Algebra

Aluffi

Authors: Shaleen Baral

Contents

1. Preliminaries

1.1. Naive Set Theory

Definition 1.1.1 . The *ordered pair* (s, t) can be defined as the set $\{s, \{s, t\}\}$. This retains both the elements of the tuple but also conveys an ordering.

Definition 1.1.2 . The *disjoint union* of two sets S, T is the set $S \sqcup T$ obtained by first producing 'copies' S' and T' and then taking the union.

Definition 1.1.3 . The *product* of two sets S, T is the set $S \times T$ defined as

$$S \times T = \{(s, t) \text{ such that } s \in S,, t \in T\}.$$

Definition 1.1.4 . A *relation* on a set S is a subset R of the product $S \times S$. If $(a, b) \in R$, we write aRb.

Definition 1.1.5 . An *equivalence relation* on a set S is any relation $\sim$ satisfying the following properties

a. *reflexivity*: $\forall a \in S.\ a \sim a$
b. *symmetry*: $\forall a \in S. \forall b \in S.\ a \sim b \Longleftrightarrow b \sim a$
c. *transitivity*: $\forall a \in S. \forall b \in S. \forall c \in S.\ a \sim b, b \sim c \Longrightarrow a \sim c.$

Definition 1.1.6 . A *partition* of S is a family of *disjoint* nonempty subsets of S whose union is S.

Definition 1.1.7 . Let $\sim$ be an equivalence relation on S. Then for every $a \in S$, the *equivalence class* of a is the subset S defined by

$$[a]_{\sim} = \{b \in S \mid b \sim a\}.$$

Further, the equivalence classes form a partition $\mathcal{P}_{\sim}$ of S.

Lemma 1.1.1: Every partition of S corresponds to an equivalence relation.

Definition 1.1.1 . The *quotient* of the set S with respect to the equivalence relation $\sim$ is the set

$$S \sim = \mathcal{P}_{\sim}$$

of equivalence classes of elements of S with respect to $\sim$.

1.2. Functions

Definition 1.2.1 . The graph of f is the set

$$\Gamma_f = \{(a, b) \in A \times B \mid b = f(a)\} \subseteq A \times B.$$

Officially, a function *is* its graph together with information of the source A and the target B of f.

Definition 1.2.2 . A function is a relation $\Gamma \subseteq A \times B$ such that $\forall a \in A, \exists! b \in B$ with $(a, b) \in \Gamma$. To denote f is a function from A to B we write $f : A \longrightarrow B$.

Definition 1.2.3 . The collection of all functions from a set A to a set B is denoted B^A.

Example: Every set A comes equipped with the *identity function*, $\mathrm{id}_A : A \longrightarrow A$, whose graph is the diagonal in $A \times A$. It is defined by $\forall a \in A.\ \mathrm{id}_A(a) = a$.

Definition 1.2.4 . If $S \subseteq A$, for $f : A \longrightarrow B$, we define $f(S) \subseteq B$ as

$$f(S) = \{b \in B \mid \exists a \in S. b = f(a)\}$$

Definition 1.2.5 . The *restriction* of $f : A \longrightarrow B$ to $S \subseteq A$, denoted $f\mid_S$ is the function $S \longrightarrow B$ defined by

$$\forall s \in S. \quad f\mid_S(s) = f(s).$$

Remark: The restriction can be equivalently described as $f \circ i$ where $i : S \longrightarrow A$ is the inclusion. Further, $f(S) = \mathrm{im}(f\mid_S)$.

Example (Multisets): A *multiset* is like a set but allows for multiple instances of each element. A multiset may be defined by giving a function $m : A \longrightarrow \mathbb{N}^\star$, where $N^\star$ is the set of positive integers. The corresponding multiset consists of the elements $a \in A$, each taken $m(a)$ times.

Example (Indexed Sets): One may think of an *indexed set* $\{a_i\}_{i\in I}$ as set whose elements are denoted by a_i for i ranging over some 'set of indices' I. Instead, it is more proper to think of an indexed set as a function $a : I \longrightarrow A$, with the understanding that a_i is a shorthand for $a(i)$. One benefit is that this allows us to consider a_0, a_1 as distinct elements of $\{a_i\}_{i\in\mathbb{N}}$ even if $a_0 = a_1$ as elements of A.

