Mathematics

Robin Adams

February 15, 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

Number Theory

2.1 Congruence

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

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

PROOF:
$\langle 1 \rangle 1$. For any integer a we have $a \equiv a \mod n$.
  PROOF: Since $n \mid 0 = a - a$.
$\langle 1 \rangle 2$. If $a \equiv b \mod n$ then $b \equiv a \mod n$.
  PROOF: If $n \mid b - a$ then $n \mid a - b = -(b - a)$.
$\langle 1 \rangle 3$. If $a \equiv b \mod n$ and $b \equiv c \mod n$ then $a \equiv c \mod n$.
  PROOF: If $n \mid b - a$ and $n \mid c - b$ then $n \mid c - a = (c - b) + (b - a)$.
$\square$

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

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

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

Proposition 2.5. *If $a \equiv a' \mod n$ and $b \equiv b' \mod n$ then $a + b \equiv a' + b' \mod n$.*

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

Proposition 2.6. *If $a \equiv a' \mod n$ and $b \equiv b' \mod n$ then $ab \equiv a'b' \mod n$.*

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

2.2 Euler's ϕ-function

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

PROOF: We prove this is well-defined.
$\langle 1\rangle 1$. If $m \equiv m' \mod n$ and $\gcd(m,n) = 1$ then $\gcd(m',n) = 1$.
 $\langle 2\rangle 1$. PICK integers a, b such that $am + bn = 1$
 $\langle 2\rangle 2$. PICK an integer c such that $m' - m = cn$
 $\langle 2\rangle 3$. $am' + (b - ac)n = 1$
□

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

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

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

Chapter 3

Categories

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

- A class $|\mathcal{C}|$ of *objects*. We write $A \in \mathcal{C}$ for $A \in |\mathcal{C}|$.
- For any objects A, B, a set $\mathcal{C}[A, B]$ of *morphisms* from A to B. We write $f : A \to B$ 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 3.2. *The identity morphism on an object is unique.*

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

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

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

Definition 3.5 (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

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

3.1 Preorders

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

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

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

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

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

3.2 Monomorphisms and Epimorphisms

Definition 3.9 (Monomorphism)**.** In a category, let $f : A \to B$. 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 3.10 (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 3.11. *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 3.12. *The composite of two epimorphisms is epi.*

PROOF: Dual. □

Proposition 3.13. *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 3.14. *Let $f : A \to B$ and $g : B \to C$. If $g \circ f$ is epi then g is epi.*

PROOF: Dual. □

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

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

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

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

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

PROOF: Immediate from definitions. ∎

3.3 Sections and Retractions

Definition 3.18 (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 3.19. *Every identity morphism is a section and retraction of itself.*

PROOF: Immediate from definitions. ∎

Proposition 3.20. *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 3.21. *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 3.22. *Every section is monic.*

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

Proposition 3.23. *Every retraction is epi.*

PROOF: Dual. ∎

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

PROOF: By the Axiom of Choice. ∎

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

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

3.4 Isomorphisms

Definition 3.26 (Isomorphism)**.** In a category $\mathcal{C}$, a morphism $f : A \to B$ 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 3.27. *The inverse of an isomorphism is unique.*

PROOF: Proposition 3.20. $\square$

Proposition 3.28. *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. $\square$

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

PROOF: Immediate from definitions. $\square$

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

PROOF: From Proposition 3.21. $\square$

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

3.5 Initial and Terminal Objects

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

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

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

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

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

PROOF:
$\langle 1 \rangle 1.$ LET: i be the unique morphism $I \to J$.
$\langle 1 \rangle 2.$ 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 $I \to I$.
$\square$

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

PROOF: Dual. $\square$

Chapter 4

Functors

Definition 4.1 (Functor)**.** Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A *functor* $F : \mathcal{C} \to \mathcal{D}$ 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 4.2 (Identity Functor)**.** For any category $\mathcal{C}$, the *identity functor* $1_\mathcal{C} : \mathcal{C} \to \mathcal{C}$ is defined by

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

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

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

4.1 Comma Categories

Definition 4.4 (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:

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

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

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

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

Part II

Group Theory

Chapter 5

Groups

Definition 5.1 (Group)**.** A *group* G consists of a set G and a binary operation $\cdot : G^2 \to G$ 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 $xx^{-1} = x^{-1}x = e$.

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

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

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

PROOF: Proposition 3.2.

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

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

Example 5.4.

- The *trivial* group is $\{e\}$ under $ee = e$.
- $\mathbb{Z}$ is a group under addition
- $\mathbb{Q}$ is a group under addition
- $\mathbb{Q} - \{0\}$ is a group under multiplication
- $\mathbb{R}$ is a group under addition
- $\mathbb{R} - \{0\}$ is a group under multiplication
- $\mathbb{C}$ is a group under addition
- $\mathbb{C} - \{0\}$ is a group under multiplication

- $\{-1, 1\}$ is a group under multiplication
- The set of 2×2 real matrices with non-zero determinant is a group under matrix multiplication.
- For any positive integer n, the set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n under addition is a group. We call this set the *cyclic* group of order n, denoted C_n.
- For any category $\mathcal{C}$ and object $A \in \mathcal{C}$, we have $\mathrm{Aut}_{\mathcal{C}}(A)$ 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.

