Mathematics

Robin Adams

March 31, 2024

Contents

Part I

Category Theory

Chapter 1

Foundations

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

Chapter 2

Categories

Definition 2.1 (Category)**.** A *category* $\mathcal{C}$ consists of:

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

such that:

Associativity Given $f : A \to B$, $g : B \to C$ and $h : C \to D$, we have $h \circ (g \circ f) = (h \circ g) \circ f$

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

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

Proposition 2.2. *The identity morphism on an object is unique.*

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

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

Definition 2.4 (Endomorphism)**.** In a category $\mathcal{C}$, an *endomorphism* on an object A is a morphism $A \to A$. We write $\mathrm{End}_{\mathcal{C}}(A)$ for $\mathcal{C}[A, A]$.

Definition 2.5 (Opposite Category)**.** For any category $\mathcal{C}$, the *opposite* category $\mathcal{C}^{\mathrm{op}}$ is the category with the same objects as $\mathcal{C}$ and

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

2.1 Preorders

Definition 2.6 (Preorder)**.** A *preorder* on a set A is a relation $\leq$ on A that is reflexive and transitive.

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

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

Example 2.7. For any ordinal α, let α be the preorder $\{\beta : \beta < \alpha\}$ under $\leq$.

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

2.2 Monomorphisms and Epimorphisms

Definition 2.9 (Monomorphism)**.** In a category, let $f : A \to B$. Then f is a *monomorphism* or *monic* iff, for every object X and morphism $x, y : X \to A$, if $fx = fy$ then $x = y$.

Definition 2.10 (Epimorphism)**.** In a category, let $f : A \to B$. Then f is a *epimorphism* or *epi* iff, for every object X and morphism $x, y : B \to X$, if $xf = yf$ then $x = y$.

Proposition 2.11. *The composite of two monomorphism is monic.*

PROOF:
⟨1⟩1. LET: $f : A \rightarrowtail B$ and $g : B \rightarrowtail C$ be monic.
⟨1⟩2. LET: $x, y : X \to A$
⟨1⟩3. ASSUME: $g \circ f \circ x = g \circ f \circ y$
⟨1⟩4. $f \circ x = f \circ y$
⟨1⟩5. $x = y$
□

Proposition 2.12. *The composite of two epimorphisms is epi.*

PROOF: Dual. □

Proposition 2.13. *Let $f : A \to B$ and $g : B \to C$. If $g \circ f$ is monic then f is monic.*

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

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

PROOF: Dual. □

Proposition 2.15. *A function is a monomorphism in* **Set** *iff it is injective.*

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

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

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

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

PROOF: Immediate from definitions. □

2.3 Sections and Retractions

Definition 2.18 (Section, Retraction)**.** In a category, let $r : A \to B$ and $s : B \to A$. Then r is a *retraction* of s, and s is a *section* of r, iff $r \circ s = \mathrm{id}_B$.

Proposition 2.19. *Every identity morphism is a section and retraction of itself.*

PROOF: Immediate from definitions. □

Proposition 2.20. *Let $r, r' : A \to B$ and $s : B \to A$. If r is a retraction of s and r' is a section of s then $r = r'$.*

PROOF:

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

□

Proposition 2.21. *Let $r_1 : A \to B$, $r_2 : B \to C$, $s_1 : B \to A$ and $s_2 : C \to B$. 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:

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

□

Proposition 2.22. *Every section is monic.*

PROOF:
$\langle 1 \rangle 1$. LET: $s : A \to B$ be a section of $r : B \to A$.
$\langle 1 \rangle 2$. LET: $x, y : X \to A$ satisfy $sx = sy$.
$\langle 1 \rangle 3$. $rsx = rsy$
$\langle 1 \rangle 4$. $x = y$
□

Proposition 2.23. *Every retraction is epi.*

PROOF: Dual. □

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

PROOF: By the Axiom of Choice. □

Example 2.25. It is not true in general that every monomorphism in any category has a section. nor that every epimorphism in any category has a retraction.

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

2.4 Isomorphisms

Definition 2.26 (Isomorphism)**.** In a category $\mathcal{C}$, a morphism $f : A \to B$ is an *isomorphism*, denoted $f : A \cong B$, iff there exists a morphism $f^{-1} : B \to A$, the *inverse* of f, such that $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$.

An *automorphism* on an object A is an isomorphism between A and itself. We write $\mathrm{Aut}_{\mathcal{C}}(A)$ 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. □

Proposition 2.28. *For any object A we have $\mathrm{id}_A : A \cong A$ and $\mathrm{id}_A^{-1} = \mathrm{id}_A$.*

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

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

PROOF: Immediate from definitions. □

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. □

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

2.5 Initial and Terminal Objects

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

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 $X \to T$.

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 $I \to J$.
$\langle 1 \rangle 2.$ LET: i^{-1} be the unique morphism $J \to I$.
$\langle 1 \rangle 3.$ $i \circ i^{-1} = \mathrm{id}_J$
  PROOF: Since there is only one morphism $J \to J$.
$\langle 1 \rangle 4.$ $i^{-1} \circ i = \mathrm{id}_I$

PROOF: Since there is only one morphism $I \to I$.
□

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

PROOF: Dual. □

Chapter 3

Functors

Definition 3.1 (Functor)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A *functor* $F : \mathcal{C} \to \mathcal{D}$ consists of:

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

such that:

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

Definition 3.2 (Identity Functor)**.** For any category $\mathcal{C}$, the *identity functor* $1_\mathcal{C} : \mathcal{C} \to \mathcal{C}$ is defined by

$$1_\mathcal{C} A = A$$
$$1_\mathcal{C} f = f$$

Definition 3.3 (Constant Functor)**.** Given categories $\mathcal{C}$, $\mathcal{D}$ and an object $D \in \mathcal{D}$, the *constant functor* $K^\mathcal{C} D : \mathcal{C} \to \mathcal{D}$ is the functor defined by

$$K^\mathcal{C} DC = D$$
$$K^\mathcal{C} Df = \mathrm{id}_D$$

3.1 Comma Categories

Definition 3.4 (Comma Category)**.** Let $F : \mathcal{C} \to \mathcal{E}$ and $G : \mathcal{D} \to \mathcal{E}$ 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 $f : FC \to GD : \mathcal{E}$

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

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

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 $1_{\mathcal{C}} \downarrow K^{\mathbf{1}}A$.

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 $K^{\mathbf{1}}A \downarrow 1_{\mathcal{C}}$.

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

Part II

Group Theory

Chapter 4

Semigroups

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

Chapter 5

Monoids

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

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

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

PROOF: Proposition 2.2.

Chapter 6

Groups

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

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

such that the following diagrams commute.

$$\begin{tikzcd} G^3 \arrow[r, "m\times \mathrm{id}_G"] \arrow[d, "\mathrm{id}_G\times m"] & G^2 \arrow[d, "m"] \\ G^2 \arrow[r, "m"] & G \end{tikzcd}$$

$$\begin{tikzcd} 1\times G \arrow[r, "e\times \mathrm{id}_G"] \arrow[dr, "\cong"] & G^2 \arrow[d, "m"] \\ & G \end{tikzcd} \qquad \begin{tikzcd} G\times 1 \arrow[r, "\mathrm{id}_G\times e"] \arrow[dr, "\cong"] & G^2 \arrow[d, "m"] \\ & G \end{tikzcd}$$

$$\begin{tikzcd} G \arrow[r, "\Delta"] \arrow[d] & G^2 \arrow[r, "\mathrm{id}_G\times i"] & G^2 \arrow[d, "m"] \\ 1 \arrow[rr, "e"] & & G \end{tikzcd} \qquad \begin{tikzcd} G \arrow[r, "\Delta"] \arrow[d] & G^2 \arrow[r, "i\times \mathrm{id}_G"] & G^2 \arrow[d, "m"] \\ 1 \arrow[rr, "e"] & & G \end{tikzcd}$$

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 $\cdot : G^2 \to G$ 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 $i = ixj = j$. □

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 $\mathrm{Aut}_{\mathcal{C}}(A)$ is a group under $gf = f \circ g$.

  For A a set, we call $S_A = \mathrm{Aut}_{\mathbf{Set}}(A)$ 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 $ga = ha$. □

Proposition 6.7. *Let G be a group and $g, h \in G$. Then $(gh)^{-1} = h^{-1}g^{-1}$.*

PROOF: Since $ghh^{-1}g^{-1} = e$. □

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*

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

PROOF:
⟨1⟩1. For all $k \in \mathbb{Z}$ we have $g^{k+1} = g^k g$
⟨2⟩1. For all $k \geq 0$ we have $g^{k+1} = g^k g$
PROOF: Immediate from definition.
⟨2⟩2. $g^{-1+1} = g^{-1}g$
PROOF: Both are equal to e.
⟨2⟩3. For all $k > 1$ we have $g^{-k+1} = g^{-k}g$
PROOF:

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

⟨1⟩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}.
⟨1⟩3. $g^{m+0} = g^m g^0$
PROOF: Since $g^m g^0 = g^m e = g^m$.
⟨1⟩4. If $g^{m+n} = g^m g^n$ then $g^{m+n+1} = g^m g^{n+1}$
PROOF:

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

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

PROOF:

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

□

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:

$$\begin{aligned} (g^m)^{n+1} &= (g^m)^n g^m && \text{(Proposition 6.9)} \\ &= g^{mn} g^m \\ &= g^{mn+m} && \text{(Proposition 6.9)} \end{aligned}$$

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

PROOF:

$$\begin{aligned} (g^m)^n &= g^{mn} \\ \therefore (g^m)^{n-1} g^m &= g^{mn-m} g^m && \text{(Proposition 6.9)} \\ \therefore (g^m)^{n-1} &= g^{mn-m} && \text{(Cancellation)} \end{aligned}$$

□

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

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

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

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

6.1 Order of an Element

Definition 6.13 (Order)**.** Let G be a group. Let $g \in G$. Then g has *finite order* iff there exists a positive integer n such that $g^n = e$. In this case, the *order* of g, denoted $|g|$, is the least positive integer n such that $g^n = e$.

