1$$

PROOF: Map a real number  $r$  to  $(\cos r, \sin r)$ . The result is a surjective group homomorphism with kernel  $\mathbb{Z}$ .  $\square$

**Proposition 7.53.** *Let  $H$  be a normal subgroup of a group  $G$ . For every subgroup  $K$  of  $G$  that includes  $H$ , we have  $H$  is a normal subgroup of  $K$ , and  $K/H$  is a subgroup of  $G/H$ . The mapping*

$$u : \{\text{subgroups of } G \text{ including } H\} \rightarrow \{\text{subgroups of } G/H\}$$

*with  $u(K) = K/H$  is a poset isomorphism.*

PROOF:

- $\langle 1 \rangle 1$ . If  $K$  is a subgroup of  $G$  that includes  $H$  then  $H$  is normal in  $K$ .
- $\langle 1 \rangle 2$ . If  $K$  is a subgroup of  $G$  that includes  $H$  then  $K/H$  is a subgroup of  $G/H$ .
- $\langle 1 \rangle 3$ . If  $H \subseteq K_1 \subseteq K_2$  then  $K_1/H \subseteq K_2/H$ .
- $\langle 1 \rangle 4$ . If  $K_1/H = K_2/H$  then  $K_1 = K_2$ 
  - $\langle 2 \rangle 1$ . ASSUME:  $K_1/H = K_2/H$
  - $\langle 2 \rangle 2$ .  $K_1 \subseteq K_2$ 
    - $\langle 3 \rangle 1$ . LET:  $k \in K_1$
    - $\langle 3 \rangle 2$ .  $kH \in K_2/H$
    - $\langle 3 \rangle 3$ . PICK  $k' \in K_2$  such that  $kH = k'H$
    - $\langle 3 \rangle 4$ .  $kk'^{-1} \in H$
    - $\langle 3 \rangle 5$ .  $kk'^{-1} \in K_2$
    - $\langle 3 \rangle 6$ .  $k \in K_2$
  - $\langle 2 \rangle 3$ .  $K_2 \subseteq K_1$
- PROOF: Similar.
- $\langle 1 \rangle 5$ . For any subgroup  $L$  of  $G/H$ , there exists a subgroup  $K$  of  $G$  that includes  $H$  such that  $L = K/H$ .
  - $\langle 2 \rangle 1$ . LET:  $L$  be a subgroup of  $G/H$ .
  - $\langle 2 \rangle 2$ . LET:  $K = \{k \in G : kH \in L\}$
  - $\langle 2 \rangle 3$ .  $K$  is a subgroup of  $G$ .
    - PROOF: Given  $k, k' \in K$  we have  $kH, k'H \in L$  hence  $kk'^{-1}H \in L$  and so  $kk'^{-1} \in K$ .
  - $\langle 2 \rangle 4$ .  $H \subseteq K$ 
    - PROOF: For all  $h \in H$  we have  $hH = H \in L$ .
  - $\langle 2 \rangle 5$ .  $L = K/H$ 
    - PROOF: By definition.

$\square$

**Proposition 7.54** (Third Isomorphism Theorem). *Let  $H$  be a normal subgroup of a group  $G$ . Let  $N$  be a subgroup of  $G$  that includes  $H$ . Then  $N/H$  is normal in  $G/H$  if and only if  $N$  is normal in  $G$ , in which case*

$$\frac{G/H}{N/H} \cong \frac{G}{N}$$

PROOF:

- ⟨1⟩1. If  $N/H$  is normal in  $G/H$  then  $N$  is normal in  $G$ .
  - ⟨2⟩1. ASSUME:  $N/H$  is normal in  $G/H$ .
  - ⟨2⟩2. LET:  $g \in G$  and  $n \in N$ .
  - ⟨2⟩3.  $gng^{-1}H \in N/H$
  - ⟨2⟩4. PICK  $n' \in N$  such that  $gng^{-1}H = n'H$
  - ⟨2⟩5.  $gng^{-1}n'^{-1} \in H$
  - ⟨2⟩6.  $gng^{-1}n'^{-1} \in N$
  - ⟨2⟩7.  $gng^{-1} \in N$
- ⟨1⟩2. If  $N$  is normal in  $G$  then  $N/H$  is normal in  $G/H$  and  $(G/H)/(N/H) \cong G/N$ .
  - ⟨2⟩1. ASSUME:  $N$  is normal in  $G$ .
  - ⟨2⟩2. LET:  $\phi : G/H \rightarrow G/N$  be the homomorphism  $\phi(gH) = gN$ 
    - ⟨3⟩1. If  $gH = g'H$  then  $gN = g'N$   
 PROOF: If  $gg'^{-1} \in H$  then  $gg'^{-1} \in N$ .
    - ⟨3⟩2.  $\phi((gH)(g'H)) = \phi(gH)\phi(g'H)$   
 PROOF: Both are  $gg'N$ .
  - ⟨2⟩3.  $\phi$  is surjective.
  - ⟨2⟩4.  $\ker \phi = N/H$
  - ⟨2⟩5.  $(G/H)/(N/H) \cong G/N$   
 PROOF: By the First Isomorphism Theorem.

□

**Proposition 7.55** (Second Isomorphism Theorem). *Let  $H$  and  $K$  be subgroups of a group  $G$ . Assume that  $H$  is normal in  $G$ . Then:*

- 1.  $HK$  is a subgroup of  $G$ , and  $H$  is normal in  $HK$ .
- 2.  $H \cap K$  is normal in  $K$ , and

$$\frac{HK}{H} \cong \frac{K}{H \cap K}.$$

PROOF:

- ⟨1⟩1.  $HK$  is a subgroup of  $G$ .  
 PROOF: Since  $hkh'k' = hh'(h'^{-1}kh')k' \in HK$ .
- ⟨1⟩2.  $H$  is normal in  $HK$ .
- ⟨1⟩3.  $H \cap K$  is normal in  $K$  and  $HK/H \cong K/(H \cap K)$   
 PROOF: The function that maps  $k$  to  $kH$  is a surjective homomorphism  $K \twoheadrightarrow HK/H$  with kernel  $H \cap K$ . Surjectivity follows because  $hkh = hkh^{-1}H$ .

□

See also Proposition 7.70 for a result that holds even if  $H$  is not normal.

## 7.8 Cosets

**Proposition 7.56.** *Let  $G$  be a group. Let  $\sim$  be an equivalence relation on  $G$  such that, for all  $a, b, g \in G$ , if  $a \sim b$  then  $ga \sim gb$ . Let  $H = \{h \in G : h \sim e\}$ .*

Then  $H$  is a subgroup of  $G$  and, for all  $a, b \in G$ , we have

$$a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH .$$

PROOF:

$\langle 1 \rangle 1.$   $e \in H$

$\langle 1 \rangle 2.$  For all  $x, y \in H$  we have  $xy^{-1} \in H$ .

$\langle 2 \rangle 1.$  ASSUME:  $x \sim e$  and  $y \sim e$ .

$\langle 2 \rangle 2.$   $e \sim y^{-1}$

PROOF: Since  $yy^{-1} \sim ey^{-1}$ .

$\langle 2 \rangle 3.$   $xy^{-1} \sim e$

PROOF: Since  $xy^{-1} \sim ey^{-1} \sim e$ .

$\langle 1 \rangle 3.$  If  $a \sim b$  then  $a^{-1}b \in H$ .

PROOF: If  $a \sim b$  then  $a^{-1}b \sim a^{-1}a = e$ .

$\langle 1 \rangle 4.$  If  $a^{-1}b \in H$  then  $aH = bH$ .

$\langle 2 \rangle 1.$  ASSUME:  $a^{-1}b \in H$

$\langle 2 \rangle 2.$   $bH \subseteq aH$

PROOF: For any  $h \in H$  we have  $bh = aa^{-1}bh \in aH$ .

$\langle 2 \rangle 3.$   $aH \subseteq bH$

PROOF: Similar since  $b^{-1}a \in H$ .

$\langle 1 \rangle 5.$  If  $aH = bH$  then  $a \sim b$ .

$\langle 2 \rangle 1.$  ASSUME:  $aH = bH$

$\langle 2 \rangle 2.$  PICK  $h \in H$  such that  $a = bh$ .

$\langle 2 \rangle 3.$   $b^{-1}a = h$

$\langle 2 \rangle 4.$   $b^{-1}a \in H$

$\langle 2 \rangle 5.$   $b^{-1}a \sim e$

$\langle 2 \rangle 6.$   $a \sim b$

PROOF:  $a = bb^{-1}a \sim be = b$ .

□

**Definition 7.57** (Coset). Let  $G$  be a group and  $H$  a subgroup of  $G$ . A *left coset* of  $H$  is a set of the form  $aH$  for  $a \in G$ . A *right coset* of  $H$  is a set of the form  $Ha$  for some  $a \in G$ .

We write  $G/H$  for the set of all left cosets of  $H$ , and  $G \backslash H$  for the set of all right cosets of  $H$ .

**Proposition 7.58.**

$$G/H \cong G \backslash H$$

PROOF: The function that maps  $aH$  to  $Ha^{-1}$  is a bijection. □

**Proposition 7.59.** Let  $G$  be a group and  $H$  a subgroup of  $G$ . Define  $\sim_H$  on  $G$  by:  $a \sim b$  iff  $a^{-1}b \in H$ . This defines a one-to-one correspondence between the subgroups of  $G$  and the equivalence relations  $\sim$  on  $G$  such that, for all  $a, b, g \in G$ , if  $a \sim b$ , then  $ga \sim gb$ . The equivalence class of  $a$  is  $aH$ .

PROOF:

$\langle 1 \rangle 1.$  For any subgroup  $H$ , we have  $\sim_H$  is an equivalence relation on  $G$ .

⟨2⟩1.  $\sim$  is reflexive.

PROOF: For any  $a \in G$  we have  $a^{-1}a = e \in H$ .

⟨2⟩2.  $\sim$  is symmetric.

PROOF: If  $a^{-1}b \in H$  then  $b^{-1}a \in H$ .

⟨2⟩3.  $\sim$  is transitive.

PROOF: If  $a^{-1}b \in H$  and  $b^{-1}c \in H$  then  $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$ .

⟨1⟩2. If  $a \sim_H b$  then  $ga \sim_H gb$ .

PROOF: If  $a^{-1}b \in H$  then  $(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b \in H$ .

⟨1⟩3. For any equivalence relation  $\sim$  on  $G$  such that, whenever  $a \sim b$ , then  $ga \sim gb$ , there exists a subgroup  $H$  such that  $\sim = \sim_H$ .

PROOF: Proposition 7.56.

⟨1⟩4. The  $\sim_H$ -equivalence class of  $a$  is  $aH$ .

PROOF:

$$\begin{aligned} a \sim b &\Leftrightarrow a^{-1}b \in H \\ &\Leftrightarrow \exists h \in H. a^{-1}b = h \\ &\Leftrightarrow \exists h \in H. b = ah \\ &\Leftrightarrow b \in aH \end{aligned}$$

□

**Proposition 7.60.** Let  $G$  be a group and  $H$  a subgroup of  $G$ . Define  $\sim_H$  on  $G$  by:  $a \sim b$  iff  $ab^{-1} \in H$ . This defines a one-to-one correspondence between the subgroups of  $G$  and the equivalence relations  $\sim$  on  $G$  such that, for all  $a, b, g \in G$ , if  $a \sim b$ , then  $ag \sim bg$ . The equivalence class of  $a$  is  $Ha$ .

PROOF: Similar. □

**Proposition 7.61.** Let  $G$  be a group and  $H$  be a subgroup of  $G$ . Define  $\sim_L$  and  $\sim_R$  on  $G$  by:

$$a \sim_L b \Leftrightarrow a^{-1}b \in H, \quad a \sim_R b \Leftrightarrow ab^{-1} \in H.$$

Then  $\sim_L = \sim_R$  if and only if  $H$  is normal.

PROOF:

⟨1⟩1. If  $\sim_L = \sim_R$  then  $H$  is normal.

⟨2⟩1. ASSUME:  $\sim_L = \sim_R$

⟨2⟩2. LET:  $h \in H$  and  $g \in G$

⟨2⟩3.  $g \sim_L gh^{-1}$

⟨2⟩4.  $g \sim_R gh^{-1}h$

⟨2⟩5.  $ghg^{-1} \in H$

⟨1⟩2. If  $H$  is normal then  $\sim_L = \sim_R$ .

⟨2⟩1. ASSUME:  $H$  is normal.

⟨2⟩2. If  $a \sim_L b$  then  $a \sim_R b$ .

⟨3⟩1. ASSUME:  $a \sim_L b$

⟨3⟩2.  $a^{-1}b \in H$

⟨3⟩3.  $aa^{-1}ba^{-1} \in H$

⟨3⟩4.  $ba^{-1} \in H$



- $\langle 3 \rangle 5. a \sim_R b$   
 $\langle 2 \rangle 3. \text{ If } a \sim_R b \text{ then } a \sim_L b.$

PROOF: Similar.

□

**Corollary 7.61.1.** *Let  $G$  be a group and  $H$  be a normal subgroup of  $G$ . Define  $\sim$  on  $G$  by  $a \sim b$  iff  $a^{-1}b \in H$ . Then  $G/\sim$  is a group under  $[a][b] = [ab]$ .*

**Definition 7.62** (Quotient Group). Let  $G$  be a group and  $H$  be a normal subgroup of  $G$ . The *quotient group*  $G/H$  is  $G/\sim$  where  $a \sim b$  iff  $a^{-1}b \in H$ , under  $[a][b] = [ab]$  or  $(aH)(bH) = abH$ .

**Corollary 7.62.1.** *Let  $H$  be a normal subgroup of a group  $G$ . For every group homomorphism  $\phi : G \rightarrow G'$  such that  $H \subseteq \ker \phi$ , there exists a unique group homomorphism  $\bar{\phi} : G/H \rightarrow G'$  such that the following diagram commutes.*

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ & \searrow \pi & \nearrow \bar{\phi} \\ & G/H & \end{array}$$

**Proposition 7.63.**  $\mathbb{Z}/n\mathbb{Z}$  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 7.64.** *Let  $m$  and  $n$  be integers with  $n > 0$ . The order of  $m$  in  $\mathbb{Z}/n\mathbb{Z}$  is  $\frac{n}{\gcd(m,n)}$ .*

PROOF: By Proposition 6.16 since the order of 1 is  $n$ . □

**Proposition 7.65.** *The integer  $m$  generates  $\mathbb{Z}/n\mathbb{Z}$  if and only if  $\gcd(m, n) = 1$ .*

PROOF: By Proposition 7.64. □

**Corollary 7.65.1.** *If  $p$  is prime then every non-zero element in  $\mathbb{Z}/p\mathbb{Z}$  is a generator.*

**Proposition 7.66.**

$$\text{Aut}_{\mathbf{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$$

PROOF: Every permutation of  $\{(1, 0), (0, 1), (1, 1)\}$  gives an automorphism of  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . □

**Example 7.67.** Not all monomorphisms split in  $\mathbf{Grp}$ .

Define  $\phi : \mathbb{Z}/3\mathbb{Z} \rightarrow S_3$  by

$$\phi(0) = \text{id}_3, \quad \phi(1) = (1 \ 3 \ 2), \quad \phi(2) = (1 \ 2 \ 3) .$$

Then  $\phi$  is monic but has no retraction.

For if  $r : S_3 \rightarrow \mathbb{Z}/3\mathbb{Z}$  is a retraction, then we would have

$$r(1\ 2) + r(2\ 3) = 1, \quad r(2\ 3) + r(1\ 2) = 2$$

which is impossible.

**Proposition 7.68.** *Let  $G$  be a group,  $H$  a subgroup of  $G$ , and  $g \in G$ . The function that maps  $h$  to  $gh$  is a bijection  $H \cong gH$ .*

PROOF: By Cancellation.  $\square$

**Proposition 7.69.** *Let  $G$  be a group,  $H$  a subgroup of  $G$ , and  $g \in G$ . The function that maps  $h$  to  $hg$  is a bijection  $H \cong Hg$ .*

PROOF: By Cancellation.  $\square$

**Proposition 7.70.** *Let  $H$  and  $K$  be finite subgroups of a group  $G$ . Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $f : \{hK : h \in H\} \rightarrow H/(H \cap K)$  be the function  $f(hK) = h(H \cap K)$

PROOF: This is well-defined because if  $hK = h'K$  then  $h^{-1}h' \in H \cap K$  so  $h(H \cap K) = h'(H \cap K)$ .

$\langle 1 \rangle 2$ .  $f$  is injective.

PROOF: If  $h(H \cap K) = h'(H \cap K)$  then  $hK = h'K$ .

