Solutions to Exercises from ‘Algebra: Chapter 0’

Abstract. Solutions to exercises from the book 'Algebra: Chapter 0' by Paolo Aluffi.

Contents

Preface

This document contains my attempt at writing (hopefully correct!) solutions to exercises from Aluffi's book, while engaging in some self-study of modern abstract algebra with the ultimate aim of teaching myself some modern algebraic geometry.

CHAPTER 1

Preliminaries: Set theory and categories

1. Naive set theory

Exercise 1.1. Let $U = \{x \mid x \notin x\}$. Then, $U \notin U \iff U \in U$, a contradiction. This is Russell's paradox. Either we assume the *set of all sets* doesn't exist, or we need to give up the axiom of *unrestricted comprehension* in set theory.

Exercise 1.2. Suppose $\sim$ is an equivalence relation on a set S. For every element $a \in S$, define the *equivalence class* of a (with respect to $\sim$) by

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

Then, we note that due to *reflexivity*, the equivalence class $[a]_\sim$ of every element $a \in S$ contains a, and hence, is nonempty. Also, $[a]_\sim \subset S$, and therefore, $\bigcup_{a \in S}[a]_\sim = S$. Finally, we show the equivalence classes are mutually disjoint. Indeed, for any two elements $a, b \in S$, if $[a]_\sim$ and $[b]_\sim$ are disjoint, then there is nothing to prove. So, suppose $[a]_\sim \cap [b]_\sim$ is nonempty. Then, there exists some $c \in S$ that belongs to such an intersection. Thus, $c \sim a$ and $c \sim b$. By symmetry, $a \sim c$, and thus, by transitivity, $a \sim b$, which by symmetry again, implies $b \sim a$. Therefore, for all $x \in [a]_\sim$, we have $x \sim a$, and since $a \sim b$, by transitivity, $x \sim b$, which implies $x \in [b]_\sim$, from which we conclude $[a]_\sim \subset [b]_\sim$. We can similarly show $[b]_\sim \subset [a]_\sim$. Hence, $[a]_\sim = [b]_\sim$. This establishes equivalence classes are mutually disjoint. Hence, the set $\mathscr{P}_\sim$ of equivalence classes of S is indeed a partition of S.

Exercise 1.3. Suppose $\mathscr{P}$ is a partition on a set S. Define a relation $\sim$ on S as follows: For any two elements $a, b \in S$, $a \sim b$ iff a and b belong to the same set in the partition. Then, it is easy to check $\sim$ is indeed an equivalence relation on S. $\mathscr{P}$ is, therefore, the corresponding partition of the aforesaid equivalence relation, and we are done.

Exercise 1.4. Note the set of equivalence relations on a set S are in a one-to-one correspondence with the set of partitions of S. Thus, the number of different equivalence relations that may be defined on $S = \{1, 2, 3\}$ equals the number of partitions of S, and this number equals 5, since the partitions of S are

$$\{\{1\}, \{2\}, \{3\}\}, \{\{1, 2\}, \{3\}\}, \{\{1, 3\}, \{2\}\}, \{\{2, 3\}, \{1\}\}, \{\{1, 2, 3\}\}.$$

The above partitions are also written as $1|2|3, 12|3, 13|2, 23|1, 123$.

Exercise 1.5. An example of a relation R (defined on a set S) that is reflexive and symmetric but not transitive is the following:

$$R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}, \text{ where } S = \{1, 2, 3\}.$$

Exercise 1.6. Define a relation $\sim$ on the set $\mathbb{R}$ of real numbers by setting

$$a \sim b \iff b - a \in \mathbb{Z}.$$

We claim $\sim$ is an equivalence relation. To that end, note, for all $a \in \mathbb{R}$, we have $a \sim a$, since $a - a = 0 \in \mathbb{Z}$. Therefore, $\sim$ is reflexive. Also, if $a \sim b$, then $b - a \in \mathbb{Z}$, which implies $a - b \in \mathbb{Z}$, and thus, $b \sim a$. Therefore, $\sim$ is symmetric. Finally, suppose $a \sim b$ and $b \sim c$. Then, $b-a, c-b \in \mathbb{Z}$, and thus, $c-a = (c-b)+(b-a) \in \mathbb{Z}$. Thus, $\sim$ is transitive. Therefore, $\sim$ is an equivalence relation on $\mathbb{R}$.

(Description of $\sim$) Note all reals that have the same decimal expansion belong to the same equivalence class under $\sim$. Thus, $[0]_\sim = \mathbb{Z}$, and for any $0 < \alpha < 1, [\alpha]_\sim = \{n+\alpha \mid n \in \mathbb{Z}\}$. This takes care of all the reals, since each real can always be written as $n + \alpha$, for some $n \in \mathbb{Z}$ and $0 < \alpha < 1$. Therefore, a 'compelling' description for $\mathbb{R}/\sim$ is the unit interval $[0, 1]$, such that the endpoints, 0 and 1, are 'glued' together. In other words, it is a 'loop' or a 1-sphere.