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

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

PROOF:
⟨1⟩1. LET: $n = q|g| + d$ where $0 \leq d < |g|$
PROOF: Division Algorithm.
⟨1⟩2. $g^d = e$
PROOF:

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

⟨1⟩3. $d = 0$
PROOF: By minimality of $|g|$.
⟨1⟩4. $n = q|g|$
□

Corollary 6.14.1. *Let G be a group. Let $g \in G$ have finite order and $n \in \mathbb{Z}$. Then $g^n = e$ if and only if $|g| \mid n$.*

Proposition 6.15. *Let G be a group and $g \in G$. Then $|g| \leq |G|$.*

PROOF:
⟨1⟩1. ASSUME: w.l.o.g. G is finite.
⟨1⟩2. PICK i, j with $0 \leq i < j \leq |G|$ such that $g^i = g^j$.
PROOF: Otherwise $g^0, g^1, \ldots, g^{|G|}$ would be $|G| + 1$ distinct elements of G.
⟨1⟩3. $g^{j-i} = e$
⟨1⟩4. g has finite order and $|g| \leq |G|$
PROOF: Since $|g| \leq j - i \leq j \leq |G|$.
□

Proposition 6.16. *Let G be a group. Let $g \in G$ have finite order. Let $m \in \mathbb{N}$. Then*

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

PROOF: Since for any integer d we have

$$\begin{aligned} g^{md} = e &\Leftrightarrow |g| \mid md && \text{(Corollary 6.14.1)} \\ &\Leftrightarrow \operatorname{lcm}(m, |g|) \mid md \\ &\Leftrightarrow \frac{\operatorname{lcm}(m, |g|)}{m} \mid d && \square \end{aligned}$$

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

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

Proposition 6.17. *Let G be a group. Let $g, h \in G$ have finite order. Assume $gh = hg$. Then $|gh|$ has finite order and*

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

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

Example 6.18. This example shows that we cannot remove the hypothesis that $gh = hg$.

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

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

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

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

PROOF:
$\langle 1 \rangle 1.$ LET: $N = |gh|$
$\langle 1 \rangle 2.$ $g^N = (h^{-1})^N$
$\langle 1 \rangle 3.$ $g^{N|g|} = e$
$\langle 1 \rangle 4.$ $|g^N| \mid |g|$
$\langle 1 \rangle 5.$ $h^{-N|h|} = e$
$\langle 1 \rangle 6.$ $|g^N| \mid |h|$
$\langle 1 \rangle 7.$ $|g^N| = 1$
  PROOF: Since $\gcd(|g|, |h|) = 1$.
$\langle 1 \rangle 8.$ $g^N = e$
$\langle 1 \rangle 9.$ $|g| \mid N$
$\langle 1 \rangle 10.$ $h^{-N} = e$
$\langle 1 \rangle 11.$ $|h| \mid N$
$\langle 1 \rangle 12.$ $N = |g||h|$
  PROOF: Using Proposition 6.17.
∎

Proposition 6.20. *Let G be a finite group. Assume there is exactly one element $f \in G$ of order 2. Then the product of all the elements of G is f.*

PROOF: Let the elements of G be g_1, g_2, …, 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 6.21. *Let G be a finite group of order n. Let m be the number of elements of G of order 2. Then $n - m$ is odd.*

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

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

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

PROOF: Since

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

∎

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

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

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

⟨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:

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

∎

6.2 Generators

Definition 6.25 (Generator)**.** Let G be a group and $a \in G$. We say a *generates* the group iff, for all $x \in G$, there exists an integer n such that $x^n = a$.

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

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

PROOF:
⟨1⟩1. LET: $H = \langle s, t \rangle$
⟨1⟩2. For all $q \in \mathbb{Z}$ we have $\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \in H$.
PROOF: It is t^q.
⟨1⟩3. For all $q \in \mathbb{Z}$ we have $\begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} \in H$.
PROOF:

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

⟨1⟩4.
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & qa+b \\ c & qc+d \end{pmatrix}$$
⟨1⟩5.
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix} = \begin{pmatrix} a+qb & b \\ c+qd & d \end{pmatrix}$$
⟨1⟩6. For any $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, if c and d are both nonzero, then there exists $N \in H$ such that the bottom row of MN has one entry the same as M and one entry with smaller absolute value.

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

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

Proof: Apply ⟨1⟩6 repeatedly.

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

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

Proof: ⟨1⟩2

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

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

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

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

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

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

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

□

Chapter 7

Group Homomorphisms

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

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

Proposition 7.2. *Let G and H be groups with identities e_G and e_H. Let $\phi : G \to H$ 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. □

Proposition 7.3. *Let $\phi : G \to H$ be a group homomorphism. For all $x \in G$ we have $\phi(x^{-1}) = \phi(x)^{-1}$.*

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

Proposition 7.4. *Let G, H and K be groups. If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms then $\psi \circ \phi : G \to K$ is a homomorphism.*

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

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

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

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

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

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

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 $\phi : G \to H$ is an isomorphism in* **Grp** *if and only if it is bijective.*

PROOF:
$\langle 1 \rangle 1$. ASSUME: ϕ is bijective.
PROVE: ϕ^{-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'.
$\langle 1 \rangle 4$. $\phi^{-1}(hh') = \phi^{-1}(h)\phi^{-1}(h')$
$\square$

Corollary 7.9.1.
$$D_6 \cong C_3$$

PROOF: The canonical homomorphism $D_6 \to C_3$ is bijective. $\square$

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. $\square$

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

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

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 $(g, h)(g^{-1}, h^{-1}) = (g^{-1}, h^{-1})(g, h) = (e_G, e_H)$.
$\langle 1 \rangle 2$. $\pi_1 : G \times H \to G$ is a group homomorphism.
PROOF: Immediate from definitions.
$\langle 1 \rangle 3$. $\pi_2 : G \times H \to H$ is a group homomorphism.
PROOF: Immediate from definitions.
$\langle 1 \rangle 4$. For any group homomorphism $\phi : K \to G$ and $\psi : K \to H$, the function $\langle \phi, \psi \rangle : K \to G \times H$ where $\langle \phi, \psi \rangle(k) = (\phi(k), \psi(k))$ is a group homomorphism.
PROOF:
$$\begin{aligned}
\langle \phi, \psi \rangle(kk') &= (\phi(kk'), \psi(kk')) \\
&= (\phi(k)\phi(k'), \psi(k)\psi(k')) \\
&= (\phi(k), \psi(k))(\phi(k'), \psi(k')) \\
&= \langle \phi, \psi \rangle(k)\langle \phi, \psi \rangle(k')
\end{aligned}$$

$\square$

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

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 $\phi : G \to H$ 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: $x, y \in \phi^{-1}(K)$

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

Corollary 7.15.3. *Let $\phi : G \to H$ 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 $y = \phi(b)$
$\langle 1\rangle 3.$ $xy^{-1} = \phi(ab^{-1})$
$\langle 1\rangle 4.$ $xy^{-1} \in \phi(K)$
$\square$

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.
  $\langle 2\rangle 5.$ $n = qd \in d\mathbb{Z}$
$\langle 1\rangle 4.$ $d\mathbb{Z} \subseteq G$
$\square$

7.2 Kernel

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

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

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

Proof: Corollary 7.15.2. $\square$

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

PROOF:
⟨1⟩1. $\phi \circ i = 0$
⟨1⟩2. For any group K and homomorphism $\alpha : K \to G$ such that $\phi \circ \alpha = 0$, there exists a unique homomorphism $\beta : K \to \ker\phi$ such that $i \circ \beta = \alpha$.
□

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

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

PROOF:
⟨1⟩1. $1 \Rightarrow 2$
⟨2⟩1. ASSUME: ϕ is monic.
⟨2⟩2. LET: $i : \ker\phi \hookrightarrow G$, $j : \{e\} \hookrightarrow \ker\phi \hookrightarrow G$ be the inclusions.
⟨2⟩3. $\phi \circ i = \phi \circ j$
⟨2⟩4. $i = j$
⟨1⟩2. $2 \Rightarrow 3$
⟨2⟩1. ASSUME: $\ker\phi = \{e\}$
⟨2⟩2. LET: $x, y \in G$
⟨2⟩3. ASSUME: $\phi(x) = \phi(y)$
⟨2⟩4. $\phi(xy^{-1}) = e$
⟨2⟩5. $xy^{-1} \in \ker\phi$
⟨2⟩6. $xy^{-1} = e$
⟨2⟩7. $x = y$
⟨1⟩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 $\gamma_g : G \to G$ defined by $\gamma_g(a) = gag^{-1}$ is an automorphism on G.*

PROOF:
⟨1⟩1. γ_g is a homomorphism.

PROOF:

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

$\langle 1\rangle 2$. γ_g is injective.
PROOF: By Cancellation.
$\langle 1\rangle 3$. γ_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 $\mathrm{Inn}(G)$ for the set of inner automorphisms of G.

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

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

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

7.4 Direct Products

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

7.5 Free Groups

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

PROOF:
$\langle 1\rangle 1$. LET: $W(A)$ be the set of words in the alphabet whose elements are the elements of A together with $\{a^{-1} : a \in A\}$.
$\langle 1\rangle 2$. LET: $r : W(A) \to W(A)$ 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 $r(w) = w$.
$\langle 1\rangle 3$. Let us say that a word w is a *reduced word* iff $r(w) = w$.
$\langle 1\rangle 4$. For any word w of length n, we have $r^{\ulcorner \frac{n}{2} \urcorner}(w)$ is a reduced word.
PROOF: Since we cannot remove more than $n/2$ pairs of letters from w.
$\langle 1\rangle 5$. LET: $R : W(A) \to W(A)$ be the function $R(w) = r^{\ulcorner \frac{n}{2} \urcorner}(w)$, where n is the length of w.
$\langle 1\rangle 6$. LET: $F(A)$ be the set of reduced words.
$\langle 1\rangle 7$. Define $\cdot : F(A)^2 \to F(A)$ by $w \cdot w' = R(ww')$

$\langle 1 \rangle 8$. $\cdot$ is associative.

