

# Mathematics

Robin Adams

June 4, 2024



# Contents

<b>I</b>	<b>Category Theory</b>	<b>9</b>
<b>1</b>	<b>Foundations</b>	<b>11</b>
<b>2</b>	<b>Categories</b>	<b>13</b>
2.1	Categories . . . . .	13
2.1.1	Definition of a Category . . . . .	13
2.1.2	Examples . . . . .	13
2.2	Objects . . . . .	14
2.3	Morphisms . . . . .	14
2.3.1	Identity Morphisms . . . . .	14
2.3.2	Endomorphisms . . . . .	14
2.4	Preorders . . . . .	14
2.5	Monomorphisms and Epimorphisms . . . . .	15
2.6	Sections and Retractions . . . . .	16
2.7	Isomorphisms . . . . .	17
2.8	Initial and Terminal Objects . . . . .	18
<b>3</b>	<b>Functors</b>	<b>19</b>
3.1	Comma Categories . . . . .	19
<b>II</b>	<b>Number Theory</b>	<b>21</b>
<b>III</b>	<b>Group Theory</b>	<b>25</b>
<b>4</b>	<b>Semigroups</b>	<b>27</b>
<b>5</b>	<b>Monoids</b>	<b>29</b>
<b>6</b>	<b>Groups</b>	<b>31</b>
6.1	Symmetric Groups . . . . .	34
6.2	Order of an Element . . . . .	35
6.3	Generators . . . . .	37
6.4	$p$ -groups . . . . .	39

<b>7</b>	<b>Group Homomorphisms</b>	<b>41</b>
7.1	Subgroups . . . . .	43
7.2	Kernel . . . . .	44
7.3	Inner Automorphisms . . . . .	45
7.4	Semidirect Products . . . . .	46
7.5	Direct Products . . . . .	48
7.6	Free Groups . . . . .	49
7.7	Normal Subgroups . . . . .	51
7.8	Quotient Groups . . . . .	52
7.9	Cosets . . . . .	57
7.10	Congruence . . . . .	61
7.11	Cyclic Groups . . . . .	61
7.12	Commutator Subgroup . . . . .	62
7.13	Presentations . . . . .	63
7.14	Index of a Subgroup . . . . .	64
7.15	Cokernels . . . . .	65
7.16	Cayley Graphs . . . . .	65
7.17	Characteristic Subgroups . . . . .	66
7.18	Simple Groups . . . . .	67
7.19	Sylow Subgroups . . . . .	67
7.20	Series of Subgroups . . . . .	68
<b>8</b>	<b>Abelian Groups</b>	<b>73</b>
8.1	The Category of Abelian Groups . . . . .	78
8.2	Free Abelian Groups . . . . .	79
8.3	Cokernels . . . . .	81
8.4	Commutator Subgroups . . . . .	82
8.5	Derived Series . . . . .	83
8.6	Solvable Groups . . . . .	84
<b>9</b>	<b>Group Actions</b>	<b>87</b>
9.1	Group Actions . . . . .	87
9.2	Category of $G$ -Sets . . . . .	90
9.3	Center . . . . .	92
9.4	Centralizer . . . . .	94
9.5	Conjugacy Class . . . . .	94
9.6	Conjugation on Sets . . . . .	97
9.7	Nilpotent Groups . . . . .	103
9.8	Symmetric Groups . . . . .	106
9.8.1	Transitive Subgroups . . . . .	107
9.9	Alternating Groups . . . . .	107
<b>10</b>	<b>Extensions</b>	<b>113</b>
<b>11</b>	<b>Classification of Groups</b>	<b>115</b>

<b>IV</b>	<b>Ring Theory</b>	<b>129</b>
<b>12</b>	<b>Rngs</b>	<b>131</b>
12.1	Commutative Rngs . . . . .	133
12.2	Rng Homomorphisms . . . . .	133
12.3	Quaternions . . . . .	133
<b>13</b>	<b>Rings</b>	<b>135</b>
13.1	Units . . . . .	136
13.2	Euler's $\phi$ -function . . . . .	138
13.3	Nilpotent Elements . . . . .	140
<b>14</b>	<b>Ring Homomorphisms</b>	<b>141</b>
14.1	Products . . . . .	143
<b>15</b>	<b>Subrings</b>	<b>145</b>
15.1	Centralizer . . . . .	145
15.2	Center . . . . .	145
<b>16</b>	<b>Monoid Rings</b>	<b>147</b>
16.1	Polynomials . . . . .	147
16.2	Laurent Polynomials . . . . .	149
16.3	Power Series . . . . .	150
<b>17</b>	<b>Ideals</b>	<b>151</b>
17.1	Characteristic . . . . .	154
17.2	Nilradical . . . . .	154
17.3	Principal Ideals . . . . .	154
17.4	Maximal Ideals . . . . .	155
<b>18</b>	<b>Integral Domains</b>	<b>157</b>
18.1	Prime Ideals . . . . .	158
<b>19</b>	<b>Unique Factorization Domains</b>	<b>161</b>
<b>20</b>	<b>Noetherian Rings</b>	<b>163</b>
<b>21</b>	<b>Principal Ideal Domains</b>	<b>165</b>
<b>22</b>	<b>Euclidean Domains</b>	<b>167</b>
<b>23</b>	<b>Division Rings</b>	<b>169</b>
<b>24</b>	<b>Simple Rings</b>	<b>171</b>
<b>25</b>	<b>Reduced Rings</b>	<b>173</b>
<b>26</b>	<b>Boolean Rings</b>	<b>175</b>

<b>27 Modules</b>	<b>177</b>
27.1 Homomorphisms . . . . .	178
27.2 Submodules . . . . .	179
27.3 Quotient Modules . . . . .	180
27.4 Products . . . . .	181
27.5 Coproducts . . . . .	181
27.6 Direct Sum . . . . .	181
27.7 Kernels and Cokernels . . . . .	182
27.8 Free Modules . . . . .	183
27.9 Generators . . . . .	184
27.10 Projections . . . . .	185
27.11 Pullbacks . . . . .	185
27.12 Pushouts . . . . .	186
<b>28 Cyclic Modules</b>	<b>187</b>
<b>29 Simple Modules</b>	<b>189</b>
<b>30 Noetherian Modules</b>	<b>191</b>
<b>31 Algebras</b>	<b>193</b>
31.1 Rees Algebra . . . . .	194
31.2 Free Algebras . . . . .	194
<b>32 Algebras of Finite Type</b>	<b>197</b>
<b>33 Finite Algebras</b>	<b>199</b>
<b>34 Division Algebras</b>	<b>201</b>
<b>35 Chain Complexes</b>	<b>203</b>
35.1 Split Exact Sequences . . . . .	214
<b>36 Homology</b>	<b>217</b>
<b>V Field Theory</b>	<b>219</b>
<b>37 Fields</b>	<b>221</b>
<b>38 Algebraically Closed Fields</b>	<b>225</b>
<b>VI Linear Algebra</b>	<b>227</b>
<b>39 Vector Spaces</b>	<b>229</b>

<i>CONTENTS</i>	7
<b>VII Linear Algebra</b>	<b>231</b>
40 Vector Spaces	233
<b>VIII Measure Theory</b>	<b>235</b>





Part I

Category Theory



# Chapter 1

## Foundations

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



# Chapter 2

## Categories

### 2.1 Categories

#### 2.1.1 Definition of a Category

**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  $f \circ \text{id}_A = f$ .

#### 2.1.2 Examples

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

## 2.2 Objects

## 2.3 Morphisms

### 2.3.1 Identity Morphisms

**Proposition 2.3.** *The identity morphism on an object is unique.*

*More specifically, let  $i : A \rightarrow A$ . Then the following are equivalent:*

1. *For every object  $B$  and morphism  $f : A \rightarrow B$  we have  $f \circ i = f$ .*
2. *For every object  $B$  and morphism  $f : B \rightarrow A$  we have  $i \circ f = f$ .*
3. *For every morphism  $f : A \rightarrow A$  we have  $f \circ i = f$ .*
4. *For every morphism  $f : A \rightarrow A$  we have  $i \circ f = f$ .*
5.  $\text{id}_A \circ i = \text{id}_A$
6.  $i \circ \text{id}_A = i$
7.  $i = \text{id}_A$

PROOF:  $1 \Rightarrow 3 \Rightarrow 5 \Rightarrow 7 \Rightarrow 1$  and  $2 \Rightarrow 4 \Rightarrow 6 \Rightarrow 7 \Rightarrow 2$  are all trivial.  $\square$

### 2.3.2 Endomorphisms

**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

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

## 2.4 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  $(A, =)$ .

## 2.5 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:

$\langle 1 \rangle 1$ . LET:  $f : A \rightarrow B$

$\langle 1 \rangle 2$ . If  $f$  is monic then  $f$  is injective.

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

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

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

$\langle 2 \rangle 4$ . LET:  $\bar{x}, \bar{y} : 1 \rightarrow A$  be the functions such that  $\bar{x}(*) = x$  and  $\bar{y}(*) = y$

$\langle 2 \rangle 5$ .  $f \circ \bar{x} = f \circ \bar{y}$

$\langle 2 \rangle 6$ .  $\bar{x} = \bar{y}$

PROOF: By  $\langle 2 \rangle 1$ .

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

$\langle 1 \rangle 3$ . If  $f$  is injective then  $f$  is monic.

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

$\langle 2 \rangle 2$ . LET:  $X$  be a set and  $x, y : X \rightarrow A$ .

$\langle 2 \rangle 3$ . ASSUME:  $f \circ x = f \circ y$

PROVE:  $x = y$   
 $\langle 2 \rangle 4$ . LET:  $t \in X$   
 PROVE:  $x(t) = y(t)$   
 $\langle 2 \rangle 5$ .  $f(x(t)) = f(y(t))$   
 $\langle 2 \rangle 6$ .  $x(t) = y(t)$   
 PROOF: By  $\langle 2 \rangle 1$ .

□

**Proposition 2.16.** *A function is an epimorphism in **Set** iff it is surjective.*

PROOF:

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

□

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

PROOF: Immediate from definitions. □

## 2.6 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. □

**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.

## 2.7 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.

## 2.8 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**

**Number Theory**



**Definition 3.8** (Partition). A *partition* of a natural number  $n$  is a nonincreasing sequence of positive integers whose sum is  $n$ .





**Part III**

**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 2.3.



# 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:

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

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

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

$\langle 1 \rangle 3$ . 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 Symmetric Groups

**Definition 6.13.** Let  $n$  be a natural number and  $a_1, \dots, a_r \in \{1, \dots, n\}$  be distinct. The *cycle* or  *$r$ -cycle*

$$(a_1 \ a_2 \ \cdots \ a_r) \in S_n$$

is the permutation that sends  $a_i$  to  $a_{i+1}$  ( $1 \leq i < r$ ) and  $a_r$  to  $a_1$ .

We call  $r$  the *length* of the cycle.

A *transposition* is a 2-cycle.

**Proposition 6.14.** *Disjoint cycles commute.*

PROOF: Easy.  $\square$

**Proposition 6.15.** *For any cycle  $(a_1 \ a_2 \ \cdots \ a_r)$  in  $S_n$  and  $\tau \in S_n$  we have*

$$\tau(a_1 \ a_2 \ \cdots \ a_r)\tau^{-1} = (\tau(a_1) \ \tau(a_2) \ \cdots \ \tau(a_r)) .$$

PROOF: Easy.  $\square$

## 6.2 Order of an Element

**Definition 6.16** (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 6.17.** *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  $|g|$ .

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

$\square$

**Corollary 6.17.1.** *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 6.18.** *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 6.19.** *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

$$g^{md} = e \Leftrightarrow |g| \mid md \quad (\text{Corollary 6.17.1})$$

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

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

and so  $|g^m| = \frac{\text{lcm}(m, |g|)}{m}$  by Corollary 6.17.1. □

**Corollary 6.19.1.** *If  $g$  has odd order then  $|g^2| = |g|$ .*

**Proposition 6.20.** *Let  $G$  be a group. Let  $g, h \in G$  have finite order. Assume  $gh = hg$ . Then  $|gh|$  has finite order and*

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

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

**Example 6.21.** 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 6.22.** *Let  $G$  be a group and  $g, h \in G$  have finite order. If  $gh = hg$  and  $\text{gcd}(|g|, |h|) = 1$  then  $|gh| = |g||h|$ .*

PROOF:

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

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

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

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

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

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

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

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

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

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

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

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

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

PROOF: Using Proposition 6.20.  
□

**Proposition 6.23.** *Let  $G$  be a finite group. Assume there is exactly one element  $f \in G$  of order 2. Then the product of all the elements of  $G$  is  $f$ .*

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

**Proposition 6.24.** *Let  $G$  be a finite group of order  $n$ . Let  $m$  be the number of elements of  $G$  of order 2. Then  $n - m$  is odd.*

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

**Corollary 6.24.1.** *If a finite group has even order, then it contains an element of order 2.*

**Proposition 6.25.** *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 6.26.** *Let  $G$  be a group and  $g, h \in G$ . Then  $|gh| = |hg|$ .*

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

**Proposition 6.27.** *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  $x$ .*

⟨1⟩1. PICK integers  $a$  and  $b$  such that  $an + bk = 1$ .

⟨1⟩2. LET:  $g \in G$

⟨1⟩3.  $g = (g^b)^k$

PROOF:

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

□

## 6.3 Generators

**Definition 6.28** (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 6.29.**  $\text{SL}_2(\mathbb{Z})$  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:

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

$\langle 1 \rangle 4$ .

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

$\langle 1 \rangle 5$ .

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

$\langle 1 \rangle 6$ . 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  $\langle 1 \rangle 4$  and  $\langle 1 \rangle 5$  taking  $q = -1$ .

$\langle 1 \rangle 7$ . 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  $\langle 1 \rangle 6$  repeatedly.

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

$\langle 2 \rangle 1$ .  $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H$

PROOF:  $\langle 1 \rangle 2$

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

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

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

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

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

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

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

□

## 6.4 $p$ -groups

**Definition 6.30** ( $p$ -group). Let  $p$  be a prime. A  $p$ -group is a finite group whose order is a power of  $p$ .





## 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:

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

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

PROOF: By Cancellation.

$\langle 1 \rangle 3$ .  $\gamma_g$  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 Semidirect Products

**Definition 7.25** (Semidirect Product). Let  $N$  and  $H$  be groups. Let  $\theta : H \rightarrow \text{Aut}_{\mathbf{Grp}}(N)$  be a homomorphism. The *semidirect product*  $N \rtimes_{\theta} H$  is the group  $N \times H$  under

$$(n_1, h_1)(n_2, h_2) = (n_1\theta(h_1)(n_2), h_1h_2)$$

If  $N$  and  $H$  are subgroups of a group  $G$ , we write  $N \rtimes H$  for  $N \rtimes_{\theta} H$  where  $\theta(n)(h) = nhn^{-1}$ .

We prove that this is a group.

PROOF:

$\langle 1 \rangle 1$ . Associativity

PROOF:

$$\begin{aligned}(n_1, h_1)((n_2, h_2)(n_3, h_3)) &= (n_1, h_1)(n_2\theta(h_2)(n_3), h_2h_3) \\ &= (n_1\theta(h_1)(n_2\theta(h_2)(n_3)), h_1h_2h_3) \\ &= (n_1\theta(h_1)(n_2)\theta(h_1h_2)(n_3), h_1h_2h_3) \\ &= (n_1\theta(h_1)(n_2), h_1h_2)(n_3, h_3) \\ &= ((n_1, h_1)(n_2, h_2))(n_3, h_3)\end{aligned}$$

$\langle 1 \rangle 2$ .  $(e_N, e_H)(n, h) = (n, h)$

PROOF:

$$\begin{aligned}(e_N, e_H)(n, h) &= (e_N\theta(e_H)(n), e_Hh) \\ &= (n, h)\end{aligned}$$

$\langle 1 \rangle 3$ .  $(n, h)(e_N, e_H) = (n, h)$

PROOF:

$$\begin{aligned}(n, h)(e_N, e_H) &= (n\theta(h)(e_N), he_H) \\ &= (n, h)\end{aligned}$$

$$\langle 1 \rangle 4. (n, h)(\theta(h^{-1})(n^{-1}), h^{-1}) = (e_N, e_H)$$

PROOF:

$$\begin{aligned}(n, h)(n^{-1}, h^{-1}) &= (n\theta(h)(\theta(h^{-1})(n^{-1})), hh^{-1}) \\ &= (nn^{-1}, hh^{-1}) \\ &= (e_N, e_H)\end{aligned}$$

$$\langle 1 \rangle 5. (\theta(h^{-1})(n^{-1}), h^{-1})(n, h) = (e_N, e_H)$$

PROOF:

$$\begin{aligned}(\theta(h^{-1})(n^{-1}), h^{-1})(n, h) &= (\theta(h^{-1})(n^{-1})\theta(h^{-1})(n), h^{-1}h) \\ &= (e_N, e_H)\end{aligned}$$

□

**Proposition 7.26.** *The function  $i : N \rightarrow N \rtimes_{\theta} H$  that maps  $n$  to  $(n, e_H)$  is a group monomorphism.*

PROOF:

$$\langle 1 \rangle 1. i(nn') = i(n)i(n')$$

PROOF:

$$\begin{aligned}i(n)i(n') &= (n, e_H)(n', e_H) \\ &= (n\theta(e_H)(n'), e_He_H) \\ &= (nn', e_H) \\ &= i(nn')\end{aligned}$$

$$\langle 1 \rangle 2. i \text{ is injective.}$$

□

**Proposition 7.27.** *The function  $J : h \rightarrow N \rtimes_{\theta} H$  that maps  $h$  to  $(e_N, h)$  is a group monomorphism.*

PROOF:

$$\langle 1 \rangle 1. j(hh') = j(h)j(h')$$

PROOF:

$$\begin{aligned}j(h)j(h') &= (e_N, h)(e_N, h') \\ &= (e_N\theta(h)(e_N), hh') \\ &= (e_N, hh') \\ &= j(hh')\end{aligned}$$

$$\langle 1 \rangle 2. j \text{ is injective.}$$

□

**Proposition 7.28.** *The natural projection  $N \rtimes_{\theta} H \rightarrow H$  is a surjective group homomorphism with kernel  $N$ .*

PROOF: Easy. □

**Proposition 7.29.** *Let  $N$  and  $H$  be groups and  $\theta : H \rightarrow \text{Aut}_{\mathbf{Grp}}(N)$  a homomorphism. Let  $G = N \rtimes_{\theta} H$ . Let  $i : H \hookrightarrow G$  and  $j : N \hookrightarrow G$  be the injections. Then  $\theta$  is realised by conjugation in  $G$ . That is, for all  $h \in H$  and  $n \in N$  we have*

$$j(\theta(h)(n)) = i(h)j(n)i(h)^{-1}$$

*I.e.*

$$j \circ \theta(h) = \gamma_{i(h)} \quad .$$

PROOF:

$$\begin{aligned} i(h)j(n)i(h)^{-1} &= (e_N, h)(n, e_H)(e_N, h)^{-1} \\ &= (e_N, h)(n, e_H)(\theta(h^{-1})(e_N), h^{-1}) \\ &= (e_N, h)(n, e_H)(e_N, h^{-1}) \\ &= (\theta(h)(n), h)(e_N, h^{-1}) \\ &= (\theta(h)(n)\theta(h)(e_N), hh^{-1}) \\ &= (\theta(h)(n), e_H) \\ &= j(\theta(h)(n)) \end{aligned} \quad \square$$

**Proposition 7.30.** *Let  $G$  be a group. Let  $N$  and  $H$  be subgroups of  $G$  with  $N$  normal. Assume  $N \cap H = \{e\}$  and  $G = NH$ . Let  $\gamma : H \rightarrow \text{Aut}_{\mathbf{Grp}}(N)$  be conjugation. Then*

$$G \cong N \rtimes_{\gamma} H$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $\phi : N \rtimes_{\gamma} H \rightarrow G$  be the homomorphism

$$\phi(n, h) = nh \quad .$$

PROOF:

$$\begin{aligned} \phi((n_1, h_1)(n_2, h_2)) &= \phi(n_1\theta(h_1)(n_2), h_1h_2) \\ &= n_1\theta(h_1)(n_2)h_1h_2 \\ &= n_1h_1n_2h_1^{-1}h_1h_2 \\ &= n_1h_1n_2h_2 \\ &= \phi(n_1, h_1)\phi(n_2, h_2) \end{aligned}$$

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

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

PROOF: Since  $G = NH$ .

$\square$

**Definition 7.31** (Internal Product). Let  $G$  be a group. Let  $N$  and  $H$  be subgroups of  $G$ . Then  $G$  is the *internal product* of  $N$  and  $H$  iff  $N$  is normal,  $N \cap H = \{e\}$  and  $G = NH$ .

## 7.5 Direct Products

**Definition 7.32** (Direct Product). The *direct product* of groups  $G$  and  $H$  is their product in  $\mathbf{Grp}$ .



**Proposition 7.33.**  $G \times H$  is the semidirect product  $G \rtimes_{\theta} H$  where  $\theta(g) = e$  for all  $g \in G$ .

PROOF: Easy.  $\square$

## 7.6 Free Groups

**Proposition 7.34.** 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  $R(w_1w_2w_3)$ .

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

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

(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  $f(a_1^{\pm 1}a_2^{\pm 1} \cdots a_n^{\pm 1}) = k(a_1)^{\pm 1}k(a_2)^{\pm 1} \cdots k(a_n)^{\pm 1}$ .

$\square$

**Definition 7.35** (Free Group). For any set  $A$ , the *free group* on  $A$  is the initial object  $(F(A), i)$  in  $\mathcal{F}^A$ .

**Proposition 7.36.**  $i : A \rightarrow F(A)$  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.  $i(x) \neq i(y)$   
 $\square$

**Proposition 7.37.**

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

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 7.38.** *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  $\phi(n) = a(0)^n$ .  $\square$

**Proposition 7.39.** *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  $k \circ \kappa_2 = g$ .  
 $\square$

**Definition 7.40** (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 7.41.** 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.  $\square$

**Corollary 7.41.1.** Let  $G$  be a group and  $g \in G$ . Then

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

**Proposition 7.42.** 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 7.43** (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 7.44.** Every subgroup of a finitely generated free group is free.

PROOF: TODO.

**Proposition 7.45.**  $F(2)$  includes subgroups isomorphic to the free group on arbitrarily many generators.

PROOF: TODO

**Proposition 7.46.**

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

PROOF: TODO

## 7.7 Normal Subgroups

**Definition 7.47** (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 7.48.** Every subgroup of  $Q_8$  is normal.

**Proposition 7.49.** *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 7.50.** *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  $gng^{-1} \in \ker \phi$ . □

**Proposition 7.51.** *If  $H$  and  $K$  are normal subgroups of a group  $G$  then  $HK$  is normal in  $G$ .*

PROOF: For  $g \in G, h \in H$  and  $k \in K$  we have  $ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$ .

□

## 7.8 Quotient Groups

**Definition 7.52.** 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 7.53.** *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.  $\square$

**Definition 7.54** (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 7.55.** *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 7.50. For the other direction, take  $K = G/H$  and  $\phi$  to be the canonical map  $G \rightarrow G/H$ .  $\square$

**Definition 7.56** (Modular Group). The *modular group*  $\text{PSL}_2(\mathbb{Z})$  is  $\text{SL}_2(\mathbb{Z})/\{I, -I\}$ .

**Proposition 7.57.**  $\text{PSL}_2(\mathbb{Z})$  is generated by  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  and  $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ .

PROOF: By Example 6.29.

**Proposition 7.58** (Roger Alperin).  $\text{PSL}_2(\mathbb{Z})$  is presented by  $(x, y | x^2, y^3)$ .

PROOF:

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

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

$\langle 1 \rangle 3.$  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  $q > 0$ .

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

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

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

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

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

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

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

$\langle 1 \rangle 6.$

$$yxr = 1 + r$$

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

$\langle 1 \rangle 7.$

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

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

$\langle 1 \rangle 8.$  If  $r > -1$  is positive then  $yxr$  is positive.

$\langle 1 \rangle 9.$  If  $r$  is positive then  $y^{-1}xr$  is positive.

$\langle 1 \rangle 10.$  If  $r < -1$  then  $y^{-1}xr$  is positive.

$\langle 1 \rangle 11.$  If  $r$  is negative then  $yr$  is positive.

$\langle 1 \rangle 12.$  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 7.58.1.**  $\text{PSL}_2(\mathbb{Z})$  is the coproduct of  $C_2$  and  $C_3$  in **Grp**.

**Theorem 7.59.** 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 7.59.1** (First Isomorphism Theorem). Let  $\phi : G \rightarrow H$  be a surjective group homomorphism. Then  $H \cong G/\ker \phi$ .

**Proposition 7.60.** 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:  $\pi \times \pi : G_1 \times G_2 \rightarrow G_1/H_1 \times G_2/H_2$  is a surjective homomorphism with kernel  $H_1 \times H_2$ . □

**Example 7.61.**

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

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

**Proposition 7.62.** 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:

(1)1. If  $K$  is a subgroup of  $G$  that includes  $H$  then  $H$  is normal in  $K$ .

(1)2. If  $K$  is a subgroup of  $G$  that includes  $H$  then  $K/H$  is a subgroup of  $G/H$ .

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

**Proposition 7.63** (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  $gg'^{-1} \in N$ .

$\langle 3 \rangle 2$ .  $\phi((gH)(g'H)) = \phi(gH)\phi(g'H)$

PROOF: Both are  $gg'N$ .

$\langle 2 \rangle 3$ .  $\phi$  is surjective.

$\langle 2 \rangle 4$ .  $\ker \phi = N/H$

$\langle 2 \rangle 5$ .  $(G/H)/(N/H) \cong G/N$

PROOF: By the First Isomorphism Theorem.

□

**Proposition 7.64** (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:

$\langle 1 \rangle 1$ .  $HK$  is a subgroup of  $G$ .

PROOF: Since  $hkh'k' = hh'(h'^{-1}kh')k' \in HK$ .

$\langle 1 \rangle 2$ .  $H$  is normal in  $HK$ .

$\langle 1 \rangle 3$ .  $H \cap K$  is normal in  $K$  and  $HK/H \cong K/(H \cap K)$

PROOF: The function that maps  $k$  to  $kH$  is a surjective homomorphism  $K \rightarrow HK/H$  with kernel  $H \cap K$ . Surjectivity follows because  $hkh = hkh^{-1}H$ .

□

See also Proposition 7.79 for a result that holds even if  $H$  is not normal.

## 7.9 Cosets

**Proposition 7.65.** *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  $a^{-1}b \sim a^{-1}a = e$ .

- ⟨1⟩4. If  $a^{-1}b \in H$  then  $aH = bH$ .  
 ⟨2⟩1. ASSUME:  $a^{-1}b \in H$   
 ⟨2⟩2.  $bH \subseteq aH$   
 PROOF: For any  $h \in H$  we have  $bh = aa^{-1}bh \in aH$ .  
 ⟨2⟩3.  $aH \subseteq bH$   
 PROOF: Similar since  $b^{-1}a \in H$ .  
 ⟨1⟩5. If  $aH = bH$  then  $a \sim b$ .  
 ⟨2⟩1. ASSUME:  $aH = bH$   
 ⟨2⟩2. PICK  $h \in H$  such that  $a = bh$ .  
 ⟨2⟩3.  $b^{-1}a = h$   
 ⟨2⟩4.  $b^{-1}a \in H$   
 ⟨2⟩5.  $b^{-1}a \sim e$   
 ⟨2⟩6.  $a \sim b$   
 PROOF:  $a = bb^{-1}a \sim be = b$ .

□

**Definition 7.66** (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 7.67.**

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

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

**Proposition 7.68.** 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:

- ⟨1⟩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 7.65.  
 ⟨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 7.69.** *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  $aH$ .*

PROOF: Similar. □

**Proposition 7.70.** *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.  $ba^{-1} \in H$

⟨3⟩5.  $a \sim_R b$

⟨2⟩3. If  $a \sim_R b$  then  $a \sim_L b$ .

PROOF: Similar.

□

**Corollary 7.70.1.** *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 7.71** (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 7.71.1.** *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.*

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

**Proposition 7.72.**  $\mathbb{Z}/n\mathbb{Z}$  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  $0 < j-i < n$ .  $\square$

**Proposition 7.73.** *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 6.19 since the order of 1 is  $n$ .  $\square$

**Proposition 7.74.** *The integer  $m$  generates  $\mathbb{Z}/n\mathbb{Z}$  if and only if  $\gcd(m, n) = 1$ .*

PROOF: By Proposition 7.73.  $\square$

**Corollary 7.74.1.** *If  $p$  is prime then every non-zero element in  $\mathbb{Z}/p\mathbb{Z}$  is a generator.*

**Proposition 7.75.**

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

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

**Example 7.76.** 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 7.77.** *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 7.78.** *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 7.79.** *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.

$\langle 1 \rangle 4$ .

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

$\square$

## 7.10 Congruence

**Definition 7.80** (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 7.81.** *Given integers  $a, b, n$  with  $n$  positive, we have  $a \equiv b \pmod{n}$  iff  $n \mid a - b$ .*

PROOF: By Proposition 7.65.  $\square$

**Proposition 7.82.** *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 7.83.** *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  $n \mid a'b' - ab = a'(b' - b) + (a' - a)b$ .  $\square$

## 7.11 Cyclic Groups

**Definition 7.84** (Cyclic Group). The *cyclic* groups are  $\mathbb{Z}$  and  $\mathbb{Z}/n\mathbb{Z}$  for positive integers  $n$ .

**Proposition 7.85.** *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 7.86.** *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 7.87.** *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 7.87.1.**  *$\mathbb{Q}$  is not finitely generated.*

## 7.12 Commutator Subgroup

**Definition 7.88** (Commutator). Let  $G$  be a group and  $g, h \in G$ . The *commutator* of  $g$  and  $h$  is

$$[g, h] = ghg^{-1}h^{-1}.$$

**Definition 7.89** (Commutator Subgroup). Let  $G$  be a group. The *commutator subgroup*, denoted  $[G, G]$  or  $G'$ , is the subgroup generated by the elements of the form  $aba^{-1}b^{-1}$ .

We write  $G^{(i)}$  for the result of taking the commutator subgroup  $i$  times starting with  $G$ .

**Lemma 7.90.** *Let  $\phi : G_1 \rightarrow G_2$  be a group homomorphism. Then, for all  $g, h \in G_1$ , we have*

$$\phi([g, h]) = [\phi(g), \phi(h)]$$

and so  $\phi(G'_1) \subseteq G'_2$ .

PROOF: Easy.  $\square$

**Lemma 7.91.** *Let  $N$  and  $H$  be normal subgroups of a group  $G$ . Then  $[N, H] \subseteq N \cap H$ .*

PROOF:

$\langle 1 \rangle$ 1. LET:  $n \in N$  and  $h \in H$

PROVE:  $nhn^{-1}h^{-1} \in N \cap H$

$\langle 1 \rangle$ 2.  $nhn^{-1} \in H$

PROOF: Since  $H$  is normal.

$\langle 1 \rangle$ 3.  $nhn^{-1}h^{-1} \in H$

$\langle 1 \rangle$ 4.  $hn^{-1}h^{-1} \in N$

PROOF: Since  $N$  is normal.

$\langle 1 \rangle$ 5.  $nhn^{-1}h^{-1} \in N$

$\langle 1 \rangle$ 6.  $nhn^{-1}h^{-1} \in N \cap H$

$\square$

**Corollary 7.91.1.** *Let  $N$  and  $H$  be normal subgroups of  $G$ . If  $N \cap H = \{e\}$ , then every element in  $N$  commutes with every element in  $H$ .*

**Proposition 7.92.** *Let  $N$  and  $H$  be normal subgroups of  $G$ . If  $N \cap H = \{e\}$  then  $NH \cong N \times H$ .*

PROOF: From Proposition 7.30.  $\square$

## 7.13 Presentations

**Definition 7.93** (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 7.94.** • 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  $D_{2n}$ .
- $(x, y | x^2y^{-2}, y^4, xyx^{-1}y)$  is a presentation of  $Q_8$ .

**Proposition 7.95** (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 7.96** (Finitely Presented). A group is *finitely presented* iff it has a presentation  $(A, R)$  where both  $A$  and  $R$  are finite.

**Proposition 7.97.** *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  $\mathbf{Grp}$ .*

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

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  $F(A \cup A') \rightarrow G * G'$

$\square$

## 7.14 Index of a Subgroup

**Definition 7.98** (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 7.99** (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  $|H|$ .  $\square$

**Corollary 7.99.1.** *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,  $G = \langle g \rangle$ .  $\square$

**Theorem 7.100** (Cauchy's Theorem). *Let  $G$  be a finite group. If  $p$  is prime and  $p \mid |G|$  then the number of cyclic subgroups of order  $p$  is congruent to 1 modulo  $p$ . In particular, there exists an element of order  $p$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $S = \{(a_1, a_2, \dots, a_p) \in G^p : a_1 a_2 \cdots a_p = e\}$

$\langle 1 \rangle 2$ .  $|S| = |G|^{p-1}$

PROOF: Given any  $a_1, \dots, a_{p-1} \in G$ , there exists a unique  $a_p$  such that  $(a_1, \dots, a_p) \in S$ , namely  $a_p = (a_1 \cdots a_{p-1})^{-1}$ .

$\langle 1 \rangle 3$ .  $p \mid |S|$

$\langle 1 \rangle 4$ . Define an action of  $\mathbb{Z}/p\mathbb{Z}$  on  $S$  by

$$m \cdot (a_1, \dots, a_p) = (a_m, a_{m+1}, \dots, a_p, a_1, a_2, \dots, a_{m-1}) .$$

PROOF: If  $(a_1, \dots, a_p) \in S$  then  $(a_2, a_3, \dots, a_p, a_1) \in S$  since  $a_1 = (a_2 \cdots a_p)^{-1}$ .

$\langle 1 \rangle 5$ . LET:  $Z$  be the set of fixed points of this action.

$\langle 1 \rangle 6$ .  $|Z| \equiv 0 \pmod{p}$

PROOF: Corollary 9.18.1,  $\langle 1 \rangle 3$ .

$\langle 1 \rangle 7$ .  $Z = \{(a, a, \dots, a) : a^p = e\}$

$\langle 1 \rangle 8$ .  $Z \neq \emptyset$

PROOF: Since  $(e, e, \dots, e) \in Z$ .

$\langle 1 \rangle 9$ . An element  $a$  has order  $p$  iff  $(a, a, \dots, a) \in Z$  and  $a \neq e$ .

$\langle 1 \rangle 10$ . LET:  $N$  be the number of cyclic subgroups of order  $p$ .

$\langle 1 \rangle 11$ . The number of elements of order  $p$  is  $N(p-1)$

$\langle 1 \rangle 12$ .  $|Z| = N(p-1) + 1$

$\langle 1 \rangle 13$ .  $-N + 1 \equiv 0 \pmod{p}$

PROOF: From  $\langle 1 \rangle 6$ .