Define a relation $\approx$ on the plane $\mathbb{R} \times \mathbb{R}$ as follows:

$$(a_1, a_2) \approx (b_1, b_2) \iff b_1 - a_1 \in \mathbb{Z} \text{ and } b_2 - a_2 \in \mathbb{Z}.$$

Then, just as above, it is easy to show $\approx$ defines an equivalence relation on $\mathbb{R} \times \mathbb{R}$. We note $[(0, 0)]_\sim = \{(m, n) \mid m, n \in \mathbb{Z}\}$, and for any $0 < \alpha, \beta < 1, [(\alpha, \beta)]_\sim = \{(m + \alpha, n + \beta) \mid m, n \in \mathbb{Z}\}$. Thus, a 'compelling' description of $\mathbb{R} \times \mathbb{R}/\approx$ is the unit square $[0, 1] \times [0, 1]$ with the four corners joined together, so that it forms a 2-sphere.

2. Functions between sets

EXERCISE 2.1. We claim the number of bijections from a set S with n elements to itself is $n!$. To begin with, any element in S can be mapped to any of the n possible elements in S. Then, the next element in S can be mapped to any of the remaining $n - 1$ elements in S, and so on, with the last element in S being mapped to the last remaining element in S. Thus, the number of bijections equals $n \cdot (n - 1) \cdot \ldots \cdot 1 = n!$, which proves our claim.

EXERCISE 2.2. Assume $A \neq \varnothing$, and let $f : A \to B$ be a function. We claim f has a right inverse iff it is surjective.

($\Longleftarrow$) Suppose f has a right inverse, $g : B \to A$, say. Then, $f \circ g = 1_B$. Thus, for all $b \in B$, $b = 1_B(b) = (f \circ g)(b) = f(g(b)) = f(a)$, where $g(b) = a \in A$. This shows f is surjective.

($\Longrightarrow$) Suppose f is surjective. Then, for any $b \in B$, the fiber of f over b is nonempty. Thus, $\{f^{-1}(b)\}_{b\in B}$ is a family of nonempty sets, and therefore, using the *axiom of choice*, we can construct a function $g : B \to A$ as follows: For all $b \in B$, $g(b) = a$ for some $a \in f^{-1}(b)$. Hence, for all $b \in B, (f \circ g)(b) = f(g(b)) = f(a) = b = 1_B(b)$, and so, $f \circ g = 1_B$. This establishes g is the right inverse of f, and we are done.

EXERCISE 2.3. Suppose $f : A \to B$ is a bijection. Then, f has an inverse $f^{-1} : B \to A$ such that $f^{-1} \circ f = 1_A$ and $f \circ f^{-1} = 1_B$. Clearly, f is an inverse of f^{-1}, showing f^{-1} is also a bijection.

Suppose $f : A \to B$ and $g : B \to C$ are bijections. We claim $g \circ f : A \to C$ is also a bijection. To that end, we show $f^{-1} \circ g^{-1} : C \to A$ is the inverse of $g \circ f$. Indeed, $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ 1_B \circ g^{-1} = g \circ g^{-1} = 1_C$. And, $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ 1_B \circ f = f^{-1} \circ f = 1_A$, and we are done.

EXERCISE 2.4. We show 'isomorphism' is an equivalence relation on any set of sets.
(Reflexivity) For all sets $A, 1_A : A \to A$ is a natural bijection, and thus, $A \cong A$.
(Symmetry) Suppose $A \cong B$ for any two sets A, B. Then, there exists a bijection $f : A \to B$, such that its inverse $f^{-1} : B \to A$ is also a bijection (as shown in the above exercise.) Thus, $B \cong A$.
(Transitivity) Finally, suppose for any three sets, A, B and C, $A \cong B$ and $B \cong C$, with $f : A \to B$ and $g : B \to C$ as bijections. Then, from the previous exercise, $g \circ f : A \to C$ is also a bijection, and thus $A \cong C$.
Thus, our original claim is established.

EXERCISE 2.5. (***Epimorphism***) A function $f : A \to B$ is an *epimorphism* (or *epi*) if the following holds: For all sets Z and all functions $\alpha', \alpha'' : B \to Z$,

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

In other words, an epimorphism f is *right cancellative.*

Proposition: A function is surjective iff it is an epimorphism.

Proof. ($\Longrightarrow$) Suppose $f : A \to B$ is an epimorphism. Assume, for the sake of contradiction, f is *not* surjective. Then, there exists an element $b_0 \in B$, such that, for all $a \in A$, $f(a) \neq b_0$. We now construct two distinct functions $\alpha', \alpha'' : B \to \{0, 1\}$ as follows:

$$\alpha'(b) = 0$$

$$\alpha''(b) = \begin{cases} 0 & \text{if } b \neq b_0 \\ 1 & \text{if } b = b_0 \end{cases}$$

Then, it is easy to check that, for all $a \in A$, $(\alpha'' \circ f)(a) = \alpha''(f(a)) = 0 = \alpha'(f(a)) = (\alpha' \circ f)(a)$, which implies $\alpha' \circ f = \alpha'' \circ f$. However, $\alpha' \neq \alpha''$, which contradicts our assumption that f is an epimorphism. Hence, we conclude f is surjective.

($\Longleftarrow$) Suppose $f : A \to B$ is surjective. Then, it has a right inverse $g : B \to A$ such that $f \circ g = 1_B$. Now, assume, for any set Z and any two functions $\alpha', \alpha'' : B \to Z$, $\alpha' \circ f = \alpha'' \circ f$. Then, $\alpha' = \alpha' \circ 1_B = \alpha' \circ (f \circ g) = (\alpha' \circ f) \circ g = (\alpha'' \circ f) \circ g = \alpha'' \circ (f \circ g) = \alpha'' \circ 1_B = \alpha''$, thus proving f is an epimorphism.