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

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

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

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

$\langle 1 \rangle 12$. LET: G be any group and $k : A \to G$ any function.

$\langle 1 \rangle 13$. The only morphism $f : (F(A), j) \to (G, k)$ 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 7.27 (Free Group)**.** For any set A, the *free group* on A is the initial object $(F(A), i)$ in $\mathcal{F}^A$.

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

PROOF:

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

$\langle 1 \rangle 2$. ASSUME: $x \neq y$
PROVE: $i(x) \neq i(y)$

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

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

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

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

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

$\square$

Proposition 7.29.

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

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

$$\begin{tikzcd}
\{e\} \arrow[r] & A \\
\emptyset \arrow[u] \arrow[ur] &
\end{tikzcd}$$

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

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

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

$$\begin{tikzcd}
& G & \\
F(A) \arrow[ur, "f"] \arrow[r, "\kappa_1"] & F(A+B) \arrow[u, "k"] & F(B) \arrow[ul, "g"'] \arrow[l, "\kappa_2"] \\
A \arrow[u, "i_A"] \arrow[r, "k_1"] & A+B \arrow[u, "j"] & B \arrow[u, "i_B"] \arrow[l, "k_2"]
\end{tikzcd}$$

PROOF:
⟨1⟩1. LET: $i_A : A \to F(A)$, $i_B : B \to F(B)$, $j : A + B \to F(A + B)$ be the canonical injections.
⟨1⟩2. LET: κ_1, κ_2 be the unique group homomorphisms that make the diagram above commute.
⟨1⟩3. LET: G be any group and $f : F(A) \to G$, $g : F(B) \to G$ any group homomorphisms.
⟨1⟩4. LET: $h : A + B \to G$ 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: $k : F(A + B) \to G$ be the unique group homomorphism such that $k \circ j = h$.
⟨1⟩6. k is the unique group homomorphism such that $k \circ \kappa_1 \circ i_A = f \circ i_A$ and $k \circ \kappa_2 \circ i_B = g \circ i_B$.
⟨1⟩7. k is the unique group homomorphism such that $k \circ \kappa_1 = f$ and $k \circ \kappa_2 = g$.
□

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

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

$$\begin{tikzcd}
F(A) \arrow[r, "\phi"] & G \\
A \arrow[u] \arrow[ur] &
\end{tikzcd}$$

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

PROOF: Immediate from definitions. □

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

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

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

PROOF: Easy. □

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

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

PROOF: TODO.

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

PROOF: TODO

Proposition 7.38.

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

PROOF: TODO

7.6 Normal Subgroups

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

Example 7.40. Every subgroup of Q_8 is normal.

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

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

PROOF:
⟨1⟩1. $1 \Leftrightarrow 2$
PROOF: Immediate from definitions.
⟨1⟩2. $2 \Rightarrow 3$
PROOF: If 2 holds then we have $gNg^{-1} \subseteq N$ and $g^{-1}Ng \subseteq N$ hence $N = gNg^{-1}$.
⟨1⟩3. $3 \Rightarrow 2$
PROOF: Trivial.
⟨1⟩4. $2 \Leftrightarrow 4$
PROOF: Easy.
⟨1⟩5. $3 \Leftrightarrow 5$
PROOF: Easy.

□

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

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

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

and so $gng^{-1} \in \ker \phi$. □

7.7 Quotient Groups

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

Proposition 7.44. *Let G be a group. Let $\sim$ be an equivalence relation on G. Then there exists an operation $\cdot : (G/\sim)^2 \to G/sim$ 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 $\pi : G \to G/\sim$ is a group homomorphism, and is universal with respect to group homomorphisms $\phi : G \to G'$ such that if $a \sim a'$ then $\phi(a) = \phi(a')$.

PROOF: Easy. □

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

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

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

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

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

PROOF: By Example 6.26.

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

PROOF:

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

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

⟨1⟩3. Define an action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathbb{R} - \mathbb{Q}$ by

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

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

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

⟨3⟩2. $aqr + bq = cpr + dp$

⟨3⟩3. $(aq - cp)r = dp - bq$

⟨3⟩4. $aq = cp = dp - bq = 0$

⟨3⟩5. $adq - cdp = 0$

⟨3⟩6. $cdp - cbq = 0$

⟨3⟩7. $(ad - cb)q = 0$

PROOF: Since $ad - cb = 1$.

⟨3⟩8. $q = 0$

⟨3⟩9. Q.E.D.

PROOF: This contradicts ⟨3⟩1.

⟨2⟩2. $-Ir = r$

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

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

PROOF:

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

⟨1⟩4.

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

⟨1⟩5.

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

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

⟨1⟩6.

$$yxr = 1 + r$$

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

⟨1⟩7.

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

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

⟨1⟩8. If $r > -1$ is positive then yxr is positive.
⟨1⟩9. If r is positive then $y^{-1}xr$ is positive.
⟨1⟩10. If $r < -1$ then $y^{-1}xr$ is positive.
⟨1⟩11. If r is negative then yr is positive.
⟨1⟩12. If r is negative then $y^{-1}r$ is positive.
⟨1⟩13. No product of the form

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

with one or more factors can equal the identity.

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

⟨1⟩14. No product of the form

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

with one or more factors can equal the identity.

PROOF: The product maps negative numbers to positive numbers.

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

□

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

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

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

PROOF: Easy. □

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

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

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

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

Example 7.52.

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

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

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

$$u : \{\textit{subgroups of } G \textit{ including } H\} \to \{\textit{subgroups of } G/H\}$$

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

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

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

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

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

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

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

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

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

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

7.8 Cosets

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

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

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

PROOF:
$\langle 1\rangle 1.$ $e \in H$
$\langle 1\rangle 2.$ For all $x, y \in H$ we have $xy^{-1} \in H$.
  $\langle 2\rangle 1.$ ASSUME: $x \sim e$ and $y \sim e$.
  $\langle 2\rangle 2.$ $e \sim y^{-1}$
    PROOF: Since $yy^{-1} \sim ey^{-1}$.
  $\langle 2\rangle 3.$ $xy^{-1} \sim e$
    PROOF: Since $xy^{-1} \sim ey^{-1} \sim e$.
$\langle 1\rangle 3.$ If $a \sim b$ then $a^{-1}b \in H$.
  PROOF: If $a \sim b$ then $a^{-1}b \sim a^{-1}a = e$.
$\langle 1\rangle 4.$ If $a^{-1}b \in H$ then $aH = bH$.
  $\langle 2\rangle 1.$ ASSUME: $a^{-1}b \in H$
  $\langle 2\rangle 2.$ $bH \subseteq aH$
    PROOF: For any $h \in H$ we have $bh = aa^{-1}bh \in aH$.
  $\langle 2\rangle 3.$ $aH \subseteq bH$
    PROOF: Similar since $b^{-1}a \in H$.
$\langle 1\rangle 5.$ If $aH = bH$ then $a \sim b$.
  $\langle 2\rangle 1.$ ASSUME: $aH = bH$
  $\langle 2\rangle 2.$ PICK $h \in H$ such that $a = bh$.
  $\langle 2\rangle 3.$ $b^{-1}a = h$
  $\langle 2\rangle 4.$ $b^{-1}a \in H$
  $\langle 2\rangle 5.$ $b^{-1}a \sim e$
  $\langle 2\rangle 6.$ $a \sim b$
    PROOF: $a = bb^{-1}a \sim be = b$.
$\square$

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

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

Proposition 7.58.

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

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

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

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

⟨2⟩1. $\sim$ is reflexive.
PROOF: For any $a \in G$ we have $a^{-1}a = e \in H$.
⟨2⟩2. $\sim$ is symmetric.
PROOF: If $a^{-1}b \in H$ then $b^{-1}a \in H$.
⟨2⟩3. $\sim$ is transitive.
PROOF: If $a^{-1}b \in H$ and $b^{-1}c \in H$ then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.
⟨1⟩2. If $a \sim_H b$ then $ga \sim_H gb$.
PROOF: If $a^{-1}b \in H$ then $(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b \in H$.
⟨1⟩3. For any equivalence relation $\sim$ on G such that, whenever $a \sim b$, then $ga \sim gb$, there exists a subgroup H such that $\sim = \sim_H$.
PROOF: Proposition 7.56.
⟨1⟩4. The $\sim_H$-equivalence class of a is aH.
PROOF:

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

□

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

PROOF: Similar. □

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

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

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

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

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

$$\begin{tikzcd} G \arrow[rr, "\phi"] \arrow[dr, "\pi"'] & & G' \\ & G/H \arrow[ur, "\overline{\phi}"'] & \end{tikzcd}$$

Proposition 7.63. *$\mathbb{Z}/n\mathbb{Z}$ has exactly n elements.*

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

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

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

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

PROOF: By Proposition 7.64. □

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

Proposition 7.66.

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

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

Example 7.67. Not all monomorphisms split in **Grp**.

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

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

Then ϕ is monic but has no retraction.

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

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

which is impossible.

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

PROOF: By Cancellation. □

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

PROOF: By Cancellation. □

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

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

PROOF:
⟨1⟩1. LET: $f : \{hK : h \in H\} \to H/(H \cap K)$ 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 $h(H \cap K) = h'(H \cap K)$.
⟨1⟩2. f is injective.
PROOF: If $h(H \cap K) = h'(H \cap K)$ then $hK = h'K$.
⟨1⟩3. f is surjective.
PROOF: Clear.
⟨1⟩4.

