

Contents

I Preliminaries: Set theory and categories	1
1 Naïve set theory	1
2 Functions between sets	2
3 Categories	4
3.1 Some examples	6
4 Morphisms	9
5 Universal properties	11
5.1 Some examples	11
II Groups, first encounter	15
1 Definition of groups	15
1.1 Multiplication tables for $ \mathbf{G} \leq 4$	17
1.2 Theory for finite products and sums	18
1.3 Basic number theory in \mathbb{Z}	20
1.4 Order	23
2 Examples of groups	25
2.1 Symmetric groups	26
2.2 Dihedral groups	27
2.3 Cyclic groups	28
3 The category Grp and its morphisms	30
3.1 Group homomorphisms	31
3.2 Group isomorphisms	34
3.3 Products of groups	35
3.4 Coproducts of groups	36
4 Free groups	38
4.1 Constructing $\mathbf{F}(\mathbf{A})$	38
4.2 Free abelian groups	41

CONTENTS

ii

Errata

42

Chapter I

Preliminaries: Set theory and categories

1 Naïve set theory

April 5, 2022

Remark. Reflexivity, symmetry and transitivity are independent for a relation on a set.

Definition 1.1 (Indexed sets). Any function.

Definition 1.2 (Multisets). Any function with a codomain containing sets.¹

Remark. One can switch back and forth between index sets and multisets.

Definition 1.3 (Pairwise disjoint union). Let A and B be sets. Let A' and B' be sets that are in bijection with A and B respectively such that $A' \cap B' = \emptyset$. Then $A' \cup B'$ is called a disjoint union of A and B .

Proposition 1.4. *Pairwise disjoint unions of given sets are unique up to bijections.*

Remark. Here, the multiplicity is important. Disjoint unions of arbitrary multisets can be defined.

Proposition 1.5. *The sets $A \times B \times C$, $(A \times B) \times C$ and $A \times (B \times C)$ are all same up to bijections.*

¹Or cardinals.

2 Functions between sets

April 5, 2022

Notation.

Functions: \rightarrow

Injections: \hookrightarrow

Surjections: \twoheadrightarrow

Bijections: \leftrightarrow

Isomorphisms: $\xrightarrow{\cong}$

Remark. By a commutative diagram, we'll mean that we can get from one node to another via any of the shown paths and the results will be all same.

Proposition 2.1 (Function compositions). *The following diagrams commute:*

$$\begin{array}{ccccc}
 & & & \xrightarrow{h \circ g} & \\
 A & \xrightarrow{f} & B & \xrightarrow{g} & C & \xrightarrow{h} & D \\
 & \searrow & \nearrow & & & & \\
 & & & \xrightarrow{g \circ f} & & &
 \end{array}$$

$$\begin{array}{ccccc}
 & & & \xrightarrow{f} & \\
 A & \xrightarrow{\text{id}_A} & A & \xrightarrow{f} & B & \xrightarrow{\text{id}_B} & B \\
 & \searrow & \nearrow & & & & \\
 & & & \xrightarrow{f} & & &
 \end{array}$$

Further,

if g is a left-inverse of f , then $A \xrightarrow{f} B \xrightarrow{g} A$ commutes; and,

if g is a right-inverse of f , then $B \xrightarrow{g} A \xrightarrow{f} B$ commutes.

Proposition 2.2 (Injectivity and surjectivity via left- and right-inverses). *Let $f: A \rightarrow B$ be a function. Then the following hold:*

- (i) If $A \neq \emptyset$, then f is injective $\iff f$ has a left-inverse.
(ii) f is surjective $\iff f$ has a right-inverse.²

Remark. Right-inverses of surjections are called sections.

Lemma 2.3. Any left-inverse of a function is equal to any of its right-inverse. Hence, if existent, the inverse is unique.

Corollary 2.4. A function is bijective \iff it is invertible.³

Result 2.5.

- (i) An injection that is not surjective has more than one left-inverses \iff the domain has more than two elements.
(ii) A surjection that is not injective necessarily has more than one right-inverses.

Definition 2.6 (Fibers). For $f: A \rightarrow B$ and $b \in B$, we call $f^{-1}(\{b\})$ the fiber of b .

Result 2.7.

- (i) A function is injective \iff all the fibers are at most singletons.
(ii) A function is surjective \iff all the fibers are at least singletons.

Definition 2.8 (Mono- and epi-morphisms). Let $f: A \rightarrow B$. Then f is

- (i) a *monomorphism* (or is *monic*) iff for any set Z and any $\alpha, \beta: Z \rightarrow A$,

$$f \circ \alpha = f \circ \beta \implies \alpha = \beta; \text{ and,}$$

- (ii) an *epimorphism* (or is *epic*) iff for any set Z and any $\alpha, \beta: B \rightarrow Z$,

$$\alpha \circ f = \beta \circ f \implies \alpha = \beta.$$

Proposition 2.9 (Injectivity and surjectivity via mono- and epi-morphisms).

²This used AC

³This can be proven without AC.

- (i) A function is injective \iff it is monic.
- (ii) A function is surjective \iff it is epic.

Theorem 2.10 (Canonical decomposition of a function). *Let $f: A \rightarrow B$. Then the diagram*

$$\begin{array}{ccccccc}
 & & & & f & & \\
 & & & & \curvearrowright & & \\
 A & \longrightarrow & A/\sim & \xrightarrow{[a] \mapsto f(a)} & \text{im } f & \longrightarrow & B \\
 & & & & \curvearrowleft & & \\
 & & & & & &
 \end{array}$$

commutes.

Remark. *We'll not write the canonical functions explicitly.*

3 Categories

April 6, 2022

Definition 3.1 (Categories). A category \mathbf{C} consists of

- (i) a class $\text{Obj}(\mathbf{C})$ of all the *objects* of the category; and
- (ii) a set $\text{Hom}_{\mathbf{C}}(A, B)$ of *morphisms* for every pair of objects A, B of \mathbf{C} such that the following hold:
 - (a) For any objects A, B of \mathbf{C} , for any $f \in \text{Hom}_{\mathbf{C}}(A, B)$ and any $g \in \text{Hom}_{\mathbf{C}}(B, C)$, there exists a unique morphism $gf \in \text{Hom}_{\mathbf{C}}(A, C)$.

$$\begin{aligned}
 \text{Hom}_{\mathbf{C}}(A, B) \times \text{Hom}_{\mathbf{C}}(B, C) &\rightarrow \text{Hom}_{\mathbf{C}}(A, C) \\
 (f, g) &\mapsto gf
 \end{aligned}$$

- (b) For any objects A, B, C, D of \mathbf{C} , if $f \in \text{Hom}_{\mathbf{C}}(A, B)$, $g \in \text{Hom}_{\mathbf{C}}(B, C)$ and $h \in \text{Hom}_{\mathbf{C}}(C, D)$, then

$$(hg)f = h(gf).$$

- (c) For every object A of \mathbf{C} , there exists a morphism $1_A \in \text{Hom}_{\mathbf{C}}(A, A)$ such that for any object B of \mathbf{C} , and any $f \in \text{Hom}_{\mathbf{C}}(A, B)$ and any $g \in \text{Hom}_{\mathbf{C}}(B, A)$, we have

$$\begin{aligned}
 f 1_A &= f, \text{ and} \\
 1_A g &= g.
 \end{aligned}$$

- (d) For any objects A, B, C, D of \mathbf{C} , the sets $\text{Hom}_{\mathbf{C}}(A, B)$ are $\text{Hom}_{\mathbf{C}}(C, D)$ are disjoint unless $A = C$ and $B = D$.⁴

A category is called *small*, if its objects can form a set.

Corollary 3.2. *It follows that the morphism $1_A \in \text{Hom}_{\mathbf{C}}(A, A)$ is unique.*

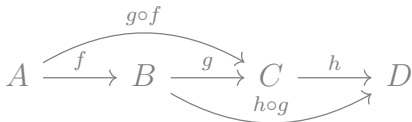
Notation.

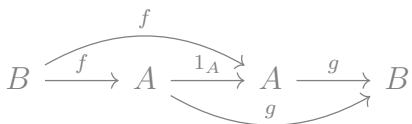
- (i) We denote $\text{Hom}_{\mathbf{C}}(A, A)$ by $\text{End}_{\mathbf{C}}(A)$.
 (ii) If the category \mathbf{C} is understood and if $f \in \text{Hom}_{\mathbf{C}}(A, B)$, then we may denote this fact by $f: A \rightarrow B$. (Note that A, B need not be sets here.)

Definition 3.3 (Diagrams). A diagram *for a category* is a set of objects in that category equipped with some given morphisms between them.

It is said to *commute* iff for any pair of “nodes”, going from one to another along any of the given “paths” yields the same result (upon morphism composition).

Remark. We can state Definition 3.1 by demanding that the following diagrams commute:

Associativity:
$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$


Identity:
$$B \xrightarrow{f} A \xrightarrow{1_A} A \xrightarrow{g} B$$


Definition 3.4 (Subcategories). Let \mathbf{C} be a category. Then a category \mathbf{C}' is called a subcategory of \mathbf{C} iff the following hold:

- (i) Objects of \mathbf{C}' are also the objects of \mathbf{C} .
 (ii) For any objects A, B of \mathbf{C}' , we have

$$\text{Hom}_{\mathbf{C}'}(A, B) \subseteq \text{Hom}_{\mathbf{C}}(A, B).$$

⁴This just says that the morphisms determine their domain and codomain objects.

- (iii) Compositions in \mathcal{C}' can be inherited from those in \mathcal{C} .
- (iv) Identities in \mathcal{C}' are also identities in \mathcal{C} .

Remark. To show the necessity of (iv) in Definition 3.4, consider a category \mathcal{C} with an object A and with an $f: A \rightarrow A$ such that $f^2 = f$. Then consider the category \mathcal{C}' with the only object A and $\text{Hom}_{\mathcal{C}'}(A, A) = \{f\}$ with $f \cdot f = f$.