$\langle 1 \rangle 14$ .  $N \equiv 1 \pmod{p}$

$\square$

**Proposition 7.101.** *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:  $g_ik_jH = g_{i'}k_{j'}H$
  - $\langle 2 \rangle 2$ .  $g_iK = g_{i'}K$
  - $\langle 2 \rangle 3$ .  $i = i'$
  - $\langle 2 \rangle 4$ .  $k_jH = k_{j'}H$
  - $\langle 2 \rangle 5$ .  $j = j'$

□

## 7.15 Cokernels

**Proposition 7.102.** *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 7.103** (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 7.104.** 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.

## 7.16 Cayley Graphs

**Definition 7.105** (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 7.106.**  *$G$  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.  $\square$

## 7.17 Characteristic Subgroups

**Definition 7.107** (Characteristic Subgroup). Let  $G$  be a group. Let  $H$  be a subgroup of  $G$ . Then  $H$  is a *characteristic* subgroup of  $G$  iff, for every automorphism  $\phi$  of  $G$ , we have  $\phi(H) \subseteq H$ .

**Proposition 7.108.** *Characteristic subgroups are normal.*

PROOF: Take  $\phi$  to be conjugation with respect to an arbitrary element.  $\square$

**Proposition 7.109.** *Let  $G$  be a group. Let  $K$  be a normal subgroup of  $G$  and  $H$  a characteristic subgroup of  $K$ . Then  $H$  is normal in  $G$ .*

PROOF: For any  $a \in G$  we have conjugation by  $a$  is an automorphism on  $K$ , hence  $H$  is closed under it.  $\square$

**Proposition 7.110.** *Let  $G$  be a group. Let  $H$  be a subgroup of  $G$ . Suppose there is no other subgroup of  $G$  isomorphic to  $H$ . Then  $H$  is characteristic, hence normal.*

PROOF: For any automorphism  $\phi$  on  $G$ , we have  $\phi(H)$  is isomorphic to  $H$ , hence  $\phi(H) = H$ .  $\square$

**Proposition 7.111.** *Let  $G$  be a finite group. Let  $K$  be a normal subgroup of  $G$ . Assume  $|K|$  and  $|G/K|$  are relatively prime. Then  $K$  is characteristic.*

PROOF:

$\langle 1 \rangle$ 1. LET:  $K'$  be a subgroup of  $G$  isomorphic to  $K$ .

PROVE:  $K' = K$

$\langle 1 \rangle$ 2.  $|K'/(K \cap K')|$  divides both  $|K'| = |K|$  and  $|G/K|$

$\langle 1 \rangle$ 3.  $|K'/(K \cap K')| = 1$

$\langle 1 \rangle$ 4.  $K' = K \cap K'$

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

$\square$

**Proposition 7.112.** *The commutator subgroup of a group is characteristic.*

PROOF: Lemma 7.90.  $\square$

## 7.18 Simple Groups

**Definition 7.113** (Simple Group). A group  $G$  is *simple* iff its only normal subgroups are  $\{e\}$  and  $G$ .

**Proposition 7.114.** *Let  $G$  be a group. Then  $G$  is simple if and only if the only homomorphic images of  $G$  are 1 and  $G$ .*

PROOF: Both are equivalent to saying that, for any surjective homomorphism  $\phi : G \rightarrow G'$ , either  $\phi$  has kernel  $\{e\}$  (in which case it is an isomorphism) or  $\phi$  has kernel  $G$  (in which case  $G' = 1$ .)  $\square$

## 7.19 Sylow Subgroups

**Definition 7.115** (Sylow Subgroup). Let  $p$  be a prime number. Let  $G$  be a finite group. A *p-Sylow subgroup* of  $G$  is a subgroup of order  $p^r$ , where  $r$  is the largest integer such that  $p^r$  divides  $|G|$ .

**Proposition 7.116.** *Let  $p$  be prime. Let  $G$  be a finite group. Let  $P$  be a p-Sylow subgroup of  $G$ . If  $P$  is normal then  $P$  is characteristic.*

PROOF: Proposition 7.111.  $\square$

**Corollary 7.116.1.** *Let  $p$  be prime. Let  $G$  be a finite group. Let  $P$  be a p-Sylow subgroup of  $G$ . Let  $H$  be a subgroup of  $G$  that includes  $P$ . If  $P$  is normal in  $H$  and  $H$  is normal in  $G$  then  $P$  is normal in  $G$ .*

**Proposition 7.117.** *Let  $G$  be a finite group. Let  $P_1, \dots, P_r$  be its nontrivial Sylow subgroups. Assume all  $P_i$  are normal in  $G$ . Then*

$$G \cong P_1 \times \cdots \times P_r .$$

PROOF:

$$\langle 1 \rangle 1. P_1 P_2 \cdots P_r \cong P_1 \times P_2 \times \cdots \times P_r$$

$$\langle 2 \rangle 1. P_1 \cong P_1$$

$$\langle 2 \rangle 2. \text{ For } 1 \leq i < r, \text{ if } P_1 P_2 \cdots P_i \cong P_1 \times P_2 \times \cdots \times P_i \text{ then } P_1 P_2 \cdots P_i P_{i+1} \cong P_1 \times P_2 \times \cdots \times P_i \times P_{i+1}$$

$$\langle 3 \rangle 1. \text{ LET: } 1 \leq i < r$$

$$\langle 3 \rangle 2. \text{ ASSUME: } P_1 P_2 \cdots P_i \cong P_1 \times P_2 \times \cdots \times P_i$$

$$\langle 3 \rangle 3. P_1 P_2 \cdots P_i \text{ is normal in } G.$$

$$\langle 3 \rangle 4. P_1 P_2 \cdots P_i \cap P_{i+1} = \{e\}$$

$$\langle 4 \rangle 1. \text{ LET: } |P_j| = p_j^{k_j} \text{ for all } j.$$

$$\langle 4 \rangle 2. \text{ The order of any element of } P_1 P_2 \cdots P_i \text{ divides } p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}$$

$$\langle 4 \rangle 3. \text{ The order of any element of } P_{i+1} \text{ divides } p_{i+1}^{k_{i+1}}$$

$$\langle 4 \rangle 4. \text{ The } p_j \text{ are all distinct.}$$

PROOF: Any  $p_j$ -Sylow subgroup is congruent to  $P_j$  hence equal to  $P_j$  since  $P_j$  is normal.

- $\langle 4 \rangle 5$ . The only element in  $P_1 P_2 \cdots P_i$  and  $P_{i+1}$  is  $e$ .  
 $\langle 3 \rangle 5$ .  $P_1 P_2 \cdots P_i P_{i+1} \cong P_1 P_2 \cdots P_i \times P_{i+1}$   
 PROOF: Proposition 7.92.  
 $\langle 3 \rangle 6$ .  $P_1 P_2 \cdots P_i P_{i+1} \cong P_1 \times P_2 \times \cdots \times P_i \times P_{i+1}$   
 $\langle 1 \rangle 2$ .  $G = P_1 P_2 \cdots P_r$   
 PROOF: Since  $|G| = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ .  
 $\square$

## 7.20 Series of Subgroups

**Definition 7.118** (Series of Subgroups). Let  $G$  be a group. A *series* of subgroups of  $G$  is a sequence  $(G_n)$  of subgroups of  $G$  such that

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots$$

It is a *normal* series iff  $G_{n+1}$  is normal in  $G_n$  for all  $n$ .

**Proposition 7.119.** *The maximal length of a normal series in  $G$  is 0 iff  $G$  is trivial.*

PROOF: Since 1 is normal in  $G$  for every  $G$ .  $\square$

**Proposition 7.120.** *The maximal length of a normal series in  $G$  is 1 iff  $G$  is non-trivial and simple.*

PROOF: Immediate from definitions.  $\square$

**Example 7.121.**  $\mathbb{Z}$  has normal series of arbitrary length.

PROOF: We have  $\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq \cdots$ .  $\square$

**Example 7.122.** The maximal length of a normal series in  $\mathbb{Z}/n\mathbb{Z}$  is the number of primes in the prime factorization of  $n$ .

PROOF: Let  $n = p_1 p_2 \cdots p_k$ . A normal series of maximal length is  
 $\mathbb{Z}/p_1 p_2 \cdots p_k \mathbb{Z} \supsetneq \mathbb{Z}/p_1 p_2 \cdots p_{k-1} \mathbb{Z} \supsetneq \cdots \supsetneq \mathbb{Z}/p_1 \mathbb{Z} \supsetneq \{e\}$ .  $\square$

**Definition 7.123** (Equivalent Normal Series). Let

$$\begin{aligned}
 G &= G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = \{e\} \\
 G &= G'_0 \supsetneq G'_1 \supsetneq G'_2 \supsetneq \cdots \supsetneq G'_m = \{e\}
 \end{aligned}$$

be two normal series in a group  $G$ . Then the two series are *equivalent* iff  $m = n$  and there exists a permutation  $\sigma \in S_n$  such that, for all  $i$ , we have  $G_i/G_{i+1} \cong G'_{\sigma(i)}/G'_{\sigma(i)+1}$ .

**Definition 7.124** (Composition Series). Let  $G$  be a group. A *composition series* for  $G$  is a series of subgroups in  $G$

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = \{e\}$$

such that, for all  $i$ , we have  $G_i/G_{i+1}$  is simple.

**Proposition 7.125.** *A normal series of maximal length in a group is a composition series.*

PROOF: Easy.  $\square$

**Corollary 7.125.1.** *Every finite group has a composition series.*

**Corollary 7.125.2.** *If a group has a composition series then every normal subgroup has a composition series.*

**Definition 7.126** (Refinement). A series of subgroups  $S_1$  is a *refinement* of the series  $S_2$  iff every subgroup in  $S_2$  appears in  $S_1$ .

**Lemma 7.127.** *Let  $G$  be a group. Let  $Q$ ,  $N$  and  $L$  be subgroups of  $G$ . Assume  $L$  is a normal subgroup of  $Q$  and  $qN = Nq$  for all  $q \in Q$ . Then*

$$\frac{QN}{LN} \cong \frac{Q}{L(Q \cap N)} .$$

PROOF:

$\langle 1 \rangle 1$ .  $QN$  is a subgroup of  $G$ .

PROOF: Since  $QN = NQ$ .

$\langle 1 \rangle 2$ .  $LN$  is a subgroup of  $G$ .

PROOF: Since  $LN = NL$ .

$\langle 1 \rangle 3$ .  $LN$  is normal in  $QN$ .

$\langle 2 \rangle 1$ . LET:  $l \in L$ ,  $q \in Q$ , and  $n, n' \in N$ .

PROVE:  $qnl n' n^{-1} q^{-1} \in LN$

$\langle 2 \rangle 2$ . PICK  $n_1 \in N$  such that  $nl = ln_1$

$\langle 2 \rangle 3$ . PICK  $n_2 \in N$  such that  $n_1 n' n^{-1} q^{-1} = q^{-1} n_2$

$\langle 2 \rangle 4$ .  $qnl n' n^{-1} q^{-1} = ql q^{-1} n_2 \in LN$

PROOF: Since  $L$  is normal in  $Q$ .

$\langle 1 \rangle 4$ . The function  $f : Q \rightarrow QN/LN$  that maps  $q$  to  $qLN$  is a surjective homomorphism.

$\langle 1 \rangle 5$ .  $\ker f = L(Q \cap N)$

$\langle 2 \rangle 1$ .  $\ker f \subseteq L(Q \cap N)$

$\langle 3 \rangle 1$ . LET:  $x \in \ker f$

$\langle 3 \rangle 2$ .  $x \in LN$

$\langle 3 \rangle 3$ . PICK  $l \in L$  and  $n \in N$  such that  $x = ln$

$\langle 3 \rangle 4$ .  $n = l^{-1}x \in Q \cap N$

$\langle 3 \rangle 5$ .  $x \in L(Q \cap N)$

$\langle 2 \rangle 2$ .  $L(Q \cap N) \subseteq \ker f$

PROOF: Since  $L(Q \cap N) \subseteq Q$  and  $L(Q \cap N) \subseteq LN$ .

$\langle 1 \rangle 6$ . Q.E.D.

PROOF: First Isomorphism Theorem.

$\square$

**Theorem 7.128** (Schreier). *Any two normal series in a group have equivalent refinements.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $G$  be a group.

$\langle 1 \rangle 2$ . LET:  $S_1 : G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_m = \{e\}$  and  $S_2 : G = H_0 \supsetneq H_1 \supsetneq H_2 \supsetneq \cdots \supsetneq H_n = \{e\}$  be two normal series in  $G$ .

$\langle 1 \rangle 3$ . For each  $i$ , we have

$$G_i = G_i \cap H_0 \supseteq G_i \cap H_1 \supseteq \cdots \supseteq G_i \cap H_n = \{e\}$$

is a series of subgroups in  $G_i$ .

$\langle 1 \rangle 4$ . For each  $i$ , we have

$$G_i = (G_i \cap H_0)G_{i+1} \supseteq (G_i \cap H_1)G_{i+1} \supseteq \cdots \supseteq (G_i \cap H_n)G_{i+1} = G_{i+1}$$

is a normal series in  $G_i$ .

$\langle 2 \rangle 1$ . LET:  $0 \leq i < m$  and  $0 \leq j < n$

PROVE:  $(G_i \cap H_{j+1})G_{i+1}$  is normal in  $(G_i \cap H_j)G_{i+1}$

$\langle 2 \rangle 2$ . LET:  $x \in G_i \cap H_{j+1}$ ,  $y \in G_{i+1}$ ,  $a \in G_i \cap H_j$  and  $b \in G_{i+1}$

PROVE:  $abxyb^{-1}a^{-1} \in (G_i \cap H_{j+1})G_{i+1}$

$\langle 2 \rangle 3$ .  $axa^{-1} \in G_i \cap H_{j+1}$

PROOF: Since  $a, x \in G_i$  and  $H_{j+1}$  is normal in  $H_j$ .

$\langle 2 \rangle 4$ .  $ax^{-1}bxa^{-1} \in G_{i+1}$

PROOF: Since  $G_{i+1}$  is normal in  $G_i$ .

$\langle 2 \rangle 5$ .  $yb^{-1} \in G_{i+1}$

$\langle 2 \rangle 6$ .  $ayb^{-1}a^{-1} \in G_{i+1}$

PROOF: Since  $G_{i+1}$  is normal in  $G_i$ .

$\langle 2 \rangle 7$ .  $abxyb^{-1}a^{-1} = (axa^{-1})(ax^{-1}bxa^{-1}ayb^{-1}a^{-1}) \in (G_i \cap H_{j+1})G_{i+1}$

$\langle 1 \rangle 5$ . Let  $S$  be the series obtained by concatenating the series  $\langle 1 \rangle 4$  for  $G_0$  to  $G_1$ ,  $G_1$  to  $G_2$ ,  $\dots$ ,  $G_{m-1}$  to  $G_m$

$\langle 1 \rangle 6$ .  $S$  is a refinement of  $S_1$ .

$\langle 1 \rangle 7$ .  $S$  is normal.

$\langle 1 \rangle 8$ . LET:  $T$  be the similarly constructed normal refinement of  $S_2$ .

$\langle 1 \rangle 9$ . For all  $i, j$  we have

$$\frac{(G_i \cap H_j)G_{i+1}}{(G_i \cap H_{j+1})G_{i+1}} \cong \frac{G_i \cap H_j}{(G_i \cap H_{j+1})(G_{i+1} \cap H_j)}$$

$\langle 2 \rangle 1$ .  $G_i \cap H_{j+1}$  is normal in  $G_i \cap H_j$

$\langle 2 \rangle 2$ . For all  $q \in G_i \cap H_j$  we have  $qG_{i+1} = G_{i+1}q$

PROOF: Since for all  $q \in G_i$  we have  $qG_{i+1} = G_{i+1}q$ .

$\langle 2 \rangle 3$ . Q.E.D.

PROOF: Lemma 7.127

$\langle 1 \rangle 10$ . For all  $i, j$  we have

$$\frac{(G_i \cap H_j)H_{j+1}}{(G_{i+1} \cap H_j)H_{j+1}} \cong \frac{G_i \cap H_j}{(G_{i+1} \cap H_j)(G_i \cap H_{j+1})}$$

PROOF: Lemma 7.127

$\langle 1 \rangle 11$ . For all  $i, j$  we have

$$\frac{(G_i \cap H_j)G_{i+1}}{(G_i \cap H_{j+1})G_{i+1}} \cong \frac{(G_i \cap H_j)H_{j+1}}{(G_{i+1} \cap H_j)H_{j+1}}$$

$\langle 1 \rangle 12$ .  $S$  and  $T$  are equivalent.

□

**Corollary 7.128.1** (Jordan-Hölder). *Any two composition series for a group*

are equivalent.

**Definition 7.129** (Composition Factors). Let  $G$  be a group that has a composition series. The multiset of *composition factors* of  $G$  is the multiset of quotients of any composition series.

**Example 7.130.** Non-isomorphic groups can have the same composition factors. For example,  $C_2 \times C_2$  and  $C_4$  both have composition factors  $\{[C_2, C_2]\}$ .

**Proposition 7.131.** Let  $G$  be a group. Let  $N$  be a normal subgroup of  $G$ . Then  $G$  has a composition series if and only if  $N$  and  $G/N$  both have composition series, in which case the composition factors of  $G$  are the union of the composition factors of  $N$  and the composition factors of  $G/N$ .

PROOF:

(1)1. If  $G$  has a composition series then  $N$  and  $G/N$  have composition series.

(2)1. LET:  $G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = \{e\}$  be a composition series for  $G$ .

(2)2.  $N$  has a composition series.

(3)1. For all  $i$ , we have  $\frac{G_i \cap N}{G_{i+1} \cap N}$  is either trivial or isomorphic to  $G_i/G_{i+1}$ .

(4)1. The homomorphism  $G_i \cap N \hookrightarrow G_i \twoheadrightarrow G_i/G_{i+1}$  has kernel  $G_{i+1} \cap N$ .

(4)2. There is an injective homomorphism  $(G_i \cap N)/(G_{i+1} \cap N) \rightarrow G_i/G_{i+1}$ .

PROOF: First Isomorphism Theorem.

(4)3.  $(G_i \cap N)/(G_{i+1} \cap N)$  is either trivial or isomorphic to  $G_i/G_{i+1}$ .

PROOF: Since  $G_i/G_{i+1}$  is simple.

(3)2. Eliminating all duplicates from the series  $N = G_0 \cap N \supseteq G_1 \cap N \supseteq G_2 \cap N \supseteq \cdots \supseteq G_n \cap N = \{e\}$  gives a composition series for  $N$ .

(2)3.  $G/N$  has a composition series.

(3)1. For all  $i$  we have  $\frac{(G_i N)/N}{(G_{i+1} N)/N}$  is either trivial or isomorphic to  $G_i/G_{i+1}$ .

(4)1. LET:  $0 \leq i < n$

(4)2.  $\frac{(G_i N)/N}{(G_{i+1} N)/N} \cong G_i N/G_{i+1} N$

PROOF: Third Isomorphism Theorem.

(4)3. There exists a surjective homomorphism

$$\frac{G_i}{G_{i+1}} \twoheadrightarrow \frac{G_i N}{G_{i+1} N}.$$

(5)1. LET:  $f$  be the homomorphism  $G_i \hookrightarrow G_i N \twoheadrightarrow G_i N/G_{i+1} N$

(5)2.  $f$  is surjective.

(5)3.  $f(G_{i+1}) = \{e\}$

(5)4. Q.E.D.

PROOF: By the universal property of quotient groups.

(4)4.  $G_i N/G_{i+1} N$  is either trivial or isomorphic to  $G_i/G_{i+1}$ .

PROOF: Proposition 7.114.

(3)2. Eliminating all duplicates from the series  $G/N = G_0 N/N \supseteq G_1 N/N \supseteq G_2 N/N \supseteq \cdots \supseteq G_n N/N = \{e\}$  gives a composition series for  $G/N$ .

(1)2. If  $N$  and  $G/N$  have composition series, then  $G$  has a composition series, and the composition factors of  $G$  are the union of the composition factors of  $N$  and the composition factors of  $G/N$ .

- (2)1. LET:  $N = N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_n = \{e\}$  be a composition series for  $N$ .  
 (2)2. LET:  $G/N = H_0 \supsetneq H_1 \supsetneq H_2 \supsetneq \cdots \supsetneq H_m = \{e\}$  be a composition series for  $G/N$ .  
 (2)3.  $G = \pi^{-1}(H_0) \supsetneq \pi^{-1}(H_1) \supsetneq \cdots \supsetneq \pi^{-1}(H_m) = N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_n$  is a composition series for  $G$ .

□

**Proposition 7.132.** *Let  $G_1$  and  $G_2$  be groups. Then  $G_1 \times G_2$  has a composition series if and only if  $G_1$  and  $G_2$  both have composition series.*

PROOF:

- (1)1. If  $G_1 \times G_2$  has a composition series then  $G_1$  has a composition series.  
 (2)1. LET:  $G_1 \times G_2 = A_0 \supsetneq A_1 \supsetneq \cdots \supsetneq A_n = \{e\}$  be a composition series.  
 (2)2. For each  $i$ , we have  $\pi_1(A_i)/\pi_1(A_{i+1})$  is either isomorphic to  $A_i/A_{i+1}$  or trivial.  
 (2)3. Eliminating duplicates from  $G_1 = \pi_1(A_0) \supsetneq \pi_1(A_1) \supsetneq \cdots \supsetneq \pi_1(A_n) = \{e\}$  gives a composition series for  $G_1$ .  
 (1)2. If  $G_1 \times G_2$  has a composition series then  $G_2$  has a composition series.

PROOF: Similar.

- (1)3. If  $G_1$  and  $G_2$  have composition series then  $G_1 \times G_2$  has a composition series.  
 (2)1. LET:  $G_1 = H_0 \supsetneq H_1 \supsetneq \cdots \supsetneq H_m = \{e\}$  be a composition series for  $G_1$ .  
 (2)2. LET:  $G_2 = K_0 \supsetneq K_1 \supsetneq \cdots \supsetneq K_n = \{e\}$  be a composition series for  $G_2$ .  
 (2)3.  $G_1 \times G_2 = H_0 \times K_0 \supsetneq H_1 \times K_0 \supsetneq \cdots \supsetneq H_m \times K_0 \supsetneq H_m \times K_1 \supsetneq \cdots \supsetneq H_m \times K_n = \{e\}$  is a composition series for  $G_1 \times G_2$ .

□

**Definition 7.133** (Cyclic Series). A normal series of subgroups is *cyclic* iff every quotient is cyclic.



## 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  $\gamma : G \rightarrow \text{Aut}_{\text{Grp}}(G)$  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 6.22.

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

$\langle 1 \rangle 5$ . 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  $i(g) = g^{-1}$ .*

**Proposition 8.20.** *Let  $G$  be a group. If every element of  $G$  has order  $\leq 2$  then  $G$  is Abelian.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $x, y \in G$

PROVE:  $xy = yx$

$\langle 1 \rangle 2$ . ASSUME: w.l.o.g.  $x \neq e \neq y$ .

$\langle 1 \rangle 3$ .  $x^2 = e = y^2$

$\langle 1 \rangle 4$ .  $x^{-1} = x$  and  $y^{-1} = y$ .

$\langle 1 \rangle 5$ . CASE:  $xy = e$

PROOF: Then  $y = x^{-1}$  and so  $xy = yx = e$ .

$\langle 1 \rangle 6$ . CASE:  $xy \neq e$

$\langle 2 \rangle 1$ .  $(xy)^2 = e$

$\langle 2 \rangle 2$ .  $xyxy = e$

$$\langle 2 \rangle 3. \quad xy = y^{-1}x^{-1}$$

$$\langle 2 \rangle 4. \quad xy = yx$$

□

**Proposition 8.21.** *Every Abelian group is solvable.*

PROOF: If  $G$  is Abelian then  $G' = \{e\}$ . □

**Proposition 8.22.** *The only non-trivial simple finite Abelian groups are  $\mathbb{Z}/p\mathbb{Z}$  for  $p$  a prime.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $G$  be a non-trivial simple finite Abelian group.

$\langle 1 \rangle 2$ . PICK a prime  $p$  that divides  $|G|$ .

$\langle 1 \rangle 3$ . PICK an element  $a \in G$  of order  $p$ .

PROOF: Cauchy's Theorem.

$\langle 1 \rangle 4$ .  $\langle a \rangle = G$

□

## 8.1 The Category of Abelian Groups

**Definition 8.23** (Category of Abelian Groups). Let **Ab** be the full subcategory of **Grp** whose objects are the Abelian groups.

**Proposition 8.24.** *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 8.25** (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 8.26.** *Given Abelian groups  $G$  and  $H$ , the direct sum  $G \oplus H$  is the coproduct of  $G$  and  $H$  in **Ab**.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $\kappa_1 : G \rightarrow G \oplus H$  be the group homomorphism  $\kappa_1(g) = (g, e_H)$ .

$\langle 1 \rangle 2$ . LET:  $\kappa_2 : H \rightarrow G \oplus H$  be the group homomorphism  $\kappa_2(h) = (e_G, h)$ .

$\langle 1 \rangle 3$ . Given group homomorphism  $\phi : G \rightarrow K$  and  $\psi : H \rightarrow K$ , define  $[\phi, \psi] : G \oplus H \rightarrow K$  by  $[\phi, \psi](g, h) = \phi(g) + \psi(h)$ .

$\langle 1 \rangle 4$ .  $[\phi, \psi]$  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 8.27.** *Every finitely generated Abelian group is a direct sum of cyclic groups.*

PROOF: TODO □

## 8.2 Free Abelian Groups

**Proposition 8.28.** *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 8.29** (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 8.30.** *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**.*

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

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  $k \circ \kappa_2 = g$ .  $\square$

**Proposition 8.31.** 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  $F^{ab}(C)/\sim$  and the finite subsets of  $C$ , which maps  $f$  to  $\{c \in C : f(c) \text{ is odd}\}$ .

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

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

**Proposition 8.32.** Let  $G$  be an Abelian group. Then  $G$  is finitely generated if and only if there exists a surjective homomorphism  $\mathbb{Z}^{\oplus n} \twoheadrightarrow G$  for some  $n$ .

PROOF:

- (1)1. If  $G$  is finitely generated then there exists a surjective homomorphism  $\mathbb{Z}^{\oplus n} \twoheadrightarrow G$  for some  $n$ .

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



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

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

□

**Proposition 8.33.** *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  $A$ .*

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

PROOF:

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

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

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

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

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

(1)5.  $h$  is the unique group homomorphism such that  $h \circ \pi \circ i = f$ .

□

**Corollary 8.33.1.** *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 8.31. □

## 8.3 Cokernels

**Proposition 8.34.** *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:

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

(1)2. LET:  $\pi \circ \phi = 0$

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

(1)4.  $\text{im } \phi \subseteq \ker \alpha$

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

□

**Definition 8.35** (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 8.36.**  $\pi : H \rightarrow \text{coker } \phi$  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.  $\square$

**Proposition 8.37.** 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**.

$\square$

## 8.4 Commutator Subgroups

**Proposition 8.38.** Let  $G$  be a group. Let  $G'$  be the commutator subgroup of  $G$ . Then  $G/G'$  is Abelian.

PROOF: Since  $ghg^{-1}h^{-1}G' = G'$  so  $ghG' = hgG'$ .  $\square$

**Proposition 8.39.** Let  $G$  be a group and  $A$  an Abelian group. Let  $\alpha : G \rightarrow A$  be a homomorphism. Then  $G' \subseteq \ker \alpha$ .

PROOF: Since  $\phi([g, h]) = \phi(g)\phi(h)\phi(g)^{-1}\phi(h)^{-1} = e$ .  $\square$

**Corollary 8.39.1.** Let  $G$  be a group. The canonical projection  $G \twoheadrightarrow G/G'$  is initial in the category of homomorphisms from  $G$  to an Abelian group.

**Definition 8.40** (Abelian Series). A normal series of subgroups is *Abelian* iff every quotient is Abelian.

**Lemma 8.41.** Let  $G$  be a group. Let  $H$  be a normal subgroup of  $G$ . If  $G/H$  is Abelian then  $G' \subseteq H$ .

PROOF: Given  $g, h \in G$  we have

$$\begin{aligned} ghH &= hgH \\ \therefore ghg^{-1}h^{-1} &\in H \end{aligned}$$

□

## 8.5 Derived Series

**Definition 8.42** (Derived Series). Let  $G$  be a group. The *derived series* of  $G$  is the series of subgroups

$$G \supseteq G' \supseteq G'' \supseteq G''' \supseteq \dots$$

where  $G'$  is the commutator subgroup of  $G$ .

We write  $G^{(i)}$  for the  $i + 1$ st entry in the derived series

**Proposition 8.43.** *Each  $G^{(i)}$  is characteristic.*

PROOF:

$\langle 1 \rangle 1.$   $G$  is characteristic in  $G$ .

PROOF: Trivial.

$\langle 1 \rangle 2.$  If  $G^{(i)}$  is characteristic in  $G$  then  $G^{(i+1)}$  is characteristic in  $G$ .

$\langle 2 \rangle 1.$  ASSUME:  $G^{(i)}$  is characteristic.

$\langle 2 \rangle 2.$  LET:  $\phi : G \cong G$  be an automorphism of  $G$ .

$\langle 2 \rangle 3.$  For all  $g, h \in G^{(i)}$  we have  $\phi([g, h]) \in G^{(i+1)}$ .

PROOF: Since  $\phi([g, h]) = [\phi(g), \phi(h)]$  and  $\phi(g), \phi(h) \in G^{(i)}$ .

$\langle 2 \rangle 4.$   $\phi(G^{(i+1)}) \subseteq G^{(i+1)}$

□

## 8.6 Solvable Groups

**Definition 8.44** (Solvable). A group is *solvable* iff its derived series terminates in  $\{e\}$ .

**Theorem 8.45** (Feit-Thompson). *Every finite group of odd order is solvable.*

**Corollary 8.45.1.** *Every non-Abelian finite simple group has even order.*

PROOF: A non-Abelian finite simple group of odd order is solvable, hence its composition factors are all Abelian. But a simple group is its own only composition factor. □

**Proposition 8.46.** *Let  $H$  be a nontrivial normal subgroup of a solvable group  $G$ . Then  $H$  contains a nontrivial Abelian subgroup that is normal in  $G$ .*

PROOF:

$\langle 1 \rangle 1.$  LET:  $r$  be the largest number such that  $H \cap G^{(r)}$  is non-trivial.

$\langle 1 \rangle 2.$  LET:  $K = H \cap G^{(r)}$

$\langle 1 \rangle 3.$   $K$  is Abelian.

PROOF: Since  $[K, K] \subseteq G^{(r+1)} = \{e\}$ .

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

PROOF: Proposition 8.44.

□

**Theorem 8.47** (Burnside). *Let  $p$  and  $q$  be primes. Every group of order  $p^a q^b$  is solvable.*

**Proposition 8.48.** *The semidirect product of two solvable groups is solvable.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $N$  and  $H$  be solvable groups.

$\langle 1 \rangle 2$ . LET:  $\theta : H \rightarrow \text{Aut}_{\mathbf{Grp}}(N)$

$$\begin{aligned} [(n_1, h_1), (n_2, h_2)] &= (n_1, h_1)(n_2, h_2)(n_1, h_1)^{-1}(n_2, h_2)^{-1} \\ &= (n_1, h_1)(n_2, h_2)(\theta(h_1^{-1})(n_1^{-1}), h_1^{-1})(\theta(h_2^{-1})(n_2^{-1}), h_2^{-1}) \\ &= (n_1\theta(h_1)(n_2), h_1h_2)(\theta(h_1^{-1})(n_1^{-1})\theta(h_1^{-1})(\theta(h_2^{-1})(n_2^{-1})), h_1^{-1}h_2^{-1}) \\ &= (n_1\theta(h_1)(n_2), h_1h_2)(\theta(h_1^{-1})(n_1^{-1}\theta(h_2^{-1})(n_2^{-1})), h_1^{-1}h_2^{-1}) \\ &= (n_1\theta(h_1)(n_2)\theta(h_1h_2)(\theta(h_1^{-1})(n_1^{-1}\theta(h_2^{-1})(n_2^{-1}))), [h_1, h_2]) \\ &= (n_1\theta_{h_1}(n_2)\theta_{h_1h_2h_1^{-1}}(n_1^{-1})\theta_{[h_1, h_2]}(n_2^{-1}), [h_1, h_2]) \end{aligned}$$

**Proposition 8.49.** *Let  $G$  be a finite group. The following are equivalent.*

1. All composition factors of  $G$  are cyclic.
2.  $G$  has a cyclic series of subgroups ending in  $\{e\}$ .
3.  $G$  has an Abelian series of subgroups ending in  $\{e\}$ .
4.  $G$  is solvable.

PROOF:

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

PROOF: Trivial.

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

PROOF: Trivial.

$\langle 1 \rangle 3$ .  $3 \Rightarrow 4$

$\langle 2 \rangle 1$ . LET:  $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$  be an Abelian series of subgroups.

$\langle 2 \rangle 2$ . For all  $i$  we have  $G^{(i)} \subseteq G_i$ .

PROOF: Lemma 8.41.

$\langle 2 \rangle 3$ .  $G^{(n)} = \{e\}$

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

PROOF: Extend the derived series of  $G$  to a composition series, using the fact that every simple Abelian group is cyclic.

□

**Corollary 8.49.1.** *All  $p$ -groups are solvable.*

PROOF: Their composition factors are simple  $p$ -groups, hence cyclic.  $\square$

**Corollary 8.49.2.** *Let  $G$  be a group and  $N$  a normal subgroup. Then  $G$  is solvable if and only if both  $N$  and  $G/N$  are solvable.*

PROOF: By Proposition 7.131.  $\square$

**Corollary 8.49.3.** *The semidirect product of two solvable groups is solvable.*

**Corollary 8.49.4.** *Let  $G$  be a finite solvable group. Then the composition factors of  $G$  are exactly  $C_p$  for  $p$  a prime factor of  $G$  (with the same multiplicities).*

PROOF: Since each composition factor is simple and cyclic hence removes one prime factor in  $|G|$ .  $\square$



## 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 7.50.

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

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. □

**Proposition 9.18.** *Let  $S$  be a finite set. Let  $G$  be a group acting on  $S$ . Let  $Z$  be the set of fixed points of the action:*

$$Z = \{a \in S : \forall g \in G. ga = a\} .$$

*Let  $A$  be a set of representatives for the nontrivial orbits of the action. Then*

$$|S| = |Z| + \sum_{a \in A} [G : \text{Stab}_G(a)] .$$

PROOF: Immediate from the fact that the orbits partition  $S$ .  $\square$

**Corollary 9.18.1.** *Let  $p$  be a prime. Let  $S$  be a finite set. Let  $G$  be a  $p$ -group acting on  $S$ . Let  $Z$  be the set of fixed points of the action. Then  $|Z| \equiv |S| \pmod{p}$ .*

**Corollary 9.18.2.** *Let  $p$  be a prime. Let  $S$  be a finite set. Let  $G$  be a  $p$ -group acting on  $S$ . If  $p$  does not divide  $|S|$  then the action has a fixed point.*

## 9.2 Category of $G$ -Sets

**Definition 9.19.** 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 9.20.** *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:

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

$\square$

**Proposition 9.21.** *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 9.21.1.** *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 9.21.2.** *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  $a = gH$ . □

**Proposition 9.22.** *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. □

**Proposition 9.23.** *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. □

**Proposition 9.24.** *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  $G/\text{Stab}_G(a_1), \dots, G/\text{Stab}_G(a_n)$ . □

**Proposition 9.25.** *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  $\phi(g)(g') = g'g^{-1}$ .

- ⟨2⟩1. LET:  $g \in G$   
 PROVE:  $\lambda_{g'} \in G.g'g^{-1}$  is an automorphism of  $G$  in  $G - \mathbf{Set}$ .  
 ⟨2⟩2.  $\phi(g)$  is  $G$ -equivariant.  
 PROOF: Since  $\phi(g)(h_1h_2) = h_1h_2g^{-1} = h_1\phi(g)(h_2)$ .  
 ⟨2⟩3.  $\phi(g)$  is injective.  
 PROOF: By Cancellation.  
 ⟨2⟩4.  $\phi(g)$  is surjective.  
 PROOF: For any  $h \in G$  we have  $h = \phi(g)(hg)$ .  
 ⟨1⟩2.  $\phi$  is a group homomorphism.  
 PROOF:  $\phi(g_1g_2)(h) = hg_2^{-1}g_1^{-1} = \phi(g_1)(\phi(g_2)(h))$ .  
 ⟨1⟩3.  $\phi$  is injective.  
 PROOF: If  $\phi(g) = \phi(g')$  then  $g = \phi(g)(e) = \phi(g')(e) = g'$ .  
 ⟨1⟩4.  $\phi$  is surjective.  
 ⟨2⟩1. LET:  $\sigma \in \text{Aut}_{G-\mathbf{Set}}(G)$   
 ⟨2⟩2. LET:  $g = \sigma(e)$   
 PROVE:  $\sigma = \phi(g^{-1})$   
 ⟨2⟩3.  $\sigma(h) = hg$   
 PROOF:  $\sigma(h) = \sigma(hg) = h\sigma(e) = hg$ .  
 □

### 9.3 Center

**Definition 9.26** (Center). The *center* of a group  $G$ ,  $Z(G)$ , is the kernel of the conjugation action  $\sigma : G \rightarrow S_G$ .