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

□

7.9 Congruence

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

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

PROOF: By Proposition 7.56. □

Proposition 7.73. *If $a \equiv a' \operatorname{mod} n$ and $b \equiv b' \operatorname{mod} n$ then $a + b \equiv a' + b' \operatorname{mod} n$.*

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

Proposition 7.74. *If $a \equiv a' \operatorname{mod} n$ and $b \equiv b' \operatorname{mod} n$ then $ab \equiv a'b' \operatorname{mod} n$.*

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

7.10 Cyclic Groups

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

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

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

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

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

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

Proof:
$\langle 1 \rangle 1$. Let: $G = \langle a_1/b, \ldots, a_n/b \rangle$ where $a_1, \ldots, a_n, b$ are integers with $b > 0$
$\langle 1 \rangle 2$. Let: $a = \gcd(a_1, \ldots, a_n)$
$\langle 1 \rangle 3$. $G = \langle a/b \rangle$
□

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

7.11 Commutator Subgroup

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

Proposition 7.80. *The commutator subgroup is normal.*

Proof: Since

$$\begin{aligned} & g a_1 b_1 {a_1}^{-1} {b_1}^{-1} a_2 b_2 {a_2}^{-1} {b_2}^{-1} \cdots a_n b_n {a_n}^{-1} {b_n}^{-1} g^{-1} \\ =& (g a_1 g^{-1})(g b_1 g^{-1})(g a_1 g^{-1})^{-1} (g b_1 g^{-1})^{-1} \cdots (g a_n g^{-1})(g b_n g^{-1})(g a_n g^{-1})^{-1} (g b_n g^{-1})^{-1} \end{aligned}$$. □

7.12 Presentations

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

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

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

Example 7.82.

- The free group on a set A is presented by $(A, \emptyset)$.
- S_3 is presented by $(x, y | x^2, y^3, xyxy)$.
- $(a, b \mid a^2, b^2, (ab)^n)$ is a presentation of D_{2n}.

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

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

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

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

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & A \cup A' \arrow[d] & A' \arrow[l] \arrow[d] \\
F(A) \arrow[r] \arrow[d] & F(A \cup A') \arrow[d] & F(A') \arrow[l] \arrow[d] \\
G \arrow[r, "\kappa_1"] & G * G' & G' \arrow[l, "\kappa_2"']
\end{tikzcd}$$

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

7.13 Index of a Subgroup

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

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

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

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

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

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

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

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

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

PROOF:
$\langle 1 \rangle 1$. LET: $G/K = \{g_1 K, g_2 K, \ldots, g_m K\}$
$\langle 1 \rangle 2$. LET: $K/H = \{k_1 H, k_2 H, \ldots, k_n H\}$
$\langle 1 \rangle 3$. $G/H = \{g_i k_j H : 1 \leq i \leq m, 1 \leq j \leq n\}$
  $\langle 2 \rangle 1$. LET: $g \in G$
  $\langle 2 \rangle 2$. PICK i such that $gK = g_i K$
  $\langle 2 \rangle 3$. $g^{-1} g_i \in K$
  $\langle 2 \rangle 4$. PICK j such that $g^{-1} g_i H = k_j H$
  $\langle 2 \rangle 5$. $g^{-1} g_i k_j \in H$
  $\langle 2 \rangle 6$. $gH = g_i k_j H$
$\langle 1 \rangle 4$. If $g_i k_j H = g_{i'} k_{j'} H$ then $i = i'$ and $j = j'$.
  $\langle 2 \rangle 1$. ASSUME: $g_i k_j H = g_{i'} k_{j'} H$
  $\langle 2 \rangle 2$. $g_i K = g_{i'} K$
  $\langle 2 \rangle 3$. $i = i'$
  $\langle 2 \rangle 4$. $k_j H = k_{j'} H$
  $\langle 2 \rangle 5$. $j = j'$
$\square$

7.14 Cokernels

Proposition 7.90. *Let $\phi : G \to H$ be a homomorphism between groups. Then there exists a group K and homomorphism $\pi : H \to K$ that is initial with respect to all homomorphism $\alpha : H \to L$ 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 $\operatorname{im} \phi$.
$\langle 1 \rangle 2$. LET: $K = H/N$ and π be the canonical homomorphism.
$\langle 1 \rangle 3$. LET: $\pi \circ \phi = 0$
$\langle 1 \rangle 4$. LET: $\alpha : H \to L$ satisfy $\alpha \circ \phi = 0$
$\langle 1 \rangle 5$. $\operatorname{im} \phi \subseteq \ker \alpha$
$\langle 1 \rangle 6$. $N \subseteq \ker \alpha$
$\langle 1 \rangle 7$. There exists a unique $\overline{\alpha} : H/ \operatorname{im} \phi \to L$ such that $\overline{\alpha} \circ \pi = \alpha$
$\square$

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

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

7.15 Cayley Graphs

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

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

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

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 ≤ 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 $x = \begin{pmatrix} 1 & 2 \end{pmatrix}$ and $y = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$ then $xy = \begin{pmatrix} 2 & 3 \end{pmatrix}$ and $yx = \begin{pmatrix} 1 & 3 \end{pmatrix}$.

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

$$\begin{aligned} ghgh &= e \\ \therefore hgh &= g && \text{(multiplying on the left by } g\text{)} \\ \therefore hg &= gh && \text{(multiplying on the right by } h\text{)} \square \end{aligned}$$

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 $gh = (g^{-1})^{-1}(h^{-1})^{-1} = (g^{-1}h^{-1})^{-1} = hg$.
□

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:
⟨1⟩1. If G is Abelian then the function that maps g to g^2 is a group homomorphism.
PROOF: Since $(gh)^2 = g^2h^2$.
⟨1⟩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 $hg = gh$.
□

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

PROOF:
⟨1⟩1. If G is Abelian then γ is trivial.
PROOF: Since $\gamma_g(a) = gag^{-1} = a$.
⟨1⟩2. If γ 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.
□

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:
⟨1⟩1. ASSUME: for a contradiction $|h| \nmid |g|$.
⟨1⟩2. PICK a prime p such that $|g| = p^m r$, $|h| = p^n s$ where $p \nmid r$, $p \nmid s$ and $m < n$.
⟨1⟩3. $|g^{p^m} h^s| = p^n r$
PROOF: Proposition 6.19.
⟨1⟩4. $|g| < |g^{p^m} h^s|$
⟨1⟩5. Q.E.D.
PROOF: This contradicts the maximality of $|g|$.
□

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

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

PROOF:
⟨1⟩1. $\phi + (\psi + \chi) = (\phi + \psi) + \chi$
⟨1⟩2. $\phi + \psi = \psi + \phi$
⟨1⟩3. LET: $0 : A \to H$ be the function $0(a) = 0$.
⟨1⟩4. $\phi + 0 = 0 + \phi = \phi$

$\langle 1 \rangle 5.$ Given $\phi : A \to H$, define $-\phi : A \to H$ 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 $\phi, \psi : G \to H$ 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. $\mathrm{Inn}(G)$ *is cyclic.*
2. $\mathrm{Inn}(G)$ *is trivial.*
3. G *is Abelian.*

Proof:
$\langle 1 \rangle 1.$ $1 \Rightarrow 2$
$\langle 2 \rangle 1.$ Assume: $\mathrm{Inn}(G) = \langle \gamma_g \rangle$
$\langle 2 \rangle 2.$ 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 $\gamma_x = \gamma_g^n$
$\langle 3 \rangle 3.$ $\forall y \in G. xyx^{-1} = g^n y g^{-n}$
$\langle 3 \rangle 4.$ $xgx^{-1} = g$
$\langle 2 \rangle 3.$ $\gamma_g = \mathrm{id}_G$
$\langle 1 \rangle 2.$ $2 \Rightarrow 3$
$\langle 2 \rangle 1.$ Assume: $\forall g \in G. \gamma_g = \mathrm{id}_G$
$\langle 2 \rangle 2.$ 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 $\mathrm{Aut}_{\mathbf{Grp}}(G)$ 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 $gng^{-1} = n \in N$. ∎

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

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

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

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.
∎

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. ∎

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 subgrop 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.
∎

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

PROOF:
⟨1⟩1. For all $g_1, g_2, h_1, h_2 \in G$ we have
$$(g_1 g_2) \circ (h_1 h_2) = (g_1 \circ h_1)(g_2 \circ h_2)$$
⟨1⟩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.
⟨1⟩3. e is the identity of $(G, \circ)$
⟨1⟩4. For all $g, h \in G$ we have
$$g \circ h = gh$$
PROOF:
$$\begin{aligned} g \circ h &= (ge) \circ (eh) \\ &= (g \circ e)(e \circ h) \\ &= gh \end{aligned}$$
⟨1⟩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 $(G, m : G^2 \to G, e : 1 \to G, i : G \to G)$ is a group object in* **Grp** *then m is the multiplication of G, $e(*)$ is the identity of G, $i(g) = g^{-1}$, and G is Abelian.*

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

8.1 The Category of Abelian Groups

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

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

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

PROOF: Immediate from Corollary 8.19.1. □

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

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

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

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

⟨1⟩5. $[\phi, \psi] \circ \kappa_1 = \phi$
PROOF:

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

⟨1⟩6. $[\phi, \psi] \circ \kappa_2 = \psi$
PROOF: Similar.
⟨1⟩7. If $f : G \oplus H \to K$ is a group homomorphism with $f \circ \kappa_1 = \phi$ and $f \circ \kappa_2 = \psi$ then $f = [\phi, \psi]$.
PROOF:

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

□

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

PROOF: TODO □

8.2 Free Abelian Groups

Proposition 8.25. *Let A be a set. Let $\mathcal{F}^A$ be the category whose objects are pairs (G, j) where G is an Abelian group and j is a function $A \to G$, with morphisms $f : (G, j) \to (H, k)$ the group homomorphisms $f : G \to H$ 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 $\alpha : A \to \mathbb{Z}$ such that $\alpha(a) = 0$ for only finitely many $a \in A$.
⟨1⟩2. Let: $i : A \to \mathbb{Z}^{\oplus A}$ 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 $j : A \to G$ any function.
⟨1⟩4. The unique homomorphism $\phi : \mathbb{Z}^{\oplus A} \to G$ required is defined by $\phi(\alpha) = \sum_{a \in A} \alpha(a) j(a)$

□

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

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

$$\begin{tikzcd}
 & G & \\
F^{ab}(A) \arrow[ur, "f"] \arrow[r, "\kappa_1"] & F^{ab}(A+B) \arrow[u, "k"] & F^{ab}(B) \arrow[ul, "g"'] \arrow[l, "\kappa_2"] \\
A \arrow[u, "i_A"] \arrow[r, "k_1"] & A+B \arrow[u, "j"] & B \arrow[u, "i_B"] \arrow[l, "k_2"]
\end{tikzcd}$$

Proof:

⟨1⟩1. Let: $i_A : A \to F^{ab}(A)$, $i_B : B \to F^{ab}(B)$, $j : A + B \to F^{ab}(A + B)$ be the canonical injections.
⟨1⟩2. Let: κ_1, κ_2 be the unique group homomorphisms that make the diagram above commute.
⟨1⟩3. Let: G be any group and $f : F^{ab}(A) \to G$, $g : F^{ab}(B) \to G$ any group homomorphisms.
⟨1⟩4. Let: $h : A + B \to G$ 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: $k : F^{ab}(A + B) \to G$ be the unique group homomorphism such that $k \circ j = h$.
⟨1⟩6. k is the unique group homomorphism such that $k \circ \kappa_1 \circ i_A = f \circ i_A$ and $k \circ \kappa_2 \circ i_B = g \circ i_B$.
⟨1⟩7. k is the unique group homomorphism such that $k \circ \kappa_1 = f$ and $k \circ \kappa_2 = g$.