Proposition 3.5 (Associativity for multiple elements). *Consider an associative operation on a set X . Inductively define*

$$\begin{aligned} x_1 \cdots x_1 &:= x_1, \\ x_1 \cdots x_{n+1} &:= (x_1 \cdots x_n)x_{n+1} \quad \text{for } n \geq 1. \end{aligned}$$

Then for any $n \geq 1$ and for any $1 \leq i < n$, we have that

$$(x_1 \cdots x_i)(x_{i+1} \cdots x_n) = x_1 \cdots x_n.$$

3.1 Some examples

April 7, 2022

Proposition 3.6 (Opposite category). *Let \mathcal{C} be a category. Then there exists a category \mathcal{C}^{op} whose objects are precisely the objects of \mathcal{C} , and*

$$\begin{aligned} \text{Hom}_{\mathcal{C}^{\text{op}}}(A, B) &:= \text{Hom}_{\mathcal{C}}(B, A), \text{ and} \\ g \cdot f &:= fg \end{aligned}$$

where \cdot is the composition in \mathcal{C}^{op} .

We also have

$$(\mathcal{C}^{\text{op}})^{\text{op}} = \mathcal{C}.$$

Proposition 3.7 (Category Set). *There exists a category Set whose objects are sets and we have*

$$\begin{aligned} \text{Hom}_{\text{Set}}(A, B) &:= B^A, \text{ and} \\ gf &:= g \circ f. \end{aligned}$$

Proposition 3.8 (Category induced by relations). *Let S be a set (or a class) and \sim be a reflexive and transitive relation on S . Then there exists a category \mathbf{C} with elements of S being its objects, together with*

$$\text{Hom}_{\mathbf{C}}(a, b) := \begin{cases} \{(a, b)\}, & a \sim b \\ \emptyset, & a \not\sim b \end{cases}, \text{ and}$$

$$(b, c)(a, b) := (a, c).$$

Further, all of the diagrams of this category are commutative.

Proposition 3.9 (Slice and coslice category). *Let \mathbf{C} be a category with an object A . Then there exists a **slice** category \mathbf{C}_A whose objects are morphisms in $\text{Hom}_{\mathbf{C}}(Z, A)$ for objects Z of \mathbf{C} , and*

$$\text{Hom}_{\mathbf{C}_A}(f_1, f_2) := \{(\sigma, f_1, f_2) : \sigma \in \text{Hom}_{\mathbf{C}}(Z_1, Z_2),$$

$$f_i \in \text{Hom}_{\mathbf{C}}(Z_i, A),$$

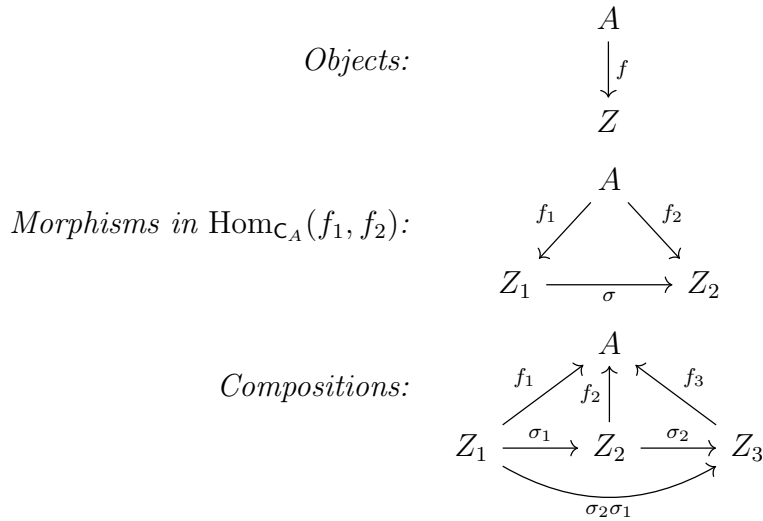
$$f_1 = f_2\sigma\}, \text{ and}$$

$$(\sigma_2, f_2, f_3)(\sigma_1, f_1, f_2) := (\sigma_2\sigma_1, f_1, f_3).$$

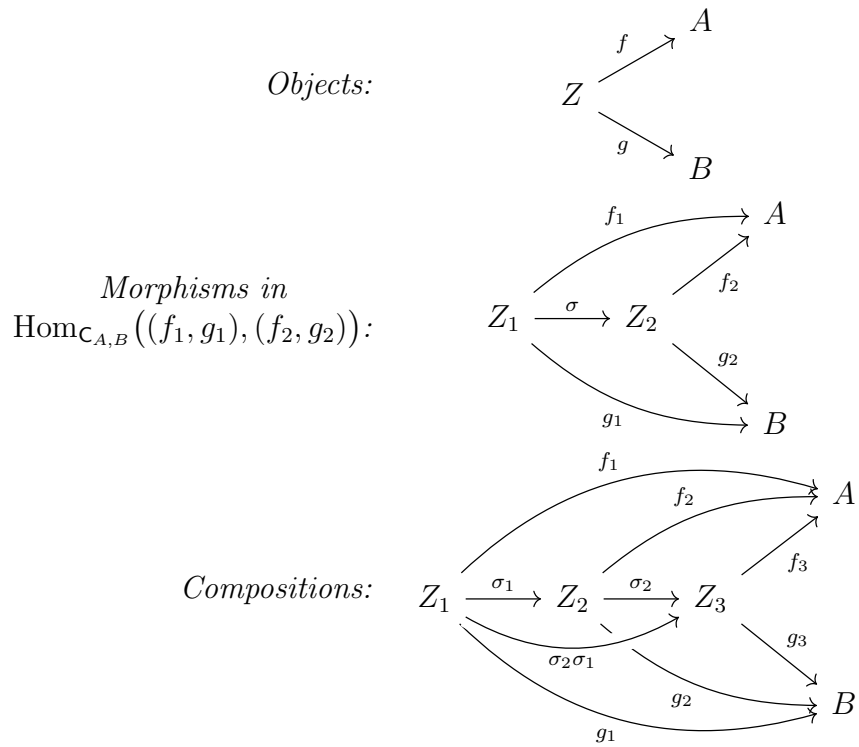
We can identify the objects and morphisms of \mathbf{C}_A with the following commutative diagrams:

$$\begin{array}{l} \text{Objects:} \\ \begin{array}{c} Z \\ \downarrow f \\ A \end{array} \\ \\ \text{Morphisms in } \text{Hom}_{\mathbf{C}_A}(f_1, f_2): \\ \begin{array}{ccc} Z_1 & \xrightarrow{\sigma} & Z_2 \\ & \searrow f_1 & \swarrow f_2 \\ & A & \end{array} \\ \\ \text{Compositions:} \\ \begin{array}{ccccc} & & \sigma_2\sigma_1 & & \\ & \nearrow & & \searrow & \\ Z_1 & \xrightarrow{\sigma_1} & Z_2 & \xrightarrow{\sigma_2} & Z_3 \\ & \searrow f_1 & \downarrow f_2 & \swarrow f_3 & \\ & & A & & \end{array} \end{array}$$

*On similar grounds, **coslice** category \mathbf{C}^A is defined with A occurring in domain's place given by the following commutative diagrams:*

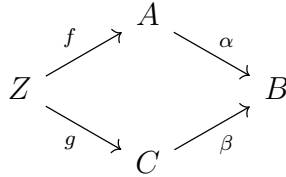


Proposition 3.10 (Categories $\mathcal{C}_{A,B}$, $\mathcal{C}^{A,B}$ and their fibered versions). *Let \mathcal{C} be a category and A, B be objects. Then the following commutative diagrams define a category $\mathcal{C}_{A,B}$:*



Similarly we can define the “co-” of the above category, $\mathcal{C}^{A,B}$.

We can also define the **fibred** version $\mathcal{C}_{\alpha,\beta}$ (and its “co-” version $\mathcal{C}^{\alpha,\beta}$) of the above starting with two fixed morphisms α and β of \mathcal{C} , with the same target, replacing the above objects with the following commutative diagrams:



4 Morphisms

April 10, 2022

Definition 4.1 (Isomorphisms). A morphism in a category that has a (two-sided) inverse is called an isomorphism.

Proposition 4.2 (Uniqueness of inverses). *Let \mathcal{C} be a category and f be a morphism. Then the following hold:*

- (i) *Any left-inverse of f is equal to any of its right-inverse.*
- (ii) *The inverse of f , if existent, is unique.*
- (iii) *f is an isomorphism \iff it has a left-inverse and a right-inverse.*

Proposition 4.3 (“Equivalence” properties of isomorphisms). *Let \mathcal{C} be a category. Then the following hold:*

- (i) *Each 1_A is an isomorphism with $1_A^{-1} = 1_A$.*
- (ii) *If f is an isomorphism, then so is f^{-1} with $(f^{-1})^{-1} = f$.*
- (iii) *If $f : A \rightarrow B$ and $g : B \rightarrow C$ are isomorphisms, then so is gf with $(gf)^{-1} = f^{-1}g^{-1}$.*

Corollary 4.4. *“Being isomorphic” is an equivalence relation on $\text{Obj}(\mathcal{C})$ for any category \mathcal{C} .*

Example 4.5.

Only 1_A ’s are isomorphisms: Categories formed by a partial orders.

All morphisms are isomorphisms: Categories formed by equivalence relations.

Definition 4.6 (Groupoids). A groupoid is a category in which every morphism is an isomorphism.

Definition 4.7 (Automorphisms). An isomorphism from an object A to itself is called an automorphism. We denote the corresponding set by $\text{Aut}_{\mathcal{C}}(A)$.

Corollary 4.8. $\text{Aut}_{\mathcal{C}}(A)$ forms a group under the morphism composition inherited from \mathcal{C} .