**Proposition 9.27.** *The center of a group  $G$  is*

$$Z(G) = \{g \in G : \forall a \in G. ag = ga\} .$$

PROOF: Immediate from definitions. □

**Lemma 9.28.** *Let  $G$  be a finite group. Assume  $G/Z(G)$  is cyclic. Then  $G$  is Abelian and so  $G/Z(G)$  is trivial.*

PROOF:

- ⟨1⟩1. PICK  $g \in G$  such that  $gZ(G)$  generates  $G/Z(G)$ .  
 ⟨1⟩2. LET:  $a, b \in G$   
 ⟨1⟩3. PICK  $r, s \in \mathbb{Z}$  such that  $aZ(G) = g^rZ(G)$  and  $bZ(G) = g^sZ(G)$   
 ⟨1⟩4. LET:  $z = g^{-r}a \in Z(G)$  and  $w = g^{-s}b \in Z(G)$   
 ⟨1⟩5.  $a = g^rz$  and  $b = g^sw$   
 ⟨1⟩6.  $ab = ba$

PROOF:

$$\begin{aligned}
 ab &= g^rzg^sw \\
 &= g^{r+s}zw \\
 &= g^swg^rz \\
 &= ba
 \end{aligned}$$

□

**Proposition 9.29.** *Let  $G$  be a group. Let  $N$  be a subgroup of  $Z(G)$ . Then  $N$  is normal in  $G$ .*

PROOF: For all  $n \in N$  and  $g \in G$  we have  $gng^{-1} = ngg^{-1} = n \in N$  since  $n \in Z(G)$ . □

**Proposition 9.30.** *For any group  $G$  we have  $G/Z(G) \cong \text{Inn}(G)$ .*

PROOF: The homomorphism  $g \mapsto \gamma_g$  is a surjective homomorphism with kernel  $Z(G)$ . □

**Proposition 9.31.** *Let  $p$  and  $q$  be prime integers. Let  $G$  be a group of order  $pq$ . Then either  $G$  is Abelian or the center of  $G$  is trivial.*

PROOF: Otherwise we would have  $|Z(G)| = p$  say and so  $|\text{Inn}(G)| = q$ , meaning  $\text{Inn}(G)$  is cyclic, hence trivial, which is a contradiction. □

**Theorem 9.32** (First Sylow Theorem). *Let  $p$  be a prime and  $k \in \mathbb{N}$ . Let  $G$  be a finite group. If  $p^k$  divides  $|G|$  then  $G$  has a subgroup of order  $p^k$ .*

PROOF:

- ⟨1⟩1. ASSUME: as induction hypothesis the statement is true for all groups smaller than  $G$ .
- ⟨1⟩2. ASSUME: w.l.o.g.  $k \neq 0$  and  $|G| \neq p$
- ⟨1⟩3. CASE: There exists a proper subgroup  $H$  of  $G$  such that  $p$  does not divide  $[G : H]$ .

PROOF: Then  $H$  has a subgroup of order  $p^k$  by induction hypothesis ⟨1⟩1.

- ⟨1⟩4. CASE: For every proper subgroup  $H$  of  $G$  we have  $p$  divides  $[G : H]$ .

- ⟨2⟩1.  $p$  divides  $|Z(G)|$ .

PROOF: By the Class Formula.

- ⟨2⟩2. PICK  $a \in Z(G)$  that has order  $p$ .

PROOF: Cauchy's Theorem.

- ⟨2⟩3. LET:  $N = \langle a \rangle$

- ⟨2⟩4.  $N$  is normal.

PROOF: Proposition 9.29.

- ⟨2⟩5.  $p^{k-1}$  divides  $|G/N|$ .

- ⟨2⟩6. PICK a subgroup  $Q$  of  $G/N$  of order  $p^{k-1}$ .

PROOF: Induction hypothesis ⟨1⟩1.

- ⟨2⟩7. LET:  $P = \pi^{-1}(Q)$

- ⟨2⟩8.  $|P| = p^k$

□

**Theorem 9.33** (Second Sylow Theorem). *Let  $G$  be a finite group. Let  $p$  be a prime. Let  $P$  be a  $p$ -Sylow subgroup of  $G$ . Let  $H$  be a subgroup of  $G$  that is a  $p$ -group. Then  $H$  is a subgroup of a conjugate of  $P$ .*

PROOF:

(1)1. PICK a fixed point  $gP$  for the action of  $H$  on the set of left cosets of  $P$  by left multiplication.

PROOF: Corollary 9.18.2.

(1)2. For all  $h \in H$  we have  $hgP = gP$

(1)3.  $H \subseteq gPg^{-1}$

□

**Proposition 9.34.**

$$Z(G \times H) = Z(G) \times Z(H)$$

PROOF:

$$(g, h) \in Z(G \times H) \Leftrightarrow \forall g' \in G. \forall h' \in H. (g, h)(g', h') = (g', h')(g, h)$$

$$\Leftrightarrow \forall g' \in G. \forall h' \in H. (gg', hh') = (g'g, h'h)$$

$$\Leftrightarrow \forall g' \in G. \forall h' \in H. (gg' = g'g \wedge hh' = h'h)$$

$$\Leftrightarrow g \in Z(G) \wedge h \in Z(H)$$

□

## 9.4 Centralizer

**Definition 9.35** (Centralizer). Let  $G$  be a group. Let  $a \in G$ . The *centralizer* of  $a$ , denoted  $Z_G(a)$ , is the stabilizer of  $a$  under the action of conjugation.

**Proposition 9.36.**

$$Z_G(a) = \{g \in G : ga = ag\}$$

PROOF: Immediate from definitions. □

## 9.5 Conjugacy Class

**Definition 9.37** (Conjugacy Class). Let  $G$  be a group. Let  $a \in G$ . The *conjugacy class* of  $a$ , denoted  $[a]$ , is the orbit of  $a$  under the action of conjugation.

**Proposition 9.38** (Class Formula). Let  $G$  be a finite group. Let  $A$  be a set of representatives of the non-trivial conjugacy classes. Then

$$|G| = |Z(G)| + \sum_{a \in A} [G : Z(a)] .$$

PROOF: Proposition 9.18. □

**Corollary 9.38.1.** Let  $p$  be a prime. Let  $G$  be a  $p$ -group and  $H$  a nontrivial normal subgroup of  $G$ . Then  $H \cap Z(G) \neq \{e\}$ .

PROOF: Let  $A$  be a set of representatives of the non-trivial conjugacy classes. Let  $A \cap H = \{a_1, \dots, a_n\}$ . Then

$$|H| = |H \cap Z(G)| + \sum_{i=1}^n [G : Z(a_i)] .$$

Since  $p \mid |H|$  and  $p \mid [G : Z(a_i)]$  for all  $i$ , we have  $p \mid |H \cap Z(G)|$ . □

**Corollary 9.38.2.** *Let  $p$  be a prime. Every  $p$ -group has a non-trivial center.*

**Corollary 9.38.3.** *Let  $p$  be a prime. Every group  $G$  of order  $p^2$  is Abelian.*

PROOF: By Proposition 9.31.  $\square$

**Proposition 9.39.** *Let  $p$  be a prime and  $r$  a non-negative integer. Let  $G$  be a group of order  $p^r$ . Then, for  $k = 0, 1, \dots, r$ , we have  $G$  has a normal subgroup of order  $p^k$ .*

PROOF:

$\langle 1 \rangle 1$ . ASSUME: as induction hypothesis the result holds for  $r' < r$ .

$\langle 1 \rangle 2$ . ASSUME: w.l.o.g.  $k > 0$

PROOF: Since  $\{e\}$  is a normal subgroup of order  $p^0$ .

$\langle 1 \rangle 3$ . PICK a subgroup  $N$  of  $Z(G)$  of order  $p$ .

$\langle 2 \rangle 1$ .  $p \mid |Z(G)|$

PROOF: From Corollary 9.38.2.

$\langle 2 \rangle 2$ .  $Z(G)$  has a subgroup of order  $p$ .

PROOF: Cauchy's Theorem.

$\langle 1 \rangle 4$ .  $N$  is normal.

PROOF: Proposition 9.29.

$\langle 1 \rangle 5$ . PICK a normal subgroup  $M$  of  $G/N$  of order  $p^{k-1}$ .

PROOF: From the induction hypothesis  $\langle 1 \rangle 1$ .

$\langle 1 \rangle 6$ .  $\pi^{-1}(M)$  is a normal subgroup of  $G$  of order  $p^k$ .

$\square$

**Example 9.40.** The only non-Abelian group of order 6 is  $S_3$ .

PROOF:

$\langle 1 \rangle 1$ . LET:  $G$  be a non-Abelian group of order 6.

$\langle 1 \rangle 2$ .  $Z(G) = \{e\}$

PROOF: Otherwise  $Z(G)$  has order 2 or 3 and is cyclic, contradicting Lemma 9.28.

$\langle 1 \rangle 3$ .  $G$  has three conjugacy classes:  $Z(G)$ , a class of size 2 and a class of size 3.

PROOF: By the Class Formula since the only way to make 6 using non-trivial factors of 6 is  $2 + 3$ .

$\langle 1 \rangle 4$ . PICK an element  $y \in G$  of order 3.

PROOF: It cannot be that every element is of order  $\leq 2$  by Proposition 8.20.

$\langle 1 \rangle 5$ .  $\langle y \rangle$  is normal in  $G$ .

PROOF: Since it has index 2.

$\langle 1 \rangle 6$ . The conjugacy class  $y$  is  $\{y, y^2\}$ .

PROOF: Since  $\langle y \rangle$  must be a union of conjugacy classes.

$\langle 1 \rangle 7$ . The conjugacy class of size 2 is  $\{y, y^2\}$ .

PROOF: Since  $y^2$  has order 3 and so its conjugacy class is of size 2 similarly, and there is only one conjugacy class of size 2.

$\langle 1 \rangle 8$ . PICK  $x \in G$  such that  $yx = xy^2$ .

PROOF:  $y^2$  is conjugate to  $y$  so there exists  $x$  such that  $x^{-1}yx = y^2$ .

⟨1⟩9.  $x$  has order 2.

PROOF:  $x$  is not in the conjugacy class of size 2 so its order cannot be 3.

⟨1⟩10.  $x$  and  $y$  generate  $G$ .

PROOF: Since  $e, y, y^2, x, xy, xy^2$  are all distinct.

⟨1⟩11.  $G \cong S_3$

PROOF: We now know the entire multiplication table of  $G$ .

□

**Proposition 9.41.** *Let  $G$  be a finite group. Let  $H$  be a subgroup of  $G$  of order 2. Let  $a \in H$ . Let  $[a]_H$  be the conjugacy class of  $a$  in  $H$ , and  $[a]_G$  the conjugacy class of  $a$  in  $G$ . If  $Z_G(a) \subseteq H$  then  $[a]_H$  is half the size of  $[a]_G$ ; otherwise,  $[a]_H = [a]_G$ .*

PROOF:

⟨1⟩1.  $H$  is normal in  $G$ .

PROOF: Corollary 9.15.2.

⟨1⟩2.  $HZ_G(a)$  is a subgroup of  $G$ .

⟨1⟩3.  $H$  is normal in  $HZ_G(a)$ .

⟨1⟩4.  $H \cap Z_G(a)$  is normal in  $Z_G(a)$ .

⟨1⟩5.

$$\frac{HZ_G(a)}{H} \cong \frac{Z_G(a)}{H \cap Z_G(a)}$$

⟨1⟩6. If  $Z_G(a) \subseteq H$  then  $|[a]_H| = |[a]_G|/2$ .

PROOF: In this case we have  $Z_H(a) = Z_G(a)$  and so  $|[a]_H| = |H|/|Z_H(a)| = (|G|/2)/|Z_G(a)| = |[a]_G|/2$ .

⟨1⟩7. If  $Z_G(a) \not\subseteq H$  then  $[a]_H = [a]_G$ .

PROOF:

⟨2⟩1. PICK  $b \in Z_G(a) - H$

⟨2⟩2.  $Hb^{-1} = G - H$

⟨2⟩3.  $G = HZ_G(a)$

PROOF: For  $x \in H$  we have  $x = xe$  and for  $x \notin H$  we have  $x \in Hb^{-1}$  hence  $xb \in H$  and  $x = (xb)b$ .

⟨2⟩4.  $|[a]_H| = |[a]_G|$

PROOF:

$$\begin{aligned} |[a]_H| &= \frac{|H|}{|Z_H(a)|} \\ &= \frac{|H|}{|H \cap Z_G(a)|} \\ &= \frac{|Z_G(a)||H|}{|Z_G(a)||H \cap Z_G(a)|} \\ &= \frac{|HZ_G(a)|}{|Z_G(a)|} \\ &= \frac{|G|}{|Z_G(a)|} \\ &= |[a]_G| \end{aligned}$$



□

## 9.6 Conjugation on Sets

**Definition 9.42** (Conjugation). Let  $G$  be a group. Define an action of  $G$  on  $\mathcal{P}G$  called *conjugation* that takes  $g$  and  $A$  to

$$gAg^{-1} = \{gag^{-1} : a \in A\} .$$

**Proposition 9.43.** *The conjugate of a subgroup is a subgroup.*

PROOF: Let  $H$  be a subgroup of  $G$ . Given  $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$ , we have

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1} . \quad \square$$

**Definition 9.44** (Normalizer). Let  $G$  be a group and  $A \subseteq G$ . The *normalizer* of  $A$ , denoted  $N_G(A)$ , is its stabilizer under conjugation.

**Proposition 9.45.** *Let  $G$  be a group,  $g \in G$  and  $A$  a finite subset of  $G$ . If  $gAg^{-1} \subseteq A$  then  $gAg^{-1} = A$  and so  $g \in N_G(A)$ .*

PROOF: Conjugation by  $g$  is an injection from  $A$  into  $A$ , hence a bijection. □

**Proposition 9.46.** *Let  $G$  be a group and  $H$  a subgroup of  $G$ . Then  $N_G(H)$  is the largest subgroup of  $G$  that includes  $H$  such that  $H$  is normal in  $N_G(H)$ .*

PROOF:

⟨1⟩1.  $N_G(H)$  is a subgroup of  $G$ .

PROOF: If  $a, b \in N_G(H)$  then  $ab^{-1}Hba^{-1} = aHa^{-1} = H$  so  $ab^{-1} \in N_G(H)$ .

⟨1⟩2.  $H \subseteq N_G(H)$

PROOF: Easy.

⟨1⟩3.  $H$  is normal in  $N_G(H)$ .

PROOF: If  $a \in N_G(H)$  then  $aHa^{-1} = H$  by definition.

⟨1⟩4. For any subgroup  $K$  of  $G$ , if  $H \subseteq K$  and  $H$  is normal in  $K$  then  $K \subseteq N_G(H)$ .

PROOF:  $H$  is normal in  $K$  means that, for all  $a \in K$ , we have  $aHa^{-1} = H$  and so  $a \in N_G(H)$ .

□

**Corollary 9.46.1.** *Let  $G$  be a group and  $H$  a subgroup of  $G$ . Then  $H$  is normal if and only if  $G = N_G(H)$ .*

**Proposition 9.47.** *Let  $G$  be a group and  $H$  a subgroup of  $G$ . If  $[G : N_G(H)]$  is finite, then it is the number of subgroups conjugate to  $H$ .*

PROOF: By the Orbit-Stabilizer Theorem. □

**Corollary 9.47.1.** *Let  $G$  be a group and  $H$  a subgroup of  $G$ . If  $[G : H]$  is finite, the the number of subgroups conjugate to  $H$  is finite and divides  $[G : H]$ .*

**Lemma 9.48.** *Let  $H$  be a  $p$ -group that is a subgroup of a finite group  $G$ . Then*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

PROOF:

$\langle 1 \rangle 1$ . ASSUME: w.l.o.g.  $H$  is non-trivial.

$\langle 1 \rangle 2$ .  $gH$  is a fixed point of the action of  $H$  on the set of left cosets of  $H$  by left multiplication if and only if  $g \in N_G(H)$ .

PROOF:

$$gH \text{ is a fixed point} \Leftrightarrow \forall h \in H. hgH = gH$$

$$\Leftrightarrow H \subseteq gHg^{-1}$$

$$\Leftrightarrow H = gHg^{-1} \quad (|gHg^{-1}| = |H|)$$

$$\Leftrightarrow g \in N_G(H)$$

$\langle 1 \rangle 3$ . The number of fixed points in  $[N_G(H) : H]$ .

$\langle 1 \rangle 4$ . Q.E.D.

PROOF: Corollary 9.18.1.

□

**Proposition 9.49.** *Let  $H$  be a  $p$ -subgroup of a finite group  $G$  that is not a  $p$ -Sylow subgroup. Then there exists a  $p$ -subgroup  $H'$  of  $G$  such that  $H$  is a normal subgroup of  $H'$  and  $[H' : H] = p$ .*

PROOF:

$\langle 1 \rangle 1$ .  $p$  divides  $[N_G(H) : H]$ .

PROOF: Lemma 9.48.

$\langle 1 \rangle 2$ . PICK  $gH \in N_G(H)/H$  of order  $p$ .

PROOF: Cauchy's Theorem.

$\langle 1 \rangle 3$ . LET:  $H' = \pi^{-1}(\langle gH \rangle)$

$\langle 1 \rangle 4$ .  $H$  is a normal subgroup of  $H'$ .

$\langle 1 \rangle 5$ .  $[H' : H] = p$

□

**Corollary 9.49.1.** *No  $p$ -group of order  $\geq p^2$  is simple.*

**Lemma 9.50.** *Let  $p$  be a prime. Let  $G$  be a finite group. Let  $P$  be a  $p$ -Sylow subgroup of  $G$ . Every  $p$ -subgroup of  $N_G(P)$  is a subgroup of  $P$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $H$  be a  $p$ -subgroup of  $N_G(P)$ .

$\langle 1 \rangle 2$ .  $P$  is normal in  $N_G(P)$ .

PROOF: Proposition 9.46.

$\langle 1 \rangle 3$ .  $PH$  is a subgroup of  $N_G(P)$ .

PROOF: Second Isomorphism Theorem.

$\langle 1 \rangle 4$ .  $|PH/P| = |H/(P \cap H)|$

PROOF: Second Isomorphism Theorem.

$\langle 1 \rangle 5$ .  $PH$  is a  $p$ -group.

$\langle 2 \rangle 1$ . ASSUME: for a contradiction  $q$  is prime,  $q \mid |PH|$  and  $q \neq p$

- $\langle 2 \rangle 2. q \mid |PH/P|$
- $\langle 2 \rangle 3. q \mid |H/(P \cap H)|$
- $\langle 2 \rangle 4. q \mid |H|$
- $\langle 2 \rangle 5. \text{Q.E.D.}$

PROOF: This contradicts the fact that  $H$  is a  $p$ -group,  $\langle 1 \rangle 1.$

- $\langle 1 \rangle 6. PH = P$

PROOF: By maximality of  $P$ .

- $\langle 1 \rangle 7. H \subseteq P$

□

**Lemma 9.51.** *Let  $p$  be a prime. Let  $G$  be a finite group. Let  $P$  be a  $p$ -Sylow subgroup of  $G$ . Let  $P$  act by conjugation on the set of  $p$ -Sylow subgroups of  $G$ . Then  $P$  is the unique fixed point of this action.*

PROOF:

- $\langle 1 \rangle 1. P$  is a fixed point of this action.

PROOF: For any  $x \in P$  we have  $xPx^{-1} = P$ .

- $\langle 1 \rangle 2. \text{If } Q \text{ is any fixed point of the action then } Q = P.$

$\langle 2 \rangle 1. \text{LET: } Q \text{ be a fixed point of the action.}$

$\langle 2 \rangle 2. \text{For all } x \in P \text{ we have } xQx^{-1} = Q.$

$\langle 2 \rangle 3. P \subseteq N_G(Q)$

$\langle 2 \rangle 4. P \subseteq Q$

PROOF: Lemma 9.50.

$\langle 2 \rangle 5. P = Q$

PROOF: Since  $|P| = |Q|$ .

□

**Theorem 9.52** (Third Sylow Theorem). *Let  $p$  be a prime. Let  $G$  be a finite group of order  $p^r m$  where  $p$  does not divide  $m$ . Then the number of  $p$ -Sylow subgroups of  $G$  divides  $m$  and is congruent to 1 modulo  $p$ .*

PROOF:

- $\langle 1 \rangle 1. \text{LET: } N_p \text{ be the number of } p\text{-Sylow subgroups of } G.$

- $\langle 1 \rangle 2. \text{PICK a } p\text{-Sylow subgroup } P.$

PROOF: One exists by the First Sylow Theorem.

- $\langle 1 \rangle 3. \text{The } p\text{-Sylow subgroups of } G \text{ are exactly the conjugates of } P.$

PROOF: Second Sylow Theorem

- $\langle 1 \rangle 4. m = N_p [N_G(P) : P]$

PROOF: Since  $N_p = [G : N_G(P)]$  by Proposition 9.47.

- $\langle 1 \rangle 5. N_p \text{ divides } m.$

- $\langle 1 \rangle 6. mN_p \equiv m \pmod{p}$

$\langle 2 \rangle 1. m \equiv [N_G(P) : P] \pmod{p}$

PROOF: Lemma 9.48.

$\langle 2 \rangle 2. mN_p \equiv m \pmod{p}$

PROOF: By  $\langle 1 \rangle 4.$

- $\langle 1 \rangle 7. N_p \equiv 1 \pmod{p}$

□

PROOF:

- <1>1. LET:  $N_p$  be the number of  $p$ -Sylow subgroups of  $G$ .  
 <1>2. PICK a  $p$ -Sylow subgroup  $P$  of  $G$ .  
 PROOF: First Sylow Theorem.  
 <1>3.  $N_p$  is the number of conjugates of  $P$ .  
 PROOF: Second Sylow Theorem.  
 <1>4.  $N_p \mid m$   
 PROOF: Corollary 9.47.1.  
 <1>5.  $P$  acts on the set of conjugates of  $P$  with one fixed point.  
 PROOF: Lemma 9.51.  
 <1>6.  $N_p \equiv 1 \pmod{p}$   
 PROOF: Corollary 9.18.1.

□

**Corollary 9.52.1.** *Let  $G$  be a finite group. Let  $p$  be a prime number. If  $|G| = mp^r$  and the only divisor  $d$  of  $m$  such that  $d \equiv 1 \pmod{p}$  is  $d = 1$ , then  $G$  is not simple.*

PROOF: There must be 1  $p$ -Sylow subgroup, which has order  $p^r$  and is normal.  
□

**Corollary 9.52.2.** *Let  $G$  be a finite group. Let  $p$  be a prime number. If  $|G| = mp^r$  where  $1 < m < p$  then  $G$  is not simple.*

**Proposition 9.53.** *Let  $p$  and  $q$  be prime numbers with  $p < q$ . Let  $G$  be a group of order  $pq$  with a normal subgroup  $H$  of order  $p$ . Then  $G$  is cyclic.*

PROOF:

- <1>1. LET:  $\gamma : G \rightarrow \text{Aut}_{\mathbf{Grp}}(H)$  be the action of conjugation.  
 <1>2.  $H$  is cyclic of order  $p$ .  
 <1>3.  $|\text{Aut}_{\mathbf{Grp}}(H)| = p - 1$   
 <1>4.  $|\text{im } \gamma| \mid pq$   
 PROOF: Since  $\text{im } \gamma$  is a quotient group of  $G$ .  
 <1>5.  $|\text{im } \gamma| \mid p - 1$   
 <1>6.  $|\text{im } \gamma| = 1$   
 <1>7.  $\gamma = 0$   
 <1>8.  $H \subseteq Z(G)$   
 <1>9.  $G$  is Abelian.

PROOF: Lemma 9.28.

- <1>10. PICK an element  $g$  of order  $p$ .  
 PROOF: Cauchy's Theorem.  
 <1>11. PICK an element  $h$  of order  $q$ .  
 PROOF: Cauchy's Theorem.  
 <1>12.  $|gh| = pq$   
 PROOF: Proposition 6.22.

□

PROOF:

- <1>1. ASSUME: w.l.o.g.  $q \not\equiv 1 \pmod{p}$

PROOF: Since the only non-cyclic group of order 6 is  $S_3$  which does not have a normal subgroup of order 2.

$\langle 1 \rangle 2$ . PICK a subgroup  $K$  of order  $q$ .

$\langle 1 \rangle 3$ .  $K$  is normal.

PROOF: Since  $K$  is the unique  $q$ -Sylow subgroup by the Third Sylow Theorem.

$\langle 1 \rangle 4$ .  $H \cap K = \{e\}$

$\langle 1 \rangle 5$ .  $HK \cong H \times K$

PROOF: Proposition ??.

$\langle 1 \rangle 6$ .  $|HK| = pq$

$\langle 1 \rangle 7$ .  $HK = G$

$\langle 1 \rangle 8$ .  $G \cong \mathbb{Z}/pq\mathbb{Z}$

PROOF:

$$\begin{aligned} G &\cong H \times K \\ &\cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ &\cong \mathbb{Z}/pq\mathbb{Z} \end{aligned}$$

□

**Corollary 9.53.1.** *Let  $p$  and  $q$  be prime numbers with  $p < q$  and  $q \not\equiv 1 \pmod{p}$ . Then the only group of order  $pq$  is the cyclic group.*

PROOF: By the Third Sylow Theorem, such a group must have exactly one  $p$ -Sylow subgroup, which is therefore normal. □

**Proposition 9.54.** *Let  $p$  be prime. Let  $G$  be a finite group. Let  $P$  be a  $p$ -Sylow subgroup of  $G$ . Then*

$$N_G(N_G(P)) = N_G(P) \ .$$

PROOF:

$\langle 1 \rangle 1$ .  $P$  is normal in  $N_G(P)$ .

PROOF: Proposition 9.46.

$\langle 1 \rangle 2$ .  $N_G(P)$  is normal in  $N_G(N_G(P))$ .

PROOF: Proposition 9.46.

$\langle 1 \rangle 3$ .  $P$  is normal in  $N_G(N_G(P))$ .

PROOF: Corollary 7.116.1.

$\langle 1 \rangle 4$ .  $N_G(N_G(P)) \subseteq N_G(P)$

PROOF: Proposition 9.46.

$\langle 1 \rangle 5$ .  $N_G(N_G(P)) = N_G(P)$

□

**Proposition 9.55.** *Let  $p, q$  and  $r$  be three distinct prime numbers. Then there is no simple group of order  $pqr$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $G$  be a group of order  $pqr$ .

$\langle 1 \rangle 2$ . ASSUME: w.l.o.g.  $p < q < r$

$\langle 1 \rangle 3$ . ASSUME: for a contradiction  $G$  is simple.

$\langle 1 \rangle 4$ . The number of subgroups of order  $p$  is at least  $p + 1$ .

PROOF: Third Sylow Theorem

(1)5. The number of subgroups of order  $q$  is at least  $q + 1$ .

PROOF: Third Sylow Theorem

(1)6. The number of subgroups of order  $r$  is  $pq$ .

PROOF: By the Third Sylow Theorem, the number divides  $pq$ , and it cannot be 1 (lest that subgroup be normal) or  $p$  or  $q$  (as these are less than  $r$  hence not congruent to 1 modulo  $r$ ).

(1)7. There are at least  $p^2 - 1$  elements of order  $p$ .

(1)8. There are at least  $q^2 - 1$  elements of order  $q$ .

(1)9. There are at least  $pqr - pq$  elements of order  $r$ .

(1)10. Q.E.D.

PROOF: This is a contradiction as the total number of elements of order 1,  $p$ ,  $q$  and  $r$  is

$$\begin{aligned} 1 + (p^2 - 1) + (q^2 - 1) + (pqr - pq) &= p^2 + q^2 + pqr - pq - 1 \\ &> pqr + p^2 - 1 \\ &> pqr \end{aligned}$$

□

**Proposition 9.56.** *Let  $G$  be a finite simple group. Let  $H$  be a subgroup of  $G$  of index  $N > 1$ . Then  $|G|$  divides  $N!$ .*

PROOF:

(1)1. PICK a subgroup  $K$  of  $H$  that is normal in  $G$  such that  $[G : K]$  divides  $\gcd(|G|, N!)$ .

(1)2.  $K = \{e\}$

(1)3.  $[G : K] = |G|$

(1)4.  $|G|$  divides  $N!$

□

**Corollary 9.56.1.** *Let  $G$  be a finite simple group. Let  $p$  be a prime factor of  $|G|$ . Let  $N_p$  be the number of  $p$ -Sylow subgroups of  $G$ . Then  $|G|$  divides  $N_p!$ .*

PROOF: Since  $N_p = [G : N_G(P)]$  and  $N_p > 1$  since  $G$  is simple. □

**Definition 9.57** (Centralizer). Let  $G$  be a group and  $A \subseteq G$ . The *centralizer* of  $A$  is

$$Z_G(A) := \{g \in G : \forall a \in A. gag^{-1} = a\}.$$

**Proposition 9.58.** *Let  $H$  and  $K$  be subgroups of  $G$  with  $H \subseteq N_G(K)$ . Then the function  $\gamma : H \rightarrow \text{Aut}_{\mathbf{Grp}}(K)$  defined by conjugation*

$$\gamma_h(k) = hkh^{-1}$$

*is a homomorphism of groups with  $\ker \gamma = H \cap Z_G(K)$ .*

PROOF:

(1)1. For all  $g, h \in H$  we have  $\gamma_{gh} = \gamma_g \circ \gamma_h$ .

PROOF: Since  $\gamma_{gh}(k) = \gamma_g(\gamma_h(k)) = ghkh^{-1}g^{-1}$ .

(1)2. For all  $h \in H$  we have  $\gamma_h = \text{id}_K$  iff  $h \in Z_G(K)$ .

PROOF: Both are equivalent to  $\forall k \in K. hkh^{-1} = k$ , i.e.  $\forall k \in K. hk = kh$ .

□

## 9.7 Nilpotent Groups

**Definition 9.59** (Nilpotent). Let  $G$  be a group. Define inductively a sequence  $(Z_n)$  of subgroups of  $G$  by  $Z_0 = \{e\}$ , and  $Z_{i+1}$  is the inverse image under  $\pi$  of the center of  $G/Z_i$ .

Then  $G$  is *nilpotent* iff  $Z_n = G$  for some  $n$ .

We prove this is well-defined by proving that, for all  $i$ , we have  $Z_i$  is normal in  $G$ .

PROOF:

$\langle 1 \rangle 1$ . ASSUME: as induction hypothesis  $Z_i$  is normal in  $G$ .

PROVE:  $Z_{i+1}$  is normal in  $G$ .

$\langle 1 \rangle 2$ . LET:  $x \in Z_{i+1}$  and  $g \in G$

PROVE:  $gxg^{-1} \in Z_{i+1}$

PROVE: For all  $h \in G$  we have  $gxg^{-1}hZ_i = hgxg^{-1}Z_i$

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

$\langle 1 \rangle 4$ .  $gxg^{-1}hZ_i = hgxg^{-1}Z_i$

PROOF:

$$\begin{aligned} gxg^{-1}hZ_i &= gg^{-1}hxZ_i \\ &= hxZ_i \\ &= hgg^{-1}xZ_i \\ &= hgxg^{-1}Z_i \end{aligned}$$

□

**Proposition 9.60.** *Every Abelian group is nilpotent.*

PROOF: Let  $G$  be an Abelian group. The center of  $G/Z_0$  is  $G/Z_0$ , hence  $Z_1 = G$ .

□

**Example 9.61.** The semidirect product of two nilpotent groups is not necessarily nilpotent.  $S_3$  is the semidirect product of  $\mathbb{Z}/2\mathbb{Z}$  and  $\mathbb{Z}/3\mathbb{Z}$  but is not nilpotent.

**Proposition 9.62.** *Let  $G$  be a group. Then  $G$  is nilpotent if and only if  $G/Z(G)$  is nilpotent.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $(Z_n)$  be the sequence of subgroups of  $G$  where  $Z_0 = \{e\}$  and  $Z_{n+1}$  is the inverse image of the center of  $G/Z_n$ .

$\langle 1 \rangle 2$ .  $G/Z_0 \cong G$

$\langle 1 \rangle 3$ .  $Z_1 = Z(G)$

$\langle 1 \rangle 4$ . The corresponding sequence of subgroups for  $G/Z(G)$  is  $G/Z(G)$ ,  $Z_2/Z(G)$ ,  $Z_3/Z(G)$ ,  $\dots$

$\langle 1 \rangle 5$ .  $G$  is nilpotent iff  $G/Z(G)$  is nilpotent.

PROOF: Both are equivalent to  $\exists n. Z_n = G$  and to  $\exists n. Z_n/Z(G) = G/Z(G)$ .

