# Honours Algebra 2, Assignment 1

Michael Snarski & Jamie Klassen

January 20, 2012

**Question 1.** *Show that the set $V = \mathbb{R}^2$, with the addition and scalar multiplication defined by the rules*

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \lambda \cdot (x, y) := (\lambda x, 0)$$

*satisfies all the axioms of a vector space* except *the property that $1 \cdot v = v$ for all $v \in V$.*

**Solution** This will eventually become an exercise in calligraphy (or typing, if you have already graduated to LaTeX), but it is important to do these so that you realize there is actually something to prove.

i. Certainly $0_V \in V$, as $(0, 0)$ satisfies the properties of a zero vector: $(0, 0) + (x, y) = (x, y) + (0, 0) = (x + 0, y + 0) = (0 + x, 0 + y) = (x, y)$.

ii. For any $v \in V$, $-v \in V$. Given $v = (x, y)$, take $-v = (-x, -y)$. Note that $-v \neq -1 \cdot v$, which is $(-x, 0)$ by definition of scalar multiplication. We *define* the additive inverse $-v$ to be $(-x, -y)$. On the other hand, in an actual vector space, $-v = -1 \cdot v$ (this fails here).

iii. Associativity of addition (ugh); we must show that $(v+w)+z = v+(w+z)$ for all $v, w, z \in V$. This follows from associativity in the field, but we can simply note that addition is defined just as in $\mathbb{R}^2$ (componentwise), which we know to be a vector space; hence associativity follows.

iv. If you wanted a proper answer for *iii.*, here's the 'standard' version for commutativity of addition: for any $v_1 = (x_1, y_1), v_2 = (x_2, y_2) \in V$,

$$v_1 + v_2 = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$= (x_2 + x_1, y_2 + y_1) = (x_2, y_2) + (x_1, y_1) = v_2 + v_1$$

v. For any $\alpha, \beta \in \mathbb{R}$, $v \in V$,

$$(\alpha\beta) \cdot v = (\alpha\beta) \cdot (x, y) = (\alpha\beta x, 0) = \alpha \cdot (\beta x, 0)$$
$$= \alpha \cdot (\beta \cdot (x, 0)) = \alpha \cdot (\beta \cdot (x, y)) = \alpha \cdot (\beta \cdot v)$$

which is the 'associativity' law for scalar multiplication.

vi. Distributivity of scalars over vectors: for any $\alpha, \beta \in \mathbb{R}$, $v \in V$,

$$(\alpha + \beta) \cdot v = (\alpha + \beta) \cdot (x, y) = ((\alpha + \beta)x, 0) = (\alpha x + \beta x, 0)$$
$$= (\alpha x, 0) + (\beta x, 0) = \alpha \cdot (x, 0) + \beta \cdot (x, 0) = \alpha \cdot (x, y) + \beta \cdot (x, y) = \alpha v + \beta v$$

vii. Distributivity of vectors over scalars: for any $\alpha \in \mathbb{R}$, $v_1, v_2 \in V$,

$$\begin{aligned}\alpha \cdot (v_1 + v_2) &= \alpha \cdot ((x_1, y_1) + (x_2, y_2)) = \alpha \cdot (x_1 + x_2, y_1 + y_2) \\ &= (\alpha(x_1 + x_2), 0) = (\alpha x_1 + \alpha x_2, 0) = (\alpha x_1, 0) + (\alpha x_2, 0) \\ &= \alpha \cdot (x_1, 0) + \alpha \cdot (x_2, 0) = \alpha \cdot (x_1, y_1) + \alpha \cdot (x_2, y_2) = \alpha \cdot v_1 + \alpha \cdot v_2\end{aligned}$$

viii. Indeed, the last one, which doesn't hold, is that the identity acts trivially on any element $v \in V$: $1_{\mathbb{R}} \cdot (x, y) = (x, 0) \neq (x, y)$. [Some gratuitous knowledge/remark: the word *acts* here is appropriate; scalar multiplication defines a group action on the set (commutative group) $(V, +)$ when $V$ is a vector space. In this case, it is the requirement for $\mathbb{R} \times V \to V$ to define an action, $1_{\mathbb{R}} \cdot v = v$ for all $v \in V$, which fails.]

The only non-'standard' thing is when we write $\alpha \cdot (x, 0) = \alpha \cdot (x, y)$ – but in this case, they *are* actually equal.

**Question 2.** *Which of the following subsets of* $\mathbb{R}^3$ *are* $\mathbb{R}$*-vector subspaces of* $\mathbb{R}^3$.

**Solution** Some remarks. First, $F$-vector space (or $F$-space) is a vector space with scalars in $F$. Second, if the subset is to be a subspace, 0 must be in there, and must be the same as the one in $\mathbb{R}^3$. Last, the inverses have to be the same as in the larger, ambient space $\mathbb{R}^3$.

1. Nope. $(-1, 0, 0)$ is an inverse for $(1, 0, 0)$ in $\mathbb{R}^3$, but $(-1, 0, 0)$ is not in this subset, hence not a subspace.

