Mathematics

Robin Adams

February 9, 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 $i = i \circ j = j$. □

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:
⟨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 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:
⟨1⟩1. Let: i be the unique morphism $I \to J$.
⟨1⟩2. Let: i^{-1} be the unique morphism $J \to I$.
⟨1⟩3. $i \circ i^{-1} = \mathrm{id}_J$
  Proof: Since there is only one morphism $J \to J$.
⟨1⟩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

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

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

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

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

Groups

Definition 4.1 (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 4.2. *The identity in a group is unique.*

Proof: Proposition 2.2.

Proposition 4.3. *The inverse of an element is unique.*

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

Example 4.4.

- 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 $\mathbb{Z}_n$ of integers modulo n under addition is a group.

Example 4.5.

- 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 4.6 (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 4.7. *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 4.8. 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 4.9. *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:
$\langle 1 \rangle$1. For all $k \in \mathbb{Z}$ we have $g^{k+1} = g^k g$
  $\langle 2 \rangle$1. For all $k \geq 0$ we have $g^{k+1} = g^k g$
    PROOF: Immediate from definition.
  $\langle 2 \rangle$2. $g^{-1+1} = g^{-1}g$
    PROOF: Both are equal to e.
  $\langle 2 \rangle$3. For all $k > 1$ we have $g^{-k+1} = g^{-k}g$
    PROOF:

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

⟨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 4.10. *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:

$$\begin{aligned} (g^m)^{n+1} &= (g^m)^n g^m && \text{(Proposition 4.8)} \\ &= g^{mn} g^m \\ &= g^{mn+m} && \text{(Proposition 4.8)} \end{aligned}$$

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

$$\begin{aligned} (g^m)^n &= g^{mn} \\ \therefore (g^m)^{n-1} g^m &= g^{mn-m} g^m && \text{(Proposition 4.8)} \\ \therefore (g^m)^{n-1} &= g^{mn-m} && \text{(Cancellation)} \end{aligned}$$

□

Definition 4.11 (Commute)**.** Let G be a group and $g, h \in G$. We say g and h *commute* iff $gh = hg$.

4.1 Order of an Element

Definition 4.12 (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 4.13. *Let G be a group. Let $g \in G$ and n be a positive integer. If $g^n = e$ then $|g| \mid n$.*

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

$$\begin{aligned} e &= g^n \\ &= g^{q|g|+d} \\ &= (g^{|g|})^q g^d && \text{(Propositions 4.8, 4.9)} \\ &= e^q g^d \\ &= g^d \end{aligned}$$

$\langle 1 \rangle 3$. $d = 0$
PROOF: By minimality of $|g|$.
$\langle 1 \rangle 4$. $n = q|g|$
$\square$

Corollary 4.13.1. *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 4.14. *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 $g^0, g^1, \ldots, g^{|G|}$ 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 $|g| \leq j - i \leq j \leq |G|$.
$\square$

Proposition 4.15. *Let G be a group. Let $g \in G$ have finite order. Let $m \in \mathbb{N}$. Then*

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

PROOF: Since for any integer d we have

$$\begin{aligned} g^{md} = e &\Leftrightarrow |g| \mid md && \text{(Corollary 4.12.1)} \\ &\Leftrightarrow \mathrm{lcm}(m, |g|) \mid md \\ &\Leftrightarrow \frac{\mathrm{lcm}(m, |g|)}{m} \mid d && \square \end{aligned}$$

and so $|g^m| = \frac{\mathrm{lcm}(m,|g|)}{m}$ by Corollary 4.12.1. $\square$

Proposition 4.16. *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 $(gh)^{\operatorname{lcm}(|g|,|h|)} = g^{\operatorname{lcm}(|g|,|h|)} h^{\operatorname{lcm}(|g|,|h|)} = e$. $\square$

Chapter 5

Abelian Groups

Definition 5.1 (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 5.2. Every group of order ≤ 4 is Abelian.

Proposition 5.3. *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

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

Part III

Linear Algebra

Definition 5.4. Let $\mathrm{GL}_n(\mathbb{R})$ be the group of invertible $n \times n$ real matrices.