$\langle 1 \rangle 3$ .  $f$  is surjective.

PROOF: Clear.

$\langle 1 \rangle 4$ .

$$\frac{|HK|}{|K|} = \frac{|H|}{|H \cap K|}$$

$\square$

## 7.9 Congruence

**Definition 7.71** (Congruence). Given integers  $a, b, n$  with  $n$  positive, we say  $a$  is *congruent to  $b$  modulo  $n$* , and write  $a \equiv b \pmod{n}$ , iff  $a + n\mathbb{Z} = b + n\mathbb{Z}$  in  $\mathbb{Z}/n\mathbb{Z}$ .

**Proposition 7.72.** *Given integers  $a, b, n$  with  $n$  positive, we have  $a \equiv b \pmod{n}$  iff  $n \mid a - b$ .*

PROOF: By Proposition 7.56.  $\square$

**Proposition 7.73.** *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  $n \mid (a' + b') - (a + b)$ .  $\square$

**Proposition 7.74.** *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  $n \mid a'b' - ab = a'(b' - b) + (a' - a)b$ .  $\square$

## 7.10 Cyclic Groups

**Definition 7.75** (Cyclic Group). The *cyclic* groups are  $\mathbb{Z}$  and  $\mathbb{Z}/n\mathbb{Z}$  for positive integers  $n$ .

**Proposition 7.76.** *If  $m$  and  $n$  are positive integers with  $\gcd(m, n) = 1$  then  $C_{mn} \cong C_m \times C_n$ .*

PROOF: The function that maps  $x$  to  $(x \bmod m, x \bmod n)$  is an isomorphism.  $\square$

**Proposition 7.77.** *Let  $G$  be a group and  $g \in G$ . Then  $\langle g \rangle$  is cyclic.*

PROOF: If  $g$  has finite order then  $\langle g \rangle \cong C_{|g|}$ , otherwise  $\langle g \rangle \cong \mathbb{Z}$ .  $\square$

**Proposition 7.78.** *Every finitely generated subgroup of  $\mathbb{Q}$  is cyclic.*

PROOF:

$\langle 1 \rangle$ 1. LET:  $G = \langle a_1/b, \dots, a_n/b \rangle$  where  $a_1, \dots, a_n, b$  are integers with  $b > 0$

$\langle 1 \rangle$ 2. LET:  $a = \gcd(a_1, \dots, a_n)$

$\langle 1 \rangle$ 3.  $G = \langle a/b \rangle$

$\square$

**Corollary 7.78.1.**  $\mathbb{Q}$  is not finitely generated.

## 7.11 Commutator Subgroup

**Definition 7.79** (Commutator Subgroup). Let  $G$  be a group. The *commutator subgroup*  $[G, G]$  is the subgroup generated by the elements of the form  $aba^{-1}b^{-1}$ .

**Proposition 7.80.** *The commutator subgroup is normal.*

PROOF: Since

$$\begin{aligned} & ga_1b_1a_1^{-1}b_1^{-1}a_2b_2a_2^{-1}b_2^{-1} \cdots a_nb_na_n^{-1}b_n^{-1}g^{-1} \\ &= (ga_1g^{-1})(gb_1g^{-1})(ga_1g^{-1})^{-1}(gb_1g^{-1})^{-1} \cdots (ga_ng^{-1})(gb_ng^{-1})(ga_ng^{-1})^{-1}(gb_ng^{-1})^{-1}. \end{aligned} \quad \square$$

## 7.12 Presentations

**Definition 7.81** (Presentation). A *presentation* of a group  $G$  is a pair  $(A, R)$  where  $A$  is a set and  $R \subseteq F(A)$  is a set of words such that

$$G \cong F(A)/N(R)$$

where  $N(R)$  is the smallest normal subgroup of  $F(A)$  that includes  $R$ .

**Example 7.82.** • The free group on a set  $A$  is presented by  $(A, \emptyset)$ .

- $S_3$  is presented by  $(x, y | x^2, y^3, xyxy)$ .
- $(a, b | a^2, b^2, (ab)^n)$  is a presentation of  $D_{2n}$ .

- $(x, y \mid x^2y^{-2}, y^4, xyx^{-1}y)$  is a presentation of  $Q_8$ .

**Proposition 7.83** (Word Problem). *Let  $(A, R)$  be a presentation of the group  $G$ . Let  $w_1, w_2 \in F(A)$  be two words. Then it is undecidable in general if  $w_1N(R) = w_2N(R)$  in  $G$ .*

**Definition 7.84** (Finitely Presented). A group is *finitely presented* iff it has a presentation  $(A, R)$  where both  $A$  and  $R$  are finite.

**Proposition 7.85.** *Let  $(A|R)$  be a presentation of  $G$  and  $(A'|R')$  a presentation of  $H$ . Assume w.l.o.g.  $A$  and  $A'$  are disjoint. Then the group  $G * G'$  presented by  $(A \cup A' | R \cup R')$  is the coproduct of  $G$  and  $G'$  in **Grp**.*

$$\begin{array}{ccccc}
 A & \longrightarrow & A \cup A' & \longleftarrow & A' \\
 \downarrow & & \downarrow & & \downarrow \\
 F(A) & \longrightarrow & F(A \cup A') & \longleftarrow & F(A') \\
 \downarrow & & \downarrow & & \downarrow \\
 G & \xrightarrow{\kappa_1} & G * G' & \xleftarrow{\kappa_2} & G'
 \end{array}$$

PROOF:

- $\langle 1 \rangle 1$ . LET:  $\kappa_1 : G \rightarrow G * G'$  and  $\kappa_2 : G' \rightarrow G * G'$  be the unique homomorphisms that make the diagram above commute.
- $\langle 1 \rangle 2$ . LET:  $\phi : G \rightarrow H$  and  $\psi : G' \rightarrow H$  be any homomorphisms.
- $\langle 1 \rangle 3$ . LET:  $[\phi, \psi] : F(A \cup A') \rightarrow H$  be the unique homomorphism such that ...
- $\langle 1 \rangle 4$ .  $R \cup R' \subseteq \ker[\phi, \psi]$
- $\langle 1 \rangle 5$ .  $[\phi, \psi]$  factors uniquely through the morphism  $F(A \cup A') \rightarrow G * G'$

□

## 7.13 Index of a Subgroup

**Definition 7.86** (Index). Let  $G$  be a group and  $H$  a subgroup of  $G$ . The *index* of  $H$  in  $G$ , denoted  $|G : H|$ , is the number of left cosets of  $H$  in  $G$  if this is finite, otherwise  $\infty$ .

**Theorem 7.87** (Lagrange's Theorem). *Let  $G$  be a finite group and  $H$  a subgroup of  $G$ . Then*

$$|G| = |G : H| |H| .$$

PROOF:  $G/H$  is a partition of  $G$  into  $|G : H|$  subsets, each of size  $|H|$ . □

**Corollary 7.87.1.** *For  $p$  a prime number, the only group of order  $p$  is  $C_p$ .*

PROOF: Let  $G$  be a group of order  $p$  and  $g \in G$  with  $g \neq e$ . Then  $|\langle g \rangle|$  divides  $p$  and is not 1, hence is  $p$ , that is,  $G = \langle g \rangle$ . □

**Theorem 7.88** (Cauchy's Theorem). *Let  $G$  be a finite group. If  $p$  is prime and  $p \mid |G|$  then  $G$  has a subgroup of order  $p$ .*

**Proposition 7.89.** *Let  $G$  be a group. Let  $K$  be a subgroup of  $G$  and  $H$  a subgroup of  $K$ . If  $|G : H|$ ,  $|G : K|$  and  $|K : H|$  are all finite then*

$$|G : H| = |G : K||K : H| .$$

PROOF:

- $\langle 1 \rangle 1$ . LET:  $G/K = \{g_1K, g_2K, \dots, g_mK\}$
- $\langle 1 \rangle 2$ . LET:  $K/H = \{k_1H, k_2H, \dots, k_nH\}$
- $\langle 1 \rangle 3$ .  $G/H = \{g_ik_jH : 1 \leq i \leq m, 1 \leq j \leq n\}$
- $\langle 2 \rangle 1$ . LET:  $g \in G$
- $\langle 2 \rangle 2$ . PICK  $i$  such that  $gK = g_iK$
- $\langle 2 \rangle 3$ .  $g^{-1}g_i \in K$
- $\langle 2 \rangle 4$ . PICK  $j$  such that  $g^{-1}g_iH = k_jH$
- $\langle 2 \rangle 5$ .  $g^{-1}g_ik_j \in H$
- $\langle 2 \rangle 6$ .  $gH = g_ik_jH$
- $\langle 1 \rangle 4$ . If  $g_ik_jH = g_{i'}k_{j'}H$  then  $i = i'$  and  $j = j'$ .
- $\langle 2 \rangle 1$ . ASSUME:  $g_ik_jH = g_{i'}k_{j'}H$
- $\langle 2 \rangle 2$ .  $g_iK = g_{i'}K$
- $\langle 2 \rangle 3$ .  $i = i'$
- $\langle 2 \rangle 4$ .  $k_jH = k_{j'}H$
- $\langle 2 \rangle 5$ .  $j = j'$

□

## 7.14 Cokernels

**Proposition 7.90.** *Let  $\phi : G \rightarrow H$  be a homomorphism between groups. Then there exists a group  $K$  and homomorphism  $\pi : H \rightarrow K$  that is initial with respect to all homomorphism  $\alpha : H \rightarrow L$  such that  $\alpha \circ \phi = 0$ .*

PROOF:

- $\langle 1 \rangle 1$ . LET:  $N$  be the intersection of all the normal subgroups of  $H$  that include  $\text{im } \phi$ .
- $\langle 1 \rangle 2$ . LET:  $K = H/N$  and  $\pi$  be the canonical homomorphism.
- $\langle 1 \rangle 3$ . LET:  $\pi \circ \phi = 0$
- $\langle 1 \rangle 4$ . LET:  $\alpha : H \rightarrow L$  satisfy  $\alpha \circ \phi = 0$
- $\langle 1 \rangle 5$ .  $\text{im } \phi \subseteq \ker \alpha$
- $\langle 1 \rangle 6$ .  $N \subseteq \ker \alpha$
- $\langle 1 \rangle 7$ . There exists a unique  $\bar{\alpha} : H/\text{im } \phi \rightarrow L$  such that  $\bar{\alpha} \circ \pi = \alpha$

□

**Definition 7.91** (Cokernel). For any homomorphism  $\phi : G \rightarrow H$  in **Grp**, the *cokernel* of  $\phi$  is the group  $\text{coker } \phi$  and homomorphism  $\pi : H \rightarrow \text{coker } \phi$  that is initial among homomorphisms  $\alpha : H \rightarrow L$  such that  $\alpha \circ \phi = 0$ .

**Example 7.92.** It is not true that a homomorphism with trivial cokernel is epi. The inclusion  $\langle (1 \ 2) \rangle \hookrightarrow S_3$  has trivial cokernel but is not epi.

## 7.15 Cayley Graphs

**Definition 7.93** (Cayley Graph). Let  $G$  be a finitely generated group. Let  $A$  be a finite set of generators for  $G$ . The *Cayley graph* of  $G$  with respect to  $A$  is the directed graph whose vertices are the elements of  $G$ , with an edge  $g_1 \rightarrow g_2$  labelled by  $a \in A$  iff  $g_2 = g_1 a$ .

**Proposition 7.94.**  *$G$  is the free group on  $A$  iff the Cayley graph with respect to  $A$  is a tree.*

PROOF: Both are equivalent to saying that the product of two different strings of elements of  $A$  and/or their inverses are not equal.  $\square$

## Chapter 8

# Abelian Groups

**Definition 8.1** (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 8.2.** Every group of order  $\leq 4$  is Abelian.

**Example 8.3.** For any positive integer  $n$ , we have  $\mathbb{Z}/n\mathbb{Z}$  is an Abelian group under addition.

**Example 8.4.**  $S_n$  is not Abelian for  $n \geq 3$ . If  $x = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$  and  $y = \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$  then  $xy = \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}$  and  $yx = \begin{pmatrix} 1 & 3 \\ 1 & 3 \end{pmatrix}$ .

**Example 8.5.** There are 42 Abelian groups of order 1024 up to isomorphism.

**Proposition 8.6.** 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 8.7.** Let  $G$  be a group. Then  $G$  is Abelian if and only if the function that maps  $g$  to  $g^{-1}$  is a group homomorphism.

PROOF:

(1)1. If  $G$  is Abelian then the function that maps  $g$  to  $g^{-1}$  is a group homomorphism.

PROOF: Since  $(gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1}$ .

(1)2. If the function that maps  $g$  to  $g^{-1}$  is a group homomorphism then  $G$  is Abelian.

PROOF: Since  $gh = (g^{-1})^{-1}(h^{-1})^{-1} = (g^{-1}h^{-1})^{-1} = hg$ .  
 $\square$

**Proposition 8.8.** *Let  $G$  be a group. Then  $G$  is Abelian if and only if the function that maps  $g$  to  $g^2$  is a group homomorphism.*

PROOF:

$\langle 1 \rangle 1$ . If  $G$  is Abelian then the function that maps  $g$  to  $g^2$  is a group homomorphism.

PROOF: Since  $(gh)^2 = g^2h^2$ .

$\langle 1 \rangle 2$ . If the function that maps  $g$  to  $g^2$  is a group homomorphism then  $G$  is Abelian.

PROOF: Since we have  $(gh)^2 = ghgh = g^2h^2$  and so  $hg = gh$ .

$\square$

**Proposition 8.9.** *Let  $G$  be a group. Then  $G$  is Abelian if and only if the homomorphism  $\gamma : G \rightarrow \text{Aut}_{\mathbf{Grp}}(G)$  is the trivial homomorphism.*

PROOF:

$\langle 1 \rangle 1$ . If  $G$  is Abelian then  $\gamma$  is trivial.

PROOF: Since  $\gamma_g(a) = gag^{-1} = a$ .

$\langle 1 \rangle 2$ . If  $\gamma$  is trivial then  $G$  is Abelian.

PROOF: If  $\gamma_g(a) = gag^{-1} = a$  for all  $g$  and  $a$  then  $ga = ag$  for all  $g, a$ .

$\square$

**Proposition 8.10.** *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 6.19.

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

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

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

$\square$

**Proposition 8.11.** *Given a set  $A$  and an Abelian group  $H$ , the set  $H^A$  is an Abelian group under*

$$(\phi + \psi)(a) = \phi(a) + \psi(a) \quad (\phi, \psi \in H^A, a \in A) .$$

PROOF:

$\langle 1 \rangle 1$ .  $\phi + (\psi + \chi) = (\phi + \psi) + \chi$

$\langle 1 \rangle 2$ .  $\phi + \psi = \psi + \phi$

$\langle 1 \rangle 3$ . LET:  $0 : A \rightarrow H$  be the function  $0(a) = 0$ .

$\langle 1 \rangle 4$ .  $\phi + 0 = 0 + \phi = \phi$



$\langle 1 \rangle 5$ . Given  $\phi : A \rightarrow H$ , define  $-\phi : A \rightarrow H$  by  $(-\phi)(a) = -(\phi(a))$ .

$\langle 1 \rangle 6$ .  $\phi + (-\phi) = (-\phi) + \phi = 0$

□

**Proposition 8.12.** *Given a group  $G$  and an Abelian group  $H$ , the set  $\mathbf{Grp}[G, H]$  is a subgroup of  $H^G$ .*

PROOF:

$\langle 1 \rangle 1$ . Given  $\phi, \psi : G \rightarrow H$  group homomorphisms, we have  $\phi - \psi$  is a group homomorphism.

PROOF:

$$\begin{aligned} (\phi - \psi)(g + g') &= \phi(g + g') - \psi(g + g') \\ &= \phi(g) + \phi(g') - \psi(g) - \psi(g') \\ &= \phi(g) - \psi(g) + \phi(g') - \psi(g') \\ &= (\phi - \psi)(g) + (\phi - \psi)(g') \end{aligned}$$

□

**Proposition 8.13.** *Let  $G$  be a group. The following are equivalent.*

1.  $\text{Inn}(G)$  is cyclic.
2.  $\text{Inn}(G)$  is trivial.
3.  $G$  is Abelian.