Definition 1.2.6 . If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are functions then so is the operation $g \circ f$ defined by

$$\forall a \in A. \quad (g \circ f)(a) = g(f(a)).$$

Pictorially, the following diagram *commutes*

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "g \circ f"'] & B \arrow[d, "g"] \\
& C
\end{tikzcd}$$

Remark: A diagram *commutes* when the result of following a path of arrows from any point of the diagram to any other point only depends on the starting and ending points and not on the particular path chosen.

Lemma 1.2.1: Composition of functions is associative. That is to say, if $f : A \longrightarrow B$, $g : B \longrightarrow C$ and $h : C \longrightarrow D$ then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Graphically, the following diagram commutes

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & B \arrow[r, "g"] \arrow[rr, bend left, "h \circ g"] & C \arrow[r, "h"] & D
\end{tikzcd}$$

Example: If $f : A \longrightarrow B$ then $\mathrm{id}_B \circ f = f$ and $f \circ \mathrm{id}_A = f$. Graphically, the following diagrams commute

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[rr, bend left, "\mathrm{id}_B \circ f"] & B \arrow[r, "\mathrm{id}_B"] & B
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "\mathrm{id}_A"] \arrow[rr, bend left, "\mathrm{id}_B \circ f"] & A \arrow[r, "f"] & B
\end{tikzcd}$$

Definition 1.2.1 . A function $f : A \longrightarrow B$ is *injective* if $\forall a', a'' \in A, a' \neq a'' \implies f(a') \neq f(a'')$.

Definition 1.2.8 . A function $f : A \longrightarrow B$ is *surjective* if $\forall b \in B, \exists a \in A$ such that $b = f(a)$. That is to say f *covers* B and equivalently, $\mathrm{im}(f) = B$.

Definition 1.2.9 . If $f : A \longrightarrow B$ is both injective and surjective then it is a *bijection*. Then we often write $f : A \xrightarrow{\sim} B$. We also say that A and B are *isomorphic* and denote this by $A \cong B$.

Definition 1.2.10 . A function $g : B \longrightarrow A$ is a *left inverse* of $f : A \longrightarrow B$ if $g \circ f = \mathrm{id}_A$. Graphically, the following diagram commutes

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend left, "\mathrm{id}_A"] & B \arrow[r, "g"] & A \end{tikzcd}$$

Definition 1.2.11 . A function $f : A \longrightarrow B$ is a *right inverse* of $g : B \longrightarrow A$ if $f \circ g = \mathrm{id}_A$. Graphically, the following diagram commutes

$$\begin{tikzcd} B \arrow[r, "g"] \arrow[rr, bend left, "\mathrm{id}_B"] & A \arrow[r, "f"] & B \end{tikzcd}$$

Definition 1.2.12 . We call $g : B \longrightarrow A$ an inverse of $f : A \longrightarrow B$ if g is both a left and right inverse of f. Then g may also be denoted f^{-1}.

Proposition 1.2.1: Assume $A \neq \emptyset$ and let $f : A \longrightarrow B$ be a function. Then

a. f has a left inverse iff it is injective.
b. f has a right inverse iff it is surjective.

Corollary 1.2.1.1: A function $f : A \longrightarrow B$ is a bijection if and only if it has a (two-sided) inverse.

Remark: An injective but not surjective function has no right inverse. If the source has more than two elements, there will be more than one left inverse.

Remark: A surjective function but not injective function will have multiple inverses. These are called *sections*.

Definition 1.2.1 . Let $f : A \longrightarrow B$ be any function and $S \subseteq B$ be a subset. Then $f^{-1}(S)$ is defined by

$$f^{-1}(S) = \{a \in A \mid f(a) \in S\}.$$

If $S = \{q\}$ is a singleton then $f^{-1}(T) = f^{-1}(q)$ is denoted the *fiber* of f over q.