Definition 4.9 (Monics and epics). Let \mathcal{C} be a category and $f: A \rightarrow B$. Then f is called

- (i) monic (or a monomorphism) iff for all objects Z and for all $\alpha, \alpha': Z \rightarrow A$, we have

$$f\alpha = f\alpha' \implies \alpha = \alpha'; \text{ and}$$

- (ii) epic (or an epimorphism) iff for all objects Z and for all $\beta, \beta': B \rightarrow Z$, we have

$$\beta f = \beta' f \implies \beta = \beta'.$$

Example 4.10. In the category induced by a reflexive and transitive relation, the following hold:

- (i) Every morphism is monic and epic.
 (ii) Left-invertible \iff isomorphism \iff right-invertible.

Proposition 4.11.

- (i) *Left-invertible \implies monic.*
 (ii) *Right-invertible \implies epic.*

Hence an isomorphism is monic and epic.

Example 4.12. The category formed by a partial order (with at least two elements) shows that the converse of Proposition 4.11 is not true.

Proposition 4.13 (Compositions).

- (i) *Compositions of monics (respectively epics) is monic (respectively epic).*
 (ii) *If gf is monic, then so is f .*
 (iii) *If gf is epic, then so is g .*

5 Universal properties

April 13, 2022

Definition 5.1 (Terminal objects). An object A in a category \mathbf{C} is called

- (i) *initial* iff for every object B , the set $\text{Hom}_{\mathbf{C}}(A, B)$ is a singleton; and,
- (ii) *final* iff for every object B , the set $\text{Hom}_{\mathbf{C}}(B, A)$ is a singleton.

An object is called *zero* iff it is both initial and final.

Proposition 5.2 (Terminal objects are “same”). *Let \mathbf{C} be a category. Then any two initial (respectively final) objects (if any) are unique up to a unique isomorphism.*

Remark. We’ll say things like “an object X is universal with respect to the property that for every object Y such that \dots , there exists a unique morphism $X \rightarrow Y$ ”, “ X satisfies the universal property that \dots ”, etc. to mean that the object X is terminal in an appropriate category.

We might even describe X incompletely, and even let the morphisms unclear.

5.1 Some examples

April 14, 2022

Corollary 5.3. *The initial (respectively final) objects in \mathbf{C} are final (respectively initial) in \mathbf{C}^{op} .*

Proposition 5.4 (Terminals in \mathbf{Set}). *In \mathbf{Set} , \emptyset is the only initial object, and the final objects are precisely the singletons.*

Proposition 5.5 (Quotients in \mathbf{Set}). *Let \sim be an equivalence relation on a set A . Then the canonical function $A \rightarrow A/\sim$ is an initial object in the full subcategory of \mathbf{Set}^A whose objects are the functions $f: A \rightarrow Z$ such that*

$$a_1 \sim a_2 \implies f(a_1) = f(a_2).$$

This category’s final objects are precisely the functions $A \rightarrow \{x\}$.

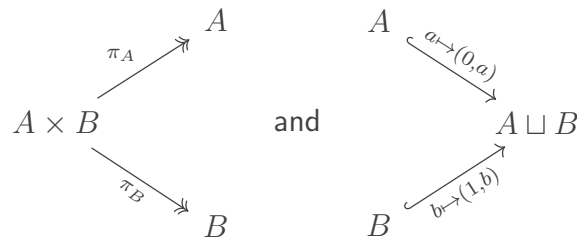
Proposition 5.6 (Terminals in pointed sets). *In the category $\mathbf{Set}^{\{*\}}$, the initial, and also the final objects, are precisely the objects associated with singletons.*

Products and coproducts

Definition 5.7 (Products and coproducts). A category \mathbf{C} is said to admit (*finite*) *products* iff for any objects A, B , the category $\mathbf{C}_{A,B}$ has final objects. We call the corresponding objects in \mathbf{C} ⁵ *products*, and usually denote them⁶ by $A \times B$.

\mathbf{C} is said to have (*finite*) *coproducts* iff for any objects A, B , the category $\mathbf{C}^{A,B}$ has initial objects. We call the corresponding objects in \mathbf{C} *coproducts*, usually denoting them by $A \sqcup B$.

Example 5.8 (Products and coproducts in Set). In Set, the Cartesian products (with the canonical projection maps) are products⁷, and the disjoint unions (with the canonical injections) are coproducts:



Example 5.9. Let \leq on a set A be reflexive, transitive and total. Then in the category formed by \leq , we have

$$\begin{aligned}
 a \times b &= \min(a, b), \text{ and} \\
 a \sqcup b &= \max(a, b).
 \end{aligned}$$

Example 5.10. In the category formed by the relation of divisibility in \mathbb{Z} (which is reflexive and transitive), we have

$$\begin{aligned}
 a \times b &= \begin{cases} \pm \gcd(a, b), & \text{one of } a, b \text{ is nonzero} \\ 0, & a = 0 = b \end{cases}, \text{ and} \\
 a \sqcup b &= \begin{cases} \pm \text{lcm}(a, b), & a, b \neq 0 \\ \text{any integer}, & \text{one of } a, b \text{ is zero} \end{cases}
 \end{aligned}$$

⁵Not in $\mathbf{C}_{A,B}$!

⁶There can be several!

⁷ A, B can be empty!

Proposition 5.11 (Commutativity and associativity). *Let \mathbf{C} be a category. If \mathbf{C} has products, then*

$$A \times B \cong B \times A, \text{ and} \\ (A \times B) \times C \cong A \times (B \times C),$$

and if \mathbf{C} has coproducts, then

$$A \sqcup B \cong B \sqcup A, \text{ and} \\ (A \sqcup B) \sqcup C \cong A \sqcup (B \sqcup C).$$

Example 5.12. We can immediately apply this result to Examples 5.9 and 5.10.

Proposition 5.13. *Let \sim_A , respectively \sim_B , be equivalence relations on sets A , respectively B . Define the relation \sim on $A \times B$ by*

$$(a, b) \sim (a', b') \quad \text{iff} \quad a \sim_A a' \text{ and } b \sim_B b'.$$

Then \sim is an equivalence relation and

$$(A \times B)/\sim \cong (A/\sim_A) \times (B/\sim_B).$$

Fibered products and coproducts

April 17, 2022

Definition 5.14 (Fibered products and coproducts). A category \mathbf{C} is said to have (*finite*) *fibered products* (respectively (*finite*) *fibered coproducts*) iff for every pair of morphisms α, β having the same target, the category $\mathbf{C}_{\alpha, \beta}$ (respectively $\mathbf{C}^{\alpha, \beta}$) has final (respectively initial) objects.

The corresponding objects of \mathbf{C} are called the fibered products and coproducts. They are usually denoted by $A \times_B C$ and $A \sqcup_B C$.⁸

Remark. *Yea, yea... The above notation is abusive...*

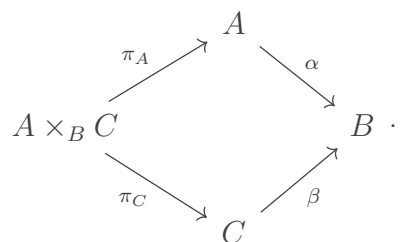
Example 5.15 (Fibered products and coproducts in \mathbf{Set}). Consider morphisms α, β in the category \mathbf{Set} . Then the following hold:

⁸ B is the common target or the common source.

(i) Let $\alpha: A \rightarrow B$ and $\beta: C \rightarrow B$. Then

$$A \times_B C \cong \{(a, c) \in A \times C : \alpha(a) = \beta(c)\}$$

and the initial objects in $\text{Set}_{\alpha, \beta}$ are isomorphic to



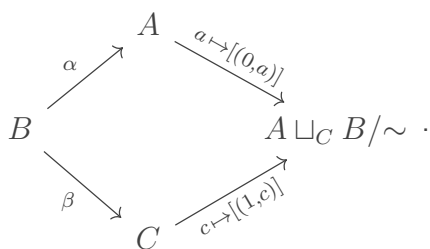
(ii) Let $\alpha: B \rightarrow A$ and $\beta: B \rightarrow C$. Define the relation \sim on $A \sqcup C$ by

- (a) $(0, a_1) \sim (0, a_2) \iff a_1 = a_2,$
- (b) $(0, a) \sim (1, c) \iff \alpha^{-1}(a) \cap \beta^{-1}(c) \neq \emptyset,$ and
- (c) $(0, c_1) \sim (0, c_2) \iff c_1 = c_2.$

Then \sim is an equivalence relation. Then

$$A \sqcup_B C \cong A \sqcup C / \sim$$

and the initial objects in $\text{Set}^{\alpha, \beta}$ are isomorphic to



Chapter II

Groups, first encounter

1 Definition of groups

April 18, 2022

Definition 1.1. A group $(G, *)$ consists of a set G and a binary operation $*$ on it such that

- (i) $*$ is *associative*; and
- (ii) there exists an *identity* $e \in G$ such that
 - (a) $e * g = g = g * e$ for all $g \in G$, and
 - (b) for each $g \in G$, there exists an *inverse* $h \in G$ such that $g * h = h * g = e$.

G is called *abelian* iff $*$ is commutative too.

Remark. When the operation \cdot on G in (G, \cdot) is obvious, we'll not mention it and will just write G in place of (G, \cdot) .

Example 1.2 (Commutative but not associative).

- (i)

a	b
a	b
b	a
- (ii) "Midpoint operation"
- (iii) $(x, y) \mapsto |x - y|$
- (iv) $(m, n) \mapsto (m \bmod k^2)(n \bmod k^2)$ for some $k \geq 2$

Proposition 1.3 (Groups as sets of morphisms of singleton groupoids). *Let G be a group and $*$ be any object. Then we can define a groupoid \mathbf{G} whose only object is $*$ with $\text{Hom}_{\mathbf{G}}(*, *) := G$ where the morphism composition is given by the group operation.*

Conversely, if \mathbf{G} is any groupoid with a single element $$, then $\text{Aut}_{\mathbf{G}}(*)$ forms a group where the group operation is given by the morphism composition.*

Example 1.4 (Some groups).