PROOF:

$\langle 1 \rangle 1$ .  $1 \Rightarrow 2$

$\langle 2 \rangle 1$ . ASSUME:  $\text{Inn}(G) = \langle \gamma_g \rangle$

$\langle 2 \rangle 2$ .  $g$  commutes with every element of  $G$

$\langle 3 \rangle 1$ . LET:  $x \in G$

$\langle 3 \rangle 2$ . PICK  $n \in \mathbb{Z}$  such that  $\gamma_x = \gamma_g^n$

$\langle 3 \rangle 3$ .  $\forall y \in G. xyx^{-1} = g^n yg^{-n}$

$\langle 3 \rangle 4$ .  $xgx^{-1} = g$

$\langle 2 \rangle 3$ .  $\gamma_g = \text{id}_G$

$\langle 1 \rangle 2$ .  $2 \Rightarrow 3$

$\langle 2 \rangle 1$ . ASSUME:  $\forall g \in G. \gamma_g = \text{id}_G$

$\langle 2 \rangle 2$ . LET:  $x, y \in G$

$\langle 2 \rangle 3$ .  $\gamma_x(y) = y$

$\langle 2 \rangle 4$ .  $xyx^{-1} = y$

$\langle 2 \rangle 5$ .  $xy = yx$

$\langle 1 \rangle 3$ .  $3 \Rightarrow 2$

PROOF: If  $xy = yx$  for all  $x, y$  then  $\gamma_x(y) = y$  for all  $x, y$ .

$\langle 1 \rangle 4$ .  $2 \Rightarrow 1$

PROOF: Easy.

□

**Corollary 8.13.1.** *If  $\text{Aut}_{\mathbf{Grp}}(G)$  is cyclic then  $G$  is Abelian.*

**Proposition 8.14.** *Every subgroup of an Abelian group is normal.*

PROOF: Let  $G$  be an Abelian group and  $N$  a subgroup of  $G$ . Given  $g \in G$  and  $n \in N$  we have  $gng^{-1} = n \in N$ .  $\square$

**Proposition 8.15.** *For any group  $G$ , the group  $G/[G, G]$  is Abelian.*

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

$$gh(hg)^{-1} \in [G, G]$$

$$\therefore gh[G, G] = hg[G, G] \quad \square$$

**Proposition 8.16.** *Let  $G$  be a finite Abelian group. Let  $p$  be a prime divisor of  $|G|$ . Then  $G$  has an element of order  $p$ .*

PROOF:

$\langle 1 \rangle 1$ . ASSUME: as induction hypothesis the result holds for all groups smaller than  $G$ .

$\langle 1 \rangle 2$ . PICK  $g \in G - \{0\}$ .

$\langle 1 \rangle 3$ . PICK an element  $h \in \langle g \rangle$  with prime order  $q$ .

$\langle 1 \rangle 4$ . CASE:  $q = p$

PROOF:  $h$  is the required element.

$\langle 1 \rangle 5$ . CASE:  $q \neq p$

$\langle 2 \rangle 1$ . PICK  $r \in G$  such that  $r + \langle h \rangle$  has order  $p$  in  $G/\langle h \rangle$ .

PROOF: By induction hypothesis since  $|G/\langle h \rangle| = |G|/q$ .

$\langle 2 \rangle 2$ .  $pr \in \langle h \rangle$

$\langle 2 \rangle 3$ . PICK  $k$  such that  $pr = kh$

$\langle 2 \rangle 4$ .  $pqr = e$

$\langle 2 \rangle 5$ .  $qr$  has order  $p$ .

$\square$

**Corollary 8.16.1.** *For  $n$  an odd integer, any Abelian group of order  $2n$  has exactly one element of order 2.*

PROOF: If  $x$  and  $y$  are distinct elements of order 2 then  $\langle x, y \rangle = \{e, x, y, xy\}$  has size 4 and so  $4 \mid 2n$  which is a contradiction.  $\square$

**Example 8.17.** It is not true that, if  $G$  is a finite group and  $d \mid |G|$ , then  $G$  has an element of order  $d$ . The quaternionic group has no element of order 4.

**Proposition 8.18.** *If  $G$  is a finite Abelian group and  $d \mid |G|$  then  $G$  has a subgroup of size  $d$ .*

PROOF:

$\langle 1 \rangle 1$ . ASSUME: as induction hypothesis the result is true for all  $d' < d$ .

$\langle 1 \rangle 2$ . ASSUME: w.l.o.g.  $d \neq 1$ .

$\langle 1 \rangle 3$ . PICK a prime  $p$  such that  $p \mid d$ .

$\langle 1 \rangle 4$ . PICK an element  $g \in G$  of order  $p$ .

$\langle 1 \rangle 5$ .  $d/p \mid |G/\langle g \rangle|$

$\langle 1 \rangle 6$ . PICK a subgroup  $H$  of  $G/\langle g \rangle$  of size  $d/p$ .

$\langle 1 \rangle 7$ .  $\pi^{-1}(H)$  is a subgroup of  $G$  of size  $d$ .

$\square$

**Proposition 8.19.** *Let  $(G, \cdot)$  be a group. Let  $\circ : G^2 \rightarrow G$  be a group homomorphism such that  $(G, \circ)$  is a group. Then  $\circ$  and  $\cdot$  coincide, and  $G$  is Abelian.*

PROOF:

$\langle 1 \rangle 1$ . For all  $g_1, g_2, h_1, h_2 \in G$  we have

$$(g_1 g_2) \circ (h_1 h_2) = (g_1 \circ h_1)(g_2 \circ h_2)$$

$\langle 1 \rangle 2$ .  $e \circ e = e$

PROOF:

$$\begin{aligned} e \circ e &= (ee) \circ (ee) \\ &= (e \circ e)(e \circ e) \end{aligned}$$

Hence  $e \circ e = e$  by Cancellation.

$\langle 1 \rangle 3$ .  $e$  is the identity of  $(G, \circ)$

$\langle 1 \rangle 4$ . For all  $g, h \in G$  we have

$$g \circ h = gh$$

PROOF:

$$\begin{aligned} g \circ h &= (ge) \circ (eh) \\ &= (g \circ e)(e \circ h) \\ &= gh \end{aligned}$$

$\langle 1 \rangle 5$ . For all  $g, h \in G$  we have  $gh = hg$ .

PROOF:

$$\begin{aligned} gh &= (e \circ g)(h \circ e) \\ &= (eh) \circ (ge) \\ &= h \circ g \\ &= hg \end{aligned}$$

□

**Corollary 8.19.1.** *If  $(G, m : G^2 \rightarrow G, e : 1 \rightarrow G, i : G \rightarrow G)$  is a group object in **Grp** then  $m$  is the multiplication of  $G$ ,  $e(*)$  is the identity of  $G$ ,  $i(g) = g^{-1}$ , and  $G$  is Abelian.*

*Conversely, if  $(G, m)$  is any Abelian group, then  $(G, m, e, i)$  is a group object in **Grp** where  $e(*) = e$  and  $i(g) = g^{-1}$ .*

## 8.1 The Category of Abelian Groups

**Definition 8.20** (Category of Abelian Groups). Let **Ab** be the full subcategory of **Grp** whose objects are the Abelian groups.

**Proposition 8.21.** *If  $(G, m : G^2 \rightarrow G, e : 1 \rightarrow G, i : G \rightarrow G)$  is a group object in **Ab** then  $m$  is the multiplication of  $G$ ,  $e(*)$  is the identity of  $G$ ,  $i(g) = g^{-1}$ , and  $G$  is Abelian.*

*Conversely, if  $(G, m)$  is any Abelian group, then  $(G, m, e, i)$  is a group object in **Ab** where  $e(*) = e$  and  $i(g) = g^{-1}$ .*

PROOF: Immediate from Corollary 8.19.1. □

**Definition 8.22** (Direct Sum). Given Abelian groups  $G$  and  $H$ , we also call the direct product of  $G$  and  $H$  the *direct sum* and denote it  $G \oplus H$ .

**Proposition 8.23.** *Given Abelian groups  $G$  and  $H$ , the direct sum  $G \oplus H$  is the coproduct of  $G$  and  $H$  in  $\mathbf{Ab}$ .*

PROOF:

- (1)1. LET:  $\kappa_1 : G \rightarrow G \oplus H$  be the group homomorphism  $\kappa_1(g) = (g, e_H)$ .  
 (1)2. LET:  $\kappa_2 : H \rightarrow G \oplus H$  be the group homomorphism  $\kappa_2(h) = (e_G, h)$ .  
 (1)3. Given group homomorphism  $\phi : G \rightarrow K$  and  $\psi : H \rightarrow K$ , define  $[\phi, \psi] : G \oplus H \rightarrow K$  by  $[\phi, \psi](g, h) = \phi(g) + \psi(h)$ .  
 (1)4.  $[\phi, \psi]$  is a group homomorphism.

PROOF:

$$\begin{aligned}
 [\phi, \psi]((g, h) + (g', h')) &= [\phi, \psi](g + g', h + h') \\
 &= \phi(g + g') + \psi(h + h') \\
 &= \phi(g) + \phi(g') + \psi(h) + \psi(h') \\
 &= \phi(g) + \psi(h) + \phi(g') + \psi(h') \\
 &= [\phi, \psi](g, h) + [\phi, \psi](g', h')
 \end{aligned}$$

- (1)5.  $[\phi, \psi] \circ \kappa_1 = \phi$

PROOF:

$$\begin{aligned}
 [\phi, \psi](\kappa_1(g)) &= [\phi, \psi](g, e_H) \\
 &= \phi(g) + \psi(e_H) \\
 &= \phi(g) + e_K \\
 &= \phi(g)
 \end{aligned}$$

- (1)6.  $[\phi, \psi] \circ \kappa_2 = \psi$

PROOF: Similar.

- (1)7. If  $f : G \oplus H \rightarrow K$  is a group homomorphism with  $f \circ \kappa_1 = \phi$  and  $f \circ \kappa_2 = \psi$  then  $f = [\phi, \psi]$ .

PROOF:

$$\begin{aligned}
 f(g, h) &= f((g, e_H) + (e_G, h)) \\
 &= f(\kappa_1(g)) + f(\kappa_2(h)) \\
 &= \phi(g) + \psi(h)
 \end{aligned}$$

□

**Theorem 8.24.** *Every finitely generated Abelian group is a direct sum of cyclic groups.*

PROOF: TODO □

## 8.2 Free Abelian Groups

**Proposition 8.25.** *Let  $A$  be a set. Let  $\mathcal{F}^A$  be the category whose objects are pairs  $(G, j)$  where  $G$  is an Abelian group and  $j$  is a function  $A \rightarrow G$ , with morphisms  $f : (G, j) \rightarrow (H, k)$  the group homomorphisms  $f : G \rightarrow H$  such that  $f \circ j = k$ . Then  $\mathcal{F}^A$  has an initial object.*

PROOF:

- (1)1. LET:  $\mathbb{Z}^{\oplus A}$  be the subgroup of  $\mathbb{Z}^A$  consisting of all functions  $\alpha : A \rightarrow \mathbb{Z}$  such that  $\alpha(a) = 0$  for only finitely many  $a \in A$ .
- (1)2. LET:  $i : A \rightarrow \mathbb{Z}^{\oplus A}$  be the function such that  $i(a)(b) = 1$  if  $a = b$  and 0 if  $a \neq b$ .
- (1)3. LET:  $G$  be any Abelian group and  $j : A \rightarrow G$  any function.
- (1)4. The unique homomorphism  $\phi : \mathbb{Z}^{\oplus A} \rightarrow G$  required is defined by  $\phi(\alpha) = \sum_{a \in A} \alpha(a)j(a)$

□

**Definition 8.26** (Free Abelian Group). For any set  $A$ , the *free Abelian group* on  $A$  is the initial object  $(F^{ab}(A), i)$  in  $\mathcal{F}^A$ .

**Proposition 8.27.** For any sets  $A$  and  $B$ , we have that  $F^{ab}(A + B)$  is the coproduct of  $F^{ab}(A)$  and  $F^{ab}(B)$  in **Grp**.

$$\begin{array}{ccccc}
 & & G & & \\
 & f \nearrow & \uparrow k & \nwarrow g & \\
 F^{ab}(A) & \xrightarrow{\kappa_1} & F^{ab}(A+B) & \xleftarrow{\kappa_2} & F^{ab}(B) \\
 i_A \uparrow & & j \uparrow & & i_B \uparrow \\
 A & \xrightarrow{k_1} & A+B & \xleftarrow{k_2} & B
 \end{array}$$

PROOF:

- (1)1. LET:  $i_A : A \rightarrow F^{ab}(A)$ ,  $i_B : B \rightarrow F^{ab}(B)$ ,  $j : A + B \rightarrow F^{ab}(A + B)$  be the canonical injections.
- (1)2. LET:  $\kappa_1, \kappa_2$  be the unique group homomorphisms that make the diagram above commute.
- (1)3. LET:  $G$  be any group and  $f : F^{ab}(A) \rightarrow G$ ,  $g : F^{ab}(B) \rightarrow G$  any group homomorphisms.
- (1)4. LET:  $h : A + B \rightarrow G$  be the unique function such that  $h \circ k_1 = f \circ i_A$  and  $h \circ k_2 = g \circ i_B$ .
- (1)5. LET:  $k : F^{ab}(A + B) \rightarrow G$  be the unique group homomorphism such that  $k \circ j = h$ .
- (1)6.  $k$  is the unique group homomorphism such that  $k \circ \kappa_1 \circ i_A = f \circ i_A$  and  $k \circ \kappa_2 \circ i_B = g \circ i_B$ .
- (1)7.  $k$  is the unique group homomorphism such that  $k \circ \kappa_1 = f$  and  $k \circ \kappa_2 = g$ .

□

**Proposition 8.28.** For  $A$  and  $B$  finite sets, if  $F^{ab}(A) \cong F^{ab}(B)$  then  $A \cong B$ .

PROOF:

- (1)1. For any set  $C$ , define  $\sim$  on  $F^{ab}(C)$  by:  $f \sim f'$  iff there exists  $g \in F^{ab}(C)$  such that  $f - f' = 2g$ .
- (1)2. For any set  $C$ ,  $\sim$  is an equivalence relation on  $F^{ab}(C)$ .
- (1)3. For any set  $C$ , we have  $F^{ab}(C) / \sim$  is finite if and only if  $C$  is finite, in which case  $|F^{ab}(C) / \sim| = 2^{|C|}$ .

PROOF: There is a bijection between  $F^{\text{ab}}(C) / \sim$  and the finite subsets of  $C$ , which maps  $f$  to  $\{c \in C : f(c) \text{ is odd}\}$ .

$\langle 1 \rangle 4$ . If  $F^{\text{ab}}(A) \cong F^{\text{ab}}(B)$  then  $A \cong B$ .

PROOF: If  $|F^{\text{ab}}(A) / \sim| = |F^{\text{ab}}(B) / \sim|$  then  $2^{|A|} = 2^{|B|}$  and so  $|A| = |B|$ .  $\square$

**Proposition 8.29.** *Let  $G$  be an Abelian group. Then  $G$  is finitely generated if and only if there exists a surjective homomorphism  $\mathbb{Z}^{\oplus n} \rightarrow G$  for some  $n$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $G$  is finitely generated then there exists a surjective homomorphism  $\mathbb{Z}^{\oplus n} \rightarrow G$  for some  $n$ .

PROOF: Let  $G = \langle a_1, \dots, a_n \rangle$ . Define  $\phi : \mathbb{Z}^{\oplus n} \rightarrow G$  by  $\phi(i_1, \dots, i_n) = i_1 \cdot a_1 + \dots + i_n \cdot a_n$ .

$\langle 1 \rangle 2$ . If there exists a surjective homomorphism  $\phi : \mathbb{Z}^{\oplus n} \rightarrow G$  for some  $n$  then  $G$  is finitely generated.

PROOF:  $G$  is generated by  $\phi(1, 0, \dots, 0), \phi(0, 1, 0, \dots, 0), \dots, \phi(0, \dots, 0, 1)$ .  $\square$

**Proposition 8.30.** *Let  $A$  be a set. Let  $i : A \hookrightarrow F(A)$  be the free group on  $A$ . Then  $\pi \circ i : A \rightarrow F(A)/[F(A), F(A)]$  is the free Abelian group on  $A$ .*

$$\begin{array}{ccc}
 & F(A)/[F(A), F(A)] & \\
 \pi \uparrow & \searrow h & \\
 F(A) & \xrightarrow{g} & G \\
 i \uparrow & \nearrow f & \\
 A & & 
 \end{array}$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $G$  be an Abelian group and  $f : A \rightarrow G$  a function.

$\langle 1 \rangle 2$ . LET:  $g : F(A) \rightarrow G$  be the unique group homomorphism such that  $g \circ i = f$ .

$\langle 1 \rangle 3$ .  $[F(A), F(A)] \subseteq \ker g$

PROOF: For all  $x, y \in F(A)$  we have  $g(xy x^{-1} y^{-1}) = g(x) + g(y) - g(x) - g(y) = 0$ .

$\langle 1 \rangle 4$ . LET:  $h : F(A)/[F(A), F(A)] \rightarrow G$  be the unique group homomorphism such that  $h \circ \pi = g$ .

