Exercises on Abstract Structures

Ashok Cutkosky

Abstract

The following questions and notes are meant to exercise fundamentals in writing proofs about abstract structures. These problems vary in difficulty, but any or all of them could be extremely tricky. If possible, it is recommended to discuss your solutions with someone more experienced in writing proofs: many of these statements will seem "obvious", but nonetheless writing a rigorous proof may be nontrivial.

These questions are meant to be solved using essentially only the definitions provided in the question. These are also basic facts that might be learned in an introductory abstract algebra or proof-based linear algebra course. If you find yourself reaching for more complicated facts about vector spaces, like existence of a basis, or dimension (or, god forbid, a singular value decomposition), you are going down the wrong path. If you get stuck, try carefully going down the list of axioms one by one to see if there is any way to use one of them. It is easy to "forget" about less commonly used axioms. Also, don't forget about the "contrapositive": the statement $A \implies B$ is equivalent to $\neg B \implies \neg A$.

1. a *vector space* (over the reals) is a set V together with two binary operations which we call addition ($+$) and scalar multiplication ($\cdot$). The addition operation is a function which takes two elements of V, say v and w, and returns a third element of V, which we write as $v + w$, while scalar multiplication is a function which takes a real number and an element of V, say s and v, and returns another element of V, which we write as $s \cdot v$. The operations are called "binary" because they take two arguments. The two operations must satisfy the following properties:

   - Addition operation is commutative: $v + w = w + v$ for all w and v.
   - There exists an additive identity element, which we write as $\vec{0}$ such that $\vec{0} + w = w$ for all w.
   - scalar multiplication distributes over addition in V: $s \cdot (v + w) = s \cdot v + s \cdot w$.
   - Scalar multiplication distributes over addition in $\mathbb{R}$: if $a, b \in \mathbb{R}$ and $w \in V$, then $(a+b) \cdot w = a \cdot w + b \cdot w$, where in the left hand side of the equation the addition is the familiar addition operation in $\mathbb{R}$, but on the right hand side the addition is the addition operation in V.
   - Associativity of addition: $(v + w) + z = v + (w + z)$.
   - Compatibility of scalar multiplication with real-number multiplication: if s and c are real numbers and $v \in V$, then $(sc) \cdot v = s \cdot (c \cdot v)$.
   - $1 \cdot v = v$ for all $v \in V$.
   - Every element $v \in V$ has an *additive inverse* w such that $v + w = \vec{0}$.

   (a) Let $V = \mathbb{R}$ and let the addition and multiplication operations be the standard addition and multiplication in $\mathbb{R}$. Show that V is a vector space.

   (b) Let X be some arbitrary space and let F be the set of functions $f : X \to \mathbb{R}$. Given any two functions f and g, we can define their sum $k := f + g$ as the function $k(x) = f(x) + g(x)$. Further, given a scalar s and a function f, we define the scalar multiplication $k := s \cdot f$ as the function $k(x) = s \times f(x)$, where $\times$ indicates standard multiplication of real numbers. Show that F with these addition and scalar multiplication operators is a vector space.

   (c) Show that the additive identity is unique. Specifically, $i \in V$ is such that there exists some $w \in V$ such that $i + w = w$, then $i = \vec{0}$.

   (d) Show that $\vec{0}$ satisfies $s \cdot \vec{0} = \vec{0}$ for all $s \in \mathbb{R}$.

   (e) Show that $0 \in \mathbb{R}$ satisfies $0 \cdot w = \vec{0}$ for all $w \in V$.

(f) Suppose (just for this question) that the vector spaces need not have additive inverses, so that you cannot rely on that axiom when proving this statement. Show that nevertheless, if $i \in V$ is such that $i + w = w$ for all w, then $i = \vec{0}$. Note that this is a weaker result than question (c) (why?).

(g) Show that the additive inverses are unique. That is, if $v \in V$ and w and w' are two additive inverses for v, then $w = w'$.