□

**Proposition 9.63.** *Every  $p$ -group is nilpotent.*

PROOF: Each  $Z_n$  is a  $p$ -group and so has non-trivial center, hence each  $Z_{n+1}$  is larger than  $Z_n$  and so the sequence must terminate.  $\square$

**Proposition 9.64.** *Every nilpotent group is solvable.*

PROOF: Let  $(Z_n)$  be the defining sequence of subgroups. Then  $Z_{n+1}/Z_n = Z(G/Z_n)$  is Abelian for all  $n$ , hence the group is solvable by Proposition 8.42.  $\square$

**Example 9.65.** The converse is not true —  $S_3$  is solvable but not nilpotent.

**Proposition 9.66.** *Let  $G$  be a nilpotent group. Then every nontrivial normal subgroup of  $G$  intersects  $Z(G)$  non-trivially.*

PROOF:

- $\langle 1 \rangle 1$ . LET:  $H$  be a nontrivial normal subgroup of  $G$ .
- $\langle 1 \rangle 2$ . LET:  $(Z_n)$  be the sequence of subgroups with  $Z_0 = \{e\}$  and  $Z_{n+1}$  the inverse image of  $Z(G/Z_n)$ .
- $\langle 1 \rangle 3$ . LET:  $r$  be least such that  $H \cap Z_r \neq \{e\}$ .
- $\langle 1 \rangle 4$ . PICK  $h \in H \cap Z_r$  with  $h \neq e$ .
- $\langle 1 \rangle 5$ .  $hZ_{r-1} \in Z(G/Z_{r-1})$
- $\langle 1 \rangle 6$ . For all  $g \in G$  we have  $ghZ_{r-1} = hgZ_{r-1}$
- $\langle 1 \rangle 7$ . For all  $g \in G$  we have  $ghg^{-1}h^{-1} \in Z_{r-1}$
- $\langle 1 \rangle 8$ . For all  $g \in G$  we have  $ghg^{-1}h^{-1} = e$
- PROOF: Since  $ghg^{-1}h^{-1} \in H$  and  $H \cap Z_{r-1} = \{e\}$ .
- $\langle 1 \rangle 9$ . For all  $g \in G$  we have  $gh = hg$
- $\langle 1 \rangle 10$ .  $h \in H \cap Z(G)$

$\square$

**Example 9.67.** We cannot weaken the hypothesis to  $G$  being solvable.  $S_3$  is solvable and  $\mathbb{Z}/2\mathbb{Z}$  is a nontrivial normal subgroup but its intersection with  $Z(S_3)$  is just  $\{e\}$ .

**Proposition 9.68.** *Let  $G$  be a finite nilpotent group. Let  $H$  be a proper subgroup of  $G$ . Then  $H \subsetneq N_G(H)$ .*

PROOF:

- $\langle 1 \rangle 1$ . ASSUME: as induction hypothesis the theorem holds for all groups smaller than  $G$ .
- $\langle 1 \rangle 2$ .  $Z(G)$  is non-trivial.
- $\langle 1 \rangle 3$ . CASE:  $Z(G) \not\subseteq H$ 
  - $\langle 2 \rangle 1$ . PICK  $g \in Z(G) - H$
  - $\langle 2 \rangle 2$ .  $g \in N_G(H) - H$
- $\langle 1 \rangle 4$ . CASE:  $Z(G) \subseteq H$ 
  - $\langle 2 \rangle 1$ .  $H/Z(G) \subsetneq N_{G/Z(G)}(H/Z(G))$
  - PROOF: By induction hypothesis  $\langle 1 \rangle 1$ .
  - $\langle 2 \rangle 2$ . PICK  $g$  such that  $gZ(G) \in N_{G/Z(G)}(H/Z(G)) - H/Z(G)$
  - $\langle 2 \rangle 3$ .  $g \in N_G(H)$
  - $\langle 3 \rangle 1$ . LET:  $h \in H$



PROVE:  $ghg^{-1} \in H$

$\langle 3 \rangle 2$ .  $ghg^{-1}Z(G) \in H/Z(G)$

$\langle 3 \rangle 3$ . PICK  $h_1 \in H$  such that  $ghg^{-1}Z(G) = h_1Z(G)$

$\langle 3 \rangle 4$ .  $ghg^{-1}h_1^{-1} \in Z(G)$

$\langle 3 \rangle 5$ .  $ghg^{-1}h_1^{-1} \in H$

PROOF:  $\langle 1 \rangle 4$

$\langle 3 \rangle 6$ .  $ghg^{-1} \in H$

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

□

**Corollary 9.68.1.** *Let  $G$  be a finite group. Then  $G$  is nilpotent if and only if every Sylow subgroup of  $G$  is normal.*

PROOF:

$\langle 1 \rangle 1$ . If  $G$  is nilpotent then every Sylow subgroup of  $G$  is normal.

$\langle 2 \rangle 1$ . ASSUME:  $G$  is nilpotent.

$\langle 2 \rangle 2$ . LET:  $P$  be Sylow subgroup of  $G$

$\langle 2 \rangle 3$ .  $N_G(P) = N_G(N_G(P))$

PROOF: Proposition 9.54.

$\langle 2 \rangle 4$ .  $N_G(P) = G$

PROOF: Proposition 9.68.

$\langle 2 \rangle 5$ .  $P$  is normal.

$\langle 1 \rangle 2$ . If every Sylow subgroup of  $G$  is normal then  $G$  is nilpotent.

$\langle 2 \rangle 1$ . ASSUME: As induction hypothesis the result holds for all groups smaller than  $G$ .

$\langle 2 \rangle 2$ . ASSUME: Every Sylow subgroup of  $G$  is normal.

$\langle 2 \rangle 3$ . LET:  $P_1, \dots, P_r$  be the nontrivial Sylow subgroups of  $G$ .

$\langle 2 \rangle 4$ .  $G \cong P_1 \times \dots \times P_r$

PROOF: Proposition 7.117.

$\langle 2 \rangle 5$ . ASSUME: w.l.o.g.  $r > 1$

PROOF: The case  $r = 1$  holds by Proposition 9.63.

$\langle 2 \rangle 6$ .  $Z(G) \cong Z(P_1) \times \dots \times Z(P_r)$

PROOF: Proposition 9.34.

$\langle 2 \rangle 7$ .  $G/Z(G) \cong P_1/Z(P_1) \times \dots \times P_r/Z(P_r)$

PROOF: Proposition 7.60.

$\langle 2 \rangle 8$ . The nontrivial Sylow subgroups of  $G/Z(G)$  are  $P_1/Z(P_1), \dots, P_r/Z(P_r)$ .

$\langle 2 \rangle 9$ . Every Sylow subgroup of  $G/Z(G)$  is normal.

$\langle 2 \rangle 10$ .  $|G/Z(G)| < |G|$

PROOF: Because of Corollary 9.38.2.

$\langle 2 \rangle 11$ .  $G/Z(G)$  is nilpotent.

PROOF: By the induction hypothesis ??.

$\langle 2 \rangle 12$ .  $G$  is nilpotent.

PROOF: Proposition 9.62.

□

## 9.8 Symmetric Groups

**Proposition 9.69.** *Every permutation in  $S_n$  is the product of a unique set of disjoint cycles.*

PROOF: Since any permutation acts as a cycle on any of its orbits.  $\square$

**Corollary 9.69.1.** *The transpositions generate  $S_n$ .*

PROOF: Since any cycle is a product of transpositions:

$$(a_1 a_2 \cdots a_n) = (a_1 a_n) \circ \cdots \circ (a_1 a_3) \circ (a_1 a_2). \square$$

**Corollary 9.69.2.**  *$S_n$  is generated by  $(1\ 2)$  and  $(1\ 2\ 3\ \cdots\ n)$ .*

PROOF:

$\langle 1 \rangle$ 1. Any transposition of the form  $(i\ i+1)$  is in the subgroup generated by these two permutations.

PROOF: It is  $(1\ 2\ \cdots\ n)^i(1\ 2)(1\ 2\ \cdots\ n)^{-i}$ .

$\langle 1 \rangle$ 2. Any transposition of the form  $(1\ i)$  is in the subgroup generated by these two permutations.

PROOF: It is  $(i-1\ i) \cdots (3\ 4)(2\ 3)(1\ 2)(2\ 3) \cdots (i-1\ i)$ .

$\langle 1 \rangle$ 3. Any transposition is in the subgroup generated by these two permutations.

PROOF: Since  $(i\ j) = (1\ i)(1\ j)(1\ i)$

$\langle 1 \rangle$ 4. These two permutations generate  $S_n$ .

PROOF: By the previous Corollary.

$\square$

**Definition 9.70** (Type). For any  $\sigma \in S_n$ , the *type* of  $\sigma$  is the partition of  $n$  consisting of the sizes of the orbits of  $\sigma$ .

**Proposition 9.71.** *Two permutations in  $S_n$  are conjugate if and only if they have the same type.*

PROOF:

$\langle 1 \rangle$ 1. Two permutations that are conjugate have the same type.

PROOF: Since

$$\tau(a_1 a_2 \cdots a_r)(b_1 b_2 \cdots b_s) \cdots (c_1 c_2 \cdots c_t) \tau^{-1} = (\tau(a_1) \tau(a_2) \cdots \tau(a_r))(\tau(b_1) \tau(b_2) \cdots \tau(b_s)) \cdots (\tau(c_1) \tau(c_2) \cdots \tau(c_t))$$

$\langle 1 \rangle$ 2. Two permutations with the same type are conjugate.

$\langle 2 \rangle$ 1. LET:  $\rho = (a_1 a_2 \cdots a_r)(b_1 b_2 \cdots b_s) \cdots (c_1 c_2 \cdots c_t)$  and  $\sigma = (a'_1 a'_2 \cdots a'_r)(b'_1 b'_2 \cdots b'_s) \cdots (c'_1 c'_2 \cdots c'_t)$

$\langle 2 \rangle$ 2. LET:  $\tau$  be the permutation  $\tau(a_i) = a'_i, \tau(b_i) = b'_i, \dots, \tau(c_i) = c'_i$

$\langle 2 \rangle$ 3.  $\sigma = \tau \rho \tau^{-1}$

$\square$

**Corollary 9.71.1.** *The number of conjugacy classes in  $S_n$  equals the number of partitions of  $n$ .*

**Definition 9.72** (Sign). Define  $\Delta_n \in \mathbb{Z}[x_1, \dots, x_n]$  by

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

Define an action of  $S_n$  on  $\mathbb{Z}[x_1, \dots, x_n]$  by

$$\sigma p(x_1, \dots, x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)}) .$$

The *sign* of a permutation  $\sigma \in S_n$  is the number  $\epsilon(\sigma) \in \{1, -1\}$  such that

$$\sigma \Delta_n = \epsilon(\sigma) \Delta_n .$$

We say  $\sigma$  is *even* if  $\epsilon(\sigma) = 1$  and *odd* if  $\epsilon(\sigma) = -1$ .

**Proposition 9.73.**  $\epsilon$  is a group homomorphism  $S_n \rightarrow \mathbb{Z}^*$ .

PROOF:

$\langle 1 \rangle 1$ . LET:  $\rho, \sigma \in S_n$

$\langle 1 \rangle 2$ .  $(\rho \circ \sigma) \Delta_n = \rho(\sigma \Delta_n)$

$\langle 1 \rangle 3$ .  $\epsilon(\rho \circ \sigma) \Delta_n = \epsilon(\rho) \epsilon(\sigma) \Delta_n$

$\langle 1 \rangle 4$ .  $\epsilon(\rho \circ \sigma) = \epsilon(\rho) \epsilon(\sigma)$

□

**Proposition 9.74.** Let  $\sigma = \tau_1 \cdots \tau_r$  where each  $\tau_i$  is a transposition. Then  $\sigma$  is even if and only if  $r$  is even.

PROOF: Since every transposition is odd and  $\epsilon$  is a homomorphism, we have  $\epsilon(\tau_1 \cdots \tau_r) = (-1)^r$ . □

**Corollary 9.74.1.** A cycle is even if and only if its length is odd.

### 9.8.1 Transitive Subgroups

**Definition 9.75** (Transitive). A subgroup of  $S_n$  is *transitive* iff its action on  $\{1, \dots, n\}$  is transitive.

**Proposition 9.76.** If  $G$  is a transitive subgroup of  $S_n$  then  $n \mid |G|$ .

PROOF: By Proposition 9.18 we have

$$n = [G : \text{Stab}_G(1)]$$

and so  $n \mid |G|$ . □

## 9.9 Alternating Groups

**Definition 9.77.** Let  $n \in \mathbb{N}$ . The *alternating group*  $A_n$  is the subgroup of  $S_n$  consisting of the even permutations.

We call  $A_5$  the *icosahedral (rotating) group*.

**Proposition 9.78.** For  $n \geq 2$  we have  $A_n$  is normal in  $S_n$  and

$$[S_n : A_n] = 2 .$$

PROOF: Since  $\epsilon : S_n \rightarrow \{1, -1\}$  is a homomorphism with kernel  $A_n$ . □

**Proposition 9.79.** *Let  $n \geq 2$  and  $\sigma \in A_n$ . Let  $[\sigma]_{A_n}$  be the conjugacy class of  $\sigma$  in  $A_n$ , and  $[\sigma]_{S_n}$  the conjugacy class of  $\sigma$  in  $S_n$ . Then:*

1. *If  $Z_{S_n}(\sigma) \subseteq A_n$  then  $|[\sigma]_{S_n}| = 2|[\sigma]_{A_n}|$ .*
2. *If not then  $[\sigma]_{S_n} = [\sigma]_{A_n}$ .*

PROOF:

$$\langle 1 \rangle 1. Z_{A_n}(\sigma) = A_n \cap Z_{S_n}(\sigma)$$

$$\langle 1 \rangle 2. |[\sigma]_{S_n}| = [S_n : Z_{S_n}(\sigma)]$$

PROOF: Orbit-Stabilizer Theorem.

$$\langle 1 \rangle 3. |[\sigma]_{A_n}| = [A_n : Z_{A_n}(\sigma)]$$

PROOF: Orbit-Stabilizer Theorem.

$$\langle 1 \rangle 4. \text{ If } Z_{S_n}(\sigma) \subseteq A_n \text{ then } |[\sigma]_{S_n}| = 2|[\sigma]_{A_n}|.$$

PROOF:

$$\begin{aligned} |[\sigma]_{S_n}| &= [S_n : Z_{S_n}(\sigma)] \\ &= [S_n : A_n][A_n : Z_{S_n}(\sigma)] \\ &= 2|[\sigma]_{A_n}| \end{aligned}$$

$$\langle 1 \rangle 5. \text{ If } Z_{S_n}(\sigma) \not\subseteq A_n \text{ then } [\sigma]_{S_n} = [\sigma]_{A_n}.$$

$$\langle 2 \rangle 1. \text{ ASSUME: } Z_{S_n}(\sigma) \not\subseteq A_n$$

$$\langle 2 \rangle 2. A_n Z_{S_n}(\sigma) = S_n$$

PROOF: Since  $A_n \subseteq A_n Z_{S_n}(\sigma)$  and  $[S_n : A_n] = 2$ .

$$\langle 2 \rangle 3. |[\sigma]_{S_n}| = |[\sigma]_{A_n}|$$

PROOF:

$$\begin{aligned} |[\sigma]_{S_n}| &= [S_n : Z_{S_n}(\sigma)] \\ &= [A_n Z_{S_n}(\sigma) : Z_{S_n}(\sigma)] \\ &= [A_n : A_n \cap Z_{S_n}(\sigma)] \quad (\text{Second Isomorphism Theorem}) \\ &= [A_n : Z_{A_n}(\sigma)] \\ &= |[\sigma]_{A_n}| \end{aligned}$$

□

**Proposition 9.80.** *Let  $n \geq 2$ . Let  $\sigma \in A_n$ . Then  $|[\sigma]_{S_n}| = 2|[\sigma]_{A_n}|$  if and only if the type of  $\sigma$  consists of distinct odd numbers.*

PROOF:

$$\langle 1 \rangle 1. \text{ If } |[\sigma]_{S_n}| = 2|[\sigma]_{A_n}| \text{ then the type of } \sigma \text{ consists of distinct odd numbers.}$$

$$\langle 2 \rangle 1. \text{ If the type of } \sigma \text{ has an even number then } Z_{S_n}(\sigma) \not\subseteq A_n.$$

PROOF: If  $(a_1 a_2 \cdots a_n)$  is an even cycle that is a factor of  $\sigma$  then  $(1 2 \cdots n)$  is an odd permutation in  $Z_{S_n}(\sigma)$ .

$$\langle 2 \rangle 2. \text{ If the type of } \sigma \text{ has an odd number repeated then } Z_{S_n}(\sigma) \not\subseteq A_n.$$

PROOF: If  $(a_1 a_2 \cdots a_n)$  and  $(b_1 b_2 \cdots b_n)$  are two distinct odd factors of  $\sigma$  then  $(a_1 b_1)(a_2 b_2) \cdots (a_n b_n)$  is an odd permutation in  $Z_{S_n}(\sigma)$ .

$$\langle 2 \rangle 3. \text{ Q.E.D.}$$

PROOF: Proposition 9.79

$$\langle 1 \rangle 2. \text{ If the type of } \sigma \text{ consists of distinct odd numbers then } |[\sigma]_{S_n}| = 2|[\sigma]_{A_n}|.$$

- ⟨2⟩1. LET:  $\sigma = (a_{11} \cdots a_{1\lambda_1})(b_{21} \cdots b_{2\lambda_2}) \cdots (c_{n1} \cdots c_{n\lambda_n})$  where the  $\lambda_i$  are all odd and distinct.  
 ⟨2⟩2. LET:  $\tau \in Z_{S_n}(\sigma)$   
 PROVE:  $\tau$  is even.  
 ⟨2⟩3.  $(\tau(a_{i1}) \cdots \tau(a_{i\lambda_i})) = (\tau_{i1} \cdots \tau_{i\lambda_i})$   
 ⟨2⟩4. The action of  $\tau$  on  $\{a_{i1}, \dots, a_{i\lambda_i}\}$  is  $(a_{i1} \cdots a_{i\lambda_i})^{r_i}$  for some  $r_i$   
 ⟨2⟩5.  $\tau = \prod_{i=1}^n (a_{i1} \cdots a_{i\lambda_i})^{r_i}$   
 ⟨2⟩6.  $\tau$  is even.

□

**Corollary 9.80.1.**  $A_5$  is simple.

PROOF:

- ⟨1⟩1. ASSUME: for a contradiction  $G$  is a non-trivial proper normal subgroup of  $A_5$ .  
 ⟨1⟩2.  $|G|$  is one of 2, 3, 4, 5, 6, 10, 12, 15, 20 or 30.  
 ⟨1⟩3. There are conjugacy classes in  $A_5$  whose sizes total to 1, 2, 3, 4, 5, 9, 11, 14, 19 or 29.  
 ⟨1⟩4. The types of the even permutations in  $S_5$  are  $[1, 1, 1, 1, 1]$ ,  $[2, 2, 1]$ ,  $[3, 1, 1]$  and  $[5]$ .  
 ⟨1⟩5. The size of the conjugacy class of type  $[2, 2, 1]$  in  $S_5$  is 15.  
 PROOF: There are 5 ways to choose the element not in the 2-cycles, and then 3 ways to arrange the other 4 elements into two 2-cycles.  
 ⟨1⟩6. The size of the conjugacy class of type  $[2, 2, 1]$  in  $A_5$  is 15.  
 PROOF: Proposition 9.80.  
 ⟨1⟩7. The size of the conjugacy class of type  $[3, 1, 1]$  in  $S_5$  is 20.  
 PROOF: There are 10 ways to choose the three elements in the 3-cycle, and then two 3-cycles that they can form.  
 ⟨1⟩8. The size of the conjugacy class of type  $[3, 1, 1]$  in  $A_5$  is 20.  
 PROOF: Proposition 9.80.  
 ⟨1⟩9. The size of the conjugacy class of type  $[5]$  in  $S_5$  is 24.  
 PROOF: There are four choices for the value at 1, then three choices for its value, then two choices for its value, then one choice for its value.  
 ⟨1⟩10. The size of the conjugacy class of type  $[5]$  in  $S_5$  is 12.  
 PROOF: Proposition 9.80.  
 ⟨1⟩11. Q.E.D.  
 PROOF: This contradicts ⟨1⟩3.

□

**Proposition 9.81.**  $A_6$  is simple.

PROOF:

- ⟨1⟩1. ASSUME: for a contradiction  $G$  is a non-trivial proper normal subgroup of  $A_6$ .  
 ⟨1⟩2.  $|G|$  is one of 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180.  
 ⟨1⟩3. There are conjugacy classes in  $A_6$  whose sizes total to 1, 2, 3, 4, 5, 7, 8, 9, 11, 14, 17, 19, 23, 29, 35, 39, 44, 59, 71, 89, 119 or 179.

- ⟨1⟩4. The types of the even permutations in  $S_6$  are  $[1, 1, 1, 1, 1, 1]$ ,  $[2, 2, 1, 1]$ ,  $[3, 1, 1, 1]$ ,  $[3, 3]$ ,  $[4, 2]$ ,  $[5, 1]$ .  
 ⟨1⟩5. The size of the conjugacy class of type  $[2, 2, 1, 1]$  in  $S_6$  is 45.  
 ⟨1⟩6. The size of the conjugacy class of type  $[2, 2, 1, 1]$  in  $A_6$  is 45.  
 ⟨1⟩7. The size of the conjugacy class of type  $[3, 1, 1, 1]$  in  $S_6$  is 40.  
 ⟨1⟩8. The size of the conjugacy class of type  $[3, 1, 1, 1]$  in  $A_6$  is 40.  
 ⟨1⟩9. The size of the conjugacy class of type  $[3, 3]$  in  $S_6$  is 80.  
 ⟨1⟩10. The size of the conjugacy class of type  $[3, 3]$  in  $A_6$  is 80.  
 ⟨1⟩11. The size of the conjugacy class of type  $[4, 2]$  in  $S_6$  is 90.  
 ⟨1⟩12. The size of the conjugacy class of type  $[4, 2]$  in  $A_6$  is 90.  
 ⟨1⟩13. The size of the conjugacy class of type  $[5, 1]$  in  $S_6$  is 144.  
 ⟨1⟩14. The size of the conjugacy class of type  $[5, 1]$  in  $A_6$  is 72.  
 ⟨1⟩15. The size of the conjugacy class of type  $[6]$  in  $S_6$  is 120.  
 ⟨1⟩16. The size of the conjugacy class of type  $[6]$  in  $A_6$  is 120.  
 ⟨1⟩17. Q.E.D.

PROOF: This is a contradiction.

□

**Proposition 9.82.** *The icosahedral group  $A_5$  is the group of symmetries of an icosahedron obtained through rigid motions.*

PROOF: Routine. □

**Proposition 9.83.** *The alternating group  $A_n$  is generated by 3-cycles.*

PROOF:

- ⟨1⟩1. The product of two transpositions is generated by 3-cycles.  
 ⟨2⟩1.  $(ab)(ab) = e$   
 ⟨2⟩2.  $(ab)(ac) = (acb)$  for  $b \neq c$   
 ⟨2⟩3.  $(ab)(cd) = (adc)(abc)$  for  $c \neq d$  and  $c, d \notin \{a, b\}$

□

**Proposition 9.84.** *Let  $n \geq 5$ . If a normal subgroup of  $A_n$  contains a 3-cycle, then it contains all 3-cycles.*

PROOF:

- ⟨1⟩1. LET:  $N$  be a normal subgroup of  $A_n$ .  
 ⟨1⟩2. LET:  $(abc) \in N$   
 ⟨1⟩3.  $N$  contains the conjugacy class of  $(abc)$ .  
 ⟨1⟩4. The conjugacy class of  $(abc)$  in  $N$  is the same as its conjugacy class in  $S_n$ .  
 PROOF: Proposition 9.80 since the type of  $(abc)$  is  $[3, 1, 1, \dots]$ .  
 ⟨1⟩5.  $N$  contains all 3-cycles.

□

**Proposition 9.85.** *For  $n \geq 4$ , the center of  $A_n$  is trivial.*

**Theorem 9.86.** *For  $n \geq 5$ , the alternating group  $A_n$  is simple.*

PROOF:

$\langle 1 \rangle 1.$   $A_5$  is simple.

PROOF: Corollary 9.80.1.

$\langle 1 \rangle 2.$  For  $n \geq 6$  we have  $A_n$  is simple.

$\langle 2 \rangle 1.$  LET:  $n \geq 6$

$\langle 2 \rangle 2.$  LET:  $N$  be a nontrivial normal subgroup of  $A_n$ .

$\langle 2 \rangle 3.$   $N$  contains a 3-cycle.

$\langle 3 \rangle 1.$  PICK  $\tau \in N$  such that  $\tau \neq \text{id}$  and  $\tau$  acts on at most 6 elements.

$\langle 3 \rangle 2.$  PICK  $T \subseteq \{1, \dots, n\}$  with  $|T| = 6$  such that  $\tau$  acts on  $T$ .

$\langle 3 \rangle 3.$  Consider  $A_6$  as a subgroup of  $A_n$  by letting it act on  $T$ .

$\langle 3 \rangle 4.$   $N \cap A_6$  is normal.

$\langle 3 \rangle 5.$   $N \cap A_6$  is nontrivial.

$\langle 3 \rangle 6.$   $N \cap A_6 = A_6$

PROOF: Proposition 9.81.

$\langle 3 \rangle 7.$   $N$  contains a 3-cycle.

$\langle 2 \rangle 4.$   $N$  contains all 3-cycles.

PROOF: Proposition 9.84.

$\langle 2 \rangle 5.$   $N = A_n$

PROOF: Proposition 9.83.

□

**Corollary 9.86.1.** For  $n \geq 5$ , we have  $S_n$  is unsolvable.

PROOF: Since the composition factors of  $S_n$  are  $C_2$  and  $A_n$ . □





# Chapter 10

## Extensions

**Definition 10.1** (Extension). Let  $G$ ,  $N$  and  $H$  be groups. Then  $G$  is an *extension* of  $H$  by  $N$  iff there exist homomorphisms  $\phi : N \rightarrow G$  and  $\psi : G \rightarrow H$  such that

$$1 \rightarrow N \xrightarrow{\phi} G \xrightarrow{\psi} H \rightarrow 1$$

is an exact sequence; i.e.  $\phi$  is injective,  $\psi$  is surjective, and  $\text{im } \phi = \ker \psi$ .

**Proposition 10.2.** *Let  $G$  be an extension of  $H$  by  $N$ . Then the composition factors of  $G$  are the union of the composition factors of  $H$  and the composition factors of  $N$ .*

PROOF: From Proposition 7.131 since  $H \cong G/N$ .  $\square$

**Definition 10.3** (Split Extension). An exact sequence of groups

$$1 \rightarrow N \xrightarrow{\phi} G \xrightarrow{\psi} H \rightarrow 1$$

*splits* iff  $H$  is a subgroup of  $G$  and  $N \cap H = \{e\}$ .

**Example 10.4.** The sequence

$$0 \rightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

is exact but does not split as there is no subgroup of  $\mathbb{Z}$  isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ .

**Proposition 10.5.** *Let  $N$  be a normal subgroup of  $G$  and let  $H$  be a subgroup such that  $G = NH$  and  $N \cap H = \{e\}$ . Then  $G$  is a split extension of  $H$  by  $N$ .*

PROOF:

$\langle 1 \rangle$ 1.  $G/N \cong H$

$\langle 2 \rangle$ 1. LET:  $\alpha$  be the homomorphism  $H \hookrightarrow G \twoheadrightarrow G/N$

$\langle 2 \rangle$ 2.  $\alpha$  is injective.

PROOF: Since  $\ker \alpha = \{e\}$

$\langle 2 \rangle$ 3.  $\alpha$  is surjective.

PROOF: For all  $g \in G$ , pick  $n \in N$  and  $h \in H$  such that  $g^{-1} = nh$ . Then  $gN = \alpha(h^{-1})$ .

$\langle 2 \rangle 4$ .  $\alpha : H \cong G/N$  is an isomorphism.

$\langle 1 \rangle 2$ . The exact sequence  $1 \rightarrow N \rightarrow G \twoheadrightarrow G/N \cong H \rightarrow 1$  splits.

□

**Proposition 10.6.** *Let  $N$  and  $H$  be groups. Let  $\theta : H \rightarrow \text{Aut}_{\mathbf{Grp}}(N)$  be a homomorphism. The sequence*

$$1 \rightarrow N \rightarrow N \rtimes_{\theta} H \rightarrow H \rightarrow 1$$

*is split exact.*

PROOF: Easy. □

## Chapter 11

# Classification of Groups

**Example 11.1.**     • The only group of order 1 is the trivial group.

- The only group of order 2 is  $C_2$ .
- The only group of order 3 is  $C_3$ .
- There are two groups of order 4:  $C_4$  and  $C_2 \times C_2$ .
- The only group of order 5 is  $C_5$ .
- There are two groups of order 6:  $C_6$  and  $S_3$ .
- The only group of order 7 is  $C_7$ .
- There are two groups of order 9:  $C_9$  and  $C_3 \times C_3$ .
- There are two groups of order 10:  $C_{10}$  and  $D_{10}$ .
- The only group of order 11 is  $C_{11}$ .
- The only group of order 13 is  $C_{13}$ .
- There are two groups of order 14:  $C_{14}$  and  $D_{14}$ .
- The only group of order 15 is  $C_{15}$ .

**Proposition 11.2.** *The only non-Abelian groups of order 8 are  $D_8$  and  $Q_8$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $G$  be a non-Abelian group of order 8.

$\langle 1 \rangle 2$ .  $G$  has no element of order 8.

PROOF: If it does then it is  $C_8$  and hence Abelian.

$\langle 1 \rangle 3$ . PICK an element  $y$  of order 4.

$\langle 2 \rangle 1$ . PICK an element  $a$  of order 2.

$\langle 2 \rangle 2$ .  $G/\langle a \rangle$  is isomorphic to  $C_4$  or  $C_2 \times C_2$ .

$\langle 2 \rangle 3$ . PICK an element  $y\langle a \rangle$  of order 2 in  $G/\langle a \rangle$

$\langle 2 \rangle 4. y^2 \in \langle a \rangle$

$\langle 2 \rangle 5. \text{ CASE:}$

$$y^2 = a$$

PROOF: In this case  $y$  is of order 4.

$\langle 2 \rangle 6. \text{ CASE:}$

$$y^2 = e$$

PROOF: In this case  $G \cong C_2^3$  which is Abelian.

$\langle 1 \rangle 4. \text{ PICK } x \notin \langle y \rangle \text{ such that } x^2 = e \text{ or } x^2 = y^2$

$\langle 2 \rangle 1. G/\langle y \rangle \cong C_2$

$\langle 2 \rangle 2. \text{ PICK } x\langle y \rangle \in G/\langle y \rangle \text{ of order 2.}$

$\langle 2 \rangle 3. x^2 \in \langle y \rangle$

$\langle 2 \rangle 4. x^2 \neq y \text{ and } x^2 \neq y^3$

$\langle 2 \rangle 5. x^2 = e \text{ or } x^2 = y^2$

$\langle 1 \rangle 5. xy = y^3x$

$\langle 2 \rangle 1. xy \neq e$

PROOF: Since  $y^{-1} = y^3 \neq x$ .

$\langle 2 \rangle 2. xy \neq y$

PROOF:  $xy = y$  implies  $x = e$ .

$\langle 2 \rangle 3. xy \neq y^2$

PROOF:  $xy = y^2$  implies  $x = y$ .

$\langle 2 \rangle 4. xy \neq y^3$

PROOF:  $xy = y^3$  implies  $x = y^2$ .

$\langle 2 \rangle 5. xy \neq x$

PROOF:  $xy = x$  implies  $y = e$ .

$\langle 2 \rangle 6. xy \neq yx$

PROOF:  $xy = yx$  implies  $G$  is Abelian.

$\langle 2 \rangle 7. xy \neq y^2x$

$\langle 3 \rangle 1. \text{ ASSUME: for a contradiction } xy = y^2x$

$\langle 3 \rangle 2. xy^2 = x$

PROOF:

$$\begin{aligned} xy^2 &= y^2xy \\ &= y^4x \\ &= x \end{aligned}$$

$\langle 3 \rangle 3. y^2 = e$

$\langle 1 \rangle 6. \text{ The multiplication table of } G \text{ is one of the following.}$

$e$	$y$	$y^2$	$y^3$	$x$	$yx$	$y^2x$	$y^3x$
$y$	$y^2$	$y^3$	$e$	$yx$	$y^2x$	$y^3x$	$x$
$y^2$	$y^3$	$e$	$y$	$y^2x$	$y^3x$	$x$	$yx$
$y^3$	$e$	$y$	$y^2$	$y^3x$	$x$	$yx$	$y^2x$
$x$	$y^3x$	$y^2x$	$yx$	$e$	$y^3$	$y^2$	$y$
$yx$	$x$	$y^3x$	$y^2x$	$y$	$e$	$y^3$	$y^2$
$y^2x$	$yx$	$x$	$y^3x$	$y^2$	$y$	$e$	$y^3$
$y^3x$	$y^2x$	$yx$	$x$	$y^3$	$y^2$	$y$	$e$

$e$	$y$	$y^2$	$y^3$	$x$	$yx$	$y^2x$	$y^3x$
$y$	$y^2$	$y^3$	$e$	$yx$	$y^2x$	$y^3x$	$x$
$y^2$	$y^3$	$e$	$y$	$y^2x$	$y^3x$	$x$	$yx$
$y^3$	$e$	$y$	$y^2$	$y^3x$	$x$	$yx$	$y^2x$
$x$	$y^3x$	$y^2x$	$yx$	$y^2$	$y$	$e$	$y^3$
$yx$	$x$	$y^3x$	$y^2x$	$y^3$	$y^2$	$y$	$e$
$y^2x$	$yx$	$x$	$y^3x$	$e$	$y^3$	$y^2$	$y$
$y^3x$	$y^2x$	$yx$	$x$	$y$	$e$	$y^3$	$y^2$

$\langle 1 \rangle 7. G \cong D_8$  or  $G \cong Q_8$ .

□

**Proposition 11.3.** *Let  $q$  be an odd prime. Then  $D_{2q}$  is the only non-Abelian group of order  $2q$ .*

PROOF:

$\langle 1 \rangle 1.$  LET:  $G$  be a non-Abelian group of order  $2q$ .

$\langle 1 \rangle 2.$  PICK  $y \in G$  of order  $q$ .

PROOF: Cauchy's Theorem

$\langle 1 \rangle 3.$   $\langle y \rangle$  is the only subgroup of order  $q$ .

PROOF: Third Sylow Theorem

$\langle 1 \rangle 4.$   $\langle y \rangle$  is normal.

$\langle 1 \rangle 5.$  PICK  $x \in G - \langle y \rangle - \{e\}$

$\langle 1 \rangle 6.$   $|x| = 2$

PROOF: We cannot have  $|x| = 2q$  since  $G$  is not cyclic, and  $|x| \neq q$  since  $\langle x \rangle$  is not the subgroup of order  $q$ .

$\langle 1 \rangle 7.$   $xyx^{-1} \in \langle y \rangle$

PROOF: Since  $x\langle y \rangle x^{-1} = \langle y \rangle$  by  $\langle 1 \rangle 3$ .

$\langle 1 \rangle 8.$  PICK  $r$  such that  $0 \leq r < q$  and  $xyx^{-1} = y^r$ .

$\langle 1 \rangle 9.$   $y^{r^2} = y$

PROOF:

$$y^{r^2} = (xyx^{-1})^r \quad (\langle 1 \rangle 8)$$

$$= xy^r x^{-1}$$

$$= x^2 y x^{-2} \quad (\langle 1 \rangle 8)$$

$$= y \quad (\langle 1 \rangle 6)$$

$\langle 1 \rangle 10.$   $q \mid (r-1)(r+1)$

PROOF: Since  $y^{(r-1)(r+1)} = e$  and  $|y| = q$  by  $\langle 1 \rangle 2$ .

