

NOTES ON

Algebra

Hao Su

Based on *Algebra Chapter 0*.

August 8, 2026

Contents

I	Preliminaries: Set theory and categories	1
1	Naive set theory	1
2	Functions between sets	3

Preliminaries: Set theory and categories

1 Naive set theory

The subsets of a set S form a set, called the *power set* or the *set of parts* of S , and is denoted $\mathcal{P}(S)$ or 2^S .

The product $A \times A$ of a set by itself is often denoted A^2 .

If S is a set of sets, consider sets

$$\bigcup_{S \in S} S, \quad \bigcap_{S \in S} S, \quad \coprod_{S \in S} S, \quad \prod_{S \in S} S,$$

for the union, intersection, disjoint union, product of all sets in S . There are important subtleties concerning these definitions, **to do**.

Definition 1.1. An *equivalence relation* on a set S is any relation satisfying *reflexivity*, *symmetry* and *transitivity*.

In terms of the corresponding subset R of $S \times S$, ‘reflexivity’ says that the diagonal is contained in R ; ‘symmetry’ says that R is unchanged if flipped about the diagonal; while unfortunately ‘transitivity’ does not have a similarly nice pictorial translation.

A *partition* $\mathcal{P}$ of S is a set of disjoint nonempty subsets of S such that $\bigcup_{P \in \mathcal{P}} P = S$. An equivalence relation $\sim$ on S indicates a partition of S and vice versa: for every element $a \in S$, the *equivalence class* of a (w.r.t. $\sim$) is the subset of S defined by $[a]_{\sim} := \{b \in S \mid b \sim a\}$, and the equivalence classes form a partition $\mathcal{P}_{\sim}$ of S .

Definition 1.2. The *quotient* of the set S w.r.t. the equivalence relation $\sim$ is the set $S / \sim := \mathcal{P}_{\sim}$ of equivalence classes of elements of S w.r.t. $\sim$.

Exercises

Exercise 1. Locate a discussion of Russell's paradox, and understand it.

Consider set $R = \{x \mid x \notin x\}$. It follows that $R \in R \Leftrightarrow \neg(R \in R)$. Modern set theories avoid this by restricting the comprehension principle, which states that for any property, there is a set of all things satisfying that property.

Exercise 2. Prove that if $\sim$ is an equivalence relation on a set S , $\mathcal{P}_\sim$ is a partition of S .

That the elements of $\mathcal{P}_\sim$ are nonempty and $\bigcup_{P \in \mathcal{P}_\sim} P = S$ are straightforward. It suffices to show that the elements of $\mathcal{P}_\sim$ is disjoint. Consider two distinct equivalent classes (if there exist) of S denoted $[a]_\sim$ and $[b]_\sim$, assume they are not disjoint, hence $\exists c, c \in [a]_\sim \wedge c \in [b]_\sim \Rightarrow a \sim b$ and contradiction.

Exercise 3. Define an equivalence relation $\sim$ on a set S such that corresponds to a given partition $\mathcal{P}$ on S .

$$\sim = \bigcup_{P \in \mathcal{P}} (P \times P).$$

Exercise 4. How many different equivalence relations may be defined on the set $\{1, 2, 3\}$?

We consider the number of distinct partitions of $\{1, 2, 3\}$, and there are 5. The answer given set $\{1, 2, \dots, n\}$ should be nontrivial.

Exercise 5. Give an example of a relation that is reflexive and symmetric but not transitive. What happens if you attempt to use this relation to define a partition on the set?

A minimal example should be $\{(a, b), (b, a), (b, c), (c, b)\}$ on $\{a, b, c\}$. Note that a and b should be in the same part and so are b and c , yet a and c should not, thus contradiction.

Exercise 6. Define a relation $\sim$ on $\mathbb{R}$ by $a \sim b \Leftrightarrow b - a \in \mathbb{Z}$. Prove that $\sim$ is an equivalence relation, and find a 'compelling' description for $\mathbb{R}/\sim$. Do the same for the relation $\approx$ on $\mathbb{R} \times \mathbb{R}$ defined by $(a_1, a_2) \approx (b_1, b_2) \Leftrightarrow b_1 - a_1 \in \mathbb{Z} \wedge b_2 - a_2 \in \mathbb{Z}$.