- (i) Trivial groups: Any singleton.
- (ii) Some commutative groups:
 - (a) $(R, +)$ for $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
 - (b) (S, \cdot) for $S = \{1, -1\}, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{S}^1$.
- (iii) $\text{Aut}_{\mathbf{C}}(A)$ for any object in a category \mathbf{C} .

Proposition 1.5 (Immediate consequences). *Consider a group. Then identity and inverses are unique. Further,*

$$\begin{aligned}(gh)^{-1} &= h^{-1}g^{-1}, \\ (g^{-1})^{-1} &= g, \text{ and}\end{aligned}$$

we have the cancellation law:

$$(ag = ah \text{ or } ga = ha) \implies g = h$$

Definition 1.6 (Powers). Let G be a group and $g \in G$. Then we define

$$\begin{aligned}g^0 &:= e, \\ g^{n+1} &:= g^n g \quad \text{for } n \geq 0, \text{ and} \\ g^{n-1} &:= g^n g^{-1} \quad \text{for } n \leq 0.\end{aligned}$$

Remark. *This is a slightly abusive notation: This “redefines” the symbol g^{-1} which we already assigned for the inverses. But no harm is done as g^{-1} now defined is exactly what was before, i.e., the inverse.*

Proposition 1.7 (Properties of powers). *Let G be a group and $g \in G$. Then for any $p, q \in \mathbb{Z}$, we have*

$$\begin{aligned}(g^p)^{-1} &= g^{-p}, \\ g^p g^q &= g^{p+q}, \text{ and} \\ (g^p)^q &= g^{pq}.\end{aligned}$$

Result 1.8. Let G be a group such that $g^2 = e$ for all $g \in G$. Then G is abelian.

1.1 Multiplication tables for $|G| \leq 4$

April 23, 2022

Definition 1.9 (Equivalence of binary operations). Two binary operations \cdot on X and $*$ on Y are called equivalent iff there exists a bijection $\phi: X \rightarrow Y$ such that

$$\phi(x \cdot y) = \phi(x) * \phi(y).$$

Two equivalent binary operations on a same set are called equivalent up to reordering.

Proposition 1.10. *The equivalence of binary operations is an equivalence relation.*

Proposition 1.11. *Commutativity, associativity, and the existence of an identity and inverses get translated via equivalent binary operations.*

Proposition 1.12. *There are the following possibilities for group operations (up to reordering).¹*

$G = \{e\}$ *The trivial operation.*

$G = \{e, a\}$

$$\begin{array}{c|c} e & a \\ \hline a & e \end{array}$$

$G = \{e, a, b\}$

$$\begin{array}{c|cc} e & a & b \\ \hline a & b & e \\ b & e & a \end{array}$$

¹The row and column corresponding to e are not shown.

$$G = \{e, a, b, c\}$$

$$\begin{array}{c|ccc} e & a & b & c \\ \hline a & b & c & e \\ b & c & e & a \\ c & e & a & b \end{array} \quad \text{and} \quad \begin{array}{c|ccc} e & a & b & c \\ \hline a & e & c & b \\ b & c & e & a \\ c & b & a & e \end{array}$$

1.2 Theory for finite products and sums

May 11, 2022

Definition 1.13 (Finite products). Let G be a group and $a: \{1, \dots, n\} \rightarrow G$ for an $n \geq 0$. Then we define the following:

For $k \in \mathbb{Z}$

$$\prod_{i=1}^k a_i := \begin{cases} e, & k < 1 \\ (\prod_{i=1}^{k-1} a_i) a_k, & 1 \leq k \leq n \\ \prod_{i=1}^{k-1} a_i, & k > n \end{cases}$$

For $1 \leq \alpha \leq \beta \leq n$

$$\prod_{i=\alpha}^{\beta} a_i := \prod_{i=1}^{\beta-\alpha+1} b_i,$$

where $b: \{1, \dots, \beta - \alpha + 1\} \rightarrow G$ with

$$b_i := a_{i+\alpha-1}.$$

For $k, l \in \mathbb{Z}$

$$\prod_{i=k}^l a_i := \begin{cases} e, & k > l \text{ or } k > n \text{ or } l < 1 \\ \prod_{i=\max(1,k)}^{\min(n,l)} a_i, & \text{otherwise} \end{cases}$$

Lemma 1.14. Let G be a group and $a: \{1, \dots, n\} \rightarrow G$ for an $n \geq 0$. The for any $1 \leq i_0 \leq n$, we have that

$$\prod_{i=i_0}^{i_0} a_i = a_{i_0}.$$

Lemma 1.15. *Let G be a group and $a: \{1, \dots, n\} \rightarrow G$ for $n \geq 0$. Let $1 \leq k \leq l \leq n$. Then*

$$\prod_{i=k}^l a_i = \left(\prod_{i=1}^{k-1} a_i \right)^{-1} \prod_{i=1}^l a_i.$$

Lemma 1.16. *Let G be a group and $a: \{1, \dots, n\} \rightarrow G$ for an $n \geq 0$. Let $1 \leq k \leq l \leq n$ and $k-1 \leq m \leq l$. Then*

$$\prod_{i=k}^l a_i = \prod_{i=k}^m a_i \prod_{i=m+1}^l a_i.$$

Lemma 1.17. *Let G be a group, and $a: \{1, \dots, m\} \rightarrow G$ and $b: \{1, \dots, n\} \rightarrow G$ for $m, n \geq 0$. Let $1 \leq k \leq l \leq m, n$ such that for all $k \leq i \leq l$, we have $a_i = b_i$. Then*

$$\prod_{i=k}^l a_i = \prod_{i=k}^l b_i.$$

Lemma 1.18. *Let G be a group and $a: \{1, \dots, n\} \rightarrow G$ for an $n \geq 0$. Let $2 \leq k \leq l \leq n$. Then*

$$\prod_{i=k}^l a_i = \prod_{i=k-1}^{l-1} b_i$$

where $b: \{1, \dots, n-1\} \rightarrow G$ such that $b_i = a_{i+1}$.

Proposition 1.19 (Finite sums over abelian groups). *Let G be an abelian group and $a: \{1, \dots, n\} \rightarrow G$ for an $n \geq 0$. Let p be a bijection on $\{1, \dots, n\}$. Then*

$$\sum_{i=1}^n a_i = \sum_{i=1}^n a_{p(i)}.$$

This allows to define sums on finite sets over abelian groups.

Definition 1.20 (Sums over finite sets in abelian groups). *Let G be an abelian group and $a: S \rightarrow G$ for a finite set S . Let $f: \{1, \dots, |S|\} \rightarrow S$ be a bijection. Then we define*

$$\sum_{x \in S} a_x := \sum_{i=1}^{|S|} a_{f(i)}.$$

Further, for a subset $T \subseteq S$, we define

$$\sum_{x \in T} a_x := \sum_{x \in T} b_x$$

where b is the restriction of a .

Lemma 1.21. *Let G be an abelian group and $a: \{1, \dots, n\} \rightarrow G$ for an $n \geq 0$. Then*

$$\sum_{i \in \{1, \dots, n\}} a_i = \sum_{i=1}^n a_i.$$

Lemma 1.22. *Let G be an abelian group and $a: S \rightarrow G$ for a finite set S . Then for an $x_0 \in S$, we have*

$$\sum_{x \in \{x_0\}} a_x = a_{x_0}.$$

Lemma 1.23. *Let G be an abelian group and $a: S \cup T \rightarrow G$ for disjoint finite sets S and T . Then*

$$\sum_{x \in S \cup T} a_x = \sum_{x \in S} a_x + \sum_{x \in T} a_x.$$

Lemma 1.24. *Let G be an abelian group and $a: S \rightarrow G$ for a finite set S . Let $f: T \rightarrow S$ be a bijection. Then*

$$\sum_{y \in S} a_y = \sum_{x \in T} a_{f(x)}.$$

1.3 Basic number theory in \mathbb{Z}

April 19, 2022

Definition 1.25 (gcd and lcm). For $a, b \neq 0$, we define

$$\text{lcm}(a, b) := \min\{\text{positive common multiples of } a \text{ and } b\}.$$

For $a \neq 0$ or $b \neq 0$, we define

$$\text{gcd}(a, b) := \max\{\text{(positive) common divisors of } a \text{ and } b\}.$$

Proposition 1.26 (Euclid's division lemma). *Let $a, b \in \mathbb{Z}$ such that $b \neq 0$. Then there exist unique integers q, r such that*

$$a = bq + r \quad \text{with} \quad 0 \leq r < |b|.$$

Proposition 1.27 (Characterizing lcm). *Let $a, b \neq 0$ be integers. Then $\text{lcm}(a, b)$ is the unique positive integer such that*

- (i) $\text{lcm}(a, b)$ is a common multiple of a and b ; and,
- (ii) any common multiple of a and b is a multiple of $\text{lcm}(a, b)$.

Proposition 1.28 (Euclidean algorithm). *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then we can construct an integer sequence r_0, r_1, \dots such that*

$$\begin{aligned} r_0 &:= |b|, \\ r_1 &:= \text{rem}(a, b) \quad \text{and}, \\ r_{n+1} &:= \text{rem}(r_{n-1}, r_n) \quad \text{for } n \geq 1, \end{aligned}$$

where rem is defined by

$$\text{rem}(m, n) := \begin{cases} \text{remainder on dividing } m \text{ by } n, & n \neq 0 \\ 0, & n = 0 \end{cases}.$$

Then the sequence r_0, r_1, \dots has the following properties:

- (i) Each r_i is a linear integral combination of a and b .
- (ii) (a) If $r_i = 0$, then $r_{i+1} = 0$.
(b) If $r_i \neq 0$, then $r_{i-1} < r_i$.
- (iii) Let n be the smallest integer such that $r_n = 0$ and $r_{n+1} = 0$. Then for all $1 \leq i \leq n$, we have that the

$$\gcd(r_i, r_{i+1}) = \gcd(r_{i-1}, r_i).$$

Hence, we have that

$$\gcd(a, b) = r_n$$

and that there exist $\alpha, \beta \in \mathbb{Z}$ such that

$$\gcd(a, b) = \alpha a + \beta b.$$

Corollary 1.29 (Characterizing gcd). *Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. Then $\gcd(a, b)$ is the unique positive integer such that*

- (i) $\gcd(a, b)$ is a common divisor of a and b ; and,
- (ii) any common divisor of a and b is a divisor of $\gcd(a, b)$.