$\langle 1 \rangle 11.$   $r = 1$  or  $r = q-1$

PROOF: Since  $0 \leq r < q$  by  $\langle 1 \rangle 8$ .

$\langle 1 \rangle 12.$   $r \neq 1$

$\langle 2 \rangle 1.$  ASSUME: for a contradiction  $r = 1$ .

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

PROOF:  $\langle 1 \rangle 8$

$\langle 2 \rangle 3.$   $|xy| = 2q$

PROOF: Proposition 6.22

$\langle 2 \rangle 4.$   $G$  is cyclic.

$\langle 2 \rangle 5.$  Q.E.D.

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

$\langle 1 \rangle 13$ .  $x^2 = e$  and  $y^q = e$  and  $yx = xy^{q-1}$

$\langle 1 \rangle 14$ .  $G \cong D_{2q}$

□

**Corollary 11.3.1.** *For  $q$  an odd prime, the only groups of order  $2q$  are  $C_{2q}$  and  $D_{2q}$ .*

**Proposition 11.4.** *There is no non-Abelian simple group of order less than 60.*

PROOF: We rule out the other sizes as follows:

- 1 — Only group is the trivial group.
- 2 — Prime therefore cyclic
- 3 — Prime therefore cyclic
- 4 — Corollary 9.49.1
- 5 — Prime therefore cyclic
- 6 — Corollary 9.52.2
- 7 — Prime therefore cyclic
- 8 — Corollary 9.49.1
- 9 — Corollary 9.49.1
- 10 — Corollary 9.52.2
- 11 — Prime therefore cyclic
- 12 —

$\langle 1 \rangle 1$ . There is no simple non-Abelian group of order 12.

$\langle 2 \rangle 1$ . ASSUME: for a contradiction  $G$  is a simple non-Abelian group of order 12.

$\langle 2 \rangle 2$ .  $G$  has 4 3-Sylow subgroups.

$\langle 2 \rangle 3$ .  $G$  has 8 elements of order 3.

$\langle 2 \rangle 4$ .  $G$  has 3 elements of order 2 or 4.

$\langle 2 \rangle 5$ .  $G$  has one 2-Sylow subgroup.

$\langle 2 \rangle 6$ . The 2-Sylow subgroup of  $G$  is normal.

$\langle 2 \rangle 7$ . Q.E.D.

PROOF: This contradicts  $\langle 2 \rangle 1$ .

- 13 — Prime therefore cyclic
- 14 — Corollary 9.52.2
- 15 — Corollary 9.52.2

- 16 — Corollary 9.49.1
  - 17 — Prime therefore cyclic
  - 18 — Corollary 9.52.2
  - 19 — Prime therefore cyclic
  - 20 — Corollary 9.52.2
  - 21 — Corollary 9.52.2
  - 22 — Corollary 9.52.2
  - 23 — Prime therefore cyclic
  - 24 —
- (1)2. There is no simple non-Abelian group of order 24.
- ⟨2⟩1. ASSUME: for a contradiction  $G$  is a simple non-Abelian group of order 24.
- ⟨2⟩2.  $G$  has 3 2-Sylow subgroups.
- ⟨2⟩3. LET:  $\gamma : G \rightarrow S_3$  be the action of conjugation of  $G$  on the set of 2-Sylow subgroups.
- ⟨2⟩4.  $\ker \gamma \neq \{e\}$   
PROOF:  $\gamma$  cannot be injective since  $|G| > |S_3|$ .
- ⟨2⟩5.  $\ker \gamma \neq G$
- ⟨2⟩6.  $\ker \gamma$  is a proper non-trivial normal subgroup of  $G$ .
- ⟨2⟩7. Q.E.D.  
PROOF: This contradicts ⟨2⟩1.
- 25 — Corollary 9.49.1
  - 26 — Corollary 9.52.2
  - 27 — Corollary 9.49.1
  - 28 — Corollary 9.52.2
  - 29 — Prime therefore cyclic
  - 30 — Proposition 9.55
  - 31 — Prime therefore cyclic
  - 32 — Corollary 9.49.1
  - 33 — Corollary 9.52.2
  - 34 — Corollary 9.52.2
  - 35 — Corollary 9.52.2

- 36 —

⟨1⟩3. There is no simple non-Abelian group of order 36.

⟨2⟩1. ASSUME: for a contradiction  $G$  is a simple non-Abelian group of order 36.

⟨2⟩2.  $G$  has 4 3-Sylow subgroups.

⟨2⟩3. LET:  $\gamma : G \rightarrow S_4$  be the action of conjugation of  $G$  on the set of 2-Sylow subgroups.

⟨2⟩4.  $\ker \gamma \neq \{e\}$

PROOF:  $\gamma$  cannot be injective since  $|G| > |S_4|$ .

⟨2⟩5.  $\ker \gamma \neq G$

⟨2⟩6.  $\ker \gamma$  is a proper non-trivial normal subgroup of  $G$ .

⟨2⟩7. Q.E.D.

PROOF: This contradicts ⟨2⟩1.

- 37 — Prime therefore cyclic

- 38 — Corollary 9.52.2

- 39 — Corollary 9.52.2

- 40 — There can be only 1 5-Sylow subgroup.

- 41 — Prime therefore cyclic

- 42 — Proposition 9.55

- 43 — Prime therefore cyclic

- 44 — Corollary 9.52.2

- 45 — There can be only 1 5-Sylow subgroup.

- 46 — Corollary 9.52.2

- 47 — Prime therefore cyclic

- 48 —

⟨1⟩4. There is no simple non-Abelian group of order 48.

⟨2⟩1. ASSUME: for a contradiction  $G$  is a simple non-Abelian group of order 48.

⟨2⟩2.  $G$  has 3 2-Sylow subgroups.

⟨2⟩3. LET:  $\gamma : G \rightarrow S_3$  be the action of conjugation of  $G$  on the set of 2-Sylow subgroups.

⟨2⟩4.  $\ker \gamma \neq \{e\}$

PROOF:  $\gamma$  cannot be injective since  $|G| > |S_3|$ .

⟨2⟩5.  $\ker \gamma \neq G$

⟨2⟩6.  $\ker \gamma$  is a proper non-trivial normal subgroup of  $G$ .

⟨2⟩7. Q.E.D.

PROOF: This contradicts ⟨2⟩1.



- 49 — Corollary 9.49.1
- 50 — Corollary 9.52.2
- 51 — Corollary 9.52.2
- 52 — Corollary 9.52.2
- 53 — Prime therefore cyclic
- 54 — Corollary 9.52.2
- 55 — Corollary 9.52.2
- 56 — Corollary 9.52.2
- 57 — Corollary 9.52.2
- 58 — Corollary 9.52.2
- 59 — Prime therefore cyclic

**Proposition 11.5.** *Every simple group of order 60 has a subgroup of index 5.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $G$  be a simple group of order 60.

$\langle 1 \rangle 2$ . The number of 2-Sylow subgroups of  $G$  is either 5 or 15.

$\langle 2 \rangle 1$ . LET:  $n$  be the number of 2-Sylow subgroups.

$\langle 2 \rangle 2$ .  $60 \mid n!$

PROOF: Corollary 9.56.1.

$\langle 2 \rangle 3$ .  $n \geq 5$

$\langle 2 \rangle 4$ .  $n \mid 15$

PROOF: Third Sylow Theorem

$\langle 2 \rangle 5$ .  $n = 5$  or  $n = 15$

$\langle 1 \rangle 3$ . ASSUME: w.l.o.g.  $G$  has 15 2-Sylow subgroups.

$\langle 1 \rangle 4$ .  $G$  has 4 or 10 3-Sylow subgroups.

$\langle 1 \rangle 5$ .  $G$  has 10 3-Sylow subgroups.

PROOF: Corollary 9.56.1.

$\langle 1 \rangle 6$ .  $G$  has exactly 6 5-Sylow subgroups.

$\langle 1 \rangle 7$ . The number of elements of order 3 is 20.

$\langle 1 \rangle 8$ . The number of elements of order 5 is 24.

$\langle 1 \rangle 9$ . The number of elements of order 2 or 4 is 15.

$\langle 1 \rangle 10$ . PICK two 2-Sylow subgroups  $H_1$  and  $H_2$  with non-trivial intersection.

$\langle 1 \rangle 11$ . LET:  $g \in G$  be such that  $H_1 \cap H_2 = \{e, g\}$ .

$\langle 1 \rangle 12$ . LET:  $K = Z_G(H_1 \cap H_2)$

$\langle 1 \rangle 13$ .  $|K| = 12$  or  $|K| = 20$

PROOF: We have  $4 \mid |K|$  since  $H_1 \leq K$ , and  $|K| \geq 6$  since  $H_1 \cup H_2 \subseteq K$ . We also have  $|K| \mid 60$ .

$\langle 1 \rangle 14$ .  $[G : K] \neq 3$

PROOF: There cannot be an embedding of  $G$  in  $S_3$ .

$\langle 1 \rangle 15. [G : K] = 5$

□

**Theorem 11.6.**  $A_5$  is the only simple group of order 60.

PROOF:

$\langle 1 \rangle 1.$  LET:  $G$  be a simple group of order 60.

$\langle 1 \rangle 2.$  PICK a subgroup  $K$  of  $G$  of index 5.

$\langle 1 \rangle 3.$  LET:  $\phi : G \rightarrow S_5$  be the action of  $G$  on  $G/K$  of left multiplication.

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

PROOF: Since  $\ker \phi$  is a proper normal subgroup of  $G$  hence  $\ker \phi = \{e\}$ .

$\langle 1 \rangle 5.$   $\phi(G)$  is a subgroup of  $S_5$  of index 2.

$\langle 1 \rangle 6.$   $\phi(G)$  is normal in  $S_5$ .

$\langle 1 \rangle 7.$   $\phi(G) \cap A_5$  is a normal subgroup of  $A_5$

$\langle 1 \rangle 8.$   $\phi(G) \cap A_5 = \{e\}$  or  $\phi(G) \cap A_5 = A_5$

PROOF: Corollary 9.80.1.

$\langle 1 \rangle 9.$   $\phi(G) \cap A_5 = A_5$

PROOF: We cannot have  $\phi(G) \cap A_5 = \{e\}$  lest

$$|\phi(G)A_5| = |\phi(G)||A_5|/|\phi(G) \cap A_5| = 3600$$

by the Second Isomorphism Theorem.

$\langle 1 \rangle 10.$   $\phi(G) = A_5$

$\langle 1 \rangle 11.$   $\phi : G \cong A_5$

□

**Proposition 11.7.** There is no non-Abelian simple group of order between 60 and 168.

PROOF: We rule out the other sizes as follows:

- 61 — prime therefore cyclic
- 62 — Corollary 9.52.2
- 63 — Corollary 9.52.1
- 64 — Corollary 9.49.1
- 65 — Corollary 9.52.2
- 66 — Corollary 9.52.2
- 67 — prime therefore cyclic
- 68 — Corollary 9.52.2
- 69 — Corollary 9.52.2
- 70 — Proposition 9.55
- 71 — prime therefore cyclic
- 72

(1)1. There is no simple non-Abelian group of order 72

PROOF:

(2)1. ASSUME: for a contradiction  $G$  is a simple non-Abelian group of order 72.

(2)2.  $G$  has 4 3-Sylow subgroups.

(2)3. LET:  $\gamma : G \rightarrow S_4$  be the action of conjugation on the set of 3-Sylow subgroups.

(2)4.  $\ker \gamma \neq 1$

PROOF: Since  $|G| > |S_4|$ .

(2)5.  $\ker \gamma$  is a non-trivial proper subgroup of  $G$ .

(2)6. Q.E.D.

PROOF: This is a contradiction.

- 73 — prime therefore cyclic
- 74 — Corollary 9.52.2
- 75 — Corollary 9.52.2
- 76 — Corollary 9.52.2
- 77 — Corollary 9.52.2
- 78 — Corollary 9.52.2
- 79 — prime therefore cyclic
- 80

(1)2. There is no simple non-Abelian group of order 80.

PROOF:

(2)1. ASSUME: for a contradiction  $G$  is a simple non-Abelian group of order 80.

(2)2.  $G$  has 5 2-Sylow subgroups.

(2)3. LET:  $\gamma : G \rightarrow S_5$  be the action of conjugation on the set of 2-Sylow subgroups.

(2)4.  $\ker \gamma \neq 1$

PROOF: Otherwise  $\text{im } \gamma$  would be a subgroup of  $S_5$  of order 80, contradicting Lagrange's Theorem.

(2)5.  $\ker \gamma$  is a non-trivial normal subgroup of  $G$ .

(2)6. Q.E.D.

PROOF: This is a contradiction.

- 81 — Corollary 9.49.1
- 82 — Corollary 9.52.2
- 83 — prime therefore cyclic
- 84 — Corollary 9.52.1

- 85 — Corollary 9.52.2
- 86 — Corollary 9.52.2
- 87 — Corollary 9.52.2
- 88 — Corollary 9.52.2
- 89 — prime therefore cyclic
- 90 — Corollary 9.52.1
- 91 — Corollary 9.52.2
- 92 — Corollary 9.52.2
- 93 — Corollary 9.52.2
- 94 — Corollary 9.52.2
- 95 — Corollary 9.52.2
- 96 — There are 3 2-Sylow subgroups. The kernel of the action of conjugation  $G \rightarrow S_3$  is a non-trivial normal subgroup of  $G$ .
- 97 — prime therefore cyclic
- 98 — Corollary 9.52.2
- 99 — Corollary 9.52.2
- 100 — Corollary 9.52.2
- 101 — prime therefore cyclic
- 102 — Proposition 9.55
- 103 — prime therefore cyclic
- 104 — Corollary 9.52.2
- 105 — Proposition 9.55
- 106 — Corollary 9.52.2
- 107 — prime therefore cyclic
- 108 — There are 4 3-Sylow subgroups. The kernel of the action of conjugation  $G \rightarrow S_4$  is a non-trivial normal subgroup of  $G$ .
- 109 — prime therefore cyclic
- 110 — Proposition 9.55
- 111 — Corollary 9.52.2

- 112

⟨1⟩3. There is no simple non-Abelian group of order 112.

⟨2⟩1. ASSUME: for a contradiction  $G$  is a simple non-Abelian group of order 112.

⟨2⟩2.  $G$  has exactly 7 2-Sylow subgroups.

⟨2⟩3. LET:  $\gamma : G \rightarrow A_7$  be the action of conjugation of  $G$  on the set of 2-Sylow subgroups.

PROOF:  $\gamma(g)$  is always an even permutation since  $G$  has no subgroup of index 2.

⟨2⟩4.  $\ker \gamma \neq 1$

PROOF: Since  $|G|$  does not divide  $|A_7| = 7!/2$ .

⟨2⟩5.  $\ker \gamma$  is a non-trivial normal subgroup of  $G$ .

⟨2⟩6. Q.E.D.

- 113 — prime therefore cyclic

- 114 — Proposition 9.55

- 115 — Corollary 9.52.2

- 116 — Corollary 9.52.2

- 117 — Corollary 9.52.2

- 118 — Corollary 9.52.2

- 119 — Corollary 9.52.2

- 120

⟨1⟩4. There is no simple non-Abelian group of order 120.

PROOF:

⟨2⟩1. ASSUME: for a contradiction  $G$  is a simple non-Abelian group of order 120.

⟨2⟩2. There are exactly 6 5-Sylow subgroups.

⟨2⟩3. LET:  $\gamma : G \rightarrow A_6$  be the action of conjugation on the set of 5-Sylow subgroups.

⟨2⟩4.  $\text{im } \gamma$  is a subgroup of  $A_6$  of order 120.

⟨2⟩5. Q.E.D.

PROOF: This is a contradiction by inspection of the list of subgroups of  $A_6$ .

- 121 — Corollary 9.49.1

- 122 — Corollary 9.52.2

- 123 — Corollary 9.52.2

- 124 — Corollary 9.52.2

- 125 — Corollary 9.49.1
- 126 — Corollary 9.52.1
- 127 — prime therefore cyclic
- 128 — Corollary 9.49.1
- 129 — Corollary 9.52.2
- 130 — Proposition 9.55
- 131 — prime therefore cyclic
- 132
  - (1)5. There is no simple non-Abelian group of order 132.
  - ⟨2⟩1. ASSUME: for a contradiction  $G$  is a simple non-Abelian group of order 132.
  - ⟨2⟩2. There are at least 4 3-Sylow subgroups.
  - ⟨2⟩3. There are at least 8 elements of order 3.
  - ⟨2⟩4. There are exactly 12 11-Sylow subgroups.
  - ⟨2⟩5. There are exactly 120 elements of order 11.
  - ⟨2⟩6. There are exactly 3 elements of order 2.
  - ⟨2⟩7. There is a unique 2-Sylow subgroups.
  - ⟨2⟩8. Q.E.D.
  - PROOF: This is a contradiction.
- 133 — Corollary 9.52.2
- 134 — Corollary 9.52.2
- 135 — Corollary 9.52.1
- 136 — Corollary 9.52.2
- 137 — prime therefore cyclic
- 138 — Proposition 9.55
- 139 — prime therefore cyclic
- 140 — Corollary 9.52.1
- 141 — Corollary 9.52.2
- 142 — Corollary 9.52.2
- 143 — Corollary 9.52.2
- 144 — Burnside's Theorem
- 145 — Burnside's Theorem

- 146 — Burnside's Theorem
- 147 — Burnside's Theorem
- 148 — Burnside's Theorem
- 149 — prime therefore cyclic
- 150 — There are exactly 6 5-Sylow subgroups. The kernel of the action of conjugation  $G \rightarrow A_5$  is a non-trivial normal subgroup since 150 does not divide  $|A_5| = 60$ .
- 151 — prime therefore cyclic
- 152 — Burnside's Theorem
- 153 — Burnside's Theorem
- 154 — Proposition 9.55
- 155 — Burnside's Theorem
- 156 — Corollary 9.52.2
- 157 — prime therefore cyclic
- 158 — Burnside's Theorem
- 159 — Burnside's Theorem
- 160 — Burnside's Theorem
- 161 — Burnside's Theorem
- 162 — Burnside's Theorem
- 163 — prime therefore cyclic
- 164 — Burnside's Theorem
- 165 — Proposition 9.55
- 166 — Burnside's Theorem
- 167 — prime therefore cyclic

**Proposition 11.8.** *Every group of order  $< 120$  and  $\neq 60$  is solvable.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $G$  be a group of order  $n$  where  $n < 120$  and  $n \neq 60$ .

$\langle 1 \rangle 2$ . If  $n$  is odd then  $G$  is solvable.

PROOF: Feit-Thompson Theorem

$\langle 1 \rangle 3$ . If  $n$  has at most two prime factors then  $G$  is solvable.

PROOF: Burnside's Theorem

$\langle 1 \rangle 4$ . CASE:  $n = pqr$  for some primes  $p, q, r$

PROOF: Its composition factors must be  $C_p, C_q$  and  $C_r$ .

$\langle 1 \rangle 5$ . CASE:  $n = 84$

PROOF: By the Third Sylow Theorem, the 7-Sylow subgroup is normal. Since every group of order 12 is solvable, so is every group of order 84.

□



**Part IV**

**Ring Theory**



# Chapter 12

## Rngs

**Definition 12.1** (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 12.2.**     • 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 12.3.** *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 12.4** (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 12.5.**  $0$  is a left- and right-zero-divisor in every non-zero rng.

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

**Proposition 12.6.** *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  $b \neq 0$

$\square$

## 12.1 Commutative Rings

**Definition 12.7** (Commutative). A ring  $R$  is *commutative* iff  $\forall x, y \in R. xy = yx$ .

**Example 12.8.** • The zero ring 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 ring  $\mathcal{P}S$  is commutative.
- If  $R$  is commutative then  $R^S$  is commutative.

## 12.2 Ring Homomorphisms

**Definition 12.9.** Let  $R$  and  $S$  be rings. A *ring 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 rings and ring homomorphisms.

## 12.3 Quaternions

**Definition 12.10** (Norm). The *norm* of a quaternion is defined by

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



# Chapter 13

## Rings

**Definition 13.1** (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 13.2.**     • 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 13.3.** *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 13.4.** *In any ring we have  $(-1)x = -x$ .*

PROOF: Since

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

$\square$

### 13.1 Units

**Definition 13.5** (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 13.6.** *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 13.7.** *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 13.8.** *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 13.9.** *No right-unit is a left-zero-divisor.*

PROOF: Similar. □

**Proposition 13.10.** *The inverse of a unit is unique.*

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

**Proposition 13.11.** *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 13.12** (Group of Units). For any ring  $R$ , we write  $R^*$  for the group of the units of  $R$  under multiplication.

**Example 13.13.** The quaternionic group is a subgroup of  $\mathbb{H}^*$ .

**Example 13.14.** 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 13.15** (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 13.16.** 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 13.17.** *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 13.18.**  $(\mathbb{Z}/12\mathbb{Z})^*$  is not cyclic. Its elements are 1, 5, 7 and 11 with orders 1, 2, 2 and 2.

**Theorem 13.19** (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 6.23.

$\langle 1 \rangle 2$ . 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 13.20.** *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 13.21.** *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  $\alpha(n) = nr \pmod{p}$ .

$\langle 1 \rangle 5$ .  $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$

□

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

**Proposition 13.22.** *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 13.23** (Euler's Totient Function). For  $n$  a positive integer, let  $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ .

**Proposition 13.24.** *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 13.25.** *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 13.26.** *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 13.27** (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 13.28.**

$$|\text{Aut}_{\mathbf{Grp}}(C_n)| = \phi(n)$$

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 13.29.**

$$\text{Aut}_{\mathbf{Grp}}(\mathbb{Z}) \cong C_2$$

PROOF: The only automorphisms are the identity and multiplication by -1.  $\square$

### 13.3 Nilpotent Elements

**Definition 13.30** (Nilpotent). Let  $R$  be a ring and  $a \in R$ . Then  $a$  is *nilpotent* iff there exists  $n$  such that  $a^n = 0$ .

**Proposition 13.31.** *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 13.32.**  *$m$  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 14

# Ring Homomorphisms

**Definition 14.1** (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 14.2.** *The zero-ring is terminal in **Ring**.*

PROOF: Easy.  $\square$

**Proposition 14.3.** *The ring  $\mathbb{Z}$  is initial in **Ring**.*

PROOF: Easy.  $\square$

**Proposition 14.4.** *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 14.5.** 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 14.6.** 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 14.7.** *Ring homomorphisms preserve units.*

PROOF: If  $uv = 1$  then  $\phi(u)\phi(v) = 1$ .  $\square$

**Proposition 14.8.** *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 14.9.** 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 14.10.**

$$\text{End}_{\mathbf{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$$

The isomorphism maps any group endomorphism  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$  to  $\phi(1)$ .

**Example 14.11.** The group of units of  $\text{End}_{\mathbf{Ab}}(G)$  is  $\text{Aut}_{\mathbf{Ab}}(G)$ .

**Example 14.12.** 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.  $\square$

## 14.1 Products

**Proposition 14.13.** *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 15

## Subrings

**Definition 15.1** (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 15.2.** *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 15.2.1.** *The zero ring is not a subring of any non-zero ring.*

**Proposition 15.3.** *Let  $\phi : R \rightarrow S$  be a ring homomorphism. Then  $\phi(R)$  is a subring of  $S$ .*

PROOF: Easy.  $\square$

### 15.1 Centralizer

**Definition 15.4** (Centralizer). Let  $R$  be a ring and  $a \in R$ . The *centralizer* of  $a$  is  $\{r \in R : ar = ra\}$ .

**Proposition 15.5.** *The centralizer of  $a$  is a subring of  $R$ .*

PROOF: Easy.  $\square$

### 15.2 Center

**Definition 15.6** (Center). The *center* of a ring  $R$  is  $\{x \in R : \forall y \in R. xy = yx\}$ .

**Proposition 15.7.** *The center of a ring is a subring.*

PROOF: Easy.  $\square$

**Proposition 15.8.** *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 15.8.1.** *If  $R$  is a commutative ring then  $R$  is isomorphic to the center of  $\text{End}_{\mathbf{Ab}}(R)$ .*

**Example 15.9.** 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 16

# Monoid Rings

**Definition 16.1** (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

$$\sum_{m \in M} a_m m ,$$

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 16.2.** 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.

### 16.1 Polynomials

**Definition 16.3** (Polynomial). Let  $R$  be a ring. The ring of *polynomials*  $R[x]$  is  $R[\mathbb{N}]$ . We write

$$\sum_n a_n x^n \text{ for } \sum_n a_n n .$$

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

$$\sum_{n=0}^{N-1} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1} .$$

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 16.4.** *For any ring  $R$ , the set of polynomials  $R[x]$  is a ring.*

PROOF: Easy.  $\square$

**Definition 16.5** (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 16.6.** *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 16.7.** *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  $p(j(0), j(1), \dots, j(n-1))$ .  $\square$

**Proposition 16.8.** *Let  $\alpha : R \rightarrow S$  be a ring homomorphism. Let  $s \in S$  commute with  $\alpha(r)$  for all  $r \in R$ . Then there exists a unique ring homomorphism  $\bar{\alpha} : R[x] \rightarrow S$  such that  $\bar{\alpha}(x) = s$  and the following diagram commutes:*

$$\begin{array}{ccc} R[x] & \xrightarrow{\bar{\alpha}} & S \\ \uparrow & \nearrow \alpha & \\ R & & \end{array}$$

PROOF: The map  $\bar{\alpha}$  is given by

$$\bar{\alpha}(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n) = \alpha(a_0) + \alpha(a_1)s + \alpha(a_2)s^2 + \cdots + \alpha(a_n)s^n .$$

$\square$

**Definition 16.9.** 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 16.10.**  $\mathbb{Z}[x, y]$  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 16.11.**  $\mathbb{Z}[x, y]$  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 16.12.** A polynomial is *monic* iff its last non-zero coefficient is 1.

**Proposition 16.13.** A monic polynomial is not a left- or right-zero-divisor.

PROOF: Easy.  $\square$

**Proposition 16.14.** Let  $R$  be a ring. Let  $f, g \in R[x]$  with  $f$  monic. Then there exist unique polynomials  $q, r \in R[x]$  with  $\deg r < \deg f$  such that

$$g = qf + r \text{ .}$$

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

$$ax^n = ax^{n-d}f + h \text{ .}$$

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

$$ax^n = qf + h \text{ .}$$

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  $a_i x^i = q_i f + h_i$

$\langle 1 \rangle 6$ .  $g = (\sum_{i=d+1}^n q_i) f + \sum_{i=d+1}^n h_i$

$\langle 1 \rangle 7$ .  $q$  and  $r$  are unique.

PROOF: If  $q_1 f + r_1 = q_2 f + r_2$  then  $r_1 - r_2 = (q_2 - q_1)f$  and so  $r_1 - r_2 = (q_2 - q_1)f = 0$  since  $\deg(r_1 - r_2) < \deg f$ .

$\square$

## 16.2 Laurent Polynomials

**Definition 16.15** (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  $\sum_n a_n n$ .

### 16.3 Power Series

**Definition 16.16** (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 16.17.** *For any ring  $R$ , the set of power series  $R[[x]]$  is a ring.*

PROOF: Easy.  $\square$

**Proposition 16.18.** *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 17

## Ideals

**Definition 17.1** (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 17.2.** 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 17.3.** 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 17.4.** 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 17.5.** 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 17.6.** 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 17.7.** 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 17.8.** 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 17.8.1.** Let  $\phi : R \rightarrow S$  be a ring homomorphism. Then  $\ker \phi$  is an ideal in  $R$ .

**Definition 17.9** (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 17.10.** 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 17.11.** 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 17.11.1.** Every ring homomorphism  $\phi : R \rightarrow S$  decomposes as follows.



$$\begin{array}{ccccc}
 & & \phi & & \\
 & \nearrow & & \searrow & \\
 R & \twoheadrightarrow & R/\ker \phi & \xrightarrow{\cong} & \operatorname{im} \phi & \hookrightarrow S
 \end{array}$$

**Corollary 17.11.2** (First Isomorphism Theorem). *Let  $\phi : R \rightarrow S$  be a surjective ring homomorphism. Then*

$$S \cong R/\ker \phi .$$

**Theorem 17.12** (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 17.12.1.** *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 17.13.** *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 17.13.1.** *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 17.14.** *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 17.15.** *The intersection of a set of ideals is an ideal.*

PROOF: Easy.  $\square$

## 17.1 Characteristic

**Definition 17.16** (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 17.17.** *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 17.18.** The zero ring is the only ring with characteristic 1.

## 17.2 Nilradical

**Definition 17.19** (Nilradical). Let  $R$  be a commutative ring. The *nilradical* of  $R$  is the set of all nilpotent elements.

**Proposition 17.20.** *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 17.21.** 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.

## 17.3 Principal Ideals

**Definition 17.22** (Principal Ideal). Let  $R$  be a commutative ring and  $a \in R$ . The *principal ideal* generated by  $a$  is  $(a) = Ra = aR$ .

**Example 17.23.**  $\{0\} = (0)$  and  $R = \{1\}$  are principal ideals.

**Definition 17.24.** 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 17.25.** 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 17.26.**

$$IJ \subseteq I \cap J$$

PROOF: Easy.  $\square$

**Proposition 17.27.** *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  $i + j = 1$ .

$\langle 1 \rangle 3$ .  $ri, rj \in IJ$

$\langle 1 \rangle 4$ .  $r = ri + rj \in IJ$

$\square$

**Proposition 17.28.** *Let  $R$  be a commutative ring. Let  $f \in R[x]$  be a monic polynomial of degree  $d$ . Then the function*

$$\phi : R[x] \rightarrow R^{\oplus d}$$

*that sends a polynomial  $g$  to the remainder of the division of  $g$  by  $f$  induces an isomorphism of Abelian groups*

$$\frac{R[x]}{(f(x))} \cong R^{\oplus d}.$$

PROOF: It is clearly a group homomorphism; it is surjective since it maps any polynomial of degree  $< d$  to itself, and its kernel is  $(f(x))$  since these are the polynomials with remainder 0.  $\square$

**Corollary 17.28.1.** *Let  $R$  be a commutative ring and  $a \in R$ . Then we have*

$$\frac{R[x]}{(x - a)} \cong R$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $\phi : R[x] \rightarrow R$  be evaluation at  $a$ .

$\langle 1 \rangle 2$ .  $\phi(g)$  is the remainder when dividing  $g$  by  $x - a$ .

PROOF: If  $g = (x - a)q + r$  then  $g(a) = (a - a)q(a) + r = r$ .

$\langle 1 \rangle 3$ .  $\phi$  induces a group isomorphism  $R[x]/(x - a) \cong R$

PROOF: By the theorem.

$\langle 1 \rangle 4$ . This isomorphism is a ring isomorphism.

PROOF: Since evaluation at  $a$  is a ring homomorphism.

$\square$

**Example 17.29.** We have

$$\frac{\mathbb{R}[x]}{(x^2 + 1)} \cong \mathbb{C}$$

as rings.

## 17.4 Maximal Ideals

**Definition 17.30** (Maximal Ideal). Let  $R$  be a ring and  $I$  an ideal in  $R$ . Then  $I$  is a *maximal ideal* iff  $I \neq R$  and, whenever  $J$  is an ideal with  $I \subseteq J$ , then either  $I = J$  or  $J = R$ .



# Chapter 18

## Integral Domains

**Definition 18.1** (Integral Domain). An *integral domain* is a non-trivial commutative ring with no nonzero zero-divisors.

**Example 18.2.**  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  are integral domains.

**Proposition 18.3.**  $\mathbb{Z}/n\mathbb{Z}$  is an integral domain if and only if  $n$  is prime.

PROOF:

$$\begin{aligned} n \text{ is prime} &\Leftrightarrow \forall a, b \in \mathbb{Z} (n \mid ab \Rightarrow n \mid a \vee n \mid b) \\ &\Leftrightarrow \forall a, b \in \mathbb{Z}/n\mathbb{Z} (ab \cong 0(\text{mod } n) \Rightarrow a \cong 0(\text{mod } n) \vee b \cong 0(\text{mod } n)) \\ &\Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ is an integral domain} \quad \square \end{aligned}$$

**Proposition 18.4.** 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 18.5.** 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 18.5.1.** Let  $R$  be a ring. Then  $R[x]$  is an integral domain if and only if  $R$  is an integral domain.

**Proposition 18.6.** 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 18.7.** *Let  $R$  be a ring and  $S$  an integral domain. Every ring 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 18.8.** *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  $n$ .

□

## 18.1 Prime Ideals

**Definition 18.9** (Prime Ideal). Let  $I$  be an ideal in a commutative ring  $R$ . Then  $I$  is a *prime ideal* iff  $R/I$  is an integral domain.

**Example 18.10.** Let  $R$  be a commutative ring and  $a \in R$ . Then  $(x - a)$  is a prime ideal in  $R$  iff  $R$  is an integral domain.

**Proposition 18.11.** *Let  $R$  be a commutative ring and  $I$  a proper ideal in  $R$ . Then  $I$  is prime iff, whenever  $ab \in I$ , then  $a \in I$  or  $b \in I$ .*

PROOF: The condition is the same as saying that, if  $(a + I)(b + I) = I$ , then  $a + I = I$  or  $b + I = I$ .  $\square$

**Definition 18.12** (Spectrum). The *spectrum* of a commutative ring  $R$ ,  $\text{Spec } R$ , is the set of prime ideals.

**Proposition 18.13.** Let  $\phi : R \rightarrow S$  be a ring homomorphism. If  $I$  is a prime ideal in  $S$  then  $\phi^{-1}(I)$  is a prime ideal in  $R$ .

PROOF: If  $ab \in \phi^{-1}(I)$  then  $\phi(a)\phi(b) \in I$  so either  $\phi(a) \in I$  or  $\phi(b) \in I$ , i.e. either  $a \in \phi^{-1}(I)$  or  $b \in \phi^{-1}(I)$ .  $\square$

**Proposition 18.14.** Let  $R$  be a commutative ring. Suppose there exists a prime ideal  $P$  in  $R$  such that the only zero-divisor in  $P$  is 0. Then  $R$  is an integral domain.

PROOF:

$\langle 1 \rangle$ 1. ASSUME:  $ab = 0$  in  $R$

$\langle 1 \rangle$ 2.  $ab \in P$

$\langle 1 \rangle$ 3.  $a \in P$  or  $b \in P$

$\langle 1 \rangle$ 4.  $a = 0$  or  $b = 0$

$\square$

**Proposition 18.15.** Let  $R$  be a commutative ring. The nilradical of  $R$  is included in every prime ideal of  $R$ .

PROOF: Let  $P$  be a prime ideal. If  $a^n = 0$  then  $a^n \in P$  hence  $a \in P$ .  $\square$

**Definition 18.16** (Krull Dimension). The (*Krull*) *dimension* of a commutative ring  $R$  is the length of the longest chain of prime ideals in  $R$ .