(h) Show that if $w \neq v$ and v' is the additive inverse of v, then $w + v' \neq \vec{0}$.

(i) Show that $-1 \in \mathbb{R}$ satisfies $(-1) \cdot v$ is the additive inverse of v for all $v \in V$. This justifies the notation $-v$ to indicate the additive inverse of v.

(j) Show that if $v \neq \vec{0}$, then $s \cdot V \neq \vec{0}$ for all $s \neq 0$.

(k) Show that if v is equal to its own additive inverse, then $v = \vec{0}$.

2. If V and W are two different vector spaces, a *linear map* L from V to W is a function $L : V \to W$ such that

- $L(v + v') = L(v) + L(v')$ for all $v, v' \in V$.
- $L(s \cdot v) = s \cdot L(v)$ for all $s \in \mathbb{R}$, $v \in V$.

(a) Show that if $L : V \to W$ and $H : W \to X$ are both linear maps, then the composition $H \circ L : V \to X$ is a linear map.

(b) Show that if $L : V \to W$ is a linear map, then $L(\vec{0}_V) = \vec{0}_W$, where $\vec{0}_V$ indicates the additive identity in V and $\vec{0}_W$ indicates the additive identity in W.

(c) The *kernel* of a linear map $L : V \to W$ is the set of points $v \in V$ such that $L(v) = \vec{0}_W$. Show that a linear map $L : V \to W$ is 1-1 if and only if the kernel of L consists of only the identity element $\vec{0}_V$.

(d) A *subspace* of a vector space V is a subset $S \subset V$ such that for all $v, w \in S$, $v + w \in S$ and for all $v \in S$ and $c \in \mathbb{R}$, $c \cdot v \in S$. That is, the subspace is *closed* under the addition and scalar multiplication operations. Show that the kernel of a linear map $L : V \to W$ forms a subspace of the space V.

(e) Show that the image of a linear map $L : V \to W$ is a subspace of W.

(f) The set of linear maps from V to W is typically denoted $\mathcal{L}(V, W)$. Define a addition operation on linear maps as follows: given $F, G \in \mathcal{L}(V, W)$, set $K = F + G$ by $K(v) = F(v) + G(v)$, where the addition on the RHS here is the addition operation in W. Similarly, given $c \in \mathbb{R}$, we define a scalar multiplication $K = c \cdot F$ by $K(v) = c \cdot F(v)$, where again the scalar multiplication is the operation in W. Show that with these operations, $\mathcal{L}(V, W)$ is a vector space.

3. Now let's go slightly more abstract. A *group* is a set G together with a binary operation $\circ$. The binary operation $\circ$ takes two elements of G, and returns an element of G. We write $x \circ y$ to indicate the returned value of $\circ$ on input x and y. Note that the ordering is important: $x \circ y$ might not be equal to $y \circ x$. If you like, you can instead think of a function $b : G \times G \to G$ where $x \circ y$ is just shorthand for $b(x, y)$. The binary operation must satisfy:

- $(x \circ y) \circ z = x \circ (y \circ z)$ for all $x, y, z \in G$.
- There must be some element $i \in G$ such that $x \circ i = i \circ x = x$ for all $x \in G$.
- For each $x \in G$, there is an element x^{-1} called the inverse of x such that $x \circ x^{-1} = x^{-1} \circ x = i$.

For the following questions, suppose that G is a finite set.

(a) Consider a set G with two elements a and b. Provide a binary operation $\circ$ that turns G into a group.

(b) Construct set G of size 4 and binary operation $\circ$ such that G forms a group and every element of G satisfies $x \circ x = i$.

(c) Construct a set G of size 4 and a function b such that G forms a group and there exists an element of G that does not satisfy $x \circ x = i$.

(d) Show that if $x \circ y = x \circ z$, then $y = z$.

(e) Show that inverse are unique: if x' satisfies $x' \circ x = i$, then $x' = x^{-1}$.