Example 5.5.

- The only group of order 1 is the trivial group.
- The only group of order 2 is $\mathbb{Z}_2$.
- The only group of order 3 is $\mathbb{Z}_3$.
- There are exactly two groups of order 4: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ under $(a, b)(c, d) = (ac, bd)$.

Example 5.6. For any positive integer n, the set

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

is a group under multiplication.

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

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

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

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

Proof: Since $ghh^{-1}g^{-1} = e$. ∎

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

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

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

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

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:

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

⟨1⟩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 5.11. *Let G be a group. Let $g \in G$ and $m, n \in \mathbb{Z}$. Then*

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

PROOF:
⟨1⟩1. $(g^m)^0 = g^0$
PROOF: Both sides are equal to e.
⟨1⟩2. If $(g^m)^n = g^{mn}$ then $(g^m)^{n+1} = g^{m(n+1)}$.
PROOF:

$$\begin{aligned}(g^m)^{n+1} &= (g^m)^n g^m && \text{(Proposition 5.10)}\\ &= g^{mn} g^m \\ &= g^{mn+m} && \text{(Proposition 5.10)}\end{aligned}$$

⟨1⟩3. If $(g^m)^n = g^{mn}$ then $(g^m)^{n-1} = g^{m(n-1)}$.
PROOF:

$$\begin{aligned}(g^m)^n &= g^{mn}\\ \therefore (g^m)^{n-1} g^m &= g^{mn-m} g^m && \text{(Proposition 5.10)}\\ \therefore (g^m)^{n-1} &= g^{mn-m} && \text{(Cancellation)}\end{aligned}$$

□

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

5.1 Order of an Element

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

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

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

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

$$\begin{aligned}e &= g^n\\ &= g^{q|g|+d}\\ &= (g^{|g|})^q g^d && \text{(Propositions 5.10, 5.11)}\\ &= e^q g^d\\ &= g^d\end{aligned}$$

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

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

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

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

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

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

PROOF: Since for any integer d we have

$$\begin{aligned} g^{md} = e &\Leftrightarrow |g| \mid md && \text{(Corollary 5.14.1)} \\ &\Leftrightarrow \operatorname{lcm}(m, |g|) \mid md \\ &\Leftrightarrow \frac{\operatorname{lcm}(m, |g|)}{m} \mid d && \square \end{aligned}$$

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

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

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

PROOF: Since the order of 1 is n. □

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

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

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

Example 5.18. 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 5.19. *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:
⟨1⟩1. LET: $N = |gh|$
⟨1⟩2. $g^N = (h^{-1})^N$
⟨1⟩3. $g^{N|g|} = e$
⟨1⟩4. $|g^N| \mid |g|$
⟨1⟩5. $h^{-N|h|} = e$
⟨1⟩6. $|g^N| \mid |h|$
⟨1⟩7. $|g^N| = 1$
PROOF: Since $\gcd(|g|, |h|) = 1$.
⟨1⟩8. $g^N = e$
⟨1⟩9. $|g| \mid N$
⟨1⟩10. $h^{-N} = e$
⟨1⟩11. $|h| \mid N$
⟨1⟩12. $N = |g||h|$
PROOF: Using Proposition 5.17.
□

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

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

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

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

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

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

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

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

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

5.2 Generators

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

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

PROOF: By Corollary 5.16.2. □

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

Chapter 6

Group Homomorphisms

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

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

Proposition 6.2. *Let G and H be groups with identities e_G and e_H. Let $\phi : G \to H$ 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 6.3. *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 6.4. *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 6.5. *Let G be a group. Then $\mathrm{id}_G : G \to G$ is a group homomorphism.*

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

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

Proposition 6.7. *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. □

Proposition 6.8. *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 $(g_1,h_1)((g_2,h_2)(g_3,h_3)) = ((g_1,h_1)(g_2,h_2))(g_3,h_3) = (g_1 g_2 g_3, h_1 h_2 h_3)$.
$\langle 2 \rangle 2$. (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:
$$\begin{aligned}
\langle \phi, \psi \rangle (kk') &= (\phi(kk'), \psi(kk')) \\
&= (\phi(k)\phi(k'), \psi(k)\psi(k')) \\
&= (\phi(k), \psi(k))(\phi(k'), \psi(k')) \\
&= \langle \phi, \psi \rangle (k) \langle \phi, \psi \rangle (k')
\end{aligned}$$

□

Definition 6.9 (Direct Product)**.** The *direct product* of groups G and H is their product in **Grp**.

Chapter 7

Abelian Groups

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

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

Example 7.2. Every group of order ≤ 4 is Abelian.

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

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

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

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

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

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

Proof:

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

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

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

Proof: Proposition 5.19.

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

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

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

$\square$

7.1 The Category of Abelian Groups

Definition 7.7 (Category of Abelian Groups)**.** Let **Ab** be the full subcategory of **Grp** whose objects are the Abelian groups.

Definition 7.8 (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 7.9. *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:

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

□

Part III

Linear Algebra

Definition 7.10. Let $\mathrm{GL}_n(\mathbb{R})$ be the group of invertible $n \times n$ real matrices.