**Example 18.17.**  $\mathbb{Z}[x]$  has Krull dimension 2.





## Chapter 19

# Unique Factorization Domains

**Example 19.1.**  $\mathbb{Z}$  is a UFD.



## Chapter 20

# Noetherian Rings

**Definition 20.1** (Noetherian Ring). A commutative ring is *Noetherian* iff every ideal is finitely generated.

**Proposition 20.2.** *The homomorphic image of a Noetherian ring is Noetherian.*

PROOF:

⟨1⟩1. LET:  $R$  be a Noetherian ring,  $S$  be a commutative ring, and  $\phi : R \rightarrow S$  a surjective ring homomorphism.

⟨1⟩2. LET:  $I$  be an ideal in  $S$ .

⟨1⟩3. LET:  $\phi^{-1}(I) = (a_1, \dots, a_n)$

⟨1⟩4.  $I = (\phi(a_1), \dots, \phi(a_n))$

□



## Chapter 21

# Principal Ideal Domains

**Definition 21.1** (Principal Ideal Domain). A commutative ring is a *principal ideal domain* (PID) iff every ideal is principal.

**Example 21.2.**  $\mathbb{Z}$  is a PID by Proposition 7.16.

**Example 21.3.**  $\mathbb{Z}[x]$  is not a PID. The ideal  $(2, x)$  is not principal.

**Proposition 21.4.** *Every PID is Noetherian.*

PROOF: Trivial.  $\square$

**Proposition 21.5.** *Every nonzero prime ideal in a PID is maximal.*

PROOF:

$\langle 1 \rangle$ 1. LET:  $R$  be a PID.

$\langle 1 \rangle$ 2. LET:  $I$  be a nonzero prime ideal in  $R$ .

$\langle 1 \rangle$ 3. PICK  $a \in R$  such that  $I = (a)$ .

$\langle 1 \rangle$ 4. LET:  $J$  be an ideal such that  $I \subseteq J$

$\langle 1 \rangle$ 5. PICK  $b \in R$  such that  $J = (b)$ .

$\langle 1 \rangle$ 6. PICK  $t \in R$  such that  $a = bt$ .

$\langle 1 \rangle$ 7.  $b \in I$  or  $t \in I$

$\langle 1 \rangle$ 8. CASE:  $b \in I$

PROOF: Then  $J \subseteq I$  so  $I = J$ .

$\langle 1 \rangle$ 9. CASE:  $t \in I$

$\langle 2 \rangle$ 1. PICK  $s \in R$  such that  $t = as$ .

$\langle 2 \rangle$ 2.  $a = ast$

$\langle 2 \rangle$ 3.  $st = 1$

PROOF: Since  $R$  is an integral domain.

$\langle 2 \rangle$ 4.  $1 \in I$

$\langle 2 \rangle$ 5.  $I = R$

$\square$

**Corollary 21.5.1.** *Any PID has Krull dimension 1.*



## Chapter 22

# Euclidean Domains

**Example 22.1.**  $\mathbb{Z}$  is a Euclidean domain.





## Chapter 23

# Division Rings

**Definition 23.1** (Division Ring). A *division ring* is a ring in which every nonzero element is a two-sided unit.

**Example 23.2.** 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 23.3.** For any ring  $R$ , the ring of polynomials  $R[x]$  is not a division ring, since  $x$  has no inverse.

**Proposition 23.4.** *Every centralizer in a division ring is a division ring.*

PROOF: If  $ar = ra$  then  $ra^{-1} = a^{-1}r$ .  $\square$

**Proposition 23.5.** *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.

⟨1⟩2. If the only left-ideals and right-ideals are  $\{0\}$  and  $R$  then  $R$  is a division ring.

□

**Proposition 23.6.** *Let  $K$  be a division ring and  $R$  a non-trivial ring. Every ring homomorphism  $K \rightarrow R$  is injective.*

PROOF:

⟨1⟩1. LET:  $\phi : K \rightarrow R$  be a ring homomorphism.

PROVE:  $\ker \phi = \{0\}$

⟨1⟩2. LET:  $x \in \ker \phi$

⟨1⟩3. ASSUME: for a contradiction  $x \neq 0$ .

⟨1⟩4.  $\phi(xx^{-1}) = 1$

⟨1⟩5.  $0 = 1$

⟨1⟩6. Q.E.D.

PROOF: This contradicts the assumption that  $R$  is non-trivial.

□

## Chapter 24

# Simple Rings

**Definition 24.1** (Simple Ring). A non-trivial ring is *R simple* iff its only two-sided ideals are  $\{0\}$  and  $R$ .

**Example 24.2.** For any simple ring  $R$  we have  $\mathfrak{gl}_n(R)$  is simple, by Corollary 17.13.1.

**Proposition 24.3.** *Let  $R$  be a ring and  $I$  an ideal in  $R$ . Then  $I$  is maximal iff  $R/I$  is simple.*

PROOF:

$$\begin{aligned} R/I \text{ is simple} &\Leftrightarrow \text{the only ideals in } R/I \text{ are } \{I\} \text{ and } R/I \\ &\Leftrightarrow \text{the only ideals in } R \text{ that include } I \text{ are } I \text{ and } R \\ &\Leftrightarrow I \text{ is maximal} \end{aligned}$$

□



## Chapter 25

# Reduced Rings

**Definition 25.1** (Reduced Ring). A ring is *reduced* iff it has no non-zero nilpotent elements.

**Proposition 25.2.** *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 25.3.** *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 26

# Boolean Rings

**Definition 26.1** (Boolean). A ring is *Boolean* iff  $a^2 = a$  for every element  $a$ .

**Example 26.2.** For any set  $S$ , the ring  $\mathcal{P}S$  is Boolean.

**Proposition 26.3.** *Every non-trivial Boolean ring has characteristic 2.*

PROOF: We have  $4 = 2$  and so  $2 = 0$ .  $\square$

**Proposition 26.4.** *Every Boolean ring is commutative.*

PROOF:

$$\begin{aligned}(a+b)^2 &= a+b \\ \therefore a^2 + ab + ba + b^2 &= a+b \\ \therefore a + ab + ba + b &= a+b \\ \therefore ab + ba &= 0 \\ \therefore ab &= -ba \\ &= ba \quad (\text{Proposition 26.3})\end{aligned}$$

**Example 26.5.** 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.  $D = \{0, 1\}$ .

**Proposition 26.6.** *Every Boolean ring has Krull dimension 0.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $R$  be a Boolean ring.

$\langle 1 \rangle 2$ . LET:  $I$  be a prime ideal in  $R$ .

PROVE:  $I$  is maximal.

$\langle 1 \rangle 3$ . LET:  $J$  be an ideal with  $I \subsetneq J$

$\langle 1 \rangle 4$ . PICK  $a \in J$  with  $a \notin I$

$\langle 1 \rangle 5$ .  $a^2 - a = 0 \in I$

$\langle 1 \rangle 6$ .  $a(a-1) \in I$

$$\langle 1 \rangle 7. \ a - 1 \in I$$

$$\langle 1 \rangle 8. \ a - 1 \in J$$

$$\langle 1 \rangle 9. \ 1 \in J$$

$$\langle 1 \rangle 10. \ J = R$$

□



## Chapter 27

# Modules

**Definition 27.1** (Left Module). Let  $R$  be a ring and  $M$  an Abelian group. A *left-action* of  $R$  on  $M$  is a ring homomorphism

$$R \rightarrow \text{End}_{\mathbf{Ab}}(M) \quad .$$

A *left  $R$ -module* consists of an Abelian group  $M$  and a left-action of  $R$  on  $M$ .

**Proposition 27.2.** *Let  $R$  be a ring and  $M$  an Abelian group. Let  $\cdot : R \times M \rightarrow M$ . Then  $\cdot$  defines a left-action of  $R$  on  $M$  if and only if, for all  $r, s \in R$  and  $m, n \in M$ :*

- $r(m + n) = rm + rn$
- $(r + s)m = rm + sm$
- $(rs)m = r(sm)$
- $1m = m$

PROOF: Immediate from definitions.  $\square$

**Proposition 27.3.** *In any  $R$ -module  $M$  we have  $0m = 0$  for all  $m \in M$ .*

PROOF: Since  $0m = (0 + 0)m = 0m + 0m$  and so  $0m = 0$  by cancellation in  $M$ .  $\square$

**Proposition 27.4.** *In any  $R$ -module  $M$  we have  $(-1)m = -m$  for all  $m \in M$ .*

PROOF: Since  $m + (-1)m = 1m + (-1)m = (1 + (-1))m = 0m = 0$ .  $\square$

**Proposition 27.5.** *Every Abelian group is a  $\mathbb{Z}$ -module in exactly one way.*

PROOF: Since  $\mathbb{Z}$  is initial in **Ring**.  $\square$

**Definition 27.6** (Right Module). Let  $R$  be a ring. A *right  $R$ -module* consists of an Abelian group  $M$  and a function  $\cdot : M \times R \rightarrow M$  such that, for all  $r, s \in R$  and  $m, n \in M$ :

- $(m + n)r = mr + nr$
- $m(r + s) = mr + ms$
- $m(rs) = (mr)s$
- $m1 = m$

## 27.1 Homomorphisms

**Definition 27.7** (Homomorphism of Left-Modules). Let  $R$  be a ring. Let  $M$  and  $N$  be left- $R$ -modules. A *homomorphism of left- $R$ -modules*  $\phi : M \rightarrow N$  is a group homomorphism such that, for all  $r \in R$  and  $m \in M$ , we have  $\phi(rm) = r\phi(m)$ .

Let  $R - \mathbf{Mod}$  be the category of left- $R$ -modules and left- $R$ -module homomorphisms.

**Example 27.8.**

$$\mathbb{Z} - \mathbf{Mod} \cong \mathbf{Ab}$$

**Example 27.9.** The trivial group  $0$  is the zero object in  $R - \mathbf{Mod}$ .

**Proposition 27.10.** *Every bijective  $R$ -module homomorphism is an isomorphism.*

PROOF: Easy.  $\square$

**Proposition 27.11.** *Let  $R$  be a ring. Let  $M$  be an  $R$ -module. Then*

$$M \cong R - \mathbf{Mod}[R, M]$$

*as  $R$ -modules.*

PROOF: The isomorphism maps  $m$  to the function  $\lambda r.rm$ . Its inverse maps an  $R$ -module homomorphism  $\alpha$  to  $\alpha(1)$ .  $\square$

**Proposition 27.12.** *Let  $R$  be a commutative ring. Let  $M$  be an  $R$ -module. Then there is a bijection between the set of  $R[x]$ -module structures on  $M$  that extend the given  $R$ -module structure and  $\text{End}_{R - \mathbf{Mod}}(M)$ .*

PROOF:

- (1)1. LET:  $\alpha : R \rightarrow \text{End}_{\mathbf{Ab}}(M)$  be the given  $R$ -module structure on  $M$ .
- (1)2. An  $R[x]$ -module structure on  $M$  that extends  $\alpha$  is a ring homomorphism  $\beta : R[x] \rightarrow \text{End}_{\mathbf{Ab}}(M)$  such that  $\beta \circ i = \alpha$ , where  $i$  is the inclusion  $R \rightarrow R[x]$ .
- (1)3. There is a bijection between the  $R[x]$ -module structures on  $M$  that extend  $\alpha$  and the elements  $s \in \text{End}_{\mathbf{Ab}}(M)$  that commute with  $\alpha(r)$  for all  $r \in R$ .

PROOF: By the universal property for polynomials.

- (1)4. There is a bijection between the  $R[x]$ -module structures on  $M$  that extend  $\alpha$  and the  $R$ -module homomorphisms  $(M, \alpha) \rightarrow (M, \alpha)$ .

□

**Proposition 27.13.** *Let  $R$  be a commutative ring. Let  $M$  and  $N$  be  $R$ -modules. Then  $R - \mathbf{Mod}[M, N]$  is an  $R$ -module under*

$$\begin{aligned}(\phi + \psi)(m) &= \phi(m) + \psi(m) \\ (r\phi)(m) &= r\phi(m)\end{aligned}$$

PROOF: Easy. □

**Proposition 27.14.** *Let  $R$  be an integral domain. Let  $I$  be a nonzero principal ideal of  $R$ . Then  $I \cong R$  in  $R - \mathbf{Mod}$ .*

PROOF:

⟨1⟩1. PICK  $a \in R$  such that  $I = (a)$ .

⟨1⟩2. LET:  $\phi : R \rightarrow I$  be the map  $\phi(r) = ra$ .

⟨1⟩3.  $\phi$  is an  $R$ -module homomorphism.

PROOF: Since  $(r + s)a = ra + sa$  and  $(rs)a = r(sa)$ .

⟨1⟩4.  $\phi$  is surjective.

⟨1⟩5.  $\phi$  is injective.

PROOF: If  $ra = sa$  then  $(r - s)a = 0$  so  $r - s = 0$  and  $r = s$ .

⟨1⟩6.  $\phi : R \cong I$

□

## 27.2 Submodules

**Definition 27.15** (Submodule). Let  $M$  be a left- $R$ -module and  $N \subseteq M$ . Then  $N$  is a *submodule* of  $M$  iff  $N$  is a subgroup of  $M$  and  $\forall r \in R, \forall n \in N, rn \in N$ .

**Proposition 27.16.** *Let  $R$  be a ring and  $I \subseteq R$ . Then  $I$  is a left-ideal in  $R$  iff  $I$  is a submodule of  $R$  as an  $R$ -module.*

PROOF: Immediate from definitions. □

**Proposition 27.17.** *Let  $R$  be a ring. Let  $M$  and  $N$  be left- $R$ -modules and  $\phi : M \rightarrow N$  an  $R$ -module homomorphism. Then  $\ker \phi$  is a submodule of  $M$  and  $\text{im } \phi$  is a submodule of  $N$ .*

PROOF: Easy. □

**Proposition 27.18.** *Let  $R$  be a commutative ring. Let  $M$  be a left- $R$ -module. Let  $r \in R$ . Then  $rM = \{rm : m \in M\}$  is a submodule of  $M$ .*

PROOF: Easy. □

**Proposition 27.19.** *Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Let  $I$  be a left-ideal in  $R$ . Then  $IM = \{rm : r \in I, m \in M\}$  is a submodule of  $M$ .*

PROOF:

- $\langle 1 \rangle 1$ .  $IM$  is a subgroup of  $M$ .  
 $\langle 2 \rangle 1$ . LET:  $r, s \in I$  and  $m, n \in M$ .  
 PROVE:  $rm + sn \in IM$   
 $\langle 2 \rangle 2$ .  $rm + sn = r(m - n) + (s - r)n$   
 $\langle 1 \rangle 2$ . For all  $r \in R$  and  $x \in IM$  we have  $rx \in IM$ .  
 $\square$

### 27.3 Quotient Modules

**Definition 27.20** (Quotient Module). Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Let  $N$  be a submodule of  $M$ . Then the *quotient module*  $M/N$  is the quotient group  $M/N$  under

$$r(m + N) = rm + N \ .$$

**Proposition 27.21.** Let  $R$  be a ring. Let  $M$  and  $P$  be left- $R$ -modules. Let  $N$  be a submodule of  $M$ . Let  $\phi : M \rightarrow P$  be an  $R$ -module homomorphism. If  $N \subseteq \ker \phi$ , then there exists a unique  $R$ -module homomorphism  $\bar{\phi} : M/N \rightarrow P$  such that the following diagram commutes.

$$\begin{array}{ccc}
 M & \xrightarrow{\phi} & P \\
 & \searrow & \nearrow \bar{\phi} \\
 & M/N &
 \end{array}$$

PROOF: Easy.  $\square$

**Theorem 27.22.** Every  $R$ -module homomorphism  $\phi : M \rightarrow M'$  may be decomposed as:

$$M \longrightarrow M/\ker \phi \xrightarrow{\cong} \text{im } \phi \longrightarrow M'$$

PROOF: Easy.  $\square$

**Corollary 27.22.1** (First Isomorphism Theorem). Let  $\phi : M \rightarrow M'$  be a surjective  $R$ -module homomorphism. Then

$$M' \cong \frac{M}{\ker \phi} \ .$$

**Proposition 27.23** (Second Isomorphism Theorem). Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Let  $N$  and  $P$  be submodules of  $M$ . Then  $N + P$  is a submodule of  $M$ ,  $N \cap P$  is a submodule of  $P$ , and

$$\frac{N + P}{N} \cong \frac{P}{N \cap P}$$

PROOF: The function that maps  $P$  to  $p + N$  is a surjective homomorphism  $P \rightarrow (N + P)/N$  with kernel  $N \cap P$ .  $\square$

**Proposition 27.24** (Third Isomorphism Theorem). *Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Let  $N$  be a submodule of  $M$  and  $P$  a submodule of  $N$ . Then  $N/P$  is a submodule of  $M/P$  and*

$$\frac{M/P}{N/P} \cong \frac{M}{N}$$

PROOF: The canonical map  $M \rightarrow M/N$  induces a surjective homomorphism  $M/P \rightarrow M/N$  which has kernel  $N/P$ .  $\square$

**Proposition 27.25.** *Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. The sum and intersection of a family of submodules of  $M$  are submodules of  $M$ .*

PROOF: Easy.  $\square$

## 27.4 Products

**Proposition 27.26.**  *$R - \mathbf{Mod}$  has products.*

PROOF: Given a family  $\{M_\alpha\}_{\alpha \in A}$  of left- $R$ -modules, we make  $\prod_{\alpha \in A} M_\alpha$  into a left- $R$ -module by

$$(f + g)(\alpha) = f(\alpha) + g(\alpha)$$

$$(rf)(\alpha) = rf(\alpha)$$

$\square$

## 27.5 Coproducts

**Proposition 27.27.**  *$R - \mathbf{Mod}$  has coproducts.*

PROOF: Given a family  $\{M_\alpha\}_{\alpha \in A}$  of left- $R$ -modules, take  $\bigoplus_{\alpha \in A} M_\alpha$  to be  $\{f \in \prod_{\alpha \in A} M_\alpha : f(\alpha) = 0 \text{ for all but finitely many } \alpha \in A\}$ .  $\square$

## 27.6 Direct Sum

**Definition 27.28** (Direct Sum). *Let  $R$  be a ring. Let  $M$  and  $N$  be left- $R$ -modules. Then the direct sum  $M \oplus N$  is an  $R$ -module under*

$$r(m, n) = (rm, rn) .$$

**Proposition 27.29.**  *$M \oplus N$  is the biproduct of  $M$  and  $N$  in  $R - \mathbf{Mod}$ .*

PROOF: Easy.  $\square$

**Example 27.30.** Infinite products and coproducts are in general different. We have  $\mathbb{Z}^{\mathbb{N}} \not\cong \mathbb{Z}^{\oplus \mathbb{N}}$  since  $\mathbb{Z}^{\mathbb{N}}$  is uncountable but  $\mathbb{Z}^{\oplus \mathbb{N}}$  is countable.

## 27.7 Kernels and Cokernels

**Proposition 27.31.** *Let  $R$  be a ring. Let  $\phi : M \rightarrow N$  be a left- $R$ -module homomorphism. Then  $\ker \phi \hookrightarrow M$  is terminal in the category of left- $R$ -module homomorphisms  $\alpha : P \rightarrow M$  such that  $\phi \circ \alpha = 0$ .*

PROOF: Easy.  $\square$

**Proposition 27.32.** *Let  $R$  be a ring. Let  $\phi : M \rightarrow N$  be a left- $R$ -module homomorphism. Then  $N \twoheadrightarrow \operatorname{coker} \phi$  is initial in the category of left- $R$ -module homomorphisms  $\alpha : N \rightarrow P$  such that  $\alpha \circ \phi = 0$ .*

PROOF: Easy.  $\square$

**Proposition 27.33.** *Let  $R$  be a ring. Let  $\phi : M \rightarrow N$  be a left- $R$ -module homomorphism. Then the following are equivalent.*

- $\phi$  is a monomorphism.
- $\ker \phi$  is trivial.
- $\phi$  is injective.

PROOF: Easy.  $\square$

**Proposition 27.34.** *Let  $R$  be a ring. Let  $\phi : M \rightarrow N$  be a left- $R$ -module homomorphism. Then the following are equivalent.*

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

PROOF: Easy.  $\square$

**Proposition 27.35.** *Every monomorphism in  $R - \mathbf{Mod}$  is the kernel of some homomorphism.*

PROOF: If  $\phi : M \rightarrow N$  is a monomorphism then it is the kernel of  $N \twoheadrightarrow N/\operatorname{im} \phi$ .  $\square$

**Proposition 27.36.** *Every epimorphism in  $R - \mathbf{Mod}$  is the cokernel of some homomorphism.*

PROOF: If  $\phi : M \rightarrow N$  is epi then it is the cokernel of  $\ker \phi \hookrightarrow M$ .  $\square$

**Example 27.37.** Monomorphisms do not split in  $R - \mathbf{Mod}$ . Multiplication by 2 is a monomorphism  $\mathbb{Z} \rightarrow \mathbb{Z}$  but has no left inverse.

**Example 27.38.** Epimorphisms do not split in  $R - \mathbf{Mod}$ . The canonical map  $\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$  is an epimorphism without a right inverse.

## 27.8 Free Modules

**Proposition 27.39.** *Let  $R$  be a ring and  $A$  a set. Then there exists a left- $R$ -module  $F^R(A)$  and function  $j : A \rightarrow F^R(A)$  such that, for any left- $R$ -module  $M$  and function  $f : A \rightarrow M$ , there exists a unique left- $R$ -module homomorphism  $\bar{f} : F^R(A) \rightarrow M$  such that the following diagram commutes.*

$$\begin{array}{ccc} F^R(A) & \xrightarrow{\bar{f}} & M \\ j \uparrow & \nearrow f & \\ A & & \end{array}$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $R^{\oplus A} = \{\alpha : A \rightarrow R : \alpha(a) = 0 \text{ for all but finitely many } a \in A\}$   
under the operations

$$\begin{aligned} (\alpha + \beta)(a) &= \alpha(a) + \beta(a) \\ (r\alpha)(a) &= r\alpha(a) \end{aligned}$$

$\langle 1 \rangle 2$ .  $R^{\oplus A}$  is a left- $R$ -module.

$\langle 1 \rangle 3$ . LET:  $j : A \rightarrow R^{\oplus A}$  be the function

$$j(a)(a') = \begin{cases} 1 & \text{if } a = a' \\ 0 & \text{if } a \neq a' \end{cases}$$

$\langle 1 \rangle 4$ . LET:  $M$  be any left- $R$ -module.

$\langle 1 \rangle 5$ . LET:  $f : A \rightarrow M$  be a function.

$\langle 1 \rangle 6$ . LET:  $\bar{f} : R^{\oplus A} \rightarrow M$  be the function

$$\bar{f}(\alpha) = \sum_{a \in A, \alpha(a) \neq 0} \alpha(a)f(a)$$

$\langle 1 \rangle 7$ .  $\bar{f}$  is a left- $R$ -module homomorphism.

$\langle 1 \rangle 8$ .  $\bar{f} \circ j = f$

$\langle 1 \rangle 9$ .  $\bar{f}$  is unique.

**Definition 27.40.** We call  $j : A \rightarrow F^R(A)$  the *free* left- $R$ -module over  $A$ .

**Proposition 27.41.**  $j$  is injective.

PROOF: By the proof of the previous proposition.  $\square$

**Proposition 27.42.** *Let  $R$  be a ring. Let  $F$  be a non-zero free left- $R$ -module. Let  $\phi : M \rightarrow N$  be a left- $R$ -module homomorphism. Then  $\phi$  is onto if and only if, for every left- $R$ -module homomorphism  $\alpha : F \rightarrow N$ , there exists a left- $R$ -module homomorphism  $\beta : F \rightarrow M$  such that the diagram below commutes.*

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ \beta \uparrow & \nearrow \alpha & \\ F & & \end{array}$$

PROOF:

- (1)1. LET:  $F$  be the free left- $R$ -module over  $A$  with injection  $j : A \rightarrow F$ .  
 (1)2. If  $\phi$  is onto then, for every homomorphism  $\alpha : F \rightarrow N$ , there exists a homomorphism  $\beta : F \rightarrow M$  such that  $\phi \circ \beta = \alpha$ .  
 (2)1. ASSUME:  $\phi$  is onto.  
 (2)2. LET:  $\alpha : F \rightarrow N$  be a homomorphism.  
 (2)3. For  $a \in A$ , PICK  $f(a) \in M$  such that  $\phi(f(a)) = \alpha(j(a))$   
 (2)4. LET:  $\beta : F \rightarrow M$  be the unique homomorphism such that  $\beta \circ j = f$   
 (2)5.  $\phi \circ \beta = \alpha$   
 PROOF: Each is the unique homomorphism such that  $\alpha \circ j = \phi \circ f$ .

□

$$\begin{array}{ccccc}
 & & M & \xrightarrow{\phi} & N \\
 & f \nearrow & \uparrow \beta & \nearrow \alpha & \\
 A & \xrightarrow{j} & F & & 
 \end{array}$$

- (1)3. If, for every homomorphism  $\alpha : F \rightarrow N$ , there exists a homomorphism  $\beta : F \rightarrow M$  such that  $\phi \circ \beta = \alpha$ , then  $\phi$  is onto.  
 (2)1. ASSUME: For every homomorphism  $\alpha : F \rightarrow N$  there exists a homomorphism  $\beta : F \rightarrow M$  such that  $\phi \circ \beta = \alpha$ .  
 (2)2. LET:  $n \in N$   
 (2)3. LET:  $\alpha : F \rightarrow N$  be the unique homomorphism such that, for all  $a \in A$ , we have  $\alpha(j(a)) = n$   
 (2)4. PICK a homomorphism  $\beta : F \rightarrow M$  such that  $\phi \circ \beta = \alpha$   
 (2)5. PICK  $a \in A$   
 (2)6.  $\phi(\beta(j(a))) = n$

□

## 27.9 Generators

**Definition 27.43** (Submodule Generated by a Set). Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Let  $A$  be a subset of  $M$ . Let  $\phi_A : F^R(A) \rightarrow M$  be the unique left- $R$ -module homomorphism such that the following diagram commutes.

$$\begin{array}{ccc}
 F^R(A) & \xrightarrow{\phi_A} & M \\
 \uparrow & \nearrow & \\
 A & & 
 \end{array}$$

The submodule of  $M$  generated by  $A$ , denoted  $\langle A \rangle$ , is defined to be  $\text{im } \phi_A$ .

**Definition 27.44** (Finitely Generated). Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Then  $M$  is *finitely generated* iff there exists a finite set  $A \subseteq M$  such that  $M = \langle A \rangle$ .

**Example 27.45.** A submodule of a finitely generated module is not necessarily finitely generated.

Let  $R = \mathbb{Z}[x_1, x_2, \dots]$ . Then  $R$  is finitely generated as an  $R$ -module, but  $(x_1, x_2, \dots)$  is not.



**Proposition 27.46.** *The homomorphic image of a finitely generated module is finitely generated.*

PROOF: Easy.  $\square$

**Proposition 27.47.** *Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Let  $N$  be a submodule of  $M$ . If  $N$  and  $M/N$  are finitely generated then  $M$  is finitely generated.*

PROOF:

$\langle 1 \rangle 1$ . PICK  $a_1, \dots, a_n$  that generate  $N$ .

$\langle 1 \rangle 2$ . PICK  $b_1, \dots, b_m$  such that  $b_1 + N, \dots, b_m + N$  generate  $M/N$ .

PROVE:  $a_1, \dots, a_n, b_1, \dots, b_m$  generate  $M$ .

$\langle 1 \rangle 3$ . LET:  $m \in M$

$\langle 1 \rangle 4$ . PICK  $r_1, \dots, r_m \in R$  such that  $m + N = r_1 b_1 + \dots + r_m b_m + N$

$\langle 1 \rangle 5$ .  $m - r_1 b_1 - \dots - r_m b_m \in N$

$\langle 1 \rangle 6$ . PICK  $s_1, \dots, s_n \in R$  such that  $m - r_1 b_1 - \dots - r_m b_m = s_1 a_1 + \dots + s_n a_n$

$\langle 1 \rangle 7$ .  $m = r_1 b_1 + \dots + r_m b_m + s_1 a_1 + \dots + s_n a_n$

$\square$

## 27.10 Projections

**Definition 27.48** (Projection). Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Let  $p : M \rightarrow M$  be a left- $R$ -module homomorphism. Then  $p$  is a *projection* iff  $p^2 = p$ .

**Proposition 27.49.** *Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Let  $p : M \rightarrow M$  be a projection. Then*

$$M \cong \ker p \oplus \operatorname{im} p .$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $\phi : M \rightarrow \ker p \oplus \operatorname{im} p$  be the map  $\phi(m) = (m - p(m), p(m))$

$\langle 1 \rangle 2$ .  $\phi$  is a left- $R$ -module homomorphism.

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

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

$\square$

## 27.11 Pullbacks

**Proposition 27.50.**  *$R - \mathbf{Mod}$  has pullbacks.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $\mu : M \rightarrow Z, \nu : N \rightarrow Z$  be left- $R$ -module homomorphisms.

$\langle 1 \rangle 2$ . LET:  $M \times_Z N = \{(m, n) \in M \times N : \mu(m) = \nu(n)\}$  under

$$(m, n) + (m', n') = (m + m', n + n')$$

$$r(m, n) = (rm, rn)$$

$\langle 1 \rangle 3$ .  $M \times_Z N$  is the pullback of  $M$  and  $N$ .

$\square$

## 27.12 Pushouts

**Proposition 27.51.**  $R - \mathbf{Mod}$  has pushouts.

PROOF:

$\langle 1 \rangle 1$ . LET:  $\mu : A \rightarrow M$  and  $\nu : A \rightarrow N$  be left- $R$ -module homomorphisms.

## Chapter 28

# Cyclic Modules

**Definition 28.1** (Cyclic Module). Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Then  $M$  is *cyclic* iff there exists  $m \in M$  such that  $M = \langle m \rangle$ .

**Proposition 28.2.** *Let  $R$  be a ring. Let  $M$  be a left- $R$ -module. Then  $M$  is cyclic if and only if there exists a left-ideal  $I$  in  $R$  such that  $M \cong R/I$ .*

PROOF:

$\langle 1 \rangle 1$ . If  $M$  is cyclic then there exists a left-ideal  $I$  in  $R$  such that  $M \cong R/I$ .

$\langle 2 \rangle 1$ . ASSUME:  $M$  is cyclic.

$\langle 2 \rangle 2$ . PICK  $m \in M$  such that  $M = \langle m \rangle$

$\langle 2 \rangle 3$ . LET:  $\phi : R \rightarrow M$  be the left- $R$ -module homomorphism  $\phi(r) = rm$ .

$\langle 2 \rangle 4$ .  $\phi$  is surjective.

$\langle 2 \rangle 5$ .  $M \cong R/\ker \phi$

$\langle 1 \rangle 2$ . For every left-ideal  $I$  in  $R$ , we have that  $R/I$  is cyclic.

PROOF:  $R/I$  is generated by  $1 + I$ .

□

**Proposition 28.3.** *A quotient of a cyclic module is cyclic.*

PROOF: If  $M$  is generated by  $m$  then  $M/N$  is generated by  $m + N$ . □

**Proposition 28.4.** *Let  $R$  be a ring. For any left-ideal  $I$  in  $R$  and any left- $R$ -module  $N$ , we have*

$$R - \mathbf{Mod}[R/I, N] \cong \{n \in N : \forall a \in I. an = 0\} .$$

PROOF:

$\langle 1 \rangle 1$ . LET:  $\Phi : R - \mathbf{Mod}[R/I, N] \rightarrow \{n \in N : \forall a \in I. an = 0\}$  be the function

$$\Phi(\alpha) = \alpha(1 + I)$$

PROOF: For all  $a \in I$  we have  $a\alpha(1 + I) = \alpha(a + I) = \alpha(I) = 0$ .

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

PROOF: If  $\alpha(1 + I) = \beta(1 + I)$  then  $\alpha(r + I) = r\alpha(1 + I) = r\beta(1 + I) = \beta(r + I)$  for all  $r \in R$ , hence  $\alpha = \beta$ .

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

PROOF: Given  $n \in N$  such that  $\forall a \in I. an = 0$ , define  $\alpha : R/I \rightarrow N$  by  $\alpha(r + I) = rn$ .

$\langle 1 \rangle 4$ . If  $R$  is commutative then  $\Phi$  is an  $R$ -module homomorphism.

□

**Corollary 28.4.1.** *For all  $a, b \in \mathbb{Z}$  we have  $\mathbf{Ab}[\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}] \cong \mathbb{Z}/\gcd(a, b)\mathbb{Z}$ .*

PROOF:

$$\begin{aligned} \mathbf{Ab}[\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}] &\cong \mathbb{Z} - \mathbf{Mod}[\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}] \\ &\cong \{n \in \mathbb{Z}/b\mathbb{Z} : \forall x \in a\mathbb{Z}. xn \cong 0(\text{mod } b)\} \\ &\cong \{n \in \mathbb{Z}/b\mathbb{Z} : \forall x \in \mathbb{Z}. b \mid xan\} \\ &= \{n \in \mathbb{Z}/b\mathbb{Z} : b \mid an\} \end{aligned}$$

## Chapter 29

# Simple Modules

**Definition 29.1** (Simple Module). Let  $R$  be a ring. An  $R$ -module  $M$  is *simple* or *irreducible* iff its only submodules are  $\{0\}$  and  $M$ .

**Proposition 29.2** (Schur's Lemma). *Let  $R$  be a ring. Let  $M$  and  $N$  be simple  $R$ -modules. Let  $\phi : M \rightarrow N$  be an  $R$ -module homomorphism. Then either  $\phi = 0$  or  $\phi$  is an isomorphism.*

PROOF:

$\langle 1 \rangle 1$ . ASSUME:  $\phi \neq 0$

$\langle 1 \rangle 2$ .  $\ker \phi = 0$

PROOF: Since  $\ker \phi$  is a submodule of  $M$  that is not  $M$ .

$\langle 1 \rangle 3$ .  $\operatorname{im} \phi = N$

PROOF: Since  $\operatorname{im} \phi$  is a submodule of  $N$  that is not  $\{0\}$ .

□

**Proposition 29.3.** *Every simple module is cyclic.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $M$  be a simple module.

$\langle 1 \rangle 2$ . ASSUME: w.l.o.g.  $M \neq \{0\}$

PROOF:  $\{0\} = \langle 0 \rangle$  is cyclic.

$\langle 1 \rangle 3$ . PICK  $m \in M$  with  $m \neq 0$

$\langle 1 \rangle 4$ .  $\langle m \rangle = M$

PROOF: Since  $\langle m \rangle$  is a submodule of  $M$  that is not  $\{0\}$ .

□



## Chapter 30

# Noetherian Modules

**Definition 30.1** (Noetherian Module). Let  $R$  be a ring. A left- $R$ -module is *Noetherian* iff every submodule is finitely generated.

**Proposition 30.2.** *Let  $R$  be a ring. Let  $M$  be a left- $R$ -module and  $N$  a submodule of  $M$ . Then  $M$  is Noetherian if and only if  $N$  and  $M/N$  are Noetherian.*

PROOF:

⟨1⟩1. If  $M$  is Noetherian then  $N$  is Noetherian.

PROOF: Every submodule of  $N$  is a submodule of  $M$ , hence finitely generated.

⟨1⟩2. If  $M$  is Noetherian then  $M/N$  is Noetherian.

⟨2⟩1. ASSUME:  $M$  is Noetherian.