The proofs are trivial.

$$\begin{aligned}\mathbb{R}/\sim &= \{\{x + k \mid k \in \mathbb{Z}\} \mid x \in [0, 1) \subseteq \mathbb{R}\}. \\ \mathbb{R} \times \mathbb{R}/\approx &= \{\{(x + k_1, y + k_2) \mid k_1, k_2 \in \mathbb{Z}\} \mid x, y \in [0, 1) \subseteq \mathbb{R}\}.\end{aligned}$$

2 Functions between sets

A common thread for just about every structure to be introduced will be to try to understand both the type of structures and the ways in which different instances of a given structure may interact.

Sets interact with each other through *functions*. The *graph* of a function f from a set A to a set B is a subset of $A \times B$:

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

Given distinction between the source and the target of f , f is exactly Γ_f . Think of f in ‘dynamic’ terms, as a way to ‘go from A to B ’. Require that $(\forall a \in A)(\exists! b \in B)(a, b) \in \Gamma_f$.

B^A denotes the set of all functions from A to B , which is a special subset of $\mathcal{P}(A \times B)$.

Define $\text{id}_A : A \rightarrow A$ by $(\forall a \in A)\text{id}_A(a) = a$.

If $S \subseteq A$, denote by $f(S)$ the subset of B defined by $f(S) := \{b \in B \mid (\exists a \in S)b = f(a)\}$. $f(A)$ is called the *image* of f , denoted ‘ $\text{im } f$ ’.

Define $f|_S : S \rightarrow B$ by $(\forall s \in S) : f|_S(s) = f(s)$. So $f|_S = f \circ i$, where $i : S \rightarrow A$ is the inclusion. Also $f(S) = \text{im } f|_S$.

Multisets may be defined by a function m from a set A to the set $\mathbb{N}^*$ such that the corresponding multiset consists of the elements $a \in A$, each taken $m(a)$ times.

An indexed list $a_1, \dots, a_n$ can be thought of as a function $I \rightarrow A$, where I is the set of indexes and A is the set from which we draw the elements a_i .

Functions may be *composed*: if $f : A \rightarrow B$ and $g : B \rightarrow C$ are functions, then so is the operation $g \circ f$ defined by

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

That is, we use f to go from A to B and apply g to reach C . Graphically we may draw pictures such as

$$\begin{array}{ccc} A & \xrightarrow{f} & B \xrightarrow{g} C \\ & \searrow & \uparrow \\ & & g \circ f \end{array} \quad \text{or} \quad \begin{array}{ccc} & & B \\ & \nearrow f & \downarrow g \\ A & \xrightarrow{g \circ f} & C \end{array}$$

These are called *diagrams*. We say that the diagrams drawn above ‘commute’, or ‘are commutative’, meaning that if we start from A and travel to C in either of the two possible ways prescribed by

the diagram, the result of applying the functions one encounters is the same. This is precisely the content of composition.

Composition is associative, or $h \circ (g \circ f) = (h \circ g) \circ f$.

A function $f : A \rightarrow B$ is *injective* (or *an injection* or *one-to-one* and drawn $\hookrightarrow$) if

$$(\forall a' \in A)(\forall a'' \in A) \quad a' \neq a'' \Rightarrow f(a') \neq f(a'').$$

A function $f : A \rightarrow B$ is *surjective* (or *a surjection* or *onto* and drawn $\twoheadrightarrow$) if

$$(\forall b \in B)(\exists a \in A) \quad b = f(a) \text{ or } \text{im } f = B.$$

If f is both injective and surjective, we say it is *bijective* (or *a bijection* or *a one-to-one correspondence* or *an isomorphism of sets* and written $f : A \xrightarrow{\sim} B$) and say that A and B are *isomorphic* (written $A \cong B$).

We may define disjoint union by employing bijections. **to do.**