$\langle 1 \rangle 5$ .  $h$  is the unique group homomorphism such that  $h \circ \pi \circ i = f$ .  $\square$

**Corollary 8.30.1.** *Let  $A$  and  $B$  be sets. Let  $F(A)$  and  $F(B)$  be the free groups on  $A$  and  $B$  respectively. If  $F(A) \cong F(B)$  then  $A \cong B$ .*

PROOF: Proposition 8.28.  $\square$

### 8.3 Cokernels

**Proposition 8.31.** *Let  $\phi : G \rightarrow H$  be a homomorphism between Abelian groups. Then there exists an Abelian group  $K$  and homomorphism  $\pi : H \rightarrow K$  that is initial with respect to all homomorphism  $\alpha : H \rightarrow L$  such that  $\alpha \circ \phi = 0$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $K = H/\text{im } \phi$  and  $\pi$  be the canonical homomorphism.

$\langle 1 \rangle 2$ . LET:  $\pi \circ \phi = 0$

$\langle 1 \rangle 3$ . LET:  $\alpha : H \rightarrow L$  satisfy  $\alpha \circ \phi = 0$

$\langle 1 \rangle 4$ .  $\text{im } \phi \subseteq \ker \alpha$

$\langle 1 \rangle 5$ . There exists a unique  $\bar{\alpha} : H/\text{im } \phi \rightarrow L$  such that  $\bar{\alpha} \circ \pi = \alpha$

□

**Definition 8.32** (Cokernel). For any homomorphism  $\phi : G \rightarrow H$  in **Ab**, the *cokernel* of  $\phi$  is the Abelian group  $\text{coker } \phi$  and homomorphism  $\pi : H \rightarrow \text{coker } \phi$  that is initial among homomorphisms  $\alpha : H \rightarrow L$  such that  $\alpha \circ \phi = 0$ .

**Proposition 8.33.**  $\pi : H \rightarrow \text{coker } \phi$  is initial among functions  $f : H \rightarrow X$  such that, for all  $x, y \in H$ , if  $x + \text{im } \phi = y + \text{im } \phi$  then  $f(x) = f(y)$ .

PROOF: Easy. □

**Proposition 8.34.** Let  $\phi : G \rightarrow H$  be a homomorphism of Abelian groups. Then the following are equivalent.

- $\phi$  is an epimorphism.
- $\text{coker } \phi$  is trivial.
- $\phi$  is surjective.

PROOF:

$\langle 1 \rangle 1$ .  $1 \Rightarrow 2$

$\langle 2 \rangle 1$ . ASSUME:  $\phi$  is epi.

$\langle 2 \rangle 2$ . LET:  $\pi : H \rightarrow \text{coker } \phi$  be the canonical homomorphism.

$\langle 2 \rangle 3$ .  $\pi \circ \phi = 0 \circ \phi$

$\langle 2 \rangle 4$ .  $\pi = 0$

$\langle 2 \rangle 5$ .  $\text{coker } \phi = \text{im } \pi$  is trivial.

$\langle 1 \rangle 2$ .  $2 \Rightarrow 3$

PROOF: If  $\text{coker } \phi = H/\text{im } \phi$  is trivial then  $\text{im } \phi = H$ .

$\langle 1 \rangle 3$ .  $3 \Rightarrow 1$

PROOF: If it is surjective then it is epi in **Set**.

□





## Chapter 9

# Group Actions

### 9.1 Group Actions

**Definition 9.1** (Action). Let  $G$  be a group. Let  $A$  be an object of a category  $\mathcal{C}$ . A (left) action of  $G$  on  $A$  is a group homomorphism  $G \rightarrow \text{Aut}_{\mathcal{C}}(A)$ .

It is *faithful* or *effective* iff it is injective.

**Proposition 9.2.** Let  $A$  be a set. An action of the group  $G$  on the set  $A$  is given by a function  $\cdot : G \times A \rightarrow A$  such that

- $\forall a \in A. ea = a$
- $\forall g, h \in G. \forall a \in A. (gh)a = g(ha)$

PROOF: Just unfolding definitions.  $\square$

**Example 9.3.** Left multiplication defines a faithful action of any group on its own underlying set.

In fact, for any subgroup  $H$  of a group  $G$ , left multiplication defines an action of  $G$  on  $G/H$ .

**Corollary 9.3.1** (Cayley's Theorem). Every group  $G$  is a subgroup of a symmetric group, namely  $\text{Aut}_{\text{Set}}(G)$ .

**Example 9.4.** Conjugation  $g * h = ghg^{-1}$  is an action of any group on its own underlying set.

**Definition 9.5** (Transitive). An action of a group  $G$  on a set  $A$  is *transitive* iff, for all  $a, b \in A$ , there exists  $g \in G$  such that  $ga = b$ .

**Example 9.6.** Left multiplication of a group  $G$  is a transitive action of  $G$  on  $G$ .

**Definition 9.7** (Orbit). Given an action of a group  $G$  on a set  $A$  and  $a \in A$ , the *orbit* of  $a$  is

$$\text{O}_G(a) := \{ga : g \in G\} .$$

**Proposition 9.8.** *Given an action of a group  $G$  on a set  $A$ , the orbits form a partition of  $A$ .*

PROOF:

$\langle 1 \rangle 1$ . Every element of  $A$  is in some orbit.

PROOF: Since  $a \in O_G(a)$ .

$\langle 1 \rangle 2$ . Distinct orbits are disjoint.

$\langle 2 \rangle 1$ . LET:  $a \in O_G(b) \cap O_G(c)$

$\langle 2 \rangle 2$ . PICK  $g, h \in G$  such that  $a = gb = hc$ .

$\langle 2 \rangle 3$ .  $O_G(b) \subseteq O_G(c)$

PROOF: For all  $k \in G$  we have  $kb = kg^{-1}hc$ .

$\langle 2 \rangle 4$ .  $O_G(c) \subseteq O_G(b)$

PROOF: Similar.

□

**Proposition 9.9.** *Given an action of a group  $G$  on a set  $A$  and  $a \in A$ , the action is transitive on  $O_G(a)$ .*

PROOF:

$\langle 1 \rangle 1$ . The restriction of the action is an action on  $O_G(a)$ .

PROOF: Since  $g(ha) = (gh)a$ , the action maps  $O_G(a)$  to itself.

$\langle 1 \rangle 2$ . The restricted action is transitive.

PROOF: Given  $ga, ha \in O_G(a)$ , we have  $ha = (hg^{-1})(ga)$ .

□

**Definition 9.10** (Stabilizer Subgroup). Given an action of a group  $G$  on a set  $A$  and  $a \in A$ , the *stabilizer subgroup* of  $a$  is

$$\text{Stab}_G(a) := \{g \in G : ga = a\} .$$

**Proposition 9.11.** *Stabilizer subgroups are subgroups.*

PROOF: If  $g, h \in \text{Stab}_G(a)$  then  $gh^{-1}a = a$  so  $gh^{-1} \in \text{Stab}_G(a)$ . □

**Proposition 9.12.** *Let  $G$  act on a set  $A$ . Let  $a \in A$  and  $g \in G$ . Then*

$$\text{Stab}_G(ga) = g\text{Stab}_G(a)g^{-1} .$$

PROOF:

$$h \in \text{Stab}_G(ga) \Leftrightarrow hga = ga$$

$$\Leftrightarrow g^{-1}hga = a$$

$$\Leftrightarrow g^{-1}hg \in \text{Stab}_G(a)$$

$$\Leftrightarrow h \in g\text{Stab}_G(a)g^{-1}$$

□

**Corollary 9.12.1.** *Let  $G$  be an action on a set  $A$  and  $a \in A$ . If  $\text{Stab}_G(a)$  is normal in  $G$ , then for any  $b \in O_G(a)$  we have  $\text{Stab}_G(a) = \text{Stab}_G(b)$ .*

**Definition 9.13** (Free). An action of a group  $G$  on a set  $A$  is *free* iff, whenever  $ga = a$ , then  $g = e$ .

**Example 9.14.** The action of left multiplication is free.

**Proposition 9.15.** *Let  $G$  be a group. Let  $H$  be a subgroup of  $G$  of finite index  $n$ . Then  $H$  includes a subgroup  $K$  that is normal in  $G$  and such that  $|G : K|$  divides  $\gcd(|G|, n!)$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $\sigma : G \rightarrow \text{Aut}_{\text{Set}}(G/H)$  be the action of left multiplication.

$\langle 1 \rangle 2$ . LET:  $K = \ker \sigma$

$\langle 1 \rangle 3$ .  $K \subseteq H$

$\langle 2 \rangle 1$ . LET:  $g \in K$

$\langle 2 \rangle 2$ .  $\sigma(g)(H) = H$

$\langle 2 \rangle 3$ .  $gH = H$

$\langle 2 \rangle 4$ .  $g \in H$

$\langle 1 \rangle 4$ .  $K$  is normal in  $G$ .

PROOF: Proposition 7.42.

$\langle 1 \rangle 5$ .  $|G : K| \mid |G|$

PROOF: Lagrange's Theorem.

$\langle 1 \rangle 6$ .  $|G : K| \mid n!$

PROOF: Since  $G/K$  is a subgroup of  $\text{Aut}_{\text{Set}}(G/H)$ .

□

**Corollary 9.15.1.** *Let  $G$  be a finite group. Let  $H$  be a subgroup of  $G$  of index  $p$  where  $p$  is the smallest prime that divides  $|G|$ . Then  $H$  is normal in  $G$ .*

PROOF:

$\langle 1 \rangle 1$ . PICK a subgroup  $K$  of  $H$  normal in  $G$  such that  $|G : K|$  divides  $\gcd(|G|, p!)$ .

$\langle 1 \rangle 2$ .  $|G : K|$  divides  $p$ .

$\langle 1 \rangle 3$ .  $|G : H| |H : K|$  divides  $p$ .

$\langle 1 \rangle 4$ .  $|H : K| = 1$

$\langle 1 \rangle 5$ .  $H = K$

$\langle 1 \rangle 6$ .  $H$  is normal.

□

**Corollary 9.15.2.** *Any subgroup of index 2 is normal.*

**Proposition 9.16.** *Let  $G$  be a group with finite set of generators  $A$ . Then left multiplication defines a free action of  $G$  on its Cayley graph.*

PROOF: Easy since if  $g_2 = g_1 a$  then  $hg_2 = hg_1 a$ . □

**Corollary 9.16.1.** *A free group acts freely on a tree.*

**Theorem 9.17.** *If a group  $G$  acts freely on a tree then  $G$  is free.*

**Corollary 9.17.1.** *Every subgroup of the free group on a finite set is free.*

PROOF: If  $H$  is a subgroup of  $F(A)$  then left multiplication defines a free action of  $H$  on the Cayley graph of  $F(A)$ , which is a tree. □

## 9.2 Category of $G$ -Sets

**Definition 9.18.** Given a group  $G$ , let  $G - \mathbf{Set}$  be the category with:

- objects all pairs  $(A, \rho)$  such that  $A$  is a set and  $\rho : G \times A \rightarrow A$  is an action of  $G$  on  $A$ ;
- morphisms  $f : (A, \rho) \rightarrow (B, \sigma)$  are functions  $f : A \rightarrow B$  that are  $(G-)$ equivariant, i.e.

$$\forall g \in G. \forall a \in A. f(\rho(g, a)) = \sigma(g, f(a)) .$$

**Proposition 9.19.** *A  $G$ -equivariant function  $f : A \rightarrow B$  is an isomorphism in  $G - \mathbf{Set}$  if and only if it is bijective.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $f : A \rightarrow B$  be  $G$ -equivariant and bijective.

PROVE:  $f^{-1}$  is  $G$ -equivariant.

$\langle 1 \rangle 2$ . LET:  $g \in G$  and  $b \in B$

$\langle 1 \rangle 3$ .  $f^{-1}(gb) = gf^{-1}(b)$

PROOF:

$$\begin{aligned} f(f^{-1}(gb)) &= gb \\ &= gf(f^{-1}(b)) \\ &= f(gf^{-1}(b)) \end{aligned}$$

□

**Proposition 9.20.** *Let  $G$  be a group and  $A$  a transitive  $G$ -set. Let  $a \in A$ . Then  $A$  is isomorphic to  $G/\text{Stab}_G(a)$  under left multiplication.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $f : G/\text{Stab}_G(a) \rightarrow A$  be the function  $f(g\text{Stab}_G(a)) = ga$ .

$\langle 2 \rangle 1$ . ASSUME:  $g\text{Stab}_G(a) = h\text{Stab}_G(a)$

PROVE:  $ga = ha$

$\langle 2 \rangle 2$ .  $g^{-1}h \in \text{Stab}_G(a)$

$\langle 2 \rangle 3$ .  $g^{-1}ha = a$

$\langle 2 \rangle 4$ .  $ha = ga$

$\langle 1 \rangle 2$ .  $f$  is  $G$ -equivariant.

PROOF: Since  $f(gh\text{Stab}_G(a)) = gha = gf(h\text{Stab}_G(a))$ .

$\langle 1 \rangle 3$ .  $f$  is injective.

PROOF: If  $ga = ha$  then  $g^{-1}h \in \text{Stab}_G(a)$  so  $g\text{Stab}_G(a) = h\text{Stab}_G(a)$ .

$\langle 1 \rangle 4$ .  $f$  is surjective.

PROOF: Since for all  $b \in A$  there exists  $g \in G$  such that  $ga = b$ .

□

**Corollary 9.20.1.** *If  $O$  is an orbit of the action of a finite group  $G$  on a set  $A$ , then  $O$  is finite and  $|O|$  divides  $|G|$ .*

**Corollary 9.20.2.** *Let  $H$  be a subgroup of  $G$  and  $g \in G$ . Then*

$$G/H \cong G/(gHg^{-1})$$

*in  $G - \mathbf{Set}$ .*

PROOF: Taking  $A = G/H$  and  $a = gH$ .  $\square$

**Proposition 9.21.** *Given a family of  $G$ -sets  $\{A_i\}_{i \in I}$ , we have  $\prod_{i \in I} A_i$  is their product in  $G - \mathbf{Set}$  under*

$$g\{a_i\}_{i \in I} = \{ga_i\}_{i \in I}.$$

PROOF: Easy.  $\square$

**Proposition 9.22.** *Given a family of  $G$ -sets  $\{A_i\}_{i \in I}$ , we have  $\coprod_{i \in I} A_i$  is their product in  $G - \mathbf{Set}$  under*

$$g(i, a_i) = (i, ga_i).$$

PROOF: Easy.  $\square$

**Proposition 9.23.** *Every finite  $G$ -set is a coproduct of  $G$ -sets of the form  $G/H$ .*

PROOF: If  $O(a_1), \dots, O(a_n)$  are the orbits of the  $G$ -set  $A$ , then  $G$  is the coproduct of  $G/\text{Stab}_G(a_1), \dots, G/\text{Stab}_G(a_n)$ .  $\square$

**Proposition 9.24.** *For any group  $G$  we have  $G \cong \text{Aut}_{G-\mathbf{Set}}(G)$  (considering  $G$  as a  $G$ -set under left multiplication).*

PROOF:

$\langle 1 \rangle 1$ . Define  $\phi : G \rightarrow \text{Aut}_{G-\mathbf{Set}}(G)$  by  $\phi(g)(g') = g'g^{-1}$ .

$\langle 2 \rangle 1$ . LET:  $g \in G$

PROVE:  $\lambda g' \in G.g'g^{-1}$  is an automorphism of  $G$  in  $G - \mathbf{Set}$ .

$\langle 2 \rangle 2$ .  $\phi(g)$  is  $G$ -equivariant.

PROOF: Since  $\phi(g)(h_1h_2) = h_1h_2g^{-1} = h_1\phi(g)(h_2)$ .

$\langle 2 \rangle 3$ .  $\phi(g)$  is injective.

PROOF: By Cancellation.

$\langle 2 \rangle 4$ .  $\phi(g)$  is surjective.

PROOF: For any  $h \in G$  we have  $h = \phi(g)(hg)$ .

$\langle 1 \rangle 2$ .  $\phi$  is a group homomorphism.

PROOF:  $\phi(g_1g_2)(h) = hg_2^{-1}g_1^{-1} = \phi(g_1)(\phi(g_2)(h))$ .

$\langle 1 \rangle 3$ .  $\phi$  is injective.

PROOF: If  $\phi(g) = \phi(g')$  then  $g = \phi(g)(e) = \phi(g')(e) = g'$ .

$\langle 1 \rangle 4$ .  $\phi$  is surjective.