(f) Show that $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

(g) A group is said to be *abelian* if $x \circ y = y \circ x$ for all x and y. Show that a group is abelian if and only if $x \circ y \circ x^{-1} \circ y^{-1} = i$ for all x and y.

4. The *dual space* to a vector space V is the set $\mathcal{L}(V, \mathbb{R})$. Elements of the space (which are linear maps $V \to \mathbb{R}$), are frequently called *linear functionals* (I don't know why - I'm not a mathematical etymologist). The dual space is frequently denoted $V^\star = V$. This is also sometimes called the *algebraic dual space*, as opposed to the *continuous* dual space that is subtly different. For the purposes of this problem, you may assume that for any $0 \neq v \in V$, there is a $w \in V^\star$ such that $w(v) = 1$ (It's good to try to prove this from first principles just to get a feel for what the difficulties might be. It is allowed to be assumed for this problem because to prove this requires Zorn's lemma (or the axiom of choice), which is much more technical than we're going for here).

   (a) Given $v \in V$, define the function $d_v : V^\star \to V$ by $d_v(w) = w(v)$. Show that d_v is a linear map. That is, d_v is an element of the *double dual space*, $\mathcal{L}(V^\star, \mathbb{R})$, which we write as $V^{\star\star}$.

   (b) Show that the function $F : V \to V^{\star\star}$ given by $F(v) = d_v$ is *also* a linear map.

   (c) Show that this function F is 1-1.

5. Suppose that $v_1, v_2, \dots$ is an infinite sequence of integers such that $v_t \in [a, b]$ for some constants a and b.

   (a) Show that there is some element c such that $v_t = c$ infinitely often.

   (b) Show that for any length L, there must be some length-L sequence of numbers $x_1, \dots, x_L$ such that this sequence appears infinitely often as a consecutive sub-sequence of the sequence v_t.

6. The following exercises deal with various concepts of infinity. Working with infinite sets is notoriously counter-intuitive, but surprisingly infinite-dimensional vector spaces show up frequently in the real world (e.g. quantum mechanics, signal processing, and even in machine learning via kernel methods). An important result in this area (which you may use without proof) is the Schröder-Bernstein theorem, which states that if $f : A \to B$ and $g : B \to A$ is are both injective functions, then there exists a bijective function $h : A \to B$. As a challenge, you can try to prove this result.

   (a) Let us say that two sets A and B have the same cardinality (i.e. size) if there is a bijection $f : A \to B$. If A and B have the same cardinality, we will write $|A| = |B|$. Suppose that $|A| = |B|$ and $|B| = |C|$. Show that $|A| = |C|$.

   (b) We will say that $|A| \geq |B|$ if there is an *injective* function $f : B \to A$. Show that if $|A| \geq |B|$ and $|B| \geq |C|$, then $|A| \geq |C|$.

   (c) Show that if $|A| \geq |B| \geq |C|$ and $|A| = |C|$, then $|A| = |B|$.

   (d) Define the natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$, the set of non-negative integers. We say that a set A is *countable* if $|A| \leq |\mathbb{N}|$. Show that the set of all integers $\mathbb{Z}$ is countable.

   (e) Show that the set of pairs of integers is countable: $|\mathbb{Z}^2| \leq |\mathbb{N}|$.

   (f) Show that the set of rational numbers $\mathbb{Q}$ is countable.

   (g) Let us define a "real number" in $[0, 1)$ as an infinite sequence of integers from 0 to 9 such that the sequence does *not* terminate in an never-ending sequence of 9s. That is, we represent any element of $[0, 1)$ with a sequence $\{x_i\}$ such that each x_i is an integer from 0 to 9, and for any N there exists an $i > N$ such that $x_i \neq 9$. Consider the following construction: suppose $f : \mathbb{N} \to [0, 1)$ is an arbitrary function. Define a sequence $\{x_i\}$ such that $x_i = 0$ if the ith element of the sequence $f(i)$ is not 0, and $x_i = 1$ otherwise. Using this (or not, if you find some other way), show that the set $[0, 1)$ is *not* countable.