⟨2⟩2. LET:  $\pi : M \rightarrow M/N$  be the canonical epimorphism.

⟨2⟩3. LET:  $P$  be a submodule of  $M/N$ .

⟨2⟩4. PICK  $a_1, \dots, a_n \in M$  that generate  $\pi^{-1}(P)$ .

⟨2⟩5.  $a_1 + N, \dots, a_n + N$  generate  $P$ .

⟨1⟩3. If  $N$  and  $M/N$  are Noetherian then  $M$  is Noetherian.

⟨2⟩1. ASSUME:  $N$  and  $M/N$  are Noetherian.

⟨2⟩2. LET:  $P$  be a submodule of  $M$ .

⟨2⟩3. PICK  $a_1, \dots, a_m \in P$  such that  $a_1 + N, \dots, a_m + N$  generate  $\pi(P)$ .

⟨2⟩4. PICK  $b_1, \dots, b_n \in M$  that generated  $P \cap N$ .

PROVE:  $a_1, \dots, a_m, b_1, \dots, b_n$  generate  $P$ .

⟨2⟩5. LET:  $p \in P$

⟨2⟩6. PICK  $r_1, \dots, r_m \in R$  such that  $p + N = r_1 a_1 + \dots + r_m a_m + N$

⟨2⟩7.  $p - r_1 a_1 - \dots - r_m a_m \in P \cap N$

⟨2⟩8. PICK  $s_1, \dots, s_n \in R$  such that  $p - r_1 a_1 - \dots - r_m a_m = s_1 b_1 + \dots + s_n b_n$

⟨2⟩9.  $p = r_1 a_1 + \dots + r_m a_m + s_1 b_1 + \dots + s_n b_n$

□

**Corollary 30.2.1.** *If  $R$  is a Noetherian ring then  $R^{\oplus n}$  is a Noetherian left- $R$ -module.*

PROOF: The proof is by induction on  $n$ . The case  $n = 1$  is immediate.

The induction step holds since  $R^{\oplus(n+1)}/R^{\oplus n} \cong R$ . □

**Corollary 30.2.2.** *If  $R$  is a Noetherian ring and  $M$  is a finitely generated left- $R$ -module then  $M$  is Noetherian.*

PROOF: There is a surjective homomorphism  $R^{\oplus n} \rightarrow M$  for some  $n$ , so  $M$  is a quotient of  $R^{\oplus n}$ .  $\square$



# Chapter 31

## Algebras

**Definition 31.1** (Algebra). Let  $R$  be a commutative ring. An  $R$ -algebra consists of a ring  $S$  and a ring homomorphism  $\alpha : R \rightarrow S$  such that  $\alpha(R)$  is included in the center of  $S$ . We write  $rs$  for  $\alpha(r)s$ .

**Proposition 31.2.** Let  $R$  be a commutative ring and  $S$  a ring. Let  $\cdot : R \times S \rightarrow S$ . Then there exists  $\alpha : R \rightarrow S$  that makes  $S$  into an  $R$ -algebra such that

$$rs = \alpha(r)s \quad (r \in R, s \in S)$$

iff  $S$  is an  $R$ -module under  $\cdot$  and, for all  $r_1, r_2 \in R$  and  $s_1, s_2 \in S$ ,

$$(r_1 s_1)(r_2 s_2) = (r_1 r_2)(s_1 s_2) .$$

PROOF: Immediate from definitions.  $\square$

**Example 31.3.** Let  $R$  be a commutative ring. Then  $R$  is an  $R$ -algebra under multiplication.

**Example 31.4.** Let  $R$  be a commutative ring and  $I$  an ideal in  $R$ . Then  $R/I$  is an  $R$ -algebra.

**Example 31.5.** Let  $R$  be a commutative ring and  $M$  an  $R$ -module. Then  $\text{End}_{R\text{-Mod}}(M)$  is an  $R$ -algebra under composition.

**Example 31.6.** Let  $R$  be a commutative ring. Then  $\mathfrak{gl}_n(R)$  is an  $R$ -algebra under matrix multiplication.

**Definition 31.7** (Algebra Homomorphism). Let  $R$  be a commutative ring. Let  $S$  and  $T$  be  $R$ -algebras. An  $R$ -algebra homomorphism  $\phi : S \rightarrow T$  is a ring homomorphism such that, for all  $r \in R$  and  $s \in S$ , we have  $\phi(rs) = r\phi(s)$ .

Let  $R\text{-Alg}$  be the category of  $R$ -algebras and  $R$ -algebra homomorphisms.

**Example 31.8.**

$$\mathbb{Z}\text{-Alg} \cong \mathbf{Ring}$$

**Example 31.9.** Let  $R$  be a commutative ring. Then  $R[x_1, \dots, x_n]$ , and any quotient ring of  $R[x_1, \dots, x_n]$ , is a commutative  $R$ -algebra.

**Example 31.10.**  $R$  is the initial object in  $R\text{-Alg}$ .

### 31.1 Rees Algebra

**Definition 31.11** (Rees Algebra). Let  $R$  be a commutative ring. Let  $I$  be an ideal in  $R$ . The *Rees algebra* is the direct sum

$$\text{Rees}_R(I) = \bigoplus_{j \geq 0} I^j$$

under the multiplication

$$\begin{aligned} (r_0, r_1, r_2, r_3, \dots)(s_0, s_1, s_2, \dots) &= (r_0s_0, r_1s_0 + r_0s_1, r_2s_0 + r_1s_1 + r_0s_2, \dots) \\ r(r_0, r_1, r_2, \dots) &= (rr_0, rr_1, rr_2, \dots) \end{aligned}$$

**Proposition 31.12.** *Let  $R$  be a commutative ring. Let  $a \in R$  be a non-zero-divisor. Then  $R[x]$  is the Rees algebra of  $(a)$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $\phi : R[x] \rightarrow \text{Rees}_R((a))$  be the function  $\phi(r_0 + r_1x + r_2x^2 + \dots) = (r_0, r_1a, r_2a^2, \dots)$ .

$\langle 1 \rangle 2$ .  $\phi$  is an  $R$ -algebra homomorphism.

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

$\langle 2 \rangle 1$ . LET:  $\phi(r_0 + r_1x + r_2x^2 + \dots) = \phi(s_0 + s_1x + s_2x^2 + \dots)$

$\langle 2 \rangle 2$ . For all  $n$  we have  $r_na^n = s_na^n$

$\langle 2 \rangle 3$ .  $(r_n - s_n)a^n = 0$

$\langle 2 \rangle 4$ .  $r_n - s_n = 0$

PROOF: Since  $a$  is not a zero-divisor.

$\langle 2 \rangle 5$ .  $r_n = s_n$

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

□

**Proposition 31.13.** *Let  $R$  be a commutative ring. Let  $a \in R$  be a non-zero-divisor. Let  $I$  be an ideal of  $R$ . Then  $\text{Rees}_R(I) \cong \text{Rees}_R(aI)$ .*

PROOF:

$\langle 1 \rangle 1$ . LET:  $\phi : \text{Rees}_R(I) \rightarrow \text{Rees}_R(aI)$  be the function  $\phi(r_0, r_1, r_2, \dots) = (r_0, ar_1, a^2r_2, \dots)$ .

$\langle 1 \rangle 2$ .  $\phi$  is an  $R$ -algebra homomorphism.

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

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

□

### 31.2 Free Algebras

**Proposition 31.14.** *Let  $R$  be a ring. Then  $R[x_1, \dots, x_n]$  is the free commutative  $R$ -algebra on  $\{1, \dots, n\}$ .*

PROOF: Easy. □

**Proposition 31.15.** *Let  $R$  be a ring and  $A$  a set. Let  $A^*$  be the free monoid on  $A$ . Then the monoid ring  $R[A^*]$  is the free  $R$ -algebra on  $A$ .*

PROOF: Easy.  $\square$

**Proposition 31.16.** *Let  $R$  be a commutative ring and  $S$  a commutative  $R$ -algebra. Then  $S$  is finitely generated as an  $R$ -algebra if and only if  $S$  is finitely generated as a commutative  $R$ -algebra.*

PROOF: Since a subalgebra of a commutative subalgebra is commutative, so the smallest algebra that contains  $\{a_1, \dots, a_n\}$  is the smallest commutative subalgebra that contains  $\{a_1, \dots, a_n\}$ .  $\square$



## Chapter 32

# Algebras of Finite Type

**Definition 32.1** (Algebra of Finite Type). Let  $R$  be a ring. Let  $S$  be an  $R$ -algebra. Then  $R$  is of *finite type* iff  $S$  is a finitely generated  $R$ -algebra.

**Proposition 32.2.** *Let  $R$  be a Noetherian ring. Let  $S$  be a finite-type  $R$ -algebra. Then  $S$  is a Noetherian ring.*



## Chapter 33

# Finite Algebras

**Definition 33.1** (Finite Algebra). Let  $R$  be a ring. Let  $S$  be an  $R$ -algebra. Then  $S$  is a *finite*  $R$ -algebra iff it is a finitely generated left- $R$ -module.

**Proposition 33.2.** *Let  $R$  be a ring. Every finite  $R$ -algebra is of finite type.*

PROOF: If  $S$  is generated by  $a_1, \dots, a_n$  as an  $R$ -module, then it is generated by  $a_1, \dots, a_n$  as an  $R$ -algebra.  $\square$

**Example 33.3.** The converse does not hold.  $R[x]$  is of finite type but is not finite.





## Chapter 34

# Division Algebras

**Definition 34.1** (Division Algebra). Let  $R$  be a commutative ring. A *division  $R$ -algebra* is an  $R$ -algebra that is a division ring.

**Example 34.2.** Let  $R$  be a commutative ring. Let  $M$  be a simple  $R$ -algebra. Then  $\text{End}_{R\text{-Mod}}(M)$  is a division algebra. For if  $\phi \circ \psi = 0$  then  $\phi$  and  $\psi$  cannot both be isomorphisms, hence  $\phi = 0$  or  $\psi = 0$  by Schur's Lemma.



## Chapter 35

# Chain Complexes

**Definition 35.1** (Chain Complex). Let  $R$  be a ring. A *chain complex of left- $R$ -modules*  $M_\bullet = (M_\bullet, d_\bullet)$  consists of a family of left- $R$ -modules  $\{M_i\}_{i \in \mathbb{Z}}$  and a family of left- $R$ -module homomorphisms  $\{d_i : M_i \rightarrow M_{i-1}\}_{i \in \mathbb{Z}}$  such that, for all  $i$ ,

$$d_i \circ d_{i+1} = 0 \ .$$

We call each  $d_i$  a *differential* and the family  $\{d_i\}_i$  the *boundary* of the chain complex.

**Definition 35.2** (Exact). A chain complex  $M_\bullet$  is *exact* at  $M_i$  iff  $\text{im } d_{i+1} = \ker d_i$ .

It is *exact* or an *exact sequence* iff it is exact at  $M_i$  for all  $i$ .

**Proposition 35.3.** A complex

$$\cdots \rightarrow 0 \rightarrow L \xrightarrow{\alpha} M \rightarrow \cdots$$

is exact at  $L$  iff  $\alpha$  is a monomorphism.

PROOF: Since both are equivalent to  $\ker \alpha = 0$ .  $\square$

**Proposition 35.4.** A complex

$$\cdots \rightarrow M \xrightarrow{\beta} N \rightarrow 0 \rightarrow \cdots$$

is exact at  $N$  iff  $\beta$  is an epimorphism.

PROOF: Since both are equivalent to  $\text{im } \beta = N$ .  $\square$

**Definition 35.5** (Short Exact Sequence). A *short exact sequence* is an exact complex of the form

$$0 \rightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \rightarrow 0 \ .$$

**Proposition 35.6** (Four-Lemma). *If*

$$\begin{array}{ccccccc} A_1 & \xrightarrow{f_1} & B_1 & \xrightarrow{g_1} & C_1 & \xrightarrow{h_1} & D_1 \\ \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \downarrow \delta \\ A_2 & \xrightarrow{f_2} & B_2 & \xrightarrow{g_2} & C_2 & \xrightarrow{h_2} & D_2 \end{array}$$

*is a commutative diagram of left- $R$ -modules with exact rows,  $\alpha$  is an epimorphism, and  $\beta$  and  $\delta$  are monomorphisms, then  $\gamma$  is an monomorphism.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $x, y \in C_1$

$\langle 1 \rangle 2$ . ASSUME:  $\gamma(x) = \gamma(y)$

$\langle 1 \rangle 3$ .  $\delta(h_1(x)) = \delta(h_1(y))$

$\langle 1 \rangle 4$ .  $h_1(x) = h_1(y)$

PROOF:  $\delta$  is injective.

$\langle 1 \rangle 5$ .  $x - y \in \ker h_1$

$\langle 1 \rangle 6$ .  $x - y \in \operatorname{im} g_1$

$\langle 1 \rangle 7$ . PICK  $b \in B_1$  such that  $g_1(b) = x - y$ .

$\langle 1 \rangle 8$ .  $g_2(\beta(b)) = 0$

PROOF:  $g_2(\beta(b)) = \gamma(g_1(b)) = \gamma(x - y) = 0$

$\langle 1 \rangle 9$ .  $\beta(b) \in \ker g_2$

$\langle 1 \rangle 10$ .  $\beta(b) \in \operatorname{im} f_2$

$\langle 1 \rangle 11$ . PICK  $a' \in A_2$  such that  $f_2(a') = \beta(b)$

$\langle 1 \rangle 12$ . PICK  $a \in A_1$  such that  $\alpha(a) = a'$

PROOF:  $\alpha$  is surjective.

$\langle 1 \rangle 13$ .  $\beta(f_1(a)) = \beta(b)$

$\langle 1 \rangle 14$ .  $f_1(a) = b$

PROOF:  $\beta$  is injective.

$\langle 1 \rangle 15$ .  $0 = g_1(b)$

PROOF: Since  $g_1(b) = g_1(f_1(a)) = 0$ .

$\langle 1 \rangle 16$ .  $x = y$

PROOF:  $\langle 1 \rangle 7$

□

**Proposition 35.7** (Four-Lemma). *If*

$$\begin{array}{ccccccc} A_1 & \xrightarrow{f_1} & B_1 & \xrightarrow{g_1} & C_1 & \xrightarrow{h_1} & D_1 \\ \downarrow \beta & & \downarrow \gamma & & \downarrow \delta & & \downarrow \epsilon \\ A_2 & \xrightarrow{f_2} & B_2 & \xrightarrow{g_2} & C_2 & \xrightarrow{h_2} & D_2 \end{array}$$

*is a commutative diagram of left- $R$ -modules with exact rows,  $\beta$  and  $\delta$  are epimorphisms, and  $\epsilon$  is a monomorphism, then  $\gamma$  is an epimorphism.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $b_2 \in B_2$

$\langle 1 \rangle 2$ . PICK  $c_1 \in C_1$  such that  $\delta(c_1) = g_2(b_2)$

PROOF:  $\delta$  is surjective.

$\langle 1 \rangle 3$ .  $\epsilon(h_1(c_1)) = 0$

$\langle 1 \rangle 4$ .  $h_1(c_1) = 0$

PROOF:  $\epsilon$  is injective.

$\langle 1 \rangle 5$ .  $c_1 \in \ker h_1$

$\langle 1 \rangle 6$ .  $c_1 \in \operatorname{im} g_1$

$\langle 1 \rangle 7$ . PICK  $b_1 \in B_1$  such that  $g_1(b_1) = c_1$

$\langle 1 \rangle 8$ .  $g_2(\gamma(b_1)) = g_2(b_2)$

$\langle 1 \rangle 9$ .  $\gamma(b_1) - b_2 \in \ker g_2$

$\langle 1 \rangle 10$ .  $\gamma(b_1) - b_2 \in \operatorname{im} f_2$

$\langle 1 \rangle 11$ . PICK  $a_2 \in A_2$  such that  $f_2(a_2) = \gamma(b_1) - b_2$ .

$\langle 1 \rangle 12$ . PICK  $a_1 \in A_1$  such that  $\beta(a_1) = a_2$ .

PROOF:  $\beta$  is surjective.

$\langle 1 \rangle 13$ .  $\gamma(f_1(a_1)) = \gamma(b_1) - b_2$

$\langle 1 \rangle 14$ .  $b_2 = \gamma(b_1 - f_1(a_1))$

□

**Theorem 35.8** (Snake Lemma). *Suppose we have  $R$ -modules and homomorphisms*

$$\begin{array}{ccccccc} 0 & \longrightarrow & L_1 & \xrightarrow{\alpha_1} & M_1 & \xrightarrow{\beta_1} & N_1 \longrightarrow 0 \\ & & \downarrow \lambda & & \downarrow \mu & & \downarrow \nu \\ 0 & \longrightarrow & L_0 & \xrightarrow{\alpha_0} & M_0 & \xrightarrow{\beta_0} & N_0 \longrightarrow 0 \end{array}$$

*such that the diagram commutes and the two rows are short exact sequences. Then there exists a homomorphism  $\delta : \ker \nu \rightarrow \operatorname{coker} \lambda$  such that the following is an exact sequence.*

$$0 \rightarrow \ker \lambda \xrightarrow{\alpha_1} \ker \mu \xrightarrow{\beta_1} \ker \nu \xrightarrow{\delta} \operatorname{coker} \lambda \xrightarrow{\alpha_0} \operatorname{coker} \mu \xrightarrow{\beta_0} \operatorname{coker} \nu \rightarrow 0 .$$

PROOF:

$\langle 1 \rangle 1$ . Define  $\delta : \ker \nu \rightarrow \operatorname{coker} \lambda$ .

$\langle 2 \rangle 1$ . LET:  $a \in \ker \nu$

$\langle 2 \rangle 2$ . PICK  $c \in M_1$  such that  $\beta_1(c) = a$ .

PROOF: Since  $\beta_1$  is surjective.

$\langle 2 \rangle 3$ . LET:  $d = \mu(c)$

$\langle 2 \rangle 4$ .  $d \in \ker \beta_0 = \operatorname{im} \alpha_0$

PROOF: Since  $\beta_0(d) = \beta_0(\mu(c)) = \nu(a) = 0$ .

$\langle 2 \rangle 5$ . LET:  $e \in L_0$  be the element such that  $\alpha_0(e) = d$ .

$\langle 2 \rangle 6$ . LET:  $\delta(a) = e + \operatorname{im} \lambda$

$\langle 1 \rangle 2$ .  $\delta$  is a left- $R$ -module homomorphism.

$\langle 2 \rangle 1$ . For  $a, a' \in \ker \nu$  we have  $\delta(a + a') = \delta(a) + \delta(a')$ .

$\langle 3 \rangle 1$ . LET:  $a, a' \in \ker \nu$

$\langle 3 \rangle 2$ . LET:  $c, c', c'' \in M_1$  and  $e, e', e'' \in L_0$  be the elements such that

$$\beta_1(c) = a$$

$$\beta_1(c') = a'$$

$$\beta_1(c'') = a + a'$$

$$\alpha_0(e) = \mu(c)$$

$$\alpha_0(e') = \mu(c')$$

$$\alpha_0(e'') = \mu(c'')$$

$$\delta(a) = e + \text{im } \lambda$$

$$\delta(a') = e' + \text{im } \lambda$$

$$\delta(a + a') = e'' + \text{im } \lambda$$

$\langle 3 \rangle 3$ .  $c'' - c - c' \in \ker \beta_1 = \text{im } \alpha_1$

$\langle 3 \rangle 4$ . PICK  $g \in L_1$  such that  $\alpha_1(g) = c'' - c - c'$ .

$\langle 3 \rangle 5$ .  $\alpha_0(\lambda(g)) = \alpha_0(e'' - e - e')$

$\langle 3 \rangle 6$ .  $\lambda(g) = e'' - e - e'$

$\langle 3 \rangle 7$ .  $e'' - e - e' \in \text{im } \lambda$

$\langle 3 \rangle 8$ .  $e'' + \text{im } \lambda = e + e' + \text{im } \lambda$

$\langle 3 \rangle 9$ .  $\delta(a + a') = \delta(a) + \delta(a')$

$\langle 2 \rangle 2$ . For  $r \in R$  and  $a \in \ker \nu$  we have  $\delta(ra) = r\delta(a)$ .

$\langle 3 \rangle 1$ . LET:  $r \in R$  and  $a \in \ker \nu$

$\langle 3 \rangle 2$ . LET:  $c, c' \in M_1$  and  $e, e' \in L_0$  be the elements such that

$$\beta_1(c) = a$$

$$\beta_1(c') = ra$$

$$\alpha_0(e) = \mu(c)$$

$$\alpha_0(e') = \mu(c')$$

$$\delta(a) = e + \text{im } \lambda$$

$$\delta(ra) = e' + \text{im } \lambda$$

$\langle 3 \rangle 3$ .  $rc - c' \in \ker \beta_1 = \text{im } \alpha_1$

$\langle 3 \rangle 4$ . PICK  $g \in L_1$  such that  $\alpha_1(g) = rc - c'$ .

$\langle 3 \rangle 5$ .  $\alpha_0(\lambda(g)) = \alpha_0(re - e')$

$\langle 3 \rangle 6$ .  $\lambda(g) = re - e'$

$\langle 3 \rangle 7$ .  $re - e' \in \text{im } \lambda$

$\langle 3 \rangle 8$ .  $re + \text{im } \lambda = e' + \text{im } \lambda$

$\langle 3 \rangle 9$ .  $r\delta(a) = \delta(ra)$

$\langle 1 \rangle 3$ . The sequence is exact at  $\ker \lambda$ .

PROOF: Since  $\alpha_1$  is injective.

$\langle 1 \rangle 4$ . The sequence is exact at  $\ker \mu$ .

PROOF: Since  $\text{im } \alpha_1 = \ker \beta_1$ .

$\langle 1 \rangle 5$ . The sequence is exact at  $\ker \nu$ , i.e.

$$\beta a_1(\ker \mu) = \ker \delta.$$

$\langle 2 \rangle 1$ . LET:  $a \in \ker \nu$

$\langle 2 \rangle 2$ . LET:  $c \in M_1$  and  $e \in L_0$  be the elements such that  $\beta_1(c) = a$ ,  $\alpha_0(e) = \mu(c)$ , and  $\delta(a) = e + \text{im } \lambda$ .

- (2)3. If  $\delta(a) = \text{im } \lambda$  then  $a \in \beta_1(\ker \mu)$   
 (3)1. ASSUME:  $\delta(a) = \text{im } \lambda$   
 (3)2.  $e \in \text{im } \lambda$   
 (3)3. PICK  $g \in L_1$  such that  $\lambda(g) = e$   
 (3)4.  $\mu(\alpha_1(g)) = \mu(c)$   
 (3)5.  $c - \alpha_1(g) \in \ker \mu$   
 (3)6.  $a = \beta_1(c - \alpha_1(g))$   
 (2)4. If  $a \in \beta_1(\ker \mu)$  then  $\delta(a) = \text{im } \lambda$   
 (3)1. ASSUME:  $c' \in \ker \mu$  and  $a = \beta_1(c')$   
 (3)2.  $c - c' \in \ker \beta_1 = \text{im } \alpha_1$   
 (3)3. PICK  $g \in L_1$  such that  $\alpha_1(g) = c - c'$   
 (3)4.  $\alpha_0(\lambda(g)) = \mu(c) - \mu(c') = \alpha_0(e) - 0 = \alpha_0(e)$   
 (3)5.  $\lambda(g) = e$   
 (3)6.  $e \in \text{im } \lambda$   
 (3)7.  $\delta(a) = \text{im } \lambda$   
 (1)6. The sequence is exact at  $\text{coker } \lambda$ .  
 (2)1. LET:  $e \in L_0$   
 PROVE:  $e + \text{im } \lambda \in \text{im } \delta$  iff  $\alpha_0(e) \in \text{im } \mu$ .  
 (2)2. For all  $a \in \ker \nu$ , if  $\delta(a) = e + \text{im } \lambda$  then  $\alpha_0(e) \in \text{im } \mu$   
 PROOF: From (1)1 and the fact that  $\alpha_0$  is injective hence  $e$  is unique given  $a$ .  
 (2)3. For all  $e \in L_0$ , if  $\alpha_0(e) \in \text{im } \mu$  then  $e + \text{im } \lambda \in \text{im } \delta$ .  
 (3)1. LET:  $e \in L_0$   
 (3)2. ASSUME:  $\alpha_0(e) \in \text{im } \mu$   
 (3)3. PICK  $c \in M_1$  such that  $\mu(c) = \alpha_0(e)$ .  
 PROVE:  $e + \text{im } \lambda = \delta(\beta_1(c))$   
 (3)4. PICK  $c' \in M_1$  and  $e' \in L_0$  such that  $\beta_1(c') = \beta_1(c)$ ,  $\alpha_0(e') = \mu(c')$   
 and  $\delta(\beta_1(c)) = e' + \text{im } \lambda$   
 (3)5.  $c - c' \in \ker \beta_1 = \text{im } \alpha_1$   
 (3)6. PICK  $g \in L_1$  such that  $\alpha_1(g) = c - c'$ .  
 (3)7.  $\alpha_0(\lambda(g)) = \alpha_0(e - e')$   
 (3)8.  $\lambda(g) = e - e'$   
 (3)9.  $e + \text{im } \lambda = e' + \text{im } \lambda = \delta(\beta_1(c))$   
 (1)7. The sequence is exact at  $\text{coker } \mu$ .  
 PROOF: Since  $\text{im } \alpha_0 = \ker \beta_0$ .  
 (1)8. The sequence is exact at  $\text{coker } \nu$ .  
 PROOF: Since  $\beta_0$  is surjective.

□

**Corollary 35.8.1.** *Suppose we have  $R$ -modules and homomorphisms*

$$\begin{array}{ccccccc}
 0 & \longrightarrow & L_1 & \xrightarrow{\alpha_1} & M_1 & \xrightarrow{\beta_1} & N_1 \longrightarrow 0 \\
 & & \downarrow \lambda & & \downarrow \mu & & \downarrow \nu \\
 0 & \longrightarrow & L_0 & \xrightarrow{\alpha_0} & M_0 & \xrightarrow{\beta_0} & N_0 \longrightarrow 0
 \end{array}$$

*such that the diagram commutes and the two rows are short exact sequences.*

Suppose  $\mu$  is surjective and  $\nu$  is injective. Then  $\lambda$  is surjective and  $\nu$  is an isomorphism.

PROOF: We have  $\ker \nu = \operatorname{coker} \mu = 0$  and so  $0 \xrightarrow{\delta} \operatorname{coker} \lambda \xrightarrow{\alpha_0} 0$  is an exact sequence, hence  $\operatorname{coker} \lambda = 0$  and so  $\lambda$  is surjective.

Since  $\operatorname{coker} \mu = 0$  we have  $0 \rightarrow \operatorname{coker} \nu \rightarrow 0$  is an exact sequence and so  $\operatorname{coker} \nu = 0$ , hence  $\nu$  is surjective, hence  $\nu$  is an isomorphism.  $\square$

**Proposition 35.9** (Short Five-Lemma). *Suppose we have  $R$ -modules and homomorphisms*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L_1 & \xrightarrow{\alpha_1} & M_1 & \xrightarrow{\beta_1} & N_1 & \longrightarrow & 0 \\ & & \downarrow \lambda & & \downarrow \mu & & \downarrow \nu & & \\ 0 & \longrightarrow & L_0 & \xrightarrow{\alpha_0} & M_0 & \xrightarrow{\beta_0} & N_0 & \longrightarrow & 0 \end{array}$$

such that the diagram commutes and the two rows are short exact sequences. If  $\lambda$  and  $\nu$  are isomorphisms then  $\mu$  is an isomorphism.

PROOF:

$\langle 1 \rangle 1$ . There exists a homomorphism  $\delta : 0 \rightarrow L_0$  such that the following is an exact sequence.

$$0 \rightarrow 0 \rightarrow \ker \mu \rightarrow 0 \xrightarrow{\delta} L_0 \xrightarrow{\alpha_0} \operatorname{coker} \mu \xrightarrow{\beta_0} N_0 \rightarrow 0.$$

PROOF: Snake Lemma

$\langle 1 \rangle 2$ .  $\ker \mu = 0$

$\langle 1 \rangle 3$ .  $\operatorname{coker} \mu = M_0$

$\square$

**Proposition 35.10.** *If  $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$  is an exact sequence and  $L$  and  $N$  are Noetherian then  $M$  is Noetherian.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $P$  be a submodule of  $M$ .

$\langle 1 \rangle 2$ . PICK  $a_1, \dots, a_m$  generate  $\alpha^{-1}(P)$ .

$\langle 1 \rangle 3$ . PICK  $c_1, \dots, c_n$  that generate  $\beta(P)$ .

$\langle 1 \rangle 4$ . For  $i = 1, \dots, n$ , PICK  $b_i$  such that  $\beta(b_i) = c_i$ .

PROVE:  $\alpha(a_1), \dots, \alpha(a_m), b_1, \dots, b_n$  generate  $P$ .

$\langle 1 \rangle 5$ . LET:  $p \in P$

$\langle 1 \rangle 6$ . PICK  $r_1, \dots, r_n \in R$  such that  $r_1 c_1 + \dots + r_n c_n = \beta(p)$

$\langle 1 \rangle 7$ .  $r_1 b_1 + \dots + r_n b_n - p \in \ker \beta = \operatorname{im} \alpha$

$\langle 1 \rangle 8$ . PICK  $s_1, \dots, s_m \in R$  such that  $\alpha(s_1 a_1 + \dots + s_m a_m) = r_1 b_1 + \dots + r_n b_n - p$ .

$\langle 1 \rangle 9$ .  $p = s_1 \alpha(a_1) + \dots + s_m \alpha(a_m) + r_1 b_1 + \dots + r_n b_n$

$\square$

**Proposition 35.11.** *Let  $R$  be a ring. Let*

$$0 \rightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \rightarrow 0$$



be a short exact sequence of left- $R$ -modules. Let  $L$  be an  $R$ -module. Then the following is an exact sequence:

$$0 \rightarrow R\text{-}\mathbf{Mod}[P, L] \xrightarrow{R\text{-}\mathbf{Mod}[\beta, \text{id}_L]} R\text{-}\mathbf{Mod}[N, L] \xrightarrow{R\text{-}\mathbf{Mod}[\alpha, \text{id}_L]} R\text{-}\mathbf{Mod}[M, L] .$$

PROOF:

$\langle 1 \rangle 1.$   $R\text{-}\mathbf{Mod}[\beta, \text{id}_L]$  is injective.

PROOF: Since  $\beta$  is epi.

$\langle 1 \rangle 2.$   $\text{im } R\text{-}\mathbf{Mod}[\beta, \text{id}_L] = \ker R\text{-}\mathbf{Mod}[\alpha, \text{id}_L]$

$\langle 2 \rangle 1.$   $\text{im } R\text{-}\mathbf{Mod}[\beta, \text{id}_L] \subseteq \ker R\text{-}\mathbf{Mod}[\alpha, \text{id}_L]$

PROOF: For any  $\gamma \in R\text{-}\mathbf{Mod}[P, L]$  we have  $\gamma \circ \beta \circ \alpha = 0$  because  $\beta \circ \alpha = 0$ .

$\langle 2 \rangle 2.$   $\ker R\text{-}\mathbf{Mod}[\alpha, \text{id}_L] \subseteq \text{im } R\text{-}\mathbf{Mod}[\beta, \text{id}_L]$

$\langle 3 \rangle 1.$  LET:  $\gamma \in \ker R\text{-}\mathbf{Mod}[\alpha, \text{id}_L]$

$\langle 3 \rangle 2.$   $\gamma \circ \alpha = 0$

$\langle 3 \rangle 3.$  PICK  $\delta : P \rightarrow L$  by: for all  $p \in P$ , we have  $\delta(p) = \gamma(n)$  where  $n \in N$  is an element such that  $\beta(n) = p$ .

PROVE:  $\delta \circ \beta = \gamma$

$\langle 3 \rangle 4.$  LET:  $n \in N$

PROVE:  $\delta(\beta(n)) = \gamma(n)$

$\langle 3 \rangle 5.$  PICK  $n' \in N$  such that  $\delta(\beta(n)) = \gamma(n')$  and  $\beta(n') = \beta(n)$

$\langle 3 \rangle 6.$   $n - n' \in \ker \beta = \text{im } \alpha$

$\langle 3 \rangle 7.$  PICK  $m \in M$  such that  $\alpha(m) = n - n'$

$\langle 3 \rangle 8.$   $0 = \gamma(\alpha(m)) = \gamma(n) - \gamma(n')$

$\langle 3 \rangle 9.$   $\gamma(n) = \gamma(n') = \delta(\beta(n))$

□

**Theorem 35.12** (Nine-Lemma). *Let the following be a commuting diagram of left- $R$ -modules.*

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L_2 & \xrightarrow{f_2} & M_2 & \xrightarrow{g_2} & N_2 \longrightarrow 0 \\
 & & \downarrow \alpha_1 & & \downarrow \beta_1 & & \downarrow \gamma_1 \\
 0 & \longrightarrow & L_1 & \xrightarrow{f_1} & M_1 & \xrightarrow{g_1} & N_1 \longrightarrow 0 \\
 & & \downarrow \alpha_0 & & \downarrow \beta_0 & & \downarrow \gamma_0 \\
 0 & \longrightarrow & L_0 & \xrightarrow{f_0} & M_0 & \xrightarrow{g_0} & N_0 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

*If the rows are exact and the two rightmost columns are exact then the left column is exact.*

PROOF:

$\langle 1 \rangle 1.$   $(L_2, f_2)$  is the kernel of  $g_2$ ,  $(L_1, f_1)$  is the kernel of  $g_1$  and  $(L_0, f_0)$  is the kernel of  $g_0$ .

$\langle 1 \rangle 2$ . 0 is the cokernel of  $g_2, g_1$  and  $g_0$ .

$\langle 1 \rangle 3$ . PICK a homomorphism  $\delta : L_0 \rightarrow 0$  such that the following is an exact sequence:

$$L_2 \xrightarrow{\beta_1 \upharpoonright L_2} L_1 \xrightarrow{\beta_0 \upharpoonright L_1} L_0 \xrightarrow{\delta} 0 \rightarrow 0 \rightarrow 0$$

PROOF: Snake Lemma.

$\langle 1 \rangle 4$ .  $\beta_1 \upharpoonright L_2 = \alpha_1$

$\langle 1 \rangle 5$ .  $\beta_0 \upharpoonright L_1 = \alpha_0$

$\langle 1 \rangle 6$ . The following is an exact sequence:

$$0 \rightarrow L_2 \xrightarrow{\alpha_1} L_1 \xrightarrow{\alpha_0} L_0 \rightarrow 0$$

□

**Theorem 35.13.** *Let the following be a commuting diagram of left- $R$ -modules.*

$$\begin{array}{ccccccc}
 & \vdots & & \vdots & & \vdots & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & L_{i+1} & \longrightarrow & M_{i+1} & \longrightarrow & N_{i+1} \longrightarrow 0 \\
 & & \downarrow \alpha_{i+1} & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L_i & \longrightarrow & M_i & \longrightarrow & N_i \longrightarrow 0 \\
 & & \downarrow \alpha_i & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L_{i-1} & \xrightarrow{f_{i-1}} & M_{i-1} & \longrightarrow & N_{i-1} \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \vdots & & \vdots & & \vdots
 \end{array}$$

*Assume the central column is a complex and every row is an exact complex. Then the left and right columns are complexes. Further, if any two of the columns are exact, then so is the third.*

PROOF:

$\langle 1 \rangle 1$ . The left column is a complex.