$\langle 2 \rangle 1$ . LET:  $\sigma \in \text{Aut}_{G-\mathbf{Set}}(G)$

$\langle 2 \rangle 2$ . LET:  $g = \sigma(e)$

PROVE:  $\sigma = \phi(g^{-1})$

$\langle 2 \rangle 3$ .  $\sigma(h) = hg$

PROOF:  $\sigma(h) = \sigma(hg) = h\sigma(e) = hg$ .

$\square$



**Part III**

**Ring Theory**





# Chapter 10

## Rngs

**Definition 10.1** (Ring). A *rng* consists of a set  $R$  and binary operations  $+, \cdot : R^2 \rightarrow R$  such that:

- $(R, +)$  is an Abelian group
- $\cdot$  is associative.
- The *distributive properties* hold: for all  $r, s, t \in R$  we have

$$(r + s)t = rt + st, \quad r(s + t) = rs + rt .$$

**Example 10.2.**     • The *zero rng* is  $\{0\}$ .

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  and  $\mathbb{C}$  are rngs.
- $2\mathbb{Z}$  is a rng.
- Given a rng  $R$  and natural number  $n$ , then the set  $\mathfrak{gl}_n(R)$  of all  $n \times n$  matrices with entries in  $R$  is a rng under matrix addition and matrix multiplication.
- For any set  $S$ , the power set  $\mathcal{P}S$  is a rng under  $A + B = (A \cup B) - (A \cap B)$  and  $AB = A \cap B$ .
- Given a rng  $R$  and a set  $S$ , then  $R^S$  is a rng under  $(f + g)(s) = f(s) + g(s)$  and  $(fg)(s) = f(s)g(s)$  for all  $f, g \in R^S$  and  $s \in S$ .
- The set  $\mathfrak{sl}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) : \text{tr } M = 0\}$  is a rng.
- The set  $\mathfrak{sl}_n(\mathbb{C}) = \{M \in \mathfrak{gl}_n(\mathbb{C}) : \text{tr } M = 0\}$  is a rng.
- $\mathbb{Z}/n\mathbb{Z}$  is a rng.

- The ring  $\mathbb{H}$  of *quaternions* is  $\mathbb{R}^4$  under the following operations, where we write  $(a, b, c, d)$  as  $a + bi + cj + dk$ :

$$\begin{aligned}
 (a + bi + cj + dk) + (a' + b'i + c'j + d'k) &= (a + a') + (b + b')i \\
 &\quad + (c + c')j + (d + d')k \\
 (a + bi + cj + dk)(a' + b'i + c'j + d'k) &= (aa' - bb' - cc' - dd') \\
 &\quad + (ab' + ba' + cd' - dc')i \\
 &\quad + (ac' - bd' + ca' + db')j \\
 &\quad + (ad' + bc' - cb' + da')k
 \end{aligned}$$

- For any Abelian group  $G$ , the set  $\text{End}_{\mathbf{Ab}}(G)$  is a ring under pointwise addition and composition.

**Proposition 10.3.** *In any rng  $R$  we have*

$$\forall x \in R. x0 = 0x = 0 \text{ .}$$

PROOF:

$$\begin{aligned}
 x0 &= x(0 + 0) \\
 &= x0 + x0
 \end{aligned}$$

and so  $x0 = 0$  by Cancellation. Similarly  $0x = 0$ .  $\square$

**Definition 10.4** (Zero Divisor). Let  $R$  be a rng and  $a \in R$ .

Then  $a$  is a *left-zero-divisor* iff there exists  $b \in R - \{0\}$  such that  $ab = 0$ .

The element  $a$  is a *right-zero-divisor* iff there exists  $b \in R - \{0\}$  such that  $ba = 0$ .

**Example 10.5.** 0 is a left- and right-zero-divisor in every non-zero rng.

The zero rng is the only ring with no zero-divisors.

**Proposition 10.6.** *Let  $R$  be a rng and  $a \in R$ . Then  $a$  is not a left-zero-divisor if and only if left multiplication by  $a$  is an injective function  $R \rightarrow R$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $a$  is not a left-zero-divisor then left multiplication by  $a$  is injective.

$\langle 2 \rangle 1$ . ASSUME:  $a$  is not a left-zero-divisor.

$\langle 2 \rangle 2$ . LET:  $ab = ac$

$\langle 2 \rangle 3$ .  $a(b - c) = 0$

$\langle 2 \rangle 4$ .  $b - c = 0$

$\langle 2 \rangle 5$ .  $b = c$

$\langle 1 \rangle 2$ . If  $a$  is a left-zero-divisor then left multiplication by  $a$  is not injective.

$\langle 2 \rangle 1$ . PICK  $b \neq 0$  such that  $ab = 0$ .

$\langle 2 \rangle 2$ .  $ab = a0$  but  $b \neq 0$

$\square$

## 10.1 Commutative Rings

**Definition 10.7** (Commutative). A rng  $R$  is *commutative* iff  $\forall x, y \in R. xy = yx$ .

**Example 10.8.** • The zero rng is commutative.

- $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  are commutative.
- $2\mathbb{Z}$  is commutative.
- $\mathfrak{gl}_2(\mathbb{R})$  is not commutative.
- For any set  $S$ , the rng  $\mathcal{P}S$  is commutative.
- If  $R$  is commutative then  $R^S$  is commutative.

## 10.2 Rng Homomorphisms

**Definition 10.9.** Let  $R$  and  $S$  be rngs. A *rng homomorphism*  $\phi : R \rightarrow S$  is a function such that, for all  $x, y \in R$ , we have

$$\begin{aligned}\phi(x + y) &= \phi(x) + \phi(y) \\ \phi(xy) &= \phi(x)\phi(y)\end{aligned}$$

Let **Rng** be the category of rngs and rng homomorphisms.

## 10.3 Quaternions

**Definition 10.10** (Norm). The *norm* of a quaternion is defined by

$$N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2 .$$



# Chapter 11

## Rings

**Definition 11.1** (Ring). A *ring*  $R$  is a rng such that there exists  $1 \in R$ , the *multiplicative identity*, such that

$$\forall x \in R. x1 = 1x = x \text{ .}$$

**Example 11.2.**     • The zero rng is a ring with  $1 = 0$ .

- $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  are rngs.
- $2\mathbb{Z}$  is not a ring.
- If  $R$  is a ring then  $\mathfrak{gl}_n(R)$  is a ring.
- For any set  $S$ , the rng  $\mathcal{P}S$  is a ring with  $1 = S$ .
- If  $R$  is a ring then  $R^S$  is a ring.
- $\mathfrak{sl}_n(\mathbb{R})$  is not a ring for  $n > 0$ .
- $\mathfrak{sl}_n(\mathbb{C})$  is not a ring for  $n > 0$ .
- $\mathfrak{so}_n(\mathbb{R}) = \{M \in \mathfrak{sl}_n(\mathbb{R}) : M + M^T = 0\}$  is not a ring.
- $\mathbb{Z}/n\mathbb{Z}$  is a ring.

**Proposition 11.3.** *In any ring  $R$ , if  $0 = 1$  then  $R$  is the zero ring.*

PROOF: For any  $x \in R$  we have  $x = 1x = 0x = 0$ .  $\square$

**Proposition 11.4.** *In any ring we have  $(-1)x = -x$ .*

PROOF: Since

$$\begin{aligned} x + (-1)x &= 1x + (-1)x \\ &= (1 + (-1))x \\ &= 0x \\ &= 0 \end{aligned}$$

$\square$

## 11.1 Units

**Definition 11.5** (Left-Unit, Right-Unit). Let  $R$  be a ring and  $a \in R$ . Then  $a$  is a *left-unit* iff there exists  $b \in R$  such that  $ab = 1$ . The element  $a$  is a *right-unit* iff there exists  $b \in R$  such that  $ba = 1$ .

An element is a *unit* iff it is a left-unit and a right-unit.

**Proposition 11.6.** *Let  $R$  be a ring and  $a \in R$ . Then  $a$  is a left-unit iff left multiplication by  $a$  is a surjective function  $R \rightarrow R$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $a$  is a left-unit then left multiplication by  $a$  is surjective.

$\langle 2 \rangle 1$ . PICK  $b \in R$  such that  $ab = 1$ .

$\langle 2 \rangle 2$ . For all  $c \in R$  we have  $c = a(bc)$ .

$\langle 1 \rangle 2$ . If left multiplication by  $a$  is surjective then  $a$  is a left-unit.

PROOF: Immediate.

□

**Proposition 11.7.** *Let  $R$  be a ring and  $a \in R$ . Then  $a$  is a right-unit iff right multiplication by  $a$  is a surjective function  $R \rightarrow R$ .*

PROOF: Similar. □

**Proposition 11.8.** *No left-unit is a right-zero-divisor.*

PROOF:

$\langle 1 \rangle 1$ . ASSUME: for a contradiction  $ab = 1$  and  $ca = 0$  where  $c \neq 0$ .

$\langle 1 \rangle 2$ .  $c = 0$

PROOF:

$$0 = 0b$$

$$= cab$$

$$= c1$$

$$= c$$

$\langle 1 \rangle 3$ . Q.E.D.

PROOF: This is a contradiction.

□

**Proposition 11.9.** *No right-unit is a left-zero-divisor.*

PROOF: Similar. □

**Proposition 11.10.** *The inverse of a unit is unique.*

PROOF: If  $ba = 1$  and  $ac = 1$  then  $b = bac = c$ . □

**Proposition 11.11.** *The units of a ring form a group under multiplication.*

PROOF:

$\langle 1 \rangle 1$ . If  $a$  and  $b$  are units then  $ab$  is a unit.

PROOF: We have  $b^{-1}a^{-1}ab = 1$  and  $abb^{-1}a^{-1} = 1$ .

⟨1⟩2. 1 is a unit.

PROOF: Since  $1 \cdot 1 = 1$ .

⟨1⟩3. If  $a$  is a unit then its inverse is a unit.

PROOF: Immediate from definitions.

□

**Definition 11.12** (Group of Units). For any ring  $R$ , we write  $R^*$  for the group of the units of  $R$  under multiplication.

**Example 11.13.** The quaternionic group is a subgroup of  $\mathbb{H}^*$ .

**Example 11.14.** The norm is a group homomorphism  $\mathbb{H}^* \rightarrow \mathbb{R}^+$  where  $\mathbb{R}^+$  is the group of positive real numbers under multiplication with kernel isomorphic to  $\text{SU}_2(\mathbb{C})$ . The isomorphism maps a quaternion  $a + bi + cj + dk$  to

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}.$$

**Theorem 11.15** (Fermat's Little Theorem). *Let  $p$  be a prime number and  $a$  any integer. Then  $a^p \equiv a \pmod{p}$ .*

PROOF: If  $p \mid a$  then  $a^p \equiv a \equiv 0 \pmod{p}$ . Otherwise, we have  $a^{p-1} \equiv 1 \pmod{p}$  by applying Lagrange's Theorem to  $(\mathbb{Z}/p\mathbb{Z})^*$ . □

**Example 11.16.** It is not true that, if  $n \mid |G|$ , then  $G$  has a subgroup of order  $n$ . The group  $A_4$  has order 12 but no subgroup of order 6.

**Proposition 11.17.** *If  $p$  is prime then  $(\mathbb{Z}/p\mathbb{Z})^*$  is cyclic.*

PROOF:

⟨1⟩1. LET:  $g$  be an element of maximal order in  $(\mathbb{Z}/p\mathbb{Z})^*$ .

⟨1⟩2. For all  $h \in (\mathbb{Z}/p\mathbb{Z})^*$  we have  $h^{|g|} = 1$ .

PROOF: Proposition 8.10.

⟨1⟩3. There are at most  $|g|$  elements  $x$  such that  $x^{|g|} = 1$  in  $\mathbb{Z}/p\mathbb{Z}$

⟨1⟩4.  $p - 1 \leq |g|$

⟨1⟩5.  $|g| = p - 1$

⟨1⟩6.  $g$  generates  $(\mathbb{Z}/p\mathbb{Z})^*$ .

□

**Example 11.18.**  $(\mathbb{Z}/12\mathbb{Z})^*$  is not cyclic. Its elements are 1, 5, 7 and 11 with orders 1, 2, 2 and 2.

**Theorem 11.19** (Wilson's Theorem). *A positive integer  $p$  is prime if and only if  $(p - 1)! \equiv -1 \pmod{p}$ .*

⟨1⟩1. If  $p$  is prime then  $(p - 1)! \equiv -1 \pmod{p}$ .

⟨2⟩1. ASSUME:  $p$  is prime.

⟨2⟩2.  $(p - 1)!$  is the product of all the elements of  $(\mathbb{Z}/p\mathbb{Z})^*$

⟨2⟩3. The only element of  $(\mathbb{Z}/p\mathbb{Z})^*$  with order 2 is  $-1$ .

⟨2⟩4.  $(p - 1)! \equiv -1 \pmod{p}$

PROOF: Proposition 6.20.

$\langle 1 \rangle 2$ . If  $(p-1)! \equiv -1 \pmod{p}$  then  $p$  is prime.

$\langle 2 \rangle 1$ . ASSUME:  $(p-1)! \equiv -1 \pmod{p}$

$\langle 2 \rangle 2$ . LET:  $d$  be a proper divisor of  $p$ .

PROVE:  $d = 1$

$\langle 2 \rangle 3$ .  $d \mid (p-1)!$

$\langle 2 \rangle 4$ .  $d \mid 1$

PROOF: Since  $d \mid p \mid (p-1)! + 1$ .

$\langle 2 \rangle 5$ .  $d = 1$

□

**Proposition 11.20.** *If  $p$  and  $q$  are distinct odd primes then  $(\mathbb{Z}/pq\mathbb{Z})^*$  is not cyclic.*

PROOF:

$\langle 1 \rangle 1$ .  $|(\mathbb{Z}/pq\mathbb{Z})^*| = (p-1)(q-1)$

$\langle 1 \rangle 2$ . LET:  $g \in (\mathbb{Z}/pq\mathbb{Z})^*$

PROVE:  $g$  does not have order  $(p-1)(q-1)$

$\langle 1 \rangle 3$ .  $g^{(p-1)(q-1)/2} \equiv 1 \pmod{p}$

$\langle 1 \rangle 4$ .  $g^{(p-1)(q-1)/2} \equiv 1 \pmod{q}$

$\langle 1 \rangle 5$ .  $pq \mid g^{(p-1)(q-1)/2} - 1$

$\langle 1 \rangle 6$ .  $g^{(p-1)(q-1)/2} \equiv 1 \pmod{pq}$

$\langle 1 \rangle 7$ .  $|g| \mid (p-1)(q-1)/2$

□

**Proposition 11.21.** *For any prime  $p$ , we have  $\text{Aut}_{\mathbf{Grp}}(C_p) \cong C_{p-1}$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $\phi : \text{Aut}_{\mathbf{Grp}}(C_p) \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$  be the function  $\phi(\alpha) = \alpha(1)$ .

PROOF:  $\alpha(1)$  has order  $p$  in  $C_p$  and so is coprime with  $p$ .

$\langle 1 \rangle 2$ .  $\phi$  is a homomorphism.

PROOF:  $\phi(\alpha \circ \beta) = \alpha(\beta(1)) = \alpha(\beta(1)1) = \beta(1)\alpha(1) = \phi(\alpha)\phi(\beta)$

$\langle 1 \rangle 3$ .  $\phi$  is injective.

PROOF: If  $\phi(\alpha) = \phi(\beta)$  then for any  $n$  we have  $\alpha(n) = n\alpha(1) = n\phi(\alpha) = n\phi(\beta) = n\beta(1) = \beta(n)$ .

$\langle 1 \rangle 4$ .  $\phi$  is surjective.

PROOF: For any  $r \in (\mathbb{Z}/p\mathbb{Z})^*$  we have  $r = \phi(\alpha)$  where  $\alpha(n) = nr \pmod{p}$ .

$\langle 1 \rangle 5$ .  $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$

□

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

**Proposition 11.22.** *For  $n$  a positive integer, we have  $(\mathbb{Z}/n\mathbb{Z})^* = \{m \in \mathbb{Z}/n\mathbb{Z} : \gcd(m, n) = 1\}$ .*



PROOF:

$$\begin{aligned} m \in (\mathbb{Z}/n\mathbb{Z})^* &\Leftrightarrow \exists a.am \equiv 1 \pmod{n} \\ &\Leftrightarrow \exists a, b.am + bn = 1 \\ &\Leftrightarrow \gcd(m, n) = 1 \quad \square \end{aligned}$$

**Definition 11.23** (Euler's Totient Function). For  $n$  a positive integer, let  $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ .

**Proposition 11.24.** *If  $n$  is an odd positive integer then  $\phi(2n) = \phi(n)$ .*

PROOF:

(1)1. LET:  $n$  be an odd positive integer.