Lemma 1.30. *Let $a, b \in \mathbb{Z}$ such that $a \mid b$ and $b \mid a$. Then $|a| = |b|$.*

Proposition 1.31. *For $a, b \neq 0$, we have*

$$\gcd(a, b) \operatorname{lcm}(a, b) = |ab|.$$

Definition 1.32 (Coprimes). $a, b \in \mathbb{Z}$, not both zero, are called coprime iff $\gcd(a, b) = 1$.

Proposition 1.33 (Bézout's lemma). *Let $a, b \in \mathbb{Z}$. Then the following are equivalent:*

- (i) $\gcd(a, b) = 1$.
- (ii) $a \mid bc \implies a \mid c$.
- (iii) $a \mid c$ and $b \mid c \implies ab \mid c$.

Definition 1.34 (Primes). $p \in \mathbb{Z}$ is called prime iff $p \neq \pm 1$ and its only divisors are ± 1 and $\pm p$.

Corollary 1.35 (Characterizing primes). *Let $p \in \mathbb{Z} \setminus \{-1, 1\}$. Then p is prime if and only if*

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Proposition 1.36 (Unique factorization). *Let $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Then there exist primes p_1, \dots, p_n for $n \geq 1$ such that*

$$a = p_1 \cdots p_n.$$

Further, if $q_1, \dots, q_i, r_1, \dots, r_j$ be primes for $i, j \geq 1$ such that

$$q_1 \cdots q_i = r_1 \cdots r_j,$$

then $i = j$, and after possibly rearranging, we have that

$$q_k = \pm r_k.$$

Remark. We don't need to define "empty products" for the above.

Proposition 1.37. *Let $a, b \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Then there exist naturals r, m, n , primes $p_1, \dots, p_m, q_1, \dots, q_n > 0$ and naturals $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n$ such that*

- (i) $|a| = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ and $|b| = q_1^{\beta_1} \cdots q_n^{\beta_n}$,
- (ii) $i \neq j \implies p_i \neq p_j$ and $q_i \neq q_j$,
- (iii) $i \leq r \implies p_i = q_i$, and
- (iv) $i, j > r \implies p_i \neq q_j$.

Proposition 1.38 (Divisors of an integer). *Let $n \geq 1$. Let $p_1, \dots, p_n > 0$ be primes and $\alpha_1, \dots, \alpha_n > 0$ be naturals. Then the divisors of $\pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ are precisely of the form*

$$\pm p_1^{\beta_1} \cdots p_n^{\beta_n}$$

for naturals $0 \leq \beta_i \leq \alpha_i$.

Proposition 1.39. *Let $a, b \in \mathbb{Z}$ such that $a \neq 0$ and $a \nmid b$. Then there exists a prime p , naturals $m, n \geq 0$ and $r, s \in \mathbb{Z}$ such that*

- (i) $a = p^m r$ and $b = p^n s$,
- (ii) $m > n$, and
- (iii) $p \nmid r$ and $p \nmid s$.

1.4 Order

April 20, 2022

Definition 1.40. Let G be a group. Then we define

$$|G| := \begin{cases} \#(G), & G \text{ is finite} \\ \infty, & G \text{ is infinite} \end{cases}.$$

For $g \in G$, we define $|g|$ as follows: Let $S := \{n > 0 : g^n = e\}$. Then

$$|g| := \begin{cases} \min(S), & S \neq \emptyset \\ \infty, & S = \emptyset \end{cases}.$$

Proposition 1.41. *Let G be a group and $g, h \in G$. Then*

$$|gh| = |hg|.$$

Proposition 1.42. *Let G be a group and $g \in G$. Then for $n \in \mathbb{Z}$, we have*

$$g^n = e \iff |g| \text{ divides } n.$$

Proposition 1.43. *For a group G and a $g \in G$, we have that*

$$|g| \leq |G|.$$

Proposition 1.44 (For powers). *Let G be a group and $g \in G$ such that $|g| < \infty$. Let $m \in \mathbb{Z}$. Then*

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

Proposition 1.45. *Let G be a group and $g, h \in G$ such that $\gcd(|g|, |h|) = 1$. Let $a, b \in \mathbb{Z}$ with $g^a = h^b$. Then*

$$g^a = e = h^b.$$

Proposition 1.46 (For commuting elements). *Let G be a group and $g, h \in G$ such that $gh = hg$ and $|g|, |h| < \infty$. Then $|gh| < \infty$ and*

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

Further, if $\gcd(|g|, |h|) = 1$, then

$$|gh| = |g||h|.$$

Proposition 1.47. *Let G be a group and g be an element of “maximal finite order” that commutes with all other elements of G . Then for any $h \in G$,*

$$|h| < \infty \implies |h| \text{ divides } |g|.$$

Remark. S_3 shows that commutativity of g is required.

Result 1.48. Let G be a finite group. Then we can partition G as

$$G = \{e\} \cup \{g \in G : |g| = 2\} \cup \underbrace{\{g \in G : |g| > 2\}}_{\text{even number of elements}}.$$

Result 1.49 (Order 2 elements in abelian groups). Let G be a finite abelian group. Then

$$\prod_{g \in G} g = \prod_{|g|=2} g.$$

Example 1.50 ($|gh|$ has no relation with $|g|$, $|h|$). For $g := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $h := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, we have that

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

Also see Corollary 2.9.

Definition 1.51 (Generators). Let G be a group and $S \subseteq G$. Then the subset of G formed by all the finite (possibly empty) products of elements S and their inverses is called the set generated by S . We'll denote it by $\langle S \rangle$ or by $\langle g_1, \dots, g_n \rangle$ when $S = \{g_1, \dots, g_n\}$.

Proposition 1.52. *Let G be a group and $S \subseteq G$. Then $\langle S \rangle$ is a group (with the inherited operation).*

Proposition 1.53 (The subgroup $\langle g \rangle$). *Let G be a group and $g \in G$. Then*

$$\langle g \rangle = \{\dots, g^{-1}, g^0, g^1, \dots\}$$

and if $|g| < \infty$, then

$$\langle g \rangle = \{g^0, \dots, g^{|g|-1}\}.$$

Hence,

$$|\langle g \rangle| = |g|.$$

2 Examples of groups

April 24, 2022

2.1 Symmetric groups

Notation. In an algebraic structure composed of morphisms, the algebraic product fg means the categorical product gf . When talking of an algebraic structure, we'll give precedence to the group notation.

Definition 2.1 (Symmetric groups). Let A be a set. Then we define the group of permutations of the symmetric group of A to be the set

$$S_A := \text{Aut}_{\text{Set}}(A).$$

If $A = \{1, \dots, n\}$ for $n \geq 0$, then we denote it by S_n .

Proposition 2.2. S_n is non-abelian $\iff n \geq 3$.

Proposition 2.3 (Generating S_3). Let

$$x := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad y := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Then

$$\begin{aligned} |x| &= 2, \\ |y| &= 3, \\ yx &= xy^2, \text{ and} \\ S_3 &= \langle x, y \rangle. \end{aligned}$$

(These relations define a group uniquely.)

Proposition 2.4 (Permutation matrices). Consider S_n for $n \geq 1$. Associate to each $\sigma \in S_n$ a matrix M_σ given by

$$(M_\sigma)_{i,j} := \delta_{j,\sigma(i)}.$$

Then we have

$$M_{\sigma\tau} = M_\sigma M_\tau.$$

2.2 Dihedral groups

Proposition 2.5 (Category of rigid motions). *There exists a category \mathbf{C} defined by the following:*

Objects *Subsets of \mathbb{R}^2 .*

Morphisms $\text{Hom}_{\mathbf{C}}(A, B)$ *is the set of all bijections f on \mathbb{R}^2 such that $f(A) \subseteq B$.*

Compositions *Given by function composition.*

If $f: A \rightarrow B$ is an isomorphism in \mathbf{C} , then $f(A) = B$.

Definition 2.6 (Dihedral groups). Let $n \geq 2$. Then group formed by the set of automorphisms of an n -sided polygon² centered at the origin in \mathbb{R}^2 in the category above in Proposition 2.5 is called the dihedral group D_{2n} , and its elements are called the *symmetries*.

Result 2.7 (Non-rigorous results). Consider a regular n -gon, for $n \geq 2$, centered at the origin.

- (i) D_{2n} contains $2n$ elements: n reflections and n rotations.
- (ii) Once we have labelled the vertices by $1, \dots, n$, we have the canonical injective assignment $D_{2n} \rightarrow S_n$. (This will not be surjective unless $n \leq 3$).
- (iii) Any such assignment is a homomorphism.

Remark. D_4 has more elements than S_2 . D_6 and S_3 are “same”. For $n > 3$, D_{2n} is a proper “subset” of S_n .

Proposition 2.8 (Generating D_{2n}). Let $n \geq 3$. Let $\sigma, \tau \in D_{2n}$ correspond respectively to the reflection about a line joining the vertex “1” to the origin and the “smallest rotation”. Then these correspond to $x, y \in S_n$ given by

$$x(i) := \begin{cases} n-1, & i \leq n-1 \\ n, & i = n \end{cases} \quad \text{and} \quad y(i) := \begin{cases} i+1, & i \leq n-1 \\ 1, & i = n \end{cases}.$$

²A polygon is not just its points, but also contains its “interior”.