□

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

Proof:

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

PROOF: There is a bijection between $F^{\mathrm{ab}}(C) / \sim$ and the finite subsets of C, which maps f to $\{c \in C : f(c) \text{ is odd}\}$.
$\langle 1 \rangle 4$. If $F^{\mathrm{ab}}(A) \cong F^{\mathrm{ab}}(B)$ then $A \cong B$.
PROOF: If $|F^{\mathrm{ab}}(A) / \sim| = |F^{\mathrm{ab}}(B) / \sim|$ then $2^{|A|} = 2^{|B|}$ and so $|A| = |B|$.
□

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

PROOF:
$\langle 1 \rangle 1$. If G is finitely generated then there exists a surjective homomorphism $\mathbb{Z}^{\oplus n} \twoheadrightarrow G$ for some n.
PROOF: Let $G = \langle a_1, \ldots, a_n \rangle$. Define $\phi : \mathbb{Z}^{\oplus n} \twoheadrightarrow G$ by $\phi(i_1, \ldots, i_n) = i_1 \cdot a_1 + \cdots + i_n \cdot a_n$.
$\langle 1 \rangle 2$. 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 $\phi(1, 0, \ldots, 0)$, $\phi(0, 1, 0, \ldots, 0)$, $\ldots$, $\phi(0, \ldots, 0, 1)$.
□

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

$$\begin{tikzcd}
F(A)/[F(A),F(A)] \arrow[dr, "h"] & \\
F(A) \arrow[u, "\pi"] \arrow[r, "g"] & G \\
A \arrow[u, hook, "i"] \arrow[ur, "f"] &
\end{tikzcd}$$

PROOF:
$\langle 1 \rangle 1$. LET: G be an Abelian group and $f : A \to G$ a function.
$\langle 1 \rangle 2$. LET: $g : F(A) \to G$ be the unique group homomorphism such that $g \circ i = f$.
$\langle 1 \rangle 3$. $[F(A), F(A)] \subseteq \ker g$
PROOF: For all $x, y \in F(A)$ we have $g(xyx^{-1}y^{-1}) = g(x) + g(y) - g(x) - g(y) = 0$.
$\langle 1 \rangle 4$. LET: $h : F(A)/[F(A), F(A)]$ be the unique group homomorphism such that $h \circ \pi = g$.
$\langle 1 \rangle 5$. h is the unique group homomorphism such that $h \circ \pi \circ i = f$.
□

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

PROOF: Proposition 8.28. □

8.3 Cokernels

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

Proof:
$\langle 1 \rangle 1$. Let: $K = H/\operatorname{im}\phi$ and π be the canonical homomorphism.
$\langle 1 \rangle 2$. Let: $\pi \circ \phi = 0$
$\langle 1 \rangle 3$. Let: $\alpha : H \to L$ satisfy $\alpha \circ \phi = 0$
$\langle 1 \rangle 4$. $\operatorname{im}\phi \subseteq \ker\alpha$
$\langle 1 \rangle 5$. There exists a unique $\overline{\alpha} : H/\operatorname{im}\phi \to L$ such that $\overline{\alpha} \circ \pi = \alpha$
□

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

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

Proof: Easy. □

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

- *ϕ is an epimorphism.*
- $\operatorname{coker}\phi$ *is trivial.*
- *ϕ is surjective.*

Proof:
$\langle 1 \rangle 1$. $1 \Rightarrow 2$
  $\langle 2 \rangle 1$. Assume: ϕ is epi.
  $\langle 2 \rangle 2$. Let: $\pi : H \to \operatorname{coker}\phi$ be the canonical homomorphism.
  $\langle 2 \rangle 3$. $\pi \circ \phi = 0 \circ \phi$
  $\langle 2 \rangle 4$. $\pi = 0$
  $\langle 2 \rangle 5$. $\operatorname{coker}\phi = \operatorname{im}\pi$ is trivial.
$\langle 1 \rangle 2$. $2 \Rightarrow 3$
  Proof: If $\operatorname{coker}\phi = H/\operatorname{im}\phi$ is trivial then $\operatorname{im}\phi = H$.
$\langle 1 \rangle 3$. $3 \Rightarrow 1$
  Proof: If it is surjective then it is epi in **Set**.
□

Chapter 9

Group Actions

9.1 Group Actions

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

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 $\cdot : G \times A \to A$ 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. □

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 $\mathrm{Aut}_{\mathbf{Set}}(G)$.*

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

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

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 $a \in \mathrm{O}_G(a)$.
$\langle 1 \rangle 2$. Distinct orbits are disjoint.
$\langle 2 \rangle 1$. Let: $a \in \mathrm{O}_G(b) \cap \mathrm{O}_G(c)$
$\langle 2 \rangle 2$. Pick $g, h \in G$ such that $a = gb = hc$.
$\langle 2 \rangle 3$. $\mathrm{O}_G(b) \subseteq \mathrm{O}_G(c)$
Proof: For all $k \in G$ we have $kb = kg^{-1}hc$.
$\langle 2 \rangle 4$. $\mathrm{O}_G(c) \subseteq \mathrm{O}_G(b)$
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 $\mathrm{O}_G(a)$.*

Proof:
$\langle 1 \rangle 1$. The restriction of the action is an action on $\mathrm{O}_G(a)$.
Proof: Since $g(ha) = (gh)a$, the action maps $\mathrm{O}_G(a)$ to itself.
$\langle 1 \rangle 2$. The restricted action is transitive.
Proof: Given $ga, ha \in \mathrm{O}_G(a)$, 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

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

Proposition 9.11. *Stabilizer subgroups are subgroups.*

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

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

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

Proof:

$$\begin{aligned} h \in \mathrm{Stab}_G(ga) &\Leftrightarrow hga = ga \\ &\Leftrightarrow g^{-1}hga = a \\ &\Leftrightarrow g^{-1}hg \in \mathrm{Stab}_G(a) \\ &\Leftrightarrow h \in g\mathrm{Stab}_G(a)\, g^{-1} \end{aligned}$$

□

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

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: $\sigma : G \to \mathrm{Aut}_{\mathbf{Set}}(G/H)$ be the action of left multiplication.
$\langle 1\rangle 2.$ LET: $K = \ker \sigma$
$\langle 1\rangle 3.$ $K \subseteq H$
  $\langle 2\rangle 1.$ LET: $g \in K$
  $\langle 2\rangle 2.$ $\sigma(g)(H) = H$
  $\langle 2\rangle 3.$ $gH = H$
  $\langle 2\rangle 4.$ $g \in H$
$\langle 1\rangle 4.$ K is normal in G.
  PROOF: Proposition 7.42.
$\langle 1\rangle 5.$ $|G : K| \mid |G|$
  PROOF: Lagrange's Theorem.
$\langle 1\rangle 6.$ $|G : K| \mid n!$
  PROOF: Since G/K is a subgroup of $\mathrm{Aut}_{\mathbf{Set}}(G/H)$.
□

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

PROOF:
$\langle 1\rangle 1.$ PICK a subgroup K of H normal in G such that $|G : K|$ divides $\gcd(|G|, p!)$.
$\langle 1\rangle 2.$ $|G : K|$ divides p.
$\langle 1\rangle 3.$ $|G : H||H : K|$ divides p.
$\langle 1\rangle 4.$ $|H : K| = 1$
$\langle 1\rangle 5.$ $H = K$
$\langle 1\rangle 6.$ H is normal.
□

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

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

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

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

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

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

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

9.2 Category of G-Sets

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

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

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

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

PROOF:
⟨1⟩1. LET: $f : A \to B$ be G-equivariant and bijective.
PROVE: f^{-1} is G-equivariant.
⟨1⟩2. LET: $g \in G$ and $b \in B$
⟨1⟩3. $f^{-1}(gb) = gf^{-1}(b)$
PROOF:

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

□

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

PROOF:
⟨1⟩1. LET: $f : G/\mathrm{Stab}_G(a) \to A$ be the function $f(g\mathrm{Stab}_G(a)) = ga$.
⟨2⟩1. ASSUME: $g\mathrm{Stab}_G(a) = h\mathrm{Stab}_G(a)$
PROVE: $ga = ha$
⟨2⟩2. $g^{-1}h \in \mathrm{Stab}_G(a)$
⟨2⟩3. $g^{-1}ha = a$
⟨2⟩4. $ha = ga$
⟨1⟩2. f is G-equivariant.
PROOF: Since $f(gh\mathrm{Stab}_G(a)) = gha = gf(h\mathrm{Stab}_G(a))$.
⟨1⟩3. f is injective.
PROOF: If $ga = ha$ then $g^{-1}h \in \mathrm{Stab}_G(a)$ so $g\mathrm{Stab}_G(a) = h\mathrm{Stab}_G(a)$.
⟨1⟩4. f is surjective.
PROOF: Since for all $b \in A$ there exists $g \in G$ such that $ga = b$.
□

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

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

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

in $G - \mathbf{Set}$.