(1)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.

(1)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.

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

□

**Theorem 11.25.** *For any positive integer  $n$  we have*

$$\sum_{m>0, m|n} \phi(m) = n.$$

PROOF:

(1)1. Define  $\chi : \{0, 1, \dots, n-1\} \rightarrow \{(m, d) : m > 0, m \mid n, d \text{ generates } \langle n/m \rangle\}$   
by:  $\chi(x) = (\gcd(x, n), x)$ .

(1)2.  $\chi$  is injective.

(1)3.  $\chi$  is surjective.

PROOF: Given  $(m, d)$  such that  $d$  generates  $\langle n/m \rangle$  we have  $\chi(d) = (m, d)$ .

(1)4.  $n = \sum_{m>0, m|n} \phi(m)$

PROOF: Since  $\langle n/m \rangle \cong C_m$  and so has  $\phi(m)$  generators.

□

**Proposition 11.26.** *For any positive integers  $a$  and  $n$ , we have  $n \mid \phi(a^n - 1)$ .*

PROOF: Since the order of  $a$  is  $n$  in  $(\mathbb{Z}/(a^n - 1)\mathbb{Z})^*$ . □

**Theorem 11.27** (Euler's Theorem). *For any coprime integers  $a$  and  $n$  we have  $a^{\phi(n)} \equiv a \pmod{n}$ .*

PROOF: Immediate from Lagrange's Theorem. □

**Proposition 11.28.**

$$|\text{Aut}_{\mathbf{Grp}}(C_n)| = \phi(n)$$

PROOF: An automorphism  $\alpha$  is determined by  $\alpha(1)$  which is any element of order  $n$ , and  $g$  has order  $n$  iff  $\gcd(g, n) = 1$ . □

**Example 11.29.**

$$\text{Aut}_{\mathbf{Grp}}(\mathbb{Z}) \cong C_2$$

PROOF: The only automorphisms are the identity and multiplication by -1.  $\square$

### 11.3 Nilpotent Elements

**Definition 11.30** (Nilpotent). Let  $R$  be a ring and  $a \in R$ . Then  $a$  is *nilpotent* iff there exists  $n$  such that  $a^n = 0$ .

**Proposition 11.31.** *Let  $R$  be a ring and  $a, b \in R$ . If  $a$  and  $b$  are nilpotent and  $ab = ba$  then  $a + b$  is nilpotent.*

PROOF:

$\langle 1 \rangle 1$ . PICK  $m$  and  $n$  such that  $a^m = b^n = 0$ .

$\langle 1 \rangle 2$ .  $(a + b)^{m+n} = 0$

PROOF: Since  $(a + b)^{m+n} = \sum_k \binom{m+n}{k} a^k b^{m+n-k}$  and every term in this sum is 0 since, for every  $k$ , either  $k \geq m$  or  $m + n - k \geq n$ .

$\square$

**Proposition 11.32.**  *$m$  is nilpotent in  $\mathbb{Z}/n\mathbb{Z}$  if and only if  $m$  is divisible by all the prime factors of  $n$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $m$  is nilpotent then  $m$  is divisible by all the prime factors of  $n$ .

$\langle 2 \rangle 1$ . ASSUME:  $m^a \equiv 0 \pmod{n}$

$\langle 2 \rangle 2$ . For every prime  $p$ , if  $p \mid n$  then  $p \mid m^a$ .

$\langle 2 \rangle 3$ . For every prime  $p$ , if  $p \mid n$  then  $p \mid m$ .

$\langle 1 \rangle 2$ . If  $m$  is divisible by all the prime factors of  $n$  then  $m$  is nilpotent in  $\mathbb{Z}/n\mathbb{Z}$ .

$\langle 2 \rangle 1$ . ASSUME:  $m$  is divisible by all the prime factors of  $n$ .

$\langle 2 \rangle 2$ . LET:  $a$  be the largest number such that  $p^a \mid n$  for some prime  $p$ .

$\langle 2 \rangle 3$ . For every prime  $p$  that divides  $n$  we have  $p^a \mid m^a$

$\langle 2 \rangle 4$ .  $n \mid m^a$

$\langle 2 \rangle 5$ .  $m^a \equiv 0 \pmod{n}$

$\langle 2 \rangle 6$ .  $m$  is nilpotent in  $\mathbb{Z}/n\mathbb{Z}$ .

$\square$

## Chapter 12

# Ring Homomorphisms

**Definition 12.1** (Ring Homomorphism). Let  $R$  and  $S$  be rings. A *ring homomorphism*  $\phi : R \rightarrow S$  is a rng homomorphism such that  $\phi(1) = 1$ .

**Proposition 12.2.** *The zero-ring is terminal in **Ring**.*

PROOF: Easy.  $\square$

**Proposition 12.3.** *The ring  $\mathbb{Z}$  is initial in **Ring**.*

PROOF: Easy.  $\square$

**Proposition 12.4.** *Let  $R$  and  $S$  be rings and  $\phi : R \rightarrow S$  be a rng homomorphism. If  $\phi$  is surjective, then  $\phi$  is a ring homomorphism.*

PROOF:

$\langle 1 \rangle 1$ . PICK  $a \in R$  such that  $\phi(a) = 1$

$\langle 1 \rangle 2$ .  $\phi(1) = 1$

PROOF:

$$\begin{aligned}\phi(1) &= \phi(1)\phi(a) \\ &= \phi(1a) \\ &= \phi(a) \\ &= 1\end{aligned}$$

$\square$

**Example 12.5.** For any set  $S$  we have  $\mathcal{P}S \cong (\mathbb{Z}/2\mathbb{Z})^S$  in **Ring** with the isomorphism

$$\begin{aligned}\phi : \mathcal{P}S &\cong (\mathbb{Z}/2\mathbb{Z})^S \\ \phi(A)(s) &= \begin{cases} 1 & \text{if } s \in A \\ 0 & \text{if } s \notin A \end{cases}\end{aligned}$$

**Example 12.6.** The function  $\mathbb{H} \rightarrow \mathfrak{gl}_4(\mathbb{R})$  that maps  $a + bi + cj + dk$  to

$$\begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

is a monomorphism in **Ring**, as is the function  $\mathbb{H} \rightarrow \mathfrak{sl}_2(\mathbb{C})$  that maps  $a + bi + cj + dk$  to

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}.$$

**Proposition 12.7.** *Ring homomorphisms preserve units.*

PROOF: If  $uv = 1$  then  $\phi(u)\phi(v) = 1$ .  $\square$

**Proposition 12.8.** *Let  $\phi : R \rightarrow S$  be a ring homomorphism. Then the following are equivalent.*

1.  $\phi$  is a monomorphism.
2.  $\ker \phi = \{0\}$
3.  $\phi$  is injective.

PROOF:

$\langle 1 \rangle 1. 1 \Rightarrow 2$

$\langle 2 \rangle 1.$  ASSUME:  $\phi$  is a monomorphism.

$\langle 2 \rangle 2.$  LET:  $r \in \ker \phi$

$\langle 2 \rangle 3.$  LET:  $\text{ev}_r : \mathbb{Z}[x] \rightarrow R$  be the unique ring homomorphism such that  $\text{ev}_r(x) = r$ .

$\langle 2 \rangle 4.$  LET:  $\text{ev}_0 : \mathbb{Z}[x] \rightarrow R$  be the unique ring homomorphism such that  $\text{ev}_0(x) = 0$ .

$\langle 2 \rangle 5.$   $\phi \circ \text{ev}_r = \phi \circ \text{ev}_0$

$\langle 2 \rangle 6.$   $\text{ev}_r = \text{ev}_0$

$\langle 2 \rangle 7.$   $r = 0$

$\langle 1 \rangle 2. 2 \Rightarrow 3$

PROOF: Proposition 7.20.

$\langle 1 \rangle 3. 3 \Rightarrow 1$

PROOF: Easy.

$\square$

**Example 12.9.** It is not true that every epimorphism in **Ring** is surjective. The inclusion  $\mathbb{Z} \hookrightarrow \mathbb{Q}$  is an epimorphism but not surjective.

The same example shows that a ring homomorphism may be a monomorphism and an epimorphism but not be an isomorphism.

**Example 12.10.**

$$\text{End}_{\mathbf{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$$

The isomorphism maps any group endomorphism  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$  to  $\phi(1)$ .

**Example 12.11.** The group of units of  $\text{End}_{\mathbf{Ab}}(G)$  is  $\text{Aut}_{\mathbf{Ab}}(G)$ .

**Example 12.12.** Let  $R$  be a ring. Then the function  $\lambda : R \rightarrow \text{End}_{\mathbf{Ab}}(R)$  defined by

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

is a ring monomorphism.

PROOF: Easy.  $\square$

## 12.1 Products

**Proposition 12.13.** *Let  $R$  and  $S$  be rings. Then  $R \times S$  is a ring under componentwise addition and multiplication, and this ring is the product of  $R$  and  $S$  in **Ring**.*

PROOF: Easy.  $\square$



# Chapter 13

## Subrings

**Definition 13.1** (Subring). Let  $S$  be a ring. A *subring* of  $S$  is a ring  $R$  such that  $R$  is a subset of  $S$  and the inclusion  $R \hookrightarrow S$  is a ring homomorphism.

**Proposition 13.2.** *Let  $R$  and  $S$  be rings. Then  $R$  is a subring of  $S$  if and only if  $R$  is a subset of  $S$ , the unit  $1$  of  $S$  is an element of  $R$ , and the operations of  $R$  are the restrictions of the operations of  $S$  to  $R$ .*

PROOF: Easy.  $\square$

**Corollary 13.2.1.** *The zero ring is not a subring of any non-zero ring.*

**Proposition 13.3.** *Let  $\phi : R \rightarrow S$  be a ring homomorphism. Then  $\phi(R)$  is a subring of  $S$ .*

PROOF: Easy.  $\square$

### 13.1 Centralizer

**Definition 13.4** (Centralizer). Let  $R$  be a ring and  $a \in R$ . The *centralizer* of  $a$  is  $\{r \in R : ar = ra\}$ .

**Proposition 13.5.** *The centralizer of  $a$  is a subring of  $R$ .*

PROOF: Easy.  $\square$

### 13.2 Center

**Definition 13.6** (Center). The *center* of a ring  $R$  is  $\{x \in R : \forall y \in R. xy = yx\}$ .

**Proposition 13.7.** *The center of a ring is a subring.*

PROOF: Easy.  $\square$

**Proposition 13.8.** *Let  $R$  be a ring. The center of  $\text{End}_{\mathbf{Ab}}(R)$  is isomorphic to the center of  $R$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $\lambda : R \rightarrow \text{End}_{\mathbf{Ab}}(R)$  be left multiplication.

$\langle 1 \rangle 2$ .  $\lambda$  maps  $Z(R)$  to  $Z(\text{End}_{\mathbf{Ab}}(R))$ .

$\langle 2 \rangle 1$ . LET:  $a \in Z(R)$

$\langle 2 \rangle 2$ . LET:  $\phi \in \text{End}_{\mathbf{Ab}}(R)$

PROVE:  $\lambda(a) \circ \phi = \phi \circ \lambda(a)$

$\langle 2 \rangle 3$ . LET:  $x \in R$

$\langle 2 \rangle 4$ .  $a + \phi(x) = \phi(a + x)$

$\langle 1 \rangle 3$ .  $\lambda(Z(R)) = Z(\text{End}_{\mathbf{Ab}}(R))$

$\langle 2 \rangle 1$ . LET:  $\phi \in Z(\text{End}_{\mathbf{Ab}}(R))$

$\langle 2 \rangle 2$ . For all  $r \in R$ ,

LET:  $\mu_r \in \text{End}_{\mathbf{Ab}}(R)$  be right multiplication by  $r$ .

$\langle 2 \rangle 3$ . For all  $r \in R$  we have  $\phi \circ \mu_r = \mu_r \circ \phi$ .

$\langle 2 \rangle 4$ . For all  $r, x \in R$  we have  $\phi(xr) = \phi(x)r$

$\langle 2 \rangle 5$ . For all  $r \in R$  we have  $\phi(r) = \phi(1)r$

$\langle 2 \rangle 6$ .  $\phi = \lambda(\phi(1))$

□

**Corollary 13.8.1.** *If  $R$  is a commutative ring then  $R$  is isomorphic to the center of  $\text{End}_{\mathbf{Ab}}(R)$ .*

**Example 13.9.** For  $n$  a positive integer we have  $\mathbb{Z}/n\mathbb{Z} \cong \text{End}_{\mathbf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ .

Since, for any  $\phi \in \text{End}_{\mathbf{Ab}}(\mathbb{Z}/n\mathbb{Z})$  we have  $\phi(m) = m\phi(1)$  and so the whole of  $\text{End}_{\mathbf{Ab}}(\mathbb{Z}/n\mathbb{Z})$  is the image of  $\lambda$ .



## Chapter 14

# Monoid Rings

**Definition 14.1** (Monoid Ring). Let  $R$  be a ring and  $M$  a monoid. Define  $R[M]$  to be the ring whose elements are the families  $\{a_m\}_{m \in M}$  such that  $a_m = 0$  for all but finitely many  $m \in M$ , written

$$\sum_{m \in M} a_m m \text{ ,}$$

under

$$\begin{aligned} \sum_m a_m m + \sum_m b_m m &= \sum_m (a_m + b_m) m \\ \left( \sum_m a_m m \right) \left( \sum_m b_m m \right) &= \sum_{m \in M} \sum_{m_1 m_2 = m} a_{m_1} b_{m_2} m \end{aligned}$$

**Example 14.2.** Ring homomorphisms do not necessarily preserve zero-divisors. The canonical homomorphism  $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/6\mathbb{Z}$  maps the non-zero-divisor 2 to a zero-divisor.

### 14.1 Polynomials

**Definition 14.3** (Polynomial). Let  $R$  be a ring. The ring of *polynomials*  $R[x]$  is  $R[\mathbb{N}]$ . We write

$$\sum_n a_n x^n \text{ for } \sum_n a_n n \text{ .}$$

Concretely, a *polynomial* in  $R$  is a sequence  $(a_n)$  in  $R$  such that there exists  $N$  such that  $\forall n \geq N. a_n = 0$ . We write the polynomial as

$$\sum_{n=0}^{N-1} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1} \text{ .}$$

We write  $R[x]$  for the set of all polynomials in  $R$ .

Define addition and multiplication on  $R[x]$  by

$$\begin{aligned}\sum_n a_n x^n + \sum_n b_n x^n &= \sum_n (a_n + b_n) x^n \\ \left( \sum_n a_n x^n \right) \left( \sum_n b_n x^n \right) &= \sum_n \sum_{i+j=n} a_i b_j x^n\end{aligned}$$

A *constant* is a polynomial of the form  $a + 0x + 0x^2 + \cdots$  for some  $a \in R$ . We write  $R[x_1, \dots, x_n]$  for  $R[x_1][x_2] \cdots [x_n]$ .

**Proposition 14.4.** *For any ring  $R$ , the set of polynomials  $R[x]$  is a ring.*

PROOF: Easy.  $\square$

**Definition 14.5** (Degree). The *degree* of a polynomial  $\sum_n a_n x^n$  is the largest integer  $d$  such that  $a_d \neq 0$ . We take the degree of the zero polynomial to be  $-\infty$ .

**Proposition 14.6.** *Let  $R$  be a ring and  $f, g \in R[x]$  be nonzero polynomials. Then*

$$\deg(f + g) \leq \max(\deg f, \deg g) .$$

PROOF: If  $a_n + b_n \neq 0$  then  $a_n \neq 0$  or  $b_n \neq 0$ .  $\square$

**Proposition 14.7.** *The function  $i : n \rightarrow \mathbb{Z}[x_1, \dots, x_n]$  that maps  $k$  to  $x_k$  is initial in the category with:*

- objects all pairs  $j : n \rightarrow R$  where  $R$  is a commutative ring and  $j$  a function
- morphisms  $\phi : (j_1, R_1) \rightarrow (j_2, R_2)$  are ring homomorphisms  $\phi : R_1 \rightarrow R_2$  such that  $\phi \circ j_1 = j_2$ .

PROOF: The unique morphism  $(i, \mathbb{Z}[x_1, \dots, x_n]) \rightarrow (j, R)$  maps a polynomial  $p$  to  $p(j(0), j(1), \dots, j(n-1))$ .  $\square$

**Definition 14.8.** Let  $R$  be a commutative ring. Given a polynomial  $p \in R[x]$ , the *polynomial function*  $p : R \rightarrow R$  is the function given by:  $p(r) = \alpha_r(p)$ , where  $\alpha_r : R[x] \rightarrow R$  is the unique ring homomorphism such that the following diagram commutes.

$$\begin{array}{ccc} R[x] & \xrightarrow{\alpha_r} & R \\ x \uparrow & \nearrow r & \\ 1 & & \end{array}$$

**Proposition 14.9.**  $\mathbb{Z}[x, y]$  is the coproduct of  $\mathbb{Z}[x]$  and  $\mathbb{Z}[y]$  in the category of commutative rings.