Then we have

$$\begin{aligned} |x| &= 2, \\ |y| &= n, \text{ and} \\ yx &= xy^{-1}. \end{aligned}$$

It follows that $e, y, \dots, y^{n-1}, x, xy, x, \dots, xy^{n-1}$ are distinct.

The same relations hold with σ and τ replaced with x and y respectively.

Hence

$$D_{2n} = \langle \sigma, \tau \rangle.$$

(The above four relations uniquely determine a group for any $n \geq 1$.)

Remark. This enables us to define D_1 also, which is the “same” as a group with two elements.

Corollary 2.9. For $n \geq 1$, there exists a group G and $g, h \in G$ such that $|g| = 2 = |h|$ and $|gh| = n$.

Proposition 2.10 (Commuting elements). Let $n \geq 3$ be even. Then the only commuting element in D_{2n} is $\tau^{n/2}$ (using Proposition 2.8’s notation), which is the half-rotation.

If n is odd, then there’s no commuting element.

2.3 Cyclic groups

Notation. The set of equivalence classes of the relation congruence modulo n , for $n \in \mathbb{Z}$, is denoted as $\mathbb{Z}/n\mathbb{Z}$ or C_n . (We’re allowing for negative n ’s.) Note that $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z} \cong C_0$.

Remark. Since $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(-n)\mathbb{Z}$, we’ll only consider $n \geq 0$.

Proposition 2.11. $\mathbb{Z}/n\mathbb{Z}$ has $|n|$ elements for $n \neq 0$:

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$$

For $n = 0$,

$$|\mathbb{Z}/0\mathbb{Z}| = \infty \quad \text{with} \quad \bar{i} = \{i\}.$$

Proposition 2.12 (Making $\mathbb{Z}/n\mathbb{Z}$ a group). *Let $n \in \mathbb{Z}$. Then we can define $+$ on $\mathbb{Z}/n\mathbb{Z}$ so that*

$$\bar{a} + \bar{b} = \overline{a + b}.$$

This operation makes $\mathbb{Z}/n\mathbb{Z}$ an abelian group with identity being $\bar{0}$ and the inverse of \bar{a} being $\overline{-a}$ and

$$|\bar{1}| = \begin{cases} |n|, & n \neq 0 \\ \infty, & n = 0 \end{cases} \text{ and hence, } \langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}.$$

Proposition 2.13 (Orders in $\mathbb{Z}/n\mathbb{Z}$). *For $n \neq 0$ and $m \in \mathbb{Z}$, the order of \bar{m} in $\mathbb{Z}/n\mathbb{Z}$ is given by*

$$|\bar{m}| = \frac{|n|}{\gcd(m, n)}.$$

In $\mathbb{Z}/0\mathbb{Z}$,

$$|\bar{m}| = \begin{cases} 1, & \bar{m} = \bar{0} \\ \infty, & \bar{m} \neq \bar{0} \end{cases}.$$

Corollary 2.14 (Generating C_n). *For $n \neq 0$ and $m \in \mathbb{Z}$, we have that*

$$\langle \bar{m} \rangle = \mathbb{Z}/n\mathbb{Z} \iff \gcd(m, n) = 1.$$

Proposition 2.15 (Multiplication on $\mathbb{Z}/n\mathbb{Z}$). *Let $n \geq 1$. Then we can define multiplication on $\mathbb{Z}/n\mathbb{Z}$ such that*

$$\bar{a}\bar{b} = \overline{ab}.$$

Proposition 2.16 (Multiplicative group). *For $n \in \mathbb{Z}$, the set*

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

forms a group under multiplication.

For prime p , we have that

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

Definition 2.17 (Euler's Φ -function). *It is defined by assigning $n \geq 1$ to*

$$\Phi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|.$$

Proposition 2.18. *For odd $n \geq 1$, the function*

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z}) &\rightarrow (\mathbb{Z}/2n\mathbb{Z}) \\ \bar{m} &\mapsto \overline{2m + n} \end{aligned}$$

is a bijection, and hence

$$\Phi(n) = \Phi(2n).$$

3 The category **Grp** and its morphisms

April 27, 2022

Lemma 3.1 (Product and coproducts of morphisms). *Let \mathcal{C} be a category with (co)products. Let $f: A \rightarrow C$ and $g: B \rightarrow D$. Then fixing products $A \times B$ and $C \times D$ with relevant morphisms, there exists a unique morphism $f \times g: A \times B \rightarrow C \times D$ such that the diagram*

$$\begin{array}{ccccc}
 & & A & \xrightarrow{f} & C \\
 & \nearrow & & & \nearrow \\
 A \times B & \xrightarrow{f \times g} & C \times D & & \\
 & \searrow & & & \searrow \\
 & & B & \xrightarrow{g} & D
 \end{array}$$

commutes.

Similarly, we have $f \sqcup g$ such that the diagram

$$\begin{array}{ccccc}
 A & \xrightarrow{f} & C & & \\
 & \searrow & & & \searrow \\
 & & A \times B & \xrightarrow{f \sqcup g} & C \times D \\
 & \nearrow & & & \nearrow \\
 B & \xrightarrow{g} & D & &
 \end{array}$$

commutes.

Further, (whenever defined) we have

$$\begin{aligned}
 f_2 f_1 \times g_2 g_1 &= (f_2 \times g_2)(f_1 \times g_1), \text{ and} \\
 f_2 f_1 \sqcup g_2 g_1 &= (f_2 \sqcup g_2)(f_1 \sqcup g_1).
 \end{aligned}$$

In **Set**, with the usual definitions of products and coproducts, we have

$$\begin{aligned}
 (f \times g)(a, b) &= (f(a), g(b)), \text{ and} \\
 (f \sqcup g)(x) &= \begin{cases} (0, f(a)), & x = (0, a) \\ (1, g(b)), & x = (1, b) \end{cases}.
 \end{aligned}$$

Proposition 3.2 (**Grp**). *There exists a category **Grp** whose objects are groups such that the sets $\text{Hom}_{\mathbf{Grp}}((G, m_G), (H, m_H))$ consist of the commutative di-*

agrams in Set of the form

$$\begin{array}{ccc} G \times G & \xrightarrow{\phi \times \phi} & H \times H \\ m_G \downarrow & & \downarrow m_H \\ G & \xrightarrow{\phi} & H \end{array} ,$$

with compositions given as

$$\begin{array}{ccccc} & & (\psi \circ \psi) \times (\psi \circ \phi) & & \\ & \searrow & \text{---} & \swarrow & \\ G \times G & \xrightarrow{\phi \times \phi} & H \times H & \xrightarrow{\psi \times \psi} & K \times K \\ m_G \downarrow & & \downarrow m_H & & \downarrow m_K \\ G & \xrightarrow{\phi} & H & \xrightarrow{\psi} & K \\ & \searrow & \text{---} & \swarrow & \\ & & \psi \circ \phi & & \end{array} .$$

Proposition 3.3 (Ab). *There is a full subcategory Ab of Grp whose objects are abelian groups.*

Example 3.4. Trivial groups are zero objects in Grp.

3.1 Group homomorphisms

Definition 3.5 (Group homomorphisms). Let G, H be groups. Then a function $\phi: G \rightarrow H$ is called a group homomorphism iff

$$\phi(ab) = \phi(a)\phi(b).$$

Corollary 3.6. *Morphisms in Grp are precisely group homomorphisms.*

Remark. *Characterizing Grp morphisms in terms of the set-theoretic group homomorphisms allows to work with diagrams in Set instead of Grp.*

Corollary 3.7 (Immediate consequences). *Let $\phi: G \rightarrow H$ be a group homomorphism. Then*

- (i) $\phi(e_G) = e_H$, and
(ii) $\phi(a^{-1}) = \phi(a)^{-1}$, i.e. the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ g \mapsto g^{-1} \downarrow & & \downarrow h \mapsto h^{-1} \\ G & \xrightarrow{\phi} & H \end{array}$$

- (iii) $|g| < \infty \implies |\phi(g)| < \infty$ and $|\phi(g)|$ divides $|g|$.

Example 3.8. $\text{Hom}_{\text{Grp}}(G, H)$ are pointed sets with a distinguished trivial homomorphism.

Definition 3.9 (Group actions). Let G be a group and A be an object of a category \mathcal{C} . Then any homomorphism

$$G \rightarrow \text{Aut}_{\mathcal{C}}(A)$$

is called a group action of G on A .

Example 3.10. The groups D_{2n} (rotations + reflections) and C_n (rotations) act on the vertices of regular n -gons (or more precisely, the set $\{1, \dots, n\}$).

Proposition 3.11 (Exponential maps). Let G be a group and $g \in G$. Then $\epsilon_g: \mathbb{Z} \rightarrow G$ defined by

$$a \mapsto g^a$$

is a homomorphism which is surjective $\iff g$ generates G .

Example 3.12. The canonical functions $\pi_n: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ are group homomorphisms.

Example 3.13. Let G be a group. Then the map $G \rightarrow \text{Aut}_{\text{Grp}}(G)$ given by $g \mapsto \gamma_g$ such that

$$\gamma_g(a) = gag^{-1}$$

is a homomorphism which is trivial if and only if G is abelian.

Proposition 3.14 ($C_m \rightarrow G$ homomorphisms). Let $m \in \mathbb{Z}$ and G be a group. Let $C_m = \langle a \rangle$.

$m = 0$ Then each $\phi: a \mapsto g \in G$ determines a homomorphism.