Remark: In this language: f is a bijection iff it has nonempty fiber over all elements of B and every fiber is a singleton.

Definition 1.2.1.1 . A function $f : A \longrightarrow B$ is a *monomorphism* (or *monic*) if for all sets Z and all functions $\alpha', \alpha'' : Z \longrightarrow A$

$$f \circ \alpha' = f \circ \alpha'' \Longrightarrow \alpha' = \alpha''.$$

Proposition 1.2.2: A function is injective iff it is a monomorphism.

Example (Projection): Let A, B be sets. Then there are *natural projections* π_A, π_B

$$\begin{tikzcd}
 & A \times B \arrow[dl, two heads, "\pi_A"'] \arrow[dr, two heads, "\pi_B"] & \\
A & & B
\end{tikzcd}$$

defined by

$$\forall (a, b) \in A \times B. \quad \pi_A((a, b)) = a, \qquad \pi_B((a, b)) = b.$$

These maps are clearly surjective.

Example (Direct Sum Injection): There are natural injections from A, B to their disjoint union $A \sqcup B$

$$\begin{tikzcd}
A \arrow[dr, hook] & & B \arrow[dl, hook'] \\
 & A \sqcup B &
\end{tikzcd}$$

obtained by sending $a \in A$ (resp. $b \in B$) to the corresponding element in the isomorphic copy A' of A (resp. B' of B) in $A \sqcup B$.

Example (Equivalence Relation Projection): Let $\sim$ be an equivalence relation on A. Then there is a surjective *canonical projection*

$$\begin{tikzcd}
A \arrow[r, two heads] & A/\sim
\end{tikzcd}$$

obtained by sending every $a \in A$ to its equivalence class $[a]_\sim \in A/\sim$.

Lemma 1.2.2: Every function $f : A \longrightarrow B$ defines an equivalence relation $\sim$ on A as follows: for every $a', a'' \in A$,

$$a' \sim a'' \iff f(a') = f(a'').$$

Proposition 1.2.3 (Canonical Decomposition): Let $f : A \longrightarrow B$ be any function and define $\sim$ as above. Then f decomposes as follows:

$$\begin{tikzcd} A \arrow[r, two heads] \arrow[rrr, bend left, "f"] & (A/\sim) \arrow[r, "\sim", "\tilde{f}"'] & \mathrm{im}(f) \arrow[r, hook] & B \end{tikzcd}$$

The first function is the canonical projection $A \longrightarrow A/\sim$. The third function is the inclusion $\mathrm{im}\, f \subseteq B$. The bijection $\tilde{f}$ in the middle is defined by

$$\tilde{f}\left([a]_{\sim}\right) = f(a)$$

for all $a \in A$.

1.3. Categories

Definition 1.2.2 . A *category* C consists of

- a class $\mathrm{Obj}(C)$ of *objects* the category.
- for every two objects A, B of C, a set $\mathrm{Hom}_C(A, B)$ of *morphisms* with the following properties
  - for every object A of C, there exists (at least) one morphism $1_A \in \mathrm{Hom}_C(A, A)$, the 'identity' on A.
  - two morphisms $f \in \mathrm{Hom}_C(A, B)$ and $g \in \mathrm{Hom}_C(B, C)$ determine a morphism $fg \in \mathrm{Hom}_C(A, C)$. That is for every triple of objects A, B, C of C there is a function (of sets)

    $$\mathrm{Hom}_C(A, B) \times \mathrm{Hom}_C(B, C) \longrightarrow \mathrm{Hom}_C(A, C)$$

    and the image of the pair (f, g) is denoted fg.
  - this composition law is associative: if $f \in \mathrm{Hom}_C(A, B)$, $g \in \mathrm{Hom}_C(B, C)$ and $h \in \mathrm{Hom}(C)(C, D)$ then $(hg)f = h(gf)$.
  - the identity morphisms are identities with respect to composition: that is for all $f \in \mathrm{Hom}_C(A, B)$ we have

    $$f \cdot 1_A = f, \quad 1_B \cdot f = f.$$