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

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

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

PROOF: Easy. ∎

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

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

PROOF: Easy. ∎

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

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

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

PROOF:
⟨1⟩1. Define $\phi : G \to \mathrm{Aut}_{G-\mathbf{Set}}(G)$ 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 $\phi(g)(h_1 h_2) = h_1 h_2 g^{-1} = h_1 \phi(g)(h_2)$.
  ⟨2⟩3. $\phi(g)$ is injective.
    PROOF: By Cancellation.
  ⟨2⟩4. $\phi(g)$ is surjective.
    PROOF: For any $h \in G$ we ahev $h = \phi(g)(hg)$.
⟨1⟩2. ϕ is a group homomorphism.
  PROOF: $\phi(g_1 g_2)(h) = h{g_2}^{-1}{g_1}^{-1} = \phi(g_1)(\phi(g_2)(h))$.
⟨1⟩3. ϕ is injective.
  PROOF: If $\phi(g) = \phi(g')$ then $g = \phi(g)(e) = \phi(g')(e) = g'$.
⟨1⟩4. ϕ is surjective.
  ⟨2⟩1. LET: $\sigma \in \mathrm{Aut}_{G-\mathbf{Set}}(G)$
  ⟨2⟩2. LET: $g = \sigma(e)$
    PROVE: $\sigma = \phi(g^{-1})$
  ⟨2⟩3. $\sigma(h) = hg$
    PROOF: $\sigma(h) = \sigma(he) = h\sigma(e) = hg$.

∎

Part III

Ring Theory

Chapter 10

Rngs

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

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

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

Example 10.2.

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

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

Proposition 10.3. *In any rng R we have*

$$\forall x \in R.x0 = 0x = 0 \quad .$$

PROOF:

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

and so $x0 = 0$ by Cancellation. Similarly $0x = 0$. □

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

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

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

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

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

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

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 $b \neq 0$
□

10.1 Commutative Rngs

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

Example 10.8.

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

10.2 Rng Homomorphisms

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

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

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

10.3 Quaternions

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

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

Chapter 11

Rings

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

$$\forall x \in R. x1 = 1x = x \ .$$

Example 11.2.

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

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

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

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

PROOF: Since

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

□

11.1 Units

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

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

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

PROOF:
⟨1⟩1. If a is a left-unit then left multiplication by a is surjective.
⟨2⟩1. PICK $b \in R$ such that $ab = 1$.
⟨2⟩2. For all $c \in R$ we have $c = a(bc)$.
⟨1⟩2. If left multiplication by a is surjective then a is a left-unit.
PROOF: Immediate.
□

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

PROOF: Similar. □

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

PROOF:
⟨1⟩1. ASSUME: for a contradiction $ab = 1$ and $ca = 0$ where $c \neq 0$.
⟨1⟩2. $c = 0$
PROOF:

$$\begin{aligned} 0 &= 0b \\ &= cab \\ &= c1 \\ &= c \end{aligned}$$

⟨1⟩3. Q.E.D.
PROOF: This is a contradiction.
□

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

PROOF: Similar. □

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

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

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

PROOF:
⟨1⟩1. If a and b are units then ab is a unit.
PROOF: We have $b^{-1}a^{-1}ab = 1$ and $abb^{-1}a^{-1} = 1$.

$\langle 1 \rangle 2$. 1 is a unit.
PROOF: Since $1 \cdot 1 = 1$.
$\langle 1 \rangle 3$. If a is a unit then its inverse is a unit.
PROOF: Immediate from definitions.
$\square$

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

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

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

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

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

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

Proposition 11.17. *If p is prime then $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.*

PROOF:
$\langle 1 \rangle 1$. LET: g be an element of maximal order in $(\mathbb{Z}/p\mathbb{Z})^*$.
$\langle 1 \rangle 2$. For all $h \in (\mathbb{Z}/p\mathbb{Z})^*$ we have $h^{|g|} = 1$.
PROOF: Proposition 8.10.
$\langle 1 \rangle 3$. There are at most $|g|$ elements x such that $x^{|g|} = 1$ in $\mathbb{Z}/p\mathbb{Z}$
$\langle 1 \rangle 4$. $p - 1 \leq |g|$
$\langle 1 \rangle 5$. $|g| = p - 1$
$\langle 1 \rangle 6$. g generates $(\mathbb{Z}/p\mathbb{Z})^*$.
$\square$

Example 11.18. $(\mathbb{Z}/12\mathbb{Z})^*$ is not cyclic. Its elements are 1, 5, 7 and 11 with orders 1, 2, 2 and 2.

Theorem 11.19 (Wilson's Theorem)**.** *A positive integer p is prime if and only if $(p-1)! \equiv 1 (\bmod p)$.*

$\langle 1 \rangle 1$. If p is prime then $(p-1)! \equiv 1 (\bmod p)$.
$\langle 2 \rangle 1$. ASSUME: p is prime.
$\langle 2 \rangle 2$. $(p-1)!$ is the product of all the elements of $(\mathbb{Z}/p\mathbb{Z})^*$
$\langle 2 \rangle 3$. The only element of $(\mathbb{Z}/p\mathbb{Z})^*$ with order 2 is -1.
$\langle 2 \rangle 4$. $(p-1)! \equiv -1 (\bmod p)$
PROOF: Proposition 6.20.

$\langle 1 \rangle 2$. If $(p-1)! \equiv -1 (\bmod p)$ then p is prime.

$\langle 2 \rangle 1$. ASSUME: (
$(p-1)! \equiv -1 (\bmod p)$)

$\langle 2 \rangle 2$. LET: d be a proper divisor of p.
PROVE: $d = 1$

$\langle 2 \rangle 3$. $d \mid (p-1)!$

$\langle 2 \rangle 4$. $d \mid 1$
PROOF: Since $d \mid p \mid (p-1)! + 1$.

$\langle 2 \rangle 5$. $d = 1$

□

Proposition 11.20. *If p and q are distinct odd primes then $(\mathbb{Z}/pq\mathbb{Z})^*$ is not cyclic.*

PROOF:

$\langle 1 \rangle 1$. $|(\mathbb{Z}/pq\mathbb{Z})^*| = (p-1)(q-1)$

$\langle 1 \rangle 2$. LET: $g \in (\mathbb{Z}/pq\mathbb{Z})^*$
PROVE: g does not have order $(p-1)(q-1)$

$\langle 1 \rangle 3$. $g^{(p-1)(q-1)/2} \equiv 1 (\bmod p)$

$\langle 1 \rangle 4$. $g^{(p-1)(q-1)/2} \equiv 1 (\bmod q)$

$\langle 1 \rangle 5$. $pq \mid g^{(p-1)(q-1)/2} - 1$

$\langle 1 \rangle 6$. $g^{(p-1)(q-1)/2} \equiv 1 (\bmod pq)$

$\langle 1 \rangle 7$. $|g| \mid (p-1)(q-1)/2$

□

Proposition 11.21. *For any prime p, we have $\mathrm{Aut}_{\mathbf{Grp}}(C_p) \cong C_{p-1}$.*

PROOF:

$\langle 1 \rangle 1$. LET: $\phi : \mathrm{Aut}_{\mathbf{Grp}}(C_p) \to (\mathbb{Z}/p\mathbb{Z})^*$ be the function $\phi(\alpha) = \alpha(1)$.
PROOF: $\alpha(1)$ has order p in C_p and so is coprime with p.

$\langle 1 \rangle 2$. ϕ is a homomorphism.
PROOF: $\phi(\alpha \circ \beta) = \alpha(\beta(1)) = \alpha(\beta(1)1) = \beta(1)\alpha(1) = \phi(\alpha)\phi(\beta)$

$\langle 1 \rangle 3$. ϕ is injective.
PROOF: If $\phi(\alpha) = \phi(\beta)$ then for any n we have $\alpha(n) = n\alpha(1) = n\phi(\alpha) = n\phi(\beta) = n\beta(1) = \beta(n)$.

$\langle 1 \rangle 4$. ϕ is surjective.
PROOF: For any $r \in (\mathbb{Z}/p\mathbb{Z})^*$ we have $r = \phi(\alpha)$ where $\alpha(n) = nr \bmod p$.

$\langle 1 \rangle 5$. $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$

□

11.2 Euler's ϕ-function

Proposition 11.22. *For n a positive integer, we have $(\mathbb{Z}/n\mathbb{Z})^* = \{m \in \mathbb{Z}/n\mathbb{Z} :$ $\gcd(m, n) = 1\}$.*

PROOF:

$$\begin{aligned} m \in (\mathbb{Z}/n\mathbb{Z})^* &\Leftrightarrow \exists a.am \equiv 1 (\operatorname{mod} n) \\ &\Leftrightarrow \exists a, b.am + bn = 1 \\ &\Leftrightarrow \gcd(m,n) = 1 \end{aligned}$$

□

Definition 11.23 (Euler's Totient Function)**.** For n a positive integer, let $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.