$m \neq 0$ Then we have the following correspondence:

$$\begin{array}{ccc} \{g \in G : |g| < \infty \text{ and } |g| \text{ divides } m\} & \longleftrightarrow & \{\text{homomorphisms } \phi: C_m \rightarrow G\} \\ g & & \phi: a \mapsto g \end{array}$$

Proposition 3.15 ($C_m \rightarrow C_n$ homomorphisms). Let $m, n \in \mathbb{Z}$. Let $C_m = \langle a \rangle$ and $C_n = \langle b \rangle$.

$m = 0$ Then each $\phi: a \mapsto b^k$ determines a homomorphism for $0 \leq k < n$.

$m \neq 0, n = 0$ Then only homomorphism is the trivial one.

$m, n \neq 0$ Then we have the following correspondence:

$$\begin{array}{ccc} \{0 \leq k < |n| : n \mid km\} & \longleftrightarrow & \{\text{homomorphisms } \phi: C_m \rightarrow C_n\} \\ k & & \phi: a \mapsto b^k \end{array}$$

Proposition 3.16 ($\mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ ring homomorphisms). Let $m, n \in \mathbb{Z}$ and $\phi: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ be a homomorphism such that

$$[1]_m \mapsto [k]_n \text{ for some } k \in \mathbb{Z}.$$

Then it preserves multiplication if and only if

$$k(k-1) \equiv 0 \pmod{n}.$$

Example 3.17 (Special case when $k = 1$). If $m, n \neq 0$. Then the ring homomorphism $\pi_n^m: [1]_m \mapsto [1]_n$ is characterized by the commutativity of the following diagram:

$$\begin{array}{ccc} & \mathbb{Z} & \\ \pi_m \swarrow & & \searrow \pi_n \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\pi_n^m} & \mathbb{Z}/n\mathbb{Z} \end{array}$$

3.2 Group isomorphisms

Proposition 3.18 (Isomorphisms in Grp). *Let G, H be groups. Then (ϕ, G, H) is an isomorphism in Grp $\iff \phi: G \rightarrow H$ is a bijective group homomorphism.*

Corollary 3.19. *Group isomorphisms preserve commutativity and orders.*

Example 3.20. $\text{Aut}_{\text{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$.

Example 3.21 (Non-isomorphic groups). None of the following groups are isomorphic:

- (i) \mathbb{Z}
- (ii) \mathbb{Q}
- (iii) \mathbb{R}

Further, $\mathbb{Q} \not\cong \mathbb{Q}^{>0}$ and $\mathbb{R}^* \not\cong \mathbb{C}^*$.

Definition 3.22 (Cyclic groups). Groups isomorphic to C_n (for any $n \in \mathbb{Z}$) are called cyclic groups.

Proposition 3.23 ($\langle g \rangle$ is cyclic). *Let G be a group and $g \in G$.*

$|g| < \infty$ *Then $\langle g \rangle \cong C_{|g|}$.*

$|g| = \infty$ *Then $\langle g \rangle \cong C_0$.*

Example 3.24 (Cyclic groups in S_n). Let $1 \leq d \leq n$ and define $\phi: \mathbb{Z}/d\mathbb{Z} \rightarrow S_n$ by

$$\phi_{\bar{r}}(i) := \begin{cases} d - r + i, & 1 \leq i \leq r \\ i - r, & r < i \leq d \\ i, & d < i \leq n \end{cases} \quad \text{for } 0 \leq r < d.$$

Then ϕ is an injective homomorphism.

Proposition 3.25 ($C_n \rightarrow C_n$ group isomorphisms). *Let $n \in \mathbb{Z}$ and $C_n = \langle a \rangle$. Then the homomorphism $C_n \rightarrow C_n$ determined by*

$$a \mapsto a^k$$

is an isomorphism if and only if

$$\gcd(n, k) = 1.$$

Corollary 3.26 (Characterizing Euler's Φ -function). *For $n \geq 1$, we have that*

$$\Phi(n) = |\text{Aut}_{\text{Grp}}(C_n)|.$$

Proposition 3.27 ($(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic). *Let $p > 0$ be prime. Assume that $x^d = \bar{1}$ has at most d solutions in $\mathbb{Z}/p\mathbb{Z}$ for $1 \leq d \leq p$. Then*

$$\text{Aut}_{\text{Grp}}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}.$$

Corollary 3.28 (Wilson's theorem). *From Proposition 3.27, we can deduce that any integer $p > 1$ is prime if and only if*

$$(p-1)! \equiv -1 \pmod{p}.$$

3.3 Products of groups

Proposition 3.29 (Products in Grp). *Let (G, m_G) and (H, m_H) be groups. Then the operation*

$$((g, h), (g', h')) \mapsto (gg', hh')$$

makes $G \times H$ a group.

$\pi_G: G \times H \rightarrow G$ and $\pi_H: G \times H \rightarrow H$ are group homomorphisms.

Define

$$\Pi_G := (\pi_G, (G \times H, m_{G \times H}), (G, m_G)), \text{ and}$$

$$\Pi_H := (\pi_H, (G \times H, m_{G \times H}), (H, m_H)).$$

Then

$$\begin{array}{ccc} & & (G, m_G) \\ & \nearrow \Pi_G & \\ (G \times H, m_{G \times H}) & & \\ & \searrow \Pi_H & \\ & & (H, m_H) \end{array}$$

is a final object in $\text{Grp}_{(G, m_G), (H, m_H)}$: If $\phi: K \rightarrow G$ and $\psi: K \rightarrow H$ are group homomorphisms, then the unique morphism $(K, m_K) \rightarrow (G \times H, m_{G \times H})$ is determined by the group homomorphism $\sigma: K \rightarrow G \times H$ given by

$$\sigma(k) := (\phi(k), \psi(k)).$$

Example 3.30 ($G \times H \cong G \not\Rightarrow H = \{e\}$). Consider $G := H^{\mathbb{N}}$ for any nontrivial H .

Example 3.31. $\mathbb{Q} \not\cong G \times H$ for nontrivial G, H .

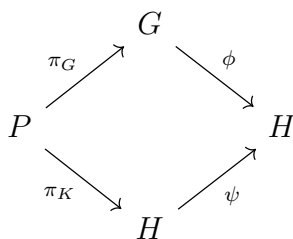
Proposition 3.32 (Cyclicity of $C_m \times C_n$). Let $m, n \in \mathbb{Z}$. Then

$$C_m \times C_n \text{ is cyclic} \iff \gcd(m, n) = 1.$$

Corollary 3.33. The group $G \times H$ is abelian $\iff G$ and H are.

Proposition 3.34. Ab has the same products as Grp .

Proposition 3.35 (Fibered products in Grp). Grp has fibered products: For homomorphisms $\phi: G \rightarrow H$ and $\psi: K \rightarrow H$,



where P is the group formed by the fibered product of G, H in Set and the operation

$$(g_1, h_1)(g_2, h_2) := (g_1g_2, h_1h_2)$$

is a final object in $\text{Grp}_{\phi, \psi}$.

3.4 Coproducts of groups

Example 3.36 (The coproduct of C_2 and C_3 in Grp). Let $G = \langle x, y \rangle$ be the group defined by the relations

$$\begin{aligned}
 |x| &= 2, \text{ and} \\
 |y| &= 3.
 \end{aligned}$$

Then G is a coproduct of C_2 and C_3 in Grp . More precisely,

$$\begin{array}{ccc} C_2 & & \\ & \searrow i & \\ & & G \\ & \nearrow j & \\ C_3 & & \end{array}$$

where

$$\begin{aligned} i(x^k) &= x^k & \text{for } 0 \leq k < 2, \\ j(x^k) &= y^k & \text{for } 0 \leq k < 3 \end{aligned}$$

is an initial object in Grp_{C_2, C_3} .³

Proposition 3.37 (Coproducts in Ab). *Let (G, m_G) and (H, m_H) be abelian groups. Then $\iota_G: G \rightarrow G \times H$ and $\iota_H: H \rightarrow G \times H$ defined by*

$$\begin{aligned} \iota_G(g) &:= (g, e_H), \text{ and} \\ \iota_H(h) &:= (e_G, h) \end{aligned}$$

are group homomorphisms.

Define

$$\begin{aligned} I_G &:= (\iota_G, (G, m_G), (G \times H, m_{G \times H})), \text{ and} \\ I_H &:= (\iota_H, (H, m_H), (G \times H, m_{G \times H})). \end{aligned}$$

Then

$$\begin{array}{ccc} (G, m_G) & & \\ & \searrow I_G & \\ & & (G \times H, m_{G \times H}) \\ & \nearrow I_H & \\ (H, m_H) & & \end{array}$$

is an initial object in $\text{Ab}_{(G, m_G), (H, m_H)}$: If $\phi: G \rightarrow K$ and $\psi: H \rightarrow K$ are group homomorphisms, then the unique morphism $(G \times H, m_{G \times H}) \rightarrow (K, m_K)$ is determined by the group homomorphism $\sigma: G \times H \rightarrow K$ given by

$$\sigma(g, h) := \phi(g)\psi(h).$$

³Usual abuse of notation.

Notation. When $G \times H$ is seen as a coproduct (when G, H are abelian), we write that as $G \oplus H$ or $G * H$.

Example 3.38 (A coproduct in Ab needn't be so in Grp). There's no homomorphism $C_2 \times C_3 \rightarrow S_3$ that corresponds to homomorphisms (as defined in Example 3.24) $C_2 \rightarrow S_3$ and $C_3 \rightarrow S_3$.

4 Free groups

April 5, 2022

Proposition 4.1 (Category \mathcal{F}^A). Let A be a set. Then there exists a category \mathcal{F}^A whose objects are set-functions $A \rightarrow G$ for groups G .⁴, morphisms are commutative diagrams (in Set) of the form

$$\begin{array}{ccc} & A & \\ j_1 \swarrow & & \searrow j_2 \\ G_1 & \xrightarrow{\phi} & G_2 \end{array}$$

where j_1, j_2 are set-functions and ϕ is a group homomorphism. The compositions are given in the obvious manner.