PROOF: Given ring homomorphisms  $f : \mathbb{Z}[x] \rightarrow R$  and  $g : \mathbb{Z}[y] \rightarrow R$ , the required morphism  $\mathbb{Z}[x, y] \rightarrow R$  maps  $p(x, y)$  to  $p(f(x), g(y))$ .  $\square$

**Example 14.10.**  $\mathbb{Z}[x, y]$  is not the coproduct of  $\mathbb{Z}[x]$  and  $\mathbb{Z}[y]$  in **Ring**. Given  $f : \mathbb{Z}[x] \rightarrow R$  and  $g : \mathbb{Z}[y] \rightarrow R$  with  $f(x) \neq g(y)$ , the mediating morphism  $\mathbb{Z}[x, y] \rightarrow R$  cannot exist since it must map  $xy$  to both  $f(x)g(y)$  and  $g(y)f(x)$ .  $\square$

**Definition 14.11.** A polynomial is *monic* iff its last non-zero coefficient is 1.

**Proposition 14.12.** A monic polynomial is not a left- or right-zero-divisor.

PROOF: Easy.  $\square$

**Proposition 14.13.** Let  $R$  be a ring. Let  $f, g \in R[x]$  with  $f$  monic. Then there exist polynomials  $q, r \in R[x]$  with  $\deg r < \deg f$  such that

$$g = qf + r .$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $d = \deg f$

$\langle 1 \rangle 2$ . For all  $a \in R$  and  $n > d$ , there exists  $h \in R[x]$  with  $\deg h < n$  such that

$$ax^n = ax^{n-d}f + h .$$

PROOF: Take  $h = ax^n - ax^{n-d}f$ .

$\langle 1 \rangle 3$ . For all  $a \in R$  and  $n > d$ , there exists  $q, h \in R[x]$  with  $\deg h \leq d$  such that

$$ax^n = qf + h .$$

PROOF: Repeating  $\langle 1 \rangle 2$  by induction.

$\langle 1 \rangle 4$ . LET:  $g = \sum_{i=0}^n a_i x^i$

$\langle 1 \rangle 5$ . For  $i > d$ , PICK  $q_i h_i \in R[x]$  with  $\deg h_i < \deg f$  such that  $a_i x^i = q_i f + h_i$

$\langle 1 \rangle 6$ .  $g = (\sum_{i=d+1}^n q_i) f + \sum_{i=d+1}^n h_i$

$\square$

## 14.2 Laurent Polynomials

**Definition 14.14** (Laurent Polynomial). Let  $R$  be a ring. The ring of *Laurent polynomials* is the group ring  $R[\mathbb{Z}]$ . We write  $\sum_{n \in \mathbb{Z}} a_n x^n$  for  $\sum_n a_n x^n$ .

## 14.3 Power Series

**Definition 14.15** (Power Series). Let  $R$  be a ring. A *power series* in  $R$  is a sequence  $(a_n)$  in  $R$ . We write the power series as

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots .$$

We write  $R[[x]]$  for the set of all power series in  $R$ .

Define addition and multiplication on  $R[[x]]$  by

$$\begin{aligned}\sum_n a_n x^n + \sum_n b_n x^n &= \sum_n (a_n + b_n) x^n \\ \left( \sum_n a_n x^n \right) \left( \sum_n b_n x^n \right) &= \sum_n \sum_{i+j=n} a_i b_j x^n\end{aligned}$$

**Proposition 14.16.** *For any ring  $R$ , the set of power series  $R[[x]]$  is a ring.*

PROOF: Easy.  $\square$

**Proposition 14.17.** *A power series  $\sum_n a_n x^n$  is a unit in  $R[[x]]$  if and only if  $a_0$  is a unit in  $R$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $\sum_n a_n x^n$  is a unit then  $a_0$  is a unit.

$\langle 2 \rangle 1$ . LET:  $\sum_n b_n x^n$  be the inverse of  $\sum_n a_n x^n$ .

$\langle 2 \rangle 2$ .  $a_0 b_0 = b_0 a_0 = 1$

$\langle 1 \rangle 2$ . If  $a_0$  is a unit then  $\sum_n a_n x^n$  is a unit.

PROOF: Define the sequence  $(b_n)$  in  $R$  by

$$b_n = -a_0^{-1} \sum_{i=1}^n a_i b_{n-i}$$

Then  $\sum_n b_n x^n$  is the inverse of  $\sum_n a_n x^n$ .

$\square$

# Chapter 15

## Ideals

**Definition 15.1** (Left-Ideal). Let  $R$  be a ring.

A subgroup  $I$  of  $R$  is a *left-ideal* iff, for all  $r \in R$ , we have  $rI \subseteq I$ .

A subgroup  $I$  of  $R$  is a *right-ideal* iff, for all  $r \in R$ , we have  $Ir \subseteq I$ .

A subgroup  $I$  of  $R$  is a (*two-sided*) *ideal* iff it is a left-ideal and a right-ideal.

**Example 15.2.** Let  $R$  be a ring and  $a \in R$ . Then  $Ra$  is a left-ideal and  $aR$  is a right-ideal.

In particular,  $\{0\}$  is always a two-sided ideal.

**Example 15.3.** Let  $S$  be a set and  $T \subseteq S$ . Then  $\{X \in \mathcal{P}S : X \subseteq T\}$  is an ideal in  $\mathcal{P}S$ .

**Proposition 15.4.** Let  $S$  be a finite set. Then every ideal in  $\mathcal{P}S$  is of the form  $\{X \in \mathcal{P}S : X \subseteq T\}$  for some  $T \subseteq S$ .

PROOF:

$\langle 1 \rangle 1$ . LET:  $I$  be an ideal in  $\mathcal{P}S$ .

$\langle 1 \rangle 2$ . LET:  $T = \bigcup I$

$\langle 1 \rangle 3$ . For all  $i \in T$  we have  $\{i\} \in I$ .

$\langle 2 \rangle 1$ . LET:  $i \in T$

$\langle 2 \rangle 2$ . PICK  $X \in I$  such that  $i \in X$

$\langle 2 \rangle 3$ .  $\{i\} = \{i\} \cap X \in I$

$\langle 1 \rangle 4$ . For all  $X \subseteq T$  we have  $X \in I$ .

PROOF: If  $X = \{x_1, \dots, x_n\}$  then  $X = \{x_1\} + \dots + \{x_n\} \in I$ .

□

**Example 15.5.** If  $S$  is an infinite set, then there is always an ideal in  $\mathcal{P}S$  that is not of the form  $\{X \in \mathcal{P}S : X \subseteq T\}$  for some  $T \subseteq S$ , namely the set of all finite subsets of  $S$ .

**Proposition 15.6.** Let  $\phi : R \twoheadrightarrow S$  be a surjective ring homomorphism. Let  $J$  be an ideal in  $R$ . Then  $\phi(J)$  is an ideal in  $S$ .

PROOF:

- $\langle 1 \rangle 1$ . LET:  $j \in J$  and  $s \in S$   
 PROVE:  $s\phi(j), \phi(j)s \in \phi(J)$   
 $\langle 1 \rangle 2$ . PICK  $r \in R$  such that  $\phi(r) = s$   
 $\langle 1 \rangle 3$ .  $rj, jr \in J$   
 $\langle 1 \rangle 4$ .  $s\phi(j), \phi(j)s \in \phi(J)$   
 $\square$

**Example 15.7.** We cannot remove the hypothesis that  $\phi$  is surjective.

Let  $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$  be the inclusion. Then  $i(2\mathbb{Z}) = 2\mathbb{Z}$  is not an ideal in  $\mathbb{Q}$ .

**Proposition 15.8.** Let  $\phi : R \rightarrow S$  be a ring homomorphism and  $I$  a (left-, right-)ideal in  $S$ . Then  $\phi^{-1}I$  is a (left-, right-)ideal in  $R$ .

PROOF: Easy.  $\square$

**Corollary 15.8.1.** Let  $\phi : R \rightarrow S$  be a ring homomorphism. Then  $\ker \phi$  is an ideal in  $R$ .

**Definition 15.9** (Quotient Ring). Let  $I$  be an ideal in  $R$ . The *quotient ring*  $R/I$  is the quotient group  $R/I$  under

$$(a + I)(b + I) = ab + I.$$

This is well-defined as, if  $a + I = a' + I$  and  $b + I = b' + I$  then

$$\begin{aligned}
 a - a' &\in I \\
 b - b' &\in I \\
 \therefore ab - a'b &\in I \\
 a'b - a'b' &\in I \\
 \therefore ab - a'b' &\in I
 \end{aligned}$$

**Proposition 15.10.** Let  $I$  be an ideal in  $R$ . Then the canonical group homomorphism  $\pi : R \rightarrow R/I$  is a ring homomorphism.

PROOF: By construction.  $\square$

**Proposition 15.11.** Let  $I$  be an ideal in a ring  $R$ . For every ring homomorphism  $\phi : R \rightarrow S$  such that  $I \subseteq \ker \phi$ , there exists a unique ring homomorphism  $\bar{\phi} : R/I \rightarrow S$  such that the following diagram commutes.

$$\begin{array}{ccc}
 R & \xrightarrow{\phi} & S \\
 \searrow \pi & & \nearrow \bar{\phi} \\
 & R/I &
 \end{array}$$

PROOF: Easy.  $\square$

**Corollary 15.11.1.** Every ring homomorphism  $\phi : R \rightarrow S$  decomposes as follows.

$$\begin{array}{ccccc}
 & & \phi & & \\
 & \searrow & \text{---} & \nearrow & \\
 R & \twoheadrightarrow & R/\ker \phi & \xrightarrow{\cong} & \text{im } \phi & \hookrightarrow & S
 \end{array}$$

**Corollary 15.11.2** (First Isomorphism Theorem). *Let  $\phi : R \rightarrow S$  be a surjective ring homomorphism. Then*

$$S \cong R/\ker \phi .$$

**Theorem 15.12** (Third Isomorphism Theorem). *Let  $I$  and  $J$  be ideals in  $R$  with  $I \subseteq J$ . Then  $J/I$  is an ideal in  $R/I$ , and*

$$\frac{R/I}{J/I} \cong R/J$$

PROOF: Since the function  $R/I \rightarrow R/J$  that maps  $r + I$  to  $r + J$  is a surjective ring homomorphism with kernel  $J/I$ .  $\square$

**Corollary 15.12.1.** *Let  $\phi : R \rightarrow S$  be a surjective ring homomorphism. Let  $J$  be an ideal in  $R$ . Then*

$$\frac{S}{\phi(J)} \cong \frac{R}{\ker \phi + J}$$

**Proposition 15.13.** *Let  $R$  be a ring and  $J$  an ideal in  $\mathfrak{gl}_n(R)$ . Let  $A \in \mathfrak{gl}_n(R)$ . Then  $A \in J$  if and only if the matrices obtained by placing any entry of  $A$  in any position and zeros elsewhere all belong to  $J$ .*

PROOF: Each such matrix can be obtained by pre- and post-multiplying  $A$  by matrices which have a single 1 and 0s elsewhere. Conversely,  $A$  is a sum of such matrices.  $\square$

**Corollary 15.13.1.** *Let  $R$  be a ring. Let  $J$  be an ideal in  $\mathfrak{gl}_n(R)$ . Let  $I$  be the set of all entries of elements of  $J$ . Then  $I$  is an ideal in  $R$ , and  $J$  is the set of all matrices whose entries are in  $I$ .*

**Proposition 15.14.** *Let  $R$  be a ring. Let  $\{I_\alpha\}_{\alpha \in A}$  be a family of ideals in  $R$ . Let*

$$\sum_{\alpha \in A} I_\alpha = \left\{ \sum_{\alpha \in A} r_\alpha : \forall \alpha, r_\alpha \in I_\alpha, r_\alpha = 0 \text{ for all but finitely many } \alpha \in A \right\} .$$

*Then  $\sum_{\alpha \in A} I_\alpha$  is an ideal, and is the smallest ideal that includes every  $I_\alpha$ .*

PROOF: Easy.  $\square$

**Proposition 15.15.** *The intersection of a set of ideals is an ideal.*

PROOF: Easy.  $\square$

## 15.1 Characteristic

**Definition 15.16** (Characteristic). The *characteristic* of a ring  $R$  is the non-negative integer  $n$  such that  $n\mathbb{Z}$  is the kernel of the unique ring homomorphism  $\mathbb{Z} \rightarrow R$ .

**Proposition 15.17.** *Let  $R$  be a ring. If the unit 1 has finite order in  $R$ , then its order is the characteristic of  $R$ ; otherwise, the characteristic of  $R$  is 0.*

PROOF: Easy.  $\square$

**Example 15.18.** The zero ring is the only ring with characteristic 1.

## 15.2 Nilradical

**Definition 15.19** (Nilradical). Let  $R$  be a commutative ring. The *nilradical* of  $R$  is the set of all nilpotent elements.

**Proposition 15.20.** *Let  $R$  be a commutative ring. The nilradical of  $R$  is an ideal in  $R$ .*

PROOF: If  $a^n = 0$  then for any  $b$  we have  $(ba)^n = 0$ .  $\square$

**Example 15.21.** We cannot remove the assumption that  $R$  is commutative. In  $\mathfrak{gl}_2(\mathbb{R})$  we have that  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$  is nilpotent but  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$  is not.

## 15.3 Principal Ideals

**Definition 15.22** (Principal Ideal). Let  $R$  be a commutative ring and  $a \in R$ . The *principal ideal* generated by  $a$  is  $(a) = Ra = aR$ .

**Example 15.23.**  $\{0\} = (0)$  and  $R = \{1\}$  are principal ideals.

**Definition 15.24.** Let  $R$  be a commutative ring and  $\{a_\alpha\}_{\alpha \in A}$  be a family of elements of  $R$ . The *ideal generated by the elements  $a_\alpha$*  is

$$(a_\alpha)_{\alpha \in A} := \sum_{\alpha \in A} (a_\alpha) \ .$$

An ideal is *finitely generated* iff it is generated by a finite family of elements.

**Definition 15.25.** Let  $R$  be a commutative ring and  $I, J$  be ideals in  $R$ . Then  $IJ$  is the ideal generated by  $\{ij\}_{i \in I, j \in J}$ .

**Proposition 15.26.**

$$IJ \subseteq I \cap J$$



PROOF: Easy.  $\square$

**Proposition 15.27.** *Let  $R$  be a commutative ring. Let  $I$  and  $J$  be ideals in  $R$ . If  $I + J = R$  then  $IJ = I \cap J$ .*

PROOF:

$\langle 1 \rangle$ 1. LET:  $r \in I \cap J$

$\langle 1 \rangle$ 2. PICK  $i \in I$  and  $j \in J$  such that  $i + j = 1$ .

$\langle 1 \rangle$ 3.  $ri, rj \in IJ$

$\langle 1 \rangle$ 4.  $r = ri + rj \in IJ$

$\square$



## Chapter 16

# Integral Domains

**Definition 16.1** (Integral Domain). An *integral domain* is a non-trivial commutative ring with no nonzero zero-divisors.

**Example 16.2.**  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  are integral domains.

**Proposition 16.3.**  $\mathbb{Z}/n\mathbb{Z}$  is an integral domain if and only if  $n$  is prime.

PROOF:

$$\begin{aligned} n \text{ is prime} &\Leftrightarrow \forall a, b \in \mathbb{Z} (n \mid ab \Rightarrow n \mid a \vee n \mid b) \\ &\Leftrightarrow \forall a, b \in \mathbb{Z}/n\mathbb{Z} (ab \cong 0(\bmod n) \Rightarrow a \cong 0(\bmod n) \vee b \cong 0(\bmod n)) \\ &\Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ is an integral domain} \quad \square \end{aligned}$$

**Proposition 16.4.** In an integral domain, if  $x^2 = 1$  then  $x = \pm 1$ .

PROOF: We have  $x^2 - 1 = (x - 1)(x + 1) = 0$  so  $x - 1 = 0$  or  $x + 1 = 0$ .  $\square$

**Proposition 16.5.** Let  $R$  be an integral domain and  $f, g \in R[x]$ . Then

$$\deg(fg) = \deg f + \deg g$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $f = \sum_n a_n x^n$  and  $g = \sum_n b_n x^n$ .

$\langle 1 \rangle 2$ . LET:  $d = \deg f$  and  $e = \deg g$ .