Proposition 11.24. *If n is an odd positive integer then $\phi(2n) = \phi(n)$.*

PROOF:
⟨1⟩1. LET: n be an odd positive integer.
⟨1⟩2. For any integer m, if $\gcd(m,n) = 1$ then $\gcd(2m+n, 2n) = 1$
PROOF: For p a prime, if $p \mid 2m+n$ and $p \mid 2n$ then $p \neq 2$ (since $2m+n$ is odd) so $p \mid n$ and hence $p \mid m$, which is a contradiction.
⟨1⟩3. For any integer r, if $\gcd(r, 2n) = 1$ then $\gcd(\frac{r+n}{2}, n) = 1$
PROOF: If $p \mid n$ and $p \mid \frac{r+n}{2}$ then $p \mid r+n$ so $p \mid r$ which is a contradiction.
⟨1⟩4. The function that maps m to $2m+n$ is a bijection between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$.
□

Theorem 11.25. *For any positive integer n we have*

$$\sum_{m>0, m|n} \phi(m) = n \ .$$

PROOF:
⟨1⟩1. Define $\chi : \{0, 1, \ldots, n-1\} \to \{(m,d) : m > 0, m \mid n, d \text{ generates } \langle n/m \rangle\}$ by: $\chi(x) = (\gcd(x,n), x)$.
⟨1⟩2. χ is injective.
⟨1⟩3. χ is surjective.
PROOF: Given (m,d) such that d generates $\langle n/m \rangle$ we have $\chi(d) = (m,d)$.
⟨1⟩4. $n = \sum_{m>0,m|n} \phi(m)$
PROOF: Since $\langle n/m \rangle \cong C_m$ and so has $\phi(m)$ generators.
□

Proposition 11.26. *For any positive integers a and n, we have $n \mid \phi(a^n - 1)$.*

PROOF: Since the order of a is n in $(\mathbb{Z}/(a^n-1)\mathbb{Z})^*$. □

Theorem 11.27 (Euler's Theorem)**.** *For any coprime integers a and n we have $a^{\phi(n)} \equiv a (\operatorname{mod} n)$.*

PROOF: Immediate from Lagrange's Theorem. □

Proposition 11.28.

$$|\mathrm{Aut}_{\mathbf{Grp}}(C_n)| = \phi(n)$$

PROOF: An automorphism α is determined by $\alpha(1)$ which is any element of order n, and g has order n iff $\gcd(g,n) = 1$. □

Example 11.29.

$$\mathrm{Aut}_{\mathbf{Grp}}(\mathbb{Z}) \cong C_2$$

PROOF: The only automorphisms are the identity and multiplication by -1. □

11.3 Nilpotent Elements

Definition 11.30 (Nilpotent)**.** Let R be a ring and $a \in R$. Then a is *nilpotent* iff there exists n such that $a^n = 0$.

Proposition 11.31. *Let R be a ring and $a, b \in R$. If a and b are nilpotent and $ab = ba$ then $a + b$ is nilpotent.*

PROOF:
⟨1⟩1. PICK m and n such that $a^m = b^n = 0$.
⟨1⟩2. $(a + b)^{m+n} = 0$

PROOF: Since $(a+b)^{m+n} = \sum_k \begin{pmatrix} m+n \\ k \end{pmatrix} a^k b^{m+n-k}$ and every term in this sum is 0 since, for every k, either $k \geq m$ or $m + n - k \geq n$.

□

Proposition 11.32. *m is nilpotent in $\mathbb{Z}/n\mathbb{Z}$ if and only if m is divisible by all the prime factors of n.*

PROOF:
⟨1⟩1. If m is nilpotent then m is divisible by all the prime factors of n.
⟨2⟩1. ASSUME: $m^a \equiv 0 (\mathrm{mod}\, n)$
⟨2⟩2. For every prime p, if $p \mid n$ then $p \mid m^a$.
⟨2⟩3. For every prime p, if $p \mid n$ then $p \mid m$.
⟨1⟩2. If m is divisible by all the prime factors of n then m is nilpotent in $\mathbb{Z}/n\mathbb{Z}$.
⟨2⟩1. ASSUME: m is divisible by all the prime factors of n.
⟨2⟩2. LET: a be the largest number such that $p^a \mid n$ for some prime p.
⟨2⟩3. For every prime p that divides n we have $p^a \mid m^a$
⟨2⟩4. $n \mid m^a$
⟨2⟩5. $m^a \equiv 0 (\mathrm{mod}\, n)$
⟨2⟩6. m is nilpotent in $\mathbb{Z}/n\mathbb{Z}$.

□

Chapter 12

Ring Homomorphisms

Definition 12.1 (Ring Homomorphism)**.** Let R and S be rings. A *ring homomorphism* $\phi : R \to S$ is a rng homomorphism such that $\phi(1) = 1$.

Proposition 12.2. *The zero-ring is terminal in* **Ring**.

PROOF: Easy. □

Proposition 12.3. *The ring* $\mathbb{Z}$ *is initial in* **Ring**.

PROOF: Easy. □

Proposition 12.4. *Let R and S be rings and $\phi : R \to S$ be a rng homomorphism. If ϕ is surjective, then ϕ 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:

$$\begin{aligned} \phi(1) &= \phi(1)\phi(a) \\ &= \phi(1a) \\ &= \phi(a) \\ &= 1 \end{aligned}$$

□

Example 12.5. For any set S we have $\mathcal{P}S \cong (\mathbb{Z}/2\mathbb{Z})^S$ in **Ring** with the isomorphism

$$\phi : \mathcal{P}S \cong (\mathbb{Z}/2\mathbb{Z})^S$$
$$\phi(A)(s) = \begin{cases} 1 & \text{if } s \in A \\ 0 & \text{if } s \notin A \end{cases}$$

Example 12.6. The function $\mathbb{H} \to \mathfrak{gl}_4(\mathbb{R})$ 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 $\mathbb{H} \to \mathfrak{sl}_2(\mathbb{C})$ that maps $a + bi + cj + dk$ to

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

Proposition 12.7. *Ring homomorphisms preserve units.*

PROOF: If $uv = 1$ then $\phi(u)\phi(v) = 1$. □

Proposition 12.8. *Let $\phi : R \to S$ be a ring homomorphism. Then the following are equivalent.*

1. *ϕ is a monomorphism.*
2. $\ker \phi = \{0\}$
3. *ϕ is injective.*

PROOF:
⟨1⟩1. $1 \Rightarrow 2$
  ⟨2⟩1. ASSUME: ϕ is a monomorphism.
  ⟨2⟩2. LET: $r \in \ker \phi$
  ⟨2⟩3. LET: $\mathrm{ev}_r : \mathbb{Z}[x] \to R$ be the unique ring homomorphism such that $\mathrm{ev}_r(x) = r$.
  ⟨2⟩4. LET: $\mathrm{ev}_0 : \mathbb{Z}[x] \to R$ be the unique ring homomorphism such that $\mathrm{ev}_0(x) = 0$.
  ⟨2⟩5. $\phi \circ \mathrm{ev}_r = \phi \circ \mathrm{ev}_0$
  ⟨2⟩6. $\mathrm{ev}_r = \mathrm{ev}_0$
  ⟨2⟩7. $r = 0$
⟨1⟩2. $2 \Rightarrow 3$
  PROOF: Proposition 7.20.
⟨1⟩3. $3 \Rightarrow 1$
  PROOF: Easy.
□

Example 12.9. It is not true that every epimorphism in **Ring** is surjective. The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism but not surjective.

The same example shows that a ring homomorphism may be a monomorphism and an epimorphism but not be an isomorphism.

12.1 Products

Proposition 12.10. *Let R and S be rings. Then $R \times S$ is a ring under componentwise addition and multiplication, and this ring is the product of R and S in* **Ring**.

PROOF: Easy. $\square$

Chapter 13

Subrings

Definition 13.1 (Subring)**.** Let S be a ring. A *subring* of S is a ring R such that R is a subset of S and the inclusion $R \hookrightarrow S$ is a ring homomorphism.

Proposition 13.2. *Let R and S be rings. Then R is a subring of S if and only if R is a subset of S, the unit 1 of S is an element of R, and the operations of R are the restrictions of the operations of S to R.*

Proof: Easy. □

Corollary 13.2.1. *The zero ring is not a subring of any non-zero ring.*

13.1 Centralizer

Definition 13.3 (Centralizer)**.** Let R be a ring and $a \in R$. The *centralizer* of a is $\{r \in R : ar = ra\}$.

Proposition 13.4. *The centralizer of a is a subring of R.*

Proof: Easy. □

13.2 Center

Definition 13.5 (Center)**.** The *center* of a ring R is $\{x \in R : \forall y \in R. xy = yx\}$.

Proposition 13.6. *The center of a ring is a subring.*

Proof: Easy. □

Chapter 14

Monoid Rings

Definition 14.1 (Monoid Ring)**.** Let R be a ring and M a monoid. Define $R[M]$ to be the ring whose elements are the families $\{a_m\}_{m \in M}$ such that $a_m = 0$ for all but finitely many $m \in M$, written

$$\sum_{m \in M} a_m m \ ,$$

under

$$\sum_m a_m m + \sum_m b_m m = \sum_m (a_m + b_m) m$$
$$\left(\sum_m a_m m \right) \left(\sum_m b_m m \right) = \sum_{m \in M} \sum_{m_1 m_2 = m} a_{m_1} b_{m_2} m$$

Example 14.2. Ring homomorphisms do not necessarily preserve zero-divisors. The canonical homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ maps the non-zero-divisor 2 to a zero-divisor.

14.1 Polynomials

Definition 14.3 (Polynomial)**.** Let R be a ring. The ring of *polynomials* $R[x]$ is $R[\mathbb{N}]$. We write

$$\sum_n a_n x^n \text{ for } \sum_n a_n n \ .$$

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

$$\sum_n a_n x^n + \sum_n b_n x^n = \sum_n (a_n + b_n) x^n$$

$$\left(\sum_n a_n x^n\right)\left(\sum_n b_n x^n\right) = \sum_n \sum_{i+j=n} a_i b_j x^n$$

A *constant* is a polynomial of the form $a + 0x + 0x^2 + \cdots$ for some $a \in R$. We write $R[x_1, \ldots, x_n]$ for $R[x_1][x_2]\cdots[x_n]$.

Proposition 14.4. *For any ring R, the set of polynomials $R[x]$ is a ring.*

Proof: Easy. □

Definition 14.5 (Degree)**.** The *degree* of a polynomial $\sum_n a_n x^n$ is the largest integer d such that $a_d \neq 0$. We take the degree of the zero polynomial to be $-\infty$.