$\langle 2 \rangle 1$ . LET:  $x \in L_{i+1}$

$\langle 2 \rangle 2$ .  $f_{i-1}(\alpha_i(\alpha_{i+1}(x))) = 0$

$\langle 2 \rangle 3$ .  $\alpha_i(\alpha_{i+1}(x)) = 0$

PROOF:  $f_{i-1}$  is injective.

$\langle 1 \rangle 2$ . The right column is a complex.

$\langle 2 \rangle 1$ . LET:  $x \in N_{i+1}$

$\langle 2 \rangle 2$ . PICK  $y \in N_{i+1}$  such that  $g_{i+1}(y) = x$

$\langle 2 \rangle 3$ .  $\gamma_i(\gamma_{i+1}(x)) = 0$

PROOF:

$$\begin{aligned}
 \gamma_i(\gamma_{i+1}(x)) &= \gamma_i(\gamma_{i+1}(g_{i+1}(y))) \\
 &= g_{i-1}(\beta_i(\beta_{i+1}(y))) \\
 &= g_{i-1}(0) \\
 &= 0
 \end{aligned}$$

- (1)3. If the left and center columns are exact then the right column is exact.
- (2)1. LET:  $n_i \in \ker \gamma_{i-1}$   
PROVE:  $n_i \in \operatorname{im} \gamma_i$
  - (2)2. PICK  $m_i \in M_i$  such that  $g_i(m_i) = n_i$
  - (2)3.  $g_{i-1}(\beta_i(m_i)) = 0$
  - (2)4.  $\beta_i(m_i) \in \ker g_{i-1} = \operatorname{im} f_{i-1}$
  - (2)5. PICK  $l_{i-1} \in L_{i-1}$  such that  $f_{i-1}(l_{i-1}) = \beta_i(m_i)$
  - (2)6.  $\beta_{i-1}(f_{i-1}(l_{i-1})) = 0$
  - (2)7.  $f_{i-2}(\alpha_{i-1}(l_{i-1})) = 0$
  - (2)8.  $\alpha_{i-1}(l_{i-1}) = 0$
  - (2)9.  $l_{i-1} \in \ker \alpha_{i-1} = \operatorname{im} \alpha_i$
  - (2)10. PICK  $l_i \in L_i$  such that  $\alpha_i(l_i) = l_{i-1}$
  - (2)11.  $\beta_i(f_i(l_i)) = \beta_i(m_i)$
  - (2)12.  $f_i(l_i) - m_i \in \ker \beta_i = \operatorname{im} \beta_{i+1}$
  - (2)13. PICK  $m_{i+1} \in M_{i+1}$  such that  $\beta_{i+1}(m_{i+1}) = f_i(l_i) - m_i$
  - (2)14.  $\gamma_{i+1}(-g_{i+1}(m_{i+1})) = n_i$
- (1)4. If the left and right columns are exact then the center column is exact.
- (2)1. LET:  $x \in \ker \beta_i$   
PROVE:  $x \in \operatorname{im} \beta_{i+1}$
  - (2)2.  $g_{i-1}(\beta_i(x)) = 0$
  - (2)3.  $\gamma_i(g_i(x)) = 0$
  - (2)4.  $g_i(x) \in \ker \gamma_i = \operatorname{im} \gamma_{i+1}$
  - (2)5. PICK  $n_{i+1} \in N_{i+1}$  such that  $\gamma_{i+1}(n_{i+1}) = g_i(x)$
  - (2)6. PICK  $m_{i+1} \in M_{i+1}$  such that  $g_{i+1}(m_{i+1}) = n_{i+1}$
  - (2)7.  $g_i(\beta_{i+1}(m_{i+1})) = g_i(x)$
  - (2)8.  $\beta_{i+1}(m_{i+1}) - x \in \ker g_i = \operatorname{im} f_i$
  - (2)9. PICK  $l_i \in L_i$  such that  $f_i(l_i) = \beta_{i+1}(m_{i+1}) - x$
  - (2)10.  $\beta_i(f_i(l_i)) = 0$
  - (2)11.  $f_{i-1}(\alpha_i(l_i)) = 0$
  - (2)12.  $\alpha_i(l_i) = 0$
  - (2)13.  $l_i \in \ker \alpha_i = \operatorname{im} \alpha_{i+1}$
  - (2)14. PICK  $l_{i+1} \in L_{i+1}$  such that  $\alpha_{i+1}(l_{i+1}) = l_i$
  - (2)15.  $\beta_{i+1}(f_{i+1}(l_{i+1})) = \beta_{i+1}(m_{i+1}) - x$
  - (2)16.  $x = \beta_{i+1}(m_{i+1} - f_{i+1}(l_{i+1}))$
- (1)5. If the center and right columns are exact then the left column is exact.
- (2)1. LET:  $l_i \in \ker \alpha_i$   
PROVE:  $l_i \in \operatorname{im} \alpha_{i+1}$
  - (2)2.  $\beta_i(f_i(l_i)) = 0$
  - (2)3.  $f_i(l_i) \in \ker \beta_i = \operatorname{im} \beta_{i+1}$
  - (2)4. PICK  $m_{i+1} \in M_{i+1}$  such that  $\beta_{i+1}(m_{i+1}) = f_i(l_i)$
  - (2)5.  $\gamma_{i+1}(g_{i+1}(m_{i+1})) = 0$
  - (2)6.  $g_{i+1}(m_{i+1}) \in \ker \gamma_{i+1} = \operatorname{im} \gamma_{i+2}$
  - (2)7. PICK  $n_{i+2} \in N_{i+2}$  such that  $\gamma_{i+2}(n_{i+2}) = g_{i+1}(m_{i+1})$
  - (2)8. PICK  $m_{i+2} \in M_{i+2}$  such that  $g_{i+2}(m_{i+2}) = n_{i+2}$
  - (2)9.  $g_{i+1}(\beta_{i+2}(n_{i+2})) = g_{i+1}(m_{i+1})$
  - (2)10.  $\beta_{i+2}(n_{i+2}) - m_{i+1} \in \ker g_{i+1} = \operatorname{im} f_{i+1}$

- (2)11. PICK  $l_{i+1} \in L_{i+1}$  such that  $f_{i+1}(l_{i+1}) = \beta_{i+2}(n_{i+2}) - m_{i+1}$   
 (2)12.  $f_i(\alpha_{i+1}(l_{i+1})) = -f_i(l_i)$   
 (2)13.  $l_i = \alpha_{i+1}(-l_{i+1})$

□

**Corollary 35.13.1** (Nine-Lemma). *Let the following be a commuting diagram of left- $R$ -modules.*

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L_2 & \xrightarrow{f_2} & M_2 & \xrightarrow{g_2} & N_2 \longrightarrow 0 \\
 & & \downarrow \alpha_1 & & \downarrow \beta_1 & & \downarrow \gamma_1 \\
 0 & \longrightarrow & L_1 & \xrightarrow{f_1} & M_1 & \xrightarrow{g_1} & N_1 \longrightarrow 0 \\
 & & \downarrow \alpha_0 & & \downarrow \beta_0 & & \downarrow \gamma_0 \\
 0 & \longrightarrow & L_0 & \xrightarrow{f_0} & M_0 & \xrightarrow{g_0} & N_0 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

*If the rows are exact and the two leftmost columns are exact then the right column is exact.*

**Proposition 35.14.** *Let the following be a commuting diagram of left- $R$ -modules.*

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L_2 & \xrightarrow{f_2} & M_2 & \xrightarrow{g_2} & N_2 \longrightarrow 0 \\
 & & \downarrow \alpha_1 & & \downarrow \beta_1 & & \downarrow \gamma_1 \\
 0 & \longrightarrow & L_1 & \xrightarrow{f_1} & M_1 & \xrightarrow{g_1} & N_1 \longrightarrow 0 \\
 & & \downarrow \alpha_0 & & \downarrow \beta_0 & & \downarrow \gamma_0 \\
 0 & \longrightarrow & L_0 & \xrightarrow{f_0} & M_0 & \xrightarrow{g_0} & N_0 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

*If the rows are exact and the left and right columns are exact then  $\beta_1$  is monic.*

PROOF: By the Snake Lemma, the following is an exact sequence

$$0 \rightarrow \ker \alpha_1 \rightarrow \ker \beta_1 \rightarrow \ker \gamma_1$$

But  $\ker \alpha_1 = \ker \gamma_1 = 0$  so  $\ker \beta_1 = 0$ . □

**Proposition 35.15.** *Let the following be a commuting diagram of left- $R$ -modules.*

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L_2 & \xrightarrow{f_2} & M_2 & \xrightarrow{g_2} & N_2 \longrightarrow 0 \\
 & & \downarrow \alpha_1 & & \downarrow \beta_1 & & \downarrow \gamma_1 \\
 0 & \longrightarrow & L_1 & \xrightarrow{f_1} & M_1 & \xrightarrow{g_1} & N_1 \longrightarrow 0 \\
 & & \downarrow \alpha_0 & & \downarrow \beta_0 & & \downarrow \gamma_0 \\
 0 & \longrightarrow & L_0 & \xrightarrow{f_0} & M_0 & \xrightarrow{g_0} & N_0 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

*If the rows are exact and the left and right columns are exact then  $\beta_0$  is epi.*

PROOF: Similar.  $\square$

**Proposition 35.16.** *Let the following be a commuting diagram of left- $R$ -modules.*

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & L_2 & \xrightarrow{f_2} & M_2 & \xrightarrow{g_2} & N_2 \longrightarrow 0 \\
 & & \downarrow \alpha_1 & & \downarrow \beta_1 & & \downarrow \gamma_1 \\
 0 & \longrightarrow & L_1 & \xrightarrow{f_1} & M_1 & \xrightarrow{g_1} & N_1 \longrightarrow 0 \\
 & & \downarrow \alpha_0 & & \downarrow \beta_0 & & \downarrow \gamma_0 \\
 0 & \longrightarrow & L_0 & \xrightarrow{f_0} & M_0 & \xrightarrow{g_0} & N_0 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

*If the rows are exact, the left and right columns are exact, and the central column is a complex, then the central column is exact.*

PROOF:

$\langle 1 \rangle 1.$  LET:  $x \in \ker \beta_0$

PROVE:  $x \in \operatorname{im} \beta_1$

$\langle 1 \rangle 2.$   $\gamma_0(g_1(x)) = 0$

$\langle 1 \rangle 3.$   $g_1(x) \in \ker \gamma_0 = \operatorname{im} \gamma_1$

$\langle 1 \rangle 4.$  PICK  $n_2 \in N_2$  such that  $\gamma_1(n_2) = g_1(x)$

$\langle 1 \rangle 5.$  PICK  $m_2 \in M_2$  such that  $g_2(m_2) = n_2$

$\langle 1 \rangle 6.$   $g_1(\beta_1(m_2)) = g_1(x)$

$\langle 1 \rangle 7.$   $\beta_1(m_2) - x \in \ker g_1 = \operatorname{im} f_1$

$\langle 1 \rangle 8.$  PICK  $l_1 \in L_1$  such that  $f_1(l_1) = \beta_1(m_2) - x$ .

- ⟨1⟩9.  $f_0(\alpha_0(l_1)) = 0$   
 ⟨1⟩10.  $\alpha_0(l_1) = 0$   
 ⟨1⟩11.  $l_1 \in \ker \alpha_0 = \operatorname{im} \alpha_1$   
 ⟨1⟩12. PICK  $l_2 \in L_2$  such that  $\alpha_1(l_2) = l_1$ .  
 ⟨1⟩13.  $\beta_1(f_2(l_2)) = \beta_1(m_2) - x$   
 ⟨1⟩14.  $x = \beta_1(m_2 - f_2(l_2))$   
 $\square$

**Example 35.17.** We cannot remove the hypothesis that the central column is a complex. Consider the situation

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xlongequal{\quad} & \mathbb{Z} \longrightarrow 0 \\
 & & \downarrow & & \downarrow \Delta & & \parallel \\
 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\kappa_1} & \mathbb{Z} \oplus \mathbb{Z} & \xrightarrow{\pi_2} & \mathbb{Z} \longrightarrow 0 \\
 & & \parallel & & \downarrow \pi_1 & & \downarrow \\
 0 & \longrightarrow & \mathbb{Z} & \xlongequal{\quad} & \mathbb{Z} & \longrightarrow & 0 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

This diagram commutes, the rows are exact, the left and right columns are exact, but the central column is not a complex and  $\operatorname{im} \Delta \neq \ker \pi_1$ .

## 35.1 Split Exact Sequences

**Definition 35.18** (Split Sequence). Let  $0 \rightarrow M_1 \xrightarrow{\alpha} N \xrightarrow{\beta} M_2 \rightarrow 0$  be a short exact sequence. Then this sequence *splits* iff there exists an isomorphism

$$\phi : N \cong M_1 \oplus M_2$$

such that  $\phi \circ \alpha = \kappa_1 : M_1 \rightarrow M_1 \oplus M_2$  and  $\beta \circ \phi^{-1} = \pi_2 : M_1 \oplus M_2 \rightarrow M_2$ .

**Proposition 35.19.** Let  $\phi : M \rightarrow N$  be a left- $R$ -module homomorphism. Then  $\phi$  has a left-inverse if and only if the sequence

$$0 \rightarrow M \xrightarrow{\phi} N \rightarrow \operatorname{coker} \phi \rightarrow 0$$

*splits*.

PROOF:

- ⟨1⟩1. If  $\phi$  has a left-inverse then the sequence splits.  
 ⟨2⟩1. ASSUME:  $\phi$  has a left-inverse  $\psi : N \rightarrow M$ .  
 ⟨2⟩2. Define  $i : N \rightarrow M \oplus \operatorname{coker} \phi$  by  $i(n) = (\psi(n), n + \operatorname{im} \phi)$ .

$\langle 2 \rangle 3$ . Define  $i^{-1} : M \oplus \text{coker } \phi$  by  $i^{-1}(m, x + \text{im } \phi) = \phi(m) + x - \phi(\psi(x))$ .

$\langle 2 \rangle 4$ .  $i \circ i^{-1} = \text{id}_{M \oplus \text{coker } \phi}$

PROOF:

$$\begin{aligned} \psi(\phi(m) + x - \phi(\psi(x))) &= m + \psi(x) - \psi(x) \\ &= m \end{aligned}$$

$\langle 2 \rangle 5$ .  $i^{-1} \circ i = \text{id}_N$

PROOF:

$$\begin{aligned} i^{-1}(\psi(n), n + \text{im } \phi) &= \phi(\psi(n)) + n - \phi(\psi(n)) \\ &= n \end{aligned}$$

$\langle 2 \rangle 6$ .  $i \circ \phi = \kappa_1 : M \rightarrow M \oplus \text{coker } \phi$

PROOF:

$$\begin{aligned} i(\phi(m)) &= (\psi(\phi(m)), \phi(m) + \text{im } \phi) \\ &= (m, \text{im } \phi) \end{aligned}$$

$\langle 2 \rangle 7$ .  $\pi \circ i^{-1} = \pi_2 : M \oplus \text{coker } \phi \rightarrow \text{coker } \phi$

PROOF:

$$\begin{aligned} i^{-1}(\psi(n), n + \text{im } \phi) + \text{im } \phi &= \phi(\psi(n)) + n - \phi(\psi(n)) + \text{im } \phi \\ &= n + \text{im } \phi \end{aligned}$$

$\langle 1 \rangle 2$ . If the sequence splits then  $\phi$  has a left-inverse.

PROOF: Since  $\kappa_1 : M \rightarrow M \oplus \text{coker } \phi$  has left inverse  $\pi_1$ .

□

**Proposition 35.20.** *Let  $\phi : M \rightarrow N$  be a left- $R$ -module homomorphism. Then  $\phi$  has a right-inverse if and only if the sequence*

$$0 \rightarrow \ker \phi \rightarrow M \xrightarrow{\phi} N \rightarrow 0$$

*splits.*

PROOF:

$\langle 1 \rangle 1$ . If  $\phi$  has a right-inverse then the sequence splits.

$\langle 2 \rangle 1$ . LET:  $\psi : N \rightarrow M$  be a right inverse to  $\phi$ .

$\langle 2 \rangle 2$ . LET:  $i : M \rightarrow \ker \phi \oplus N$  be the function  $i(m) = (m - \psi(\phi(m)), \phi(m))$ .

PROOF:  $m - \psi(\phi(m)) \in \ker \phi$  since  $\phi(m - \psi(\phi(m))) = \phi(m) - \phi(m) = 0$ .

$\langle 2 \rangle 3$ . LET:  $i^{-1} : \ker \phi \oplus N \rightarrow M$  be the function  $i^{-1}(x, n) = x + \psi(n)$ .

$\langle 2 \rangle 4$ .  $i \circ i^{-1} = \text{id}_{\ker \phi \oplus N}$

PROOF:

$$\begin{aligned} i(i^{-1}(x, n)) &= i(x + \psi(n)) \\ &= (x + \psi(n) - \psi(\phi(x)) - \psi(\phi(\psi(n))), \phi(x) + \phi(\psi(n))) \\ &= (x + \psi(n) - \psi(n), n) \\ &= (x, n) \end{aligned}$$

$\langle 2 \rangle 5$ .  $i^{-1} \circ i = \text{id}_M$

PROOF:

$$\begin{aligned} i^{-1}(i(m)) &= m - \psi(\phi(m)) + \psi(\phi(m)) \\ &= m \end{aligned}$$

$\langle 2 \rangle 6$ .  $i \circ \iota = \kappa_1$

PROOF: For  $m \in \ker \phi$  we have  $i(m) = (m - \psi(\phi(m)), \phi(m)) = (m, 0)$ .

$\langle 2 \rangle 7$ .  $\phi \circ i^{-1} = \pi_2$

PROOF:

$$\begin{aligned}\phi(i^{-1}(x, n)) &= \phi(x) + \phi(\psi(n)) \\ &= 0 + n \\ &= n\end{aligned}$$

$\langle 1 \rangle 2$ . If the sequence splits then  $\phi$  has a right-inverse.

PROOF: Since  $\kappa_2 : N \rightarrow M \oplus N$  is a right-inverse to  $\pi_2$ .

□

**Proposition 35.21.** *Let*

$$0 \rightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} F \rightarrow 0$$

*be a short exact sequence where  $F$  is free. Then the sequence splits.*

PROOF:

$\langle 1 \rangle 1$ . LET:  $F = R^{\oplus A}$

$\langle 1 \rangle 2$ . PICK  $\gamma : F \rightarrow N$  such that  $\text{id}_F = \beta \circ \gamma$

$\langle 1 \rangle 3$ . LET:  $i : M \oplus F \rightarrow N$  be the homomorphism  $i(m, f) = \alpha(m) + \gamma(f)$

$\langle 1 \rangle 4$ .  $i$  is injective.

$\langle 2 \rangle 1$ . ASSUME:  $i(m, f) = i(m', f')$

$\langle 2 \rangle 2$ .  $\alpha(m) + \gamma(f) = \alpha(m') + \gamma(f')$

$\langle 2 \rangle 3$ .  $\alpha(m - m') = \gamma(f - f')$

$\langle 2 \rangle 4$ .  $f - f' = 0$

PROOF: Applying  $\beta$  to both sides of  $\langle 2 \rangle 3$ .

$\langle 2 \rangle 5$ .  $f = f'$

$\langle 2 \rangle 6$ .  $\alpha(m - m') = 0$

$\langle 2 \rangle 7$ .  $m = m'$

PROOF: Since  $\alpha$  is injective.

$\langle 1 \rangle 5$ .  $i$  is surjective.

$\langle 2 \rangle 1$ . LET:  $n \in N$

$\langle 2 \rangle 2$ .  $n - \gamma(\beta(n)) \in \ker \beta = \text{im } \alpha$

$\langle 2 \rangle 3$ . PICK  $m \in M$  such that  $\alpha(m) = n - \gamma(\beta(n))$

$\langle 2 \rangle 4$ .  $n = i(m, \beta(n))$

$\langle 1 \rangle 6$ .  $\alpha = i \circ \kappa_1$

$\langle 1 \rangle 7$ .  $\beta \circ i = \pi_2$

□



## Chapter 36

# Homology

**Definition 36.1** (Homology). Let  $(M_\bullet, d_\bullet)$  be a chain complex. The *i*th homology of the complex is the  $R$ -module

$$H_i(M_\bullet) := \frac{\ker d_i}{\operatorname{im} d_{i+1}} .$$

**Proposition 36.2.** *Consider the complex*

$$0 \rightarrow M_1 \xrightarrow{\phi} M_0 \rightarrow 0 .$$

*The 1st homology is  $\ker \phi$ , and the 0th homology is  $\operatorname{coker} \phi$ .*



**Part V**

**Field Theory**



# Chapter 37

## Fields

**Definition 37.1** (Field). A *field* is a non-trivial commutative division ring.

**Example 37.2.**  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  are fields.

**Proposition 37.3.** *Every field is an integral domain.*

PROOF: By Propositions 13.8 and 13.9.  $\square$

**Example 37.4.** The converse does not hold:  $\mathbb{Z}$  is an integral domain but not a field.

**Proposition 37.5.** *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 37.5.1.** *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 37.6** (Wedderburn's Little Theorem). *Every finite division ring is a field.*

**Proposition 37.7.** *Every subring of a field is an integral domain.*

PROOF: Easy.  $\square$

**Proposition 37.8.** *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 37.9.** 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 37.10.** *A commutative ring is a field if and only if it is simple.*

PROOF: Proposition 23.5. □

**Corollary 37.10.1.** *Every field has Krull dimension 0.*

**Proposition 37.11.** *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  $g = qf + r$

$\langle 1 \rangle 5$ .  $r \in I$

$\langle 1 \rangle 6$ .  $r = 0$

$\langle 1 \rangle 7$ .  $g \in (f)$

□

**Proposition 37.12.** *Let  $R$  be a commutative ring and  $I$  an ideal in  $R$ . Then  $I$  is maximal iff  $R/I$  is a field.*

PROOF: From Proposition 24.3. □

**Example 37.13.** Let  $R$  be a commutative ring and  $a \in R$ . Then  $(x - a)$  is a maximal ideal in  $R[x]$  iff  $R$  is a field, since  $R[x]/(x - a) \cong R$ .

**Example 37.14.** The ideal  $(2, x)$  is a maximal ideal in  $\mathbb{Z}[x]$ , since  $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$ .

**Proposition 37.15.** *Every maximal ideal in a commutative ring is a prime ideal.*

PROOF: Since every field is an integral domain. □

**Proposition 37.16.** *Let  $R$  be a commutative ring and  $I$  an ideal in  $R$ . If  $I$  is a prime ideal and  $R/I$  is finite then  $I$  is a maximal ideal.*

PROOF: Since every finite integral domain is a field.  $\square$

**Proposition 37.17.** *Let  $R$  be a commutative ring and  $I$  a proper ideal in  $R$ . Then  $I$  is maximal iff, whenever  $J$  is an ideal and  $I \subseteq J$ , then  $I = J$  or  $J = R$ .*

**Example 37.18.** The inverse image of a maximal ideal under a homomorphism is not necessarily maximal.

Let  $i : \mathbb{Z}[x] \rightarrow \mathbb{Q}[x]$  be the inclusion. Then  $(x)$  is maximal in  $\mathbb{Q}[x]$  but its inverse image  $(x)$  is not maximal in  $\mathbb{Z}[x]$ .

**Definition 37.19** (Maximal Spectrum). Let  $R$  be a commutative ring. The *maximal spectrum* of  $R$  is the set of all maximal ideals in  $R$ .

**Proposition 37.20.** *Let  $K$  be a field. The Krull dimension of  $K[x_1, \dots, x_n]$  is  $n$ .*

**Theorem 37.21** (Hilbert's Nullstellensatz). *Let  $K$  be a field and  $L$  a subfield of  $K$ . If  $K$  is an  $L$ -algebra of finite type, then  $K$  is a finite  $L$ -algebra.*

**Proposition 37.22.** *Let  $K$  be a subfield of  $L$ . Then  $L$  is a  $K$ -algebra under multiplication.*

PROOF: Easy.  $\square$





## Chapter 38

# Algebraically Closed Fields

**Definition 38.1** (Algebraically Closed). A field  $K$  is *algebraically closed* iff, for every  $f \in K[x]$  that is not constant, there exists  $r \in K$  such that  $f(r) = 0$ .

**Theorem 38.2.**  $\mathbb{C}$  is algebraically closed.

**Proposition 38.3.** Let  $K$  be an algebraically closed field. Let  $I$  be an ideal in  $K[x]$ . Then  $I$  is maximal if and only if  $I = (x - c)$  for some  $c \in K$ .

PROOF:

$\langle 1 \rangle 1$ . If  $I$  is maximal then there exists  $c \in K$  such that  $I = (x - c)$ .

$\langle 2 \rangle 1$ . ASSUME:  $I$  is maximal.

$\langle 2 \rangle 2$ . PICK  $f$  monic of minimal degree such that  $f \in I$ .

$\langle 2 \rangle 3$ .  $f$  is not constant.

PROOF: Otherwise  $f = 1$  and  $I = K[x]$ .

$\langle 2 \rangle 4$ . PICK  $c \in K$  such that  $f(c) = 0$

$\langle 2 \rangle 5$ .  $x - c \mid f$

$\langle 2 \rangle 6$ .  $I \subseteq (x - c)$

$\langle 2 \rangle 7$ .  $I = (x - c)$

$\langle 1 \rangle 2$ . For all  $c \in K$  we have  $(x - c)$  is maximal.

PROOF: Example 37.13.

□



**Part VI**

**Linear Algebra**



## Chapter 39

# Vector Spaces

**Definition 39.1** (Vector Space). Let  $K$  be a field. A  $K$ -vector space is a  $K$ -module. A *linear map* is a homomorphism of  $K$ -modules. We write  $K - \mathbf{Vect}$  for  $K - \mathbf{Mod}$ .

**Definition 39.2.** Let  $\mathrm{GL}_n(\mathbb{R})$  be the group of invertible  $n \times n$  real matrices.  $\mathrm{GL}_n(\mathbb{R})$  acts on  $\mathbb{R}^n$  by matrix multiplication.

**Definition 39.3.** Let  $\mathrm{GL}_n(\mathbb{C})$  be the group of invertible  $n \times n$  complex matrices.  $\mathrm{GL}_n(\mathbb{C})$  acts on  $\mathbb{C}^n$  by matrix multiplication.

**Definition 39.4.** Let  $\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : \det M = 1\}$ .

**Proposition 39.5.**  $\mathrm{SL}_n(\mathbb{R})$  is a normal subgroup of  $\mathrm{GL}_n(\mathbb{R})$ .

PROOF: If  $\det M = 1$  then  $\det(AMA^{-1}) = (\det A)(\det M)(\det A)^{-1} = 1$ .  $\square$

**Proposition 39.6.**

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$$

**Definition 39.7.** Let  $\mathrm{SL}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : \det M = 1\}$ .

**Definition 39.8.** Let  $\mathrm{O}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : MM^T = M^T M = I_n\}$ .

**Proposition 39.9.** The action of  $\mathrm{O}_n(\mathbb{R})$  on  $\mathbb{R}^n$  preserves lengths and angles.

**Definition 39.10.** Let  $\mathrm{SO}_n(\mathbb{R}) = \{M \in \mathrm{O}_n(\mathbb{R}) : \det M = 1\}$ .

**Definition 39.11.** Let  $\mathrm{U}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : MM^\dagger = M^\dagger M = I_n\}$ .

**Definition 39.12.** Let  $\mathrm{SU}_n(\mathbb{C}) = \{M \in \mathrm{U}_n(\mathbb{C}) : \det M = 1\}$ .

**Proposition 39.13.** Every matrix in  $\mathrm{SU}_2(\mathbb{C})$  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:

$$\langle 1 \rangle 1. \text{ LET: } M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SU}_2(\mathbb{C})$$

$$\langle 1 \rangle 2. M^{-1} = M^\dagger$$

$$\langle 1 \rangle 3. \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} \bar{\alpha} & \bar{\gamma} \\ \bar{\beta} & \bar{\delta} \end{pmatrix}$$

$$\langle 1 \rangle 4. \text{ LET: } \alpha = a + bi \text{ and } \beta = c + di.$$

$$\langle 1 \rangle 5. \delta = \bar{\alpha} = a - bi$$

$$\langle 1 \rangle 6. \gamma = -\bar{\beta} = -c + di$$

$$\langle 1 \rangle 7. \det M = a^2 + b^2 + c^2 + d^2 = 1$$

□

**Corollary 39.13.1.**  $\text{SU}_2(\mathbb{C})$  is simply connected.

**Corollary 39.13.2.**

$$\text{SO}_3(\mathbb{R}) \cong \text{SU}_2(\mathbb{C}) / \{I, -I\}$$

PROOF: The function that maps  $\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$  to  $\begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2(bc - ad) & 2(ad + bc) \\ 2(ad + bc) & a^2 - b^2 + c^2 - d^2 & 2(bd - ac) \\ 2(bd - ac) & 2(ab + cd) & a^2 - b^2 - c^2 - d^2 \end{pmatrix}$

is a surjective homomorphism with kernel  $\{I, -I\}$ . □

**Corollary 39.13.3.** The fundamental group of  $\text{SO}_3(\mathbb{R})$  is  $C_2$ .

**Part VII**

**Linear Algebra**





# Chapter 40

## Vector Spaces

**Definition 40.1** (Vector Space). Let  $K$  be a field. A *vector space* over  $K$  is a module over  $K$ . A *linear transformation* is a  $K$ -module homomorphism.

**Definition 40.2** (Bilinear Map). Let  $K$  be a field. Let  $U, V$  and  $W$  be vector spaces over  $K$ . A function  $f : U \times V \rightarrow W$  is *bilinear* iff, for all  $u_1, u_2 \in U$  and  $v_1, v_2 \in V$  and  $\alpha \in K$ ,

$$\begin{aligned} f(u_1 + \alpha u_2, v_1) &= f(u_1, v_1) + \alpha f(u_2, v_1) \\ f(u_1, v_1 + \alpha v_2) &= f(u_1, v_1) + \alpha f(u_1, v_2) \end{aligned}$$

**Theorem 40.3.** Let  $K$  be a field. Let  $U$  and  $V$  be vector spaces. There exists a vector space  $U \otimes V$  over  $K$  and bilinear map  $-\otimes- : U \times V \rightarrow U \otimes V$ , unique up to isomorphism, such that, for every vector space  $W$  over  $K$  and bilinear map  $f : U \times V \rightarrow W$ , there exists a unique linear map  $\bar{f} : U \otimes V \rightarrow W$  such that the following diagram commutes.

$$\begin{array}{ccc} U \otimes V & \xrightarrow{\bar{f}} & W \\ -\otimes- \uparrow & \nearrow f & \\ U \times V & & \end{array}$$

Further,  $-\otimes-$  is injective and its image spans  $U \otimes V$ .

PROOF: We can construct  $U \otimes V$  as follows. Let  $L$  be the free vector space generated by  $U \times V$ . Let  $R$  be the subspace generated by all vectors of the form

$$(u_1 + \alpha u_2, v) - (u_1, v) - \alpha(u_2, v) \quad (u, v_1 + \alpha v_2) - (u, v_1) - \alpha(u, v_2)$$

Take  $U \otimes V := L/R$ .  $\square$

**Proposition 40.4.** If  $\sum_{i=1}^n u_i \otimes v_i = 0$  and  $v_1, \dots, v_n$  are linearly independent in  $V$  then  $u_1 = \dots = u_n = 0$ .

PROOF:

$\langle 1 \rangle$ 1. LET:  $f : U \times V \rightarrow V^{U*}$  be the function  $f(u, v)(\Phi) = \Phi(u)v$

- ⟨1⟩2.  $f$  is bilinear.  
 ⟨1⟩3. LET:  $\bar{f} : U \otimes V \rightarrow V^{U*}$  be the induced linear transformation.  
 ⟨1⟩4.  $\bar{f}(\sum_{i=1}^n u_i \otimes v_i) = 0$   
 ⟨1⟩5.  $\sum_{i=1}^n f(u_i, v_i) = 0$   
 ⟨1⟩6. For all  $\Phi \in U^*$  we have  $\sum_{i=1}^n \Phi(u_i)v_i = 0$   
 ⟨1⟩7. For all  $\Phi \in U^*$  we have  $\Phi(u_1) = \cdots = \Phi(u_n) = 0$   
 ⟨1⟩8.  $u_1 = \cdots = u_n = 0$   
 $\square$

**Proposition 40.5.** *Let  $U$  and  $V$  be vector spaces over  $K$  with bases  $\mathcal{B}_1$  and  $\mathcal{B}_2$ . Then  $\mathcal{B} = \{b_1 \otimes b_2 : b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2\}$  is a basis for  $U \otimes V$ .*

PROOF:

- ⟨1⟩1.  $\mathcal{B}$  is linearly independent.  
 ⟨2⟩1. ASSUME:  $\sum_{i=1}^m \sum_{j=1}^n \alpha_{ij} b_i \otimes b'_j = 0$   
 ⟨2⟩2. For all  $j$  we have  $\sum_{i=1}^m \alpha_{ij} b_i = 0$   
 PROOF: Proposition 40.4.  
 ⟨2⟩3. Each  $\alpha_{ij}$  is 0.  
 ⟨1⟩2.  $\mathcal{B}$  spans  $U \otimes V$ .

PROOF: If  $u = \alpha_1 b_1 + \cdots + \alpha_m b_m$  and  $v = \beta_1 b'_1 + \cdots + \beta_n b'_n$  then

$$u \otimes v = \sum_{i=1}^m \sum_{j=1}^n \alpha_i \beta_j (b_i \otimes b'_j)$$

The result follows since the vectors of the form  $u \otimes v$  span  $U \otimes V$ .

$\square$

**Corollary 40.5.1.** *If  $U$  and  $V$  are finite dimensional vector spaces over  $K$  then*

$$\dim(U \otimes V) = (\dim U)(\dim V) .$$

**Proposition 40.6.**  $\mathbf{Vect}_K$  is a symmetric monoidal category under  $\otimes$ .

**Part VIII**

**Measure Theory**



**Definition 40.7** ( $\sigma$ -algebra). Let  $X$  be a set. A  $\sigma$ -algebra on  $X$  is a nonempty set  $\Sigma \subseteq \mathcal{P}X$  that is closed under complement, countable union, and countable intersection.

A *measurable space* consists of a set with a  $\sigma$ -algebra.

**Definition 40.8** (Measure). Let  $(X, \sigma)$  be a measurable space. A *measure* on  $(X, \sigma)$  is a function  $\mu : \Sigma \rightarrow \mathbb{R}_{\geq 0} \cup \{+\infty\}$  such that:

- $\mu(\emptyset) = 0$
- For any countable set of pairwise disjoint sets  $\{E_n : n \in \mathbb{N}\}$  in  $\Sigma$ ,

$$\mu\left(\bigcup_{n=0}^{\infty} E_n\right) = \sum_{n=0}^{\infty} \mu(E_n) \ .$$