$\langle 1 \rangle 3$ . The  $d + e$ th term of  $fg$  is

$$a_d b_e x^{d+e}$$

which is non-zero.

$\langle 1 \rangle 4$ . For  $n > d + e$  the  $n$ th term of  $fg$  is 0.

$\square$

**Corollary 16.5.1.** Let  $R$  be a ring. Then  $R[x]$  is an integral domain if and only if  $R$  is an integral domain.

**Proposition 16.6.** Let  $R$  be a ring. Then  $R[[x]]$  is an integral domain if and only if  $R$  is an integral domain.

PROOF:

$\langle 1 \rangle 1$ . If  $R[[x]]$  is an integral domain then  $R$  is an integral domain.

PROOF: Easy.

$\langle 1 \rangle 2$ . If  $R$  is an integral domain then  $R[[x]]$  is an integral domain.

$\langle 2 \rangle 1$ . ASSUME:  $R$  is an integral domain.

$\langle 2 \rangle 2$ . LET:  $(\sum_n a_n x^n)(\sum_n b_n x^n) = 0$

$\langle 2 \rangle 3$ .  $a_0 b_0 = 0$

$\langle 2 \rangle 4$ .  $a_0 = 0$  or  $b_0 = 0$

$\langle 2 \rangle 5$ . ASSUME: w.l.o.g.  $b_0 \neq 0$

PROVE: For all  $n$  we have  $a_n = 0$

$\langle 2 \rangle 6$ . ASSUME: as induction hypothesis  $a_0 = a_1 = \cdots = a_{n-1} = 0$

$\langle 2 \rangle 7$ .  $\sum_{i=0}^n a_i b_{n-i} = 0$

$\langle 2 \rangle 8$ .  $a_n b_0 = 0$

$\langle 2 \rangle 9$ .  $a_n = 0$

□

**Proposition 16.7.** *Let  $R$  be a ring and  $S$  an integral domain. Every rng homomorphism  $\phi : R \rightarrow S$  is a ring homomorphism.*

PROOF:

$$\begin{aligned}\phi(1) &= \phi(1 \cdot 1) \\ &= \phi(1)\phi(1)\end{aligned}$$

and so  $\phi(1) = 1$  by Cancellation. □

**Proposition 16.8.** *The characteristic of an integral domain is either 0 or a prime number.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $D$  be an integral domain.

$\langle 1 \rangle 2$ . LET:  $n$  be the characteristic of  $D$

$\langle 1 \rangle 3$ . ASSUME:  $n \neq 0$

$\langle 1 \rangle 4$ . ASSUME:  $n = ab$

$\langle 1 \rangle 5$ .  $ab = 0$  in  $D$

$\langle 1 \rangle 6$ .  $a = 0$  or  $b = 0$  in  $D$

$\langle 1 \rangle 7$ .  $n \mid a$  or  $n \mid b$

$\langle 1 \rangle 8$ . One of  $a, b$  is 1 and the other is  $n$ .

□

## Chapter 17

# Unique Factorization Domains

**Example 17.1.**  $\mathbb{Z}$  is a UFD.



## Chapter 18

# Noetherian Rings

**Definition 18.1** (Noetherian Ring). A commutative ring is *Noetherian* iff every ideal is finitely generated.

**Proposition 18.2.** *The homomorphic image of a Noetherian ring is Noetherian.*

PROOF:

$\langle 1 \rangle$ 1. LET:  $R$  be a Noetherian ring,  $S$  be a commutative ring, and  $\phi : R \rightarrow S$  a surjective ring homomorphism.

$\langle 1 \rangle$ 2. LET:  $I$  be an ideal in  $S$ .

$\langle 1 \rangle$ 3. LET:  $\phi^{-1}(I) = (a_1, \dots, a_n)$

$\langle 1 \rangle$ 4.  $I = (\phi(a_1), \dots, \phi(a_n))$

□





## Chapter 19

# Principal Ideal Domains

**Definition 19.1** (Principal Ideal Domain). A commutative ring is a *principal ideal domain* (*PID*) iff every ideal is principal.

**Example 19.2.**  $\mathbb{Z}$  is a PID by Proposition 7.16.

**Example 19.3.**  $\mathbb{Z}[x]$  is not a PID. The ideal  $(2, x)$  is not principal.

**Proposition 19.4.** *Every PID is Noetherian.*

PROOF: Trivial.  $\square$



## Chapter 20

# Euclidean Domains

**Example 20.1.**  $\mathbb{Z}$  is a Euclidean domain.



## Chapter 21

# Division Rings

**Definition 21.1** (Division Ring). A *division ring* is a ring in which every nonzero element is a two-sided unit.

**Example 21.2.** The quaternions form a division ring, with the inverse of a non-zero element  $a + bi + cj + dk$  being

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

**Example 21.3.** For any ring  $R$ , the ring of polynomials  $R[x]$  is not a division ring, since  $x$  has no inverse.

**Proposition 21.4.** *Every centralizer in a division ring is a division ring.*

PROOF: If  $ar = ra$  then  $ra^{-1} = a^{-1}r$ .  $\square$

**Proposition 21.5.** *A non-trivial ring  $R$  is a division ring if and only if its only left-ideals and right-ideals are  $\{0\}$  and  $R$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $R$  is a division ring then the only left-ideals and right-ideals are  $\{0\}$  and  $R$ .

$\langle 2 \rangle 1$ . ASSUME:  $R$  is a division ring.

$\langle 2 \rangle 2$ . The only left-ideals are  $\{0\}$  and  $R$ .

$\langle 3 \rangle 1$ . LET:  $I$  be a left-ideal that is not  $\{0\}$ .

PROVE:  $I = R$

$\langle 3 \rangle 2$ . PICK  $a \in I - \{0\}$

$\langle 3 \rangle 3$ . PICK a left inverse  $b$  for  $a$

$\langle 3 \rangle 4$ .  $1 \in I$

PROOF: Since  $1 = ba$ .

$\langle 3 \rangle 5$ .  $I = R$

PROOF: For any  $r \in R$  we have  $r = r1 \in I$ .

$\langle 2 \rangle 3$ . The only right-ideals are  $\{0\}$  and  $R$ .

PROOF: Similar.

$\langle 1 \rangle 2$ . If the only left-ideals and right-ideals are  $\{0\}$  and  $R$  then  $R$  is a division ring.

□

**Proposition 21.6.** *Let  $K$  be a division ring and  $R$  a non-trivial ring. Every ring homomorphism  $K \rightarrow R$  is injective.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $\phi : K \rightarrow R$  be a ring homomorphism.

PROVE:  $\ker \phi = \{0\}$

$\langle 1 \rangle 2$ . LET:  $x \in \ker \phi$

$\langle 1 \rangle 3$ . ASSUME: for a contradiction  $x \neq 0$ .

$\langle 1 \rangle 4$ .  $\phi(xx^{-1}) = 1$

$\langle 1 \rangle 5$ .  $0 = 1$

$\langle 1 \rangle 6$ . Q.E.D.

PROOF: This contradicts the assumption that  $R$  is non-trivial.

□

## Chapter 22

# Simple Rings

**Definition 22.1** (Simple Ring). A non-trivial ring is *R simple* iff its only two-sided ideals are  $\{0\}$  and  $R$ .

**Example 22.2.** For any simple ring  $R$  we have  $\mathfrak{gl}_n(R)$  is simple, by Corollary 15.13.1.





## Chapter 23

# Reduced Rings

**Definition 23.1** (Reduced Ring). A ring is *reduced* iff it has no non-zero nilpotent elements.

**Proposition 23.2.** *Let  $R$  be a commutative ring. Let  $N$  be its nilradical. Then  $R/N$  is reduced.*

PROOF:

- $\langle 1 \rangle 1.$  LET:  $r + N$  be nilpotent.
- $\langle 1 \rangle 2.$  PICK  $n$  such that  $(r + N)^n = N$
- $\langle 1 \rangle 3.$   $r^n \in N$
- $\langle 1 \rangle 4.$  PICK  $k$  such that  $(r^n)^k = 0$
- $\langle 1 \rangle 5.$   $r^{nk} = 0$
- $\langle 1 \rangle 6.$   $r \in N$
- $\langle 1 \rangle 7.$   $r + N = N$

□

**Proposition 23.3.** *Let  $R$  be a commutative ring. Let  $I$  and  $J$  be ideals in  $R$ . If  $R/IJ$  is reduced then  $IJ = I \cap J$ .*

PROOF:

- $\langle 1 \rangle 1.$  LET:  $r \in I \cap J$   
PROVE:  $r \in IJ$
- $\langle 1 \rangle 2.$   $r^2 \in IJ$
- $\langle 1 \rangle 3.$   $(r + IJ)^2 = IJ$
- $\langle 1 \rangle 4.$   $r + IJ = IJ$

PROOF: Since  $R/IJ$  is reduced.

- $\langle 1 \rangle 5.$   $r \in IJ$

□



## Chapter 24

# Boolean Rings

**Definition 24.1** (Boolean). A ring is *Boolean* iff  $a^2 = a$  for every element  $a$ .

**Example 24.2.** For any set  $S$ , the ring  $\mathcal{P}S$  is Boolean.

**Proposition 24.3.** *Every non-trivial Boolean ring has characteristic 2.*

PROOF: We have  $4 = 2$  and so  $2 = 0$ .  $\square$

**Proposition 24.4.** *Every Boolean ring is commutative.*

PROOF:

$$\begin{aligned}(ab)^2 &= a = b \\ \therefore a^2 + ab + ba + b^2 &= a + b \\ \therefore a + ab + ba + b &= a + b \\ \therefore ab + ba &= 0 \\ \therefore ab &= -ba \\ &= ba \quad \text{(Proposition 24.3)}\end{aligned}$$

**Example 24.5.** The only Boolean integral domain is  $\mathbb{Z}/2\mathbb{Z}$ . For, if  $D$  is a Boolean integral domain and  $x \in D$ , we have  $x^2 = x$ , so  $x^2 - x = x(x - 1) = 0$  and so  $x = 0$  or  $x = 1$ , i.e.  $D = \{0, 1\}$ .



**Part IV**

**Field Theory**



# Chapter 25

## Fields

**Definition 25.1** (Field). A *field* is a non-trivial commutative division ring.

**Example 25.2.**  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  are fields.

**Proposition 25.3.** *Every field is an integral domain.*

PROOF: By Propositions 11.8 and 11.9.  $\square$

**Example 25.4.** The converse does not hold:  $\mathbb{Z}$  is an integral domain but not a field.

**Proposition 25.5.** *Every finite integral domain is a field.*

PROOF: In a finite integral domain, multiplication by any non-zero element is injective, hence surjective.  $\square$

**Corollary 25.5.1.** *For any positive integer  $n$ , the following are equivalent:*

- $n$  is prime.
- $\mathbb{Z}/n\mathbb{Z}$  is an integral domain.
- $\mathbb{Z}/n\mathbb{Z}$  is a field.

**Theorem 25.6** (Wedderburn's Little Theorem). *Every finite division ring is a field.*

**Proposition 25.7.** *Every subring of a field is an integral domain.*

PROOF: Easy.  $\square$

**Proposition 25.8.** *The center of a division ring is a field.*

PROOF:

$\langle 1 \rangle$ 1. LET:  $R$  be a division ring.

$\langle 1 \rangle$ 2. LET:  $Z$  be the center of  $R$ .

$\langle 1 \rangle$ 3.  $Z$  is non-trivial.

PROOF: Since  $1 \in Z$ .

$\langle 1 \rangle 4$ .  $Z$  is commutative.

$\langle 1 \rangle 5$ .  $Z$  is a division ring.

$\langle 2 \rangle 1$ . LET:  $a \in Z$

$\langle 2 \rangle 2$ .  $a^{-1} \in Z$

$\langle 3 \rangle 1$ . LET:  $x \in R$

$\langle 3 \rangle 2$ .  $ax = xa$

$\langle 3 \rangle 3$ .  $xa^{-1} = a^{-1}x$

□

**Definition 25.9.** For any prime  $p$  and positive integer  $r$ , define a multiplication on  $(\mathbb{Z}/p\mathbb{Z})^r$  that makes this group into a field by:

**Proposition 25.10.** *A commutative ring is a field if and only if it is simple.*

PROOF: Proposition 21.5. □

**Proposition 25.11.** *Let  $K$  be a field. Then  $K[x]$  is a PID, and every non-zero ideal in  $K[x]$  is generated by a unique monic polynomial.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $I$  be a non-zero ideal in  $K[x]$

$\langle 1 \rangle 2$ . PICK a monic polynomial  $f \in K[x]$  of minimal degree.

PROVE:  $I = (f)$

$\langle 1 \rangle 3$ . LET:  $g \in I$

$\langle 1 \rangle 4$ . PICK polynomials  $q, r$  with  $\deg r < \deg f$  such that  $g = qf + r$

$\langle 1 \rangle 5$ .  $r \in I$

$\langle 1 \rangle 6$ .  $r = 0$

$\langle 1 \rangle 7$ .  $g \in (f)$

□



**Part V**

**Linear Algebra**



**Definition 25.12.** Let  $\text{GL}_n(\mathbb{R})$  be the group of invertible  $n \times n$  real matrices.  $\text{GL}_n(\mathbb{R})$  acts on  $\mathbb{R}^n$  by matrix multiplication.

**Definition 25.13.** Let  $\text{GL}_n(\mathbb{C})$  be the group of invertible  $n \times n$  complex matrices.  $\text{GL}_n(\mathbb{C})$  acts on  $\mathbb{C}^n$  by matrix multiplication.

**Definition 25.14.** Let  $\text{SL}_n(\mathbb{R}) = \{M \in \text{GL}_n(\mathbb{R}) : \det M = 1\}$ .

**Proposition 25.15.**  $\text{SL}_n(\mathbb{R})$  is a normal subgroup of  $\text{GL}_n(\mathbb{R})$ .

PROOF: If  $\det M = 1$  then  $\det(AMA^{-1}) = (\det A)(\det M)(\det A)^{-1} = 1$ .  $\square$

**Proposition 25.16.**

$$\text{GL}_n(\mathbb{R})/\text{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$$

**Definition 25.17.** Let  $\text{SL}_n(\mathbb{C}) = \{M \in \text{GL}_n(\mathbb{C}) : \det M = 1\}$ .

**Definition 25.18.** Let  $\text{O}_n(\mathbb{R}) = \{M \in \text{GL}_n(\mathbb{R}) : MM^T = M^T M = I_n\}$ .

**Proposition 25.19.** The action of  $\text{O}_n(\mathbb{R})$  on  $\mathbb{R}^n$  preserves lengths and angles.

**Definition 25.20.** Let  $\text{SO}_n(\mathbb{R}) = \{M \in \text{O}_n(\mathbb{R}) : \det M = 1\}$ .

**Definition 25.21.** Let  $\text{U}_n(\mathbb{C}) = \{M \in \text{GL}_n(\mathbb{C}) : MM^\dagger = M^\dagger M = I_n\}$ .

**Definition 25.22.** Let  $\text{SU}_n(\mathbb{C}) = \{M \in \text{U}_n(\mathbb{C}) : \det M = 1\}$ .

**Proposition 25.23.** Every matrix in  $\text{SU}_2(\mathbb{C})$  can be written in the form

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

for some  $a, b, c, d \in \mathbb{R}$  with  $a^2 + b^2 + c^2 + d^2 = 1$ .

PROOF:

$$\langle 1 \rangle 1. \text{ LET: } M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SU}_2(\mathbb{C})$$

$$\langle 1 \rangle 2. M^{-1} = M^\dagger$$

$$\langle 1 \rangle 3. \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} \bar{\alpha} & \bar{\gamma} \\ \bar{\beta} & \bar{\delta} \end{pmatrix}$$

$$\langle 1 \rangle 4. \text{ LET: } \alpha = a+bi \text{ and } \beta = c+di.$$

$$\langle 1 \rangle 5. \delta = \bar{\alpha} = a-bi$$

$$\langle 1 \rangle 6. \gamma = -\bar{\beta} = -c+di$$

$$\langle 1 \rangle 7. \det M = a^2 + b^2 + c^2 + d^2 = 1$$

$\square$

**Corollary 25.23.1.**  $\text{SU}_2(\mathbb{C})$  is simply connected.

**Corollary 25.23.2.**

$$\text{SO}_3(\mathbb{R}) \cong \text{SU}_2(\mathbb{C})/\{I, -I\}$$

PROOF: The function that maps  $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$  to  $\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$

is a surjective homomorphism with kernel  $\{I, -I\}$ .  $\square$

**Corollary 25.23.3.** The fundamental group of  $\text{SO}_3(\mathbb{R})$  is  $C_2$ .