Definition 4.2 (Free groups). A free group $F(A)$ of a set A is (the group component of) an initial object of the category \mathcal{F}^A .

Proposition 4.3.

- (i) $F(\emptyset) \cong \{e\}$.
- (ii) $F(\{a\}) \cong \mathbb{Z}$.

4.1 Constructing $F(A)$

Let A be a set. Let A' be an equinumerous but disjoint set with the correspondence given by

$$a \mapsto \text{inv}(a).$$

⁴Apparently, we can form a class out of union over classes.

We define the following “*inverse*” on $A \cup A'$:

$$\alpha \mapsto \alpha^{-1} := \begin{cases} \text{inv}(\alpha), & \alpha \in A \\ \text{inv}^{-1}(\alpha), & \alpha \in A' \end{cases}$$

Lemma 4.4.

- (i) $(\alpha^{-1})^{-1} = \alpha$.
- (ii) $\alpha \in A \iff \alpha^{-1} \in A'$.
- (iii) $\alpha \in A' \iff \alpha^{-1} \in A$.

Let $W(A)$ be the set of all “*words*” of finite length (possibly of length zero)⁵ whose “*letters*”⁶ are taken from $A \cup A'$.

An occurrence of the pattern “ α, α^{-1} ” for $\alpha \in A \cup A'$ in a word is called its *reduction point*.

We define the following operations on $W(A)$:

Concatenation: $(w_1, w_2) \mapsto w_1 * w_2$. This concatenates the words.

Lemma 4.5.

- (i) *Concatenation is associative.*
- (ii) $(\alpha_1, \dots, \alpha_n) = (\alpha_1) * \dots * (\alpha_n)$.

Inverse: $w \mapsto \iota(w)$. For $w = (\alpha_1, \dots, \alpha_n)$, we define $\iota(w) := (\alpha_n^{-1}, \dots, \alpha_1^{-1})$.

Lemma 4.6. *For $w \in W(A)$, we have that $\iota(\iota(w)) = w$.*

Elementary reduction: $w \mapsto r(w)$. Take a word $w \in W(A)$. If there exists a reduction point in w (in which case, w is called *reducible*), then r returns the word in $W(A)$ omitting the first reduction point from left. Otherwise (here w is called *irreducible*), r returns w as it is.

Lemma 4.7.

- (i) *If w_1 has a reduction point, then $r(w_1 * w_2) = r(w_1) * w_2$.*
- (ii) *If w_1 is irreducible and w_2 is reducible, then $r^2(w_1 * w_2) = r(w_1 * r(w_2))$.*

⁵More precisely, finite sequences.

⁶More precisely, the elements of the sequence.

(iii) For a word $w \in W(A)$ of length $n \geq 0$, we have that $r^{\lfloor \frac{n}{2} \rfloor}(w)$ is irreducible.

Reduction: $w \mapsto R(w) := r^{\lfloor \frac{n}{2} \rfloor}(w)$.

Lemma 4.8.

- (i) $R(r(w)) = R(w)$.
- (ii) $R(r(w_1) * w_2) = R(w_1 * w_2) = R(w_1 * r(w_2))$.

We define $F(A)$ to be the set $\text{im}(R)$ with the following “**multiplication**”:

$$w_1 w_2 := R(w_1 * w_2)$$

Lemma 4.9.

- (i) $F(A)$ is closed under ι .
- (ii) For $w \in F(A)$, we have $w \iota(w) = () = \iota(w) w$.

Proposition 4.10. $F(A)$ forms a group with the above multiplication with the identity given by the empty word, and the inverse of w given by $\iota(w)$.

Lemma 4.11. Let $f: A \rightarrow G$ be a set-function for a group G . Define a set-function $\tilde{\phi}: W(A) \rightarrow G$ by

$$\tilde{\phi}(\alpha) := \begin{cases} f(\alpha), & \alpha \in A \\ (f(\alpha^{-1}))^{-1}, & \alpha \in A' \end{cases}, \text{ and}$$

$$\tilde{\phi}(\alpha_1, \dots, \alpha_n) := \tilde{\phi}(\alpha_1) \cdots \tilde{\phi}(\alpha_n).$$

Then this function satisfies

$$\tilde{\phi}(w_1 * w_2) = \tilde{\phi}(w_1) \tilde{\phi}(w_2), \text{ and}$$

$$\tilde{\phi}(r(w)) = \tilde{\phi}(w).$$

Moreover, the restriction of $\tilde{\phi}$ to $F(A)$ is a group homomorphism.

Proposition 4.12. $(j, F(A))$ is an initial object in \mathcal{F}^A , where $j: A \rightarrow F(A)$ is the ‘canonical’ injection.

4.2 Free abelian groups

May 10, 2022

Proposition 4.13 $((\mathcal{F}^{\text{ab}})^A)$. *Let A be a set. Then there exists a full subcategory $(\mathcal{F}^{\text{ab}})^A$ of \mathcal{F}^A whose objects are set-functions $A \rightarrow H$ for abelian groups H .*

Definition 4.14 (Free abelian groups). *The initial objects of $(\mathcal{F}^{\text{ab}})^A$, denoted by $F^{\text{ab}}(A)$ are called free abelian groups.*

Proposition 4.15 (Groups H^A and $H^{\oplus A}$). *Let A be a set and G a group. Then the set G^A forms a group with the following operation:*

$$(fg)(a) := f(a)g(a)$$

Further, the set

$$G^{\oplus A} := \{\alpha \in G^A : \alpha(a) \neq 0 \text{ for finitely many } a \in A\}$$

forms a group with the inherited operation.

G^A and $G^{\oplus A}$ are abelian if G is.

Proposition 4.16. *For a group G and $n \geq 0$, we have that*

$$G^n \cong G^{\oplus\{1, \dots, n\}}.$$

Proposition 4.17 (Constructing free abelian groups). *Let A be a set. Then the group $\mathbb{Z}^{\oplus A}$ along with the set-function $j: A \rightarrow \mathbb{Z}^{\oplus A}$ given by*

$$j_a(x) := \begin{cases} 0, & x \neq a \\ 1, & x = a \end{cases}$$

is an initial object in $(\mathcal{F}^{\text{ab}})^A$.

Errata

1

Clarification 1.1 (p. 17).

- (i) At the end of the first paragraph, it's written that the "same considerations [of definition up to isomorphism] apply to products and quotients". For the Cartesian product, this is plausible. But what ever was the problem with quotients?
- (ii) In footnote 12, "*fibred*" flavors of products and disjoint unions are talked about. Put a reference to Exercise 5.12.

Clarification 1.2 (p. 19). Clarify the meaning of 'pointed set' in the penultimate paragraph.

2

Math 2.1 (p. 47). In Proposition 1.13, it should be that $m > 0$ and not $m \geq 0$ for $\text{lcm}(m, |g|)/m$ (or even $\text{lcm}(m, |g|)!$) to make sense. However, for the expression involving gcd , there's no such problem, and the statement holds for $m = 0$ too.

Suggestion 2.1 (p. 49). In Exercise 1.15, commutativity of the entire group can be replaced by the weaker condition that g should commute with all the elements.

Math 2.2 (p. 52). In the third-to-last paragraph, "(thereby excluding translations as possible symmetries)" is not correct.

Math 2.3 (p. 55). In the last paragraph, well-definedness of $(\mathbb{Z}/n\mathbb{Z})^*$ need *not* be checked. It's well-defined as it is.

Math 2.4 (p. 57). Exercise 2.4: In the hint, to show that the relations really determine D_{2n} , the claim that any product $x^{i_1}y^{i_2}\dots$ equals x^iy^j does *not* suffice. Instead, $2n$ *distinct* elements must be shown to be generated from x, y .

Typo 2.1. Exercise 2.15: Inconsistency in using ϕ and Φ .

Math 2.5 (p. 58). Exercise 2.18: $d \geq 1$ must be mentioned.

Suggestion 2.2 (p. 62). It'd be helpful to note that despite the identical notations, the function $\phi_G \times \phi_H$ in the proof of Proposition 3.4 is *not* the same as the “function product” ($\phi \times \phi$ on p. 58) in defining the group homomorphisms.

Typo 2.2 (p. 62). In the paragraph after the proof, it's written “...so the reader will have to deal with them on his or her own.” If the author cares for the LGBTQIA+ inclusion, “his or her” *should* be replaced (or appended) with “their”.

Typo 2.3 (p. 63). Exercise 3.3: There is no §3.6 in the book, that is referenced.

Exercise 3.9: It should be “fibered” products and not fiber products.

Math 2.6 (p. 66). Example 4.2: Mention $n \neq 0$.

Math 2.7 (p. 69). Exercise 4.11: Mention that $1 \leq d \leq p$. Also, the equation “ $x^d = 1$ ” must more precisely be written as “ $x^d = [1]_p$ ”. Similarly for Exercise 4.12's “ $x^3 - 9 = 0$ ”.

Suggestion 2.3 (p. 73). At the top, the definition of r is incomplete in a subtle way: Add that r returns w as it is if there are no patterns of aa^{-1} or $a^{-1}a$.

Math 2.8 (p. 74). Several issues with the proof of Proposition 5.2:

- (i) It should be commented that the compatibility of $\tilde{\varphi}$ with juxtaposition

$$\tilde{\varphi}(ww') = \tilde{\varphi}(w)\tilde{\varphi}(w')$$

is indeed possible.

- (ii) The proof is divided in two parts:

- (a) A group homomorphism φ is uniquely determined by demanding the commutativity of the diagram, that fixes φ 's values over single letters (and their inverses).
- (b) If $\varphi: F(A) \rightarrow G$ is a function such that it agrees with $\tilde{\varphi}$ on reduced words, then φ is a group homomorphism.

However, in the latter part, it was never shown that such a φ exists! It should be commented that we can take this φ to be the restriction of $\tilde{\varphi}$ on $F(A)$.