Proposition 14.6. *Let R be a ring and $f, g \in R[x]$ be nonzero polynomials. Then*

$$\deg(f+g) \leq \max(\deg f, \deg g) \quad .$$

Proof: If $a_n + b_n \neq 0$ then $a_n \neq 0$ or $b_n \neq 0$. □

Proposition 14.7. *The function $i : n \to \mathbb{Z}[x_1, \ldots, x_n]$ that maps k to x_k is initial in the category with:*

- *objects all pairs $j : n \to R$ where R is a commutative ring and j a function*
- *morphisms $\phi : (j_1, R_1) \to (j_2, R_2)$ are ring homomorphisms $\phi : R_1 \to R_2$ such that $\phi \circ j_1 = j_2$.*

Proof: The unique morphism $(i, \mathbb{Z}[x_1, \ldots, x_n]) \to (j, R)$ maps a polynomial p to $p(j(0), j(1), \ldots, j(n-1))$. □

Definition 14.8. Let R be a commutative ring. Given a polynomial $p \in R[x]$, the *polynomial function* $p : R \to R$ is the function given by: $p(r) = \alpha_r(p)$, where $\alpha_r : R[x] \to R$ is the unique ring homomorphism such that the following diagram commutes.

$$\begin{tikzcd} R[x] \arrow[r, "\alpha_r"] & R \\ 1 \arrow[u, "x"] \arrow[ur, "r"] & \end{tikzcd}$$

Proposition 14.9. *$\mathbb{Z}[x, y]$ is the coproduct of $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ in the category of commutative rings.*

Proof: Given ring homomorphisms $f : \mathbb{Z}[x] \to R$ and $g : \mathbb{Z}[y] \to R$, the required morphism $\mathbb{Z}[x, y] \to R$ maps $p(x, y)$ to $p(f(x), g(y))$. □

Example 14.10. $\mathbb{Z}[x, y]$ is not the coproduct of $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ in **Ring**. Given $f : \mathbb{Z}[x] \to R$ and $g : \mathbb{Z}[y] \to R$ with $f(x) \neq g(y)$, the mediating morphism $\mathbb{Z}[x, y] \to R$ cannot exist since it must map xy to both $f(x)g(y)$ and $g(y)f(x)$. □

14.2 Laurent Polynomials

Definition 14.11 (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 $\sum_n a_n n$.

14.3 Power Series

Definition 14.12 (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

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots \quad .$$

We write $R[[x]]$ for the set of all power series in R.

Define addition and multiplication on $R[[x]]$ by

$$\sum_n a_n x^n + \sum_n b_n x^n = \sum_n (a_n + b_n) x^n$$

$$\left(\sum_n a_n x^n \right) \left(\sum_n b_n x^n \right) = \sum_n \sum_{i+j=n} a_i b_j x^n$$

Proposition 14.13. *For any ring R, the set of power series $R[[x]]$ is a ring.*

Proof: Easy. ∎

Proposition 14.14. *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:
⟨1⟩1. If $\sum_n a_n x^n$ is a unit then a_0 is a unit.
  ⟨2⟩1. Let: $\sum_n b_n x^n$ be the inverse of $\sum_n a_n x^n$.
  ⟨2⟩2. $a_0 b_0 = b_0 a_0 = 1$
⟨1⟩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 $\sum_n a_n x^n$.
∎

Chapter 15

Integral Domains

Definition 15.1 (Integral Domain)**.** An *integral domain* is a non-trivial commutative ring with no nonzero zero-divisors.

Example 15.2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are integral domains.

Proposition 15.3. *$\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime.*

PROOF:

$$\begin{aligned} n \text{ is prime} &\Leftrightarrow \forall a, b \in \mathbb{Z}(n \mid ab \Rightarrow n \mid a \vee n \mid b) \\ &\Leftrightarrow \forall a, b \in \mathbb{Z}/n\mathbb{Z}(ab \cong 0 (\operatorname{mod} n) \Rightarrow a \cong 0 (\operatorname{mod} n) \vee b \cong 0 (\operatorname{mod} n)) \\ &\Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ is an integral domain} \end{aligned}$$

∎

Proposition 15.4. *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 $x + 1 = 0$. ∎

Proposition 15.5. *Let R be an integral domain and $f, g \in R[x]$. Then*

$$\deg(fg) = \deg f + \deg g$$

PROOF:

⟨1⟩1. LET: $f = \sum_n a_n x^n$ and $g = \sum_n b_n x^n$.

⟨1⟩2. LET: $d = \deg f$ and $e = \deg g$.

⟨1⟩3. The $d + e$th term of fg is

$$a_d b_e x^{d+e}$$

which is non-zero.

⟨1⟩4. For $n > d + e$ the nth term of fg is 0.

∎

Corollary 15.5.1. *Let R be a ring. Then $R[x]$ is an integral domain if and only if R is an integral domain.*

Proposition 15.6. *Let R be a ring. Then $R[[x]]$ is an integral domain if and only if R is an integral domain.*

PROOF:
⟨1⟩1. If $R[[x]]$ is an integral domain then R is an integral domain.
  PROOF: Easy.
⟨1⟩2. If R is an integral domain then $R[[x]]$ is an integral domain.
  ⟨2⟩1. ASSUME: R is an integral domain.
  ⟨2⟩2. LET: $\left(\sum_n a_n x^n\right)\left(\sum_n b_n x^n\right) = 0$
  ⟨2⟩3. $a_0 b_0 = 0$
  ⟨2⟩4. $a_0 = 0$ or $b_0 = 0$
  ⟨2⟩5. ASSUME: w.l.o.g. $b_0 \neq 0$
     PROVE: For all n we have $a_n = 0$
  ⟨2⟩6. ASSUME: as induction hypothesis $a_0 = a_1 = \cdots = a_{n-1} = 0$
  ⟨2⟩7. $\sum_{i=0}^{n} a_i b_{n-i} = 0$
  ⟨2⟩8. $a_n b_0 = 0$
  ⟨2⟩9. $a_n = 0$
□

Proposition 15.7. *Let R be a ring and S an integral domain. Every rng homomorphism $\phi : R \to S$ 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. □

Chapter 16

Unique Factorization Domains

Example 16.1. $\mathbb{Z}$ is a UFD.

Chapter 17

Principal Ideal Domains

Example 17.1. $\mathbb{Z}$ is a PID.

Chapter 18

Euclidean Domains

Example 18.1. $\mathbb{Z}$ is a Euclidean domain.

Chapter 19

Division Rings

Definition 19.1 (Division Ring)**.** A *division ring* is a ring in which every nonzero element is a two-sided unit.

Example 19.2. 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 19.3. For any ring R, the ring of polynomials $R[x]$ is not a division ring, since x has no inverse.

Proposition 19.4. *Every centralizer in a division ring is a division ring.*

Proof: If $ar = ra$ then $ra^{-1} = a^{-1}r$. □

Part IV

Field Theory

Chapter 20

Fields

Definition 20.1 (Field)**.** A *field* is a non-trivial commutative division ring.

Example 20.2. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

Proposition 20.3. *Every field is an integral domain.*

PROOF: By Propositions 11.8 and 11.9. □

Example 20.4. The converse does not hold: $\mathbb{Z}$ is an integral domain but not a field.

Proposition 20.5. *Every finite integral domain is a field.*

PROOF: In a finite integral domain, multiplication by any non-zero element is injective, hence surjective. □

Corollary 20.5.1. *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 20.6 (Wedderburn's Little Theorem)**.** *Every finite division ring is a field.*

Proposition 20.7. *Every subring of a field is an integral domain.*

PROOF: Easy. □

Proposition 20.8. *The center of a division ring is a field.*

PROOF:
⟨1⟩1. LET: R be a division ring.
⟨1⟩2. LET: Z be the center of R.
⟨1⟩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: $x \in R$
$\langle 3 \rangle 2.$ $ax = xa$
$\langle 3 \rangle 3.$ $xa^{-1} = a^{-1}x$
$\square$

Definition 20.9. 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:

Part V

Linear Algebra

Definition 20.10. 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 20.11. 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 20.12. Let $\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : \det M = 1\}$.

Proposition 20.13. *$\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$.*

Proof: If $\det M = 1$ then $\det(AMA^{-1}) = (\det A)(\det M)(\det A)^{-1} = 1$. ∎

Proposition 20.14.

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$$

Definition 20.15. Let $\mathrm{SL}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : \det M = 1\}$.

Definition 20.16. Let $\mathrm{O}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) : MM^{\mathrm{T}} = M^{\mathrm{T}}M = I_n\}$.

Proposition 20.17. *The action of $\mathrm{O}_n(\mathbb{R})$ on $\mathbb{R}^n$ preserves lengths and angles.*

Definition 20.18. Let $\mathrm{SO}_n(\mathbb{R}) = \{M \in \mathrm{O}_n(\mathbb{R}) : \det M = 1\}$.

Definition 20.19. Let $\mathrm{U}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) : MM^\dagger = M^\dagger M = I_n\}$.

Definition 20.20. Let $\mathrm{SU}_n(\mathbb{C}) = \{M \in U_n(\mathbb{C}) : \det M = 1\}$.

Proposition 20.21. *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:

⟨1⟩1. Let: $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SU}_2(\mathbb{C})$

⟨1⟩2. $M^{-1} = M^\dagger$

⟨1⟩3. $\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} \overline{\alpha} & \overline{\gamma} \\ \overline{\beta} & \overline{\delta} \end{pmatrix}$

⟨1⟩4. Let: $\alpha = a + bi$ and $\beta = c + di$.

⟨1⟩5. $\delta = \overline{\alpha} = a - bi$

⟨1⟩6. $\gamma = -\overline{\beta} = -c + di$

⟨1⟩7. $\det M = a^2 + b^2 + c^2 + d^2 = 1$

∎

Corollary 20.21.1. *$\mathrm{SU}_2(\mathbb{C})$ is simply connected.*

Corollary 20.21.2.

$$\mathrm{SO}_3(\mathbb{R}) \cong \mathrm{SU}_2(\mathbb{C})/\{I, -I\}$$

Proof: The function that maps $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ to $\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$ is a surjective homomorphism with kernel $\{I, -I\}$. ∎

Corollary 20.21.3. *The fundamental group of $\mathrm{SO}_3(\mathbb{R})$ is C_2.*