2. Sure. The easy way to see this is $x + y - 2z = 0$, which is a plane through the origin, and this is always a subspace. More pedantically, if $v_1 = (x_1, y_1, z_1), v_2 = (x_2, y_2, z_2)$ are in this subset, $v_1 + v_2 = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$

   $$(x_1 + x_2) + (y_1 + y_2) = 2z_1 + 2z_2 = 2(z_1 + z_2)$$

   so $v_1 + v_2$ is in there. For any $\alpha \in \mathbb{R}$, $\alpha \cdot (x, y, z) = (\alpha x, \alpha y, \alpha z)$, and

   $$\alpha x + \alpha y = \alpha(x + y) = \alpha(2z) = 2(\alpha z)$$

   so $\alpha \cdot (x, y, z)$ is also in there. Thus, we have closure under addition and scalar multiplication, and $(0, 0, 0)$ is in this subset, so we have a subspace.

3. Nope. $(1, 0, 0)$ and $(0, 1, 0)$ are in there, but their sum $(1, 1, 0)$ isn't.

4. Yep. The zero vector is in there; for any $v_1 = (0, 0, z_1), v_2 = (0, 0, z_2), v_1 + v_2 = (0, 0, z_1 + z_2)$, which is also in our subset. For any $\alpha \in \mathbb{R}$, $\alpha \cdot (0, 0, z) = (0, 0, \alpha z)$, also in our subset. Closure under $+$ and $\cdot$, with $0 \Rightarrow$ subspace.

5. Nope, closure under scalar multiplcation fails. This is an $\mathbb{R}$-space, so the scalars are in $\mathbb{R}$. Taking $(1, 0, 0)$ (which is in our subset) and $e = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n$, $e \cdot (1, 0, 0) = (e, 0, 0)$ is not in our space (since $e$ is transcendetal, hence irrational, hence not in $\mathbb{Q}$). Overkill much?

**Question 3.** *Let $V_1$ and $V_2$ be subspaces of an $F-$space $V$. Show that the union $V_1 \cup V_2$ can only be a subspace of $V$ if one of the spaces $V_i$ $(i = 1, 2)$ is contained in the other.*

**Solution** If $V_1 \subset V_2$ or vice-versa, then without loss of generality $V_1 \cup V_2 = V_2$ and this is a subspace by assumption. Conversely, suppose $V' = V_1 \cup V_2 = \{v \mid v \in V_1 \text{ and/or } v \in V_2\}$ is a subspace, and suppose there are $x_1 \in V_1 \setminus V_2$ and $x_2 \in V_2 \setminus V_1$ (so that neither subspace is contained in the other). Then $x_1, x_2 \in V'$, and so $x_1 + x_2 \in V'$ since $V'$ is assumed to be a subspace. By definition of $V'$, $x_1 + x_2 \in V_1$ and/or $x_1 + x_2 \in V_2$. In the first case, $x_2 \in V_2$, so $x_1 + x_2 + (-x_2) \in V_2 \Rightarrow x_1 \in V_2$, a contradiction. Same argument holds in the second case. Thus our assumption that neither subspace is contained in the other is false, or $V_1 \cup V_2$ is not a subspace.

I wrote out all the details here to make sure you understand the definition of union, but this is most easily seen with the following picture: draw two linearly independent lines in $\mathbb{R}^2$; take a point (vector) in each, and add the two points together. The resulting point *does not* lie on either line, so it is not in their union. It is, however, in their *sum*: $V_1 + V_2 = \{\alpha_1 v_1 + \alpha_2 v_2 \mid \alpha_i \in F, v_i \in V_i\}$.

**Question 4.** *Let $V$ be the vector space of $n \times m$ matrices with entries in a field $F$. What is the dimension of $V$? Give an explicit basis for $V$ over $F$.*

**Solution** By definition, in finite dimensions the dimension of a space is the cardinality of its basis, so we start with that first. Define $a_{i,j}$ to be the $i, j^{th}$ entry of $A$ ($i^{th}$ row, $j^{th}$ column). Let $A_{i,j}$ be the matrix such that $a_{i,j} = 1$ and 0 otherwise. For instance, $A_{2,3}$ for $3 \times 4$ matrices looks like this:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

I claim that $\mathcal{B} = \{A_{i,j} \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for $V$. You should see that it spans $V$ (if you don't, write the basis down for, say, $n = 2, m = 3$, and consider an arbitrary matrix). Indeed, let $P \in V$, and let $p_{i,j}$ be the $i, j$ entry of $P$. Then,

$$\begin{aligned} M = p_{1,1}A_{1,1} + p_{1,2}A_{1,2} + \cdots + p_{1,m}A_{1,m} \\ + p_{2,1}A_{2,1} + p_{2,2}A_{2,2} + \cdots + p_{2,m}A_{2,m} \\ + \ldots \\ + p_{n,1}A_{n,1} + p_{n,2}A_{n,2} + \cdots + p_{n,m}A_{n,m} \\ = \sum_{i=1}^{n} \sum_{j=1}^{m} p_{i,j} A_{i,j} \end{aligned}$$

Since $\mathcal{B}$ spans $V$ and is clearly linearly independent (for the same reason the vectors $(1, 0)$ and $(0, 1)$ are), $\mathcal{B}$ must be a basis for $V$. There are $nm$ elements in $\mathcal{B}$, so $\dim V = nm$.

Another way of viewing this vector space is as the space of linear transformations from $F^m$ to $F^n$ (input $m-$vectors, output $n-$vectors). Indeed, $V \cong \mathrm{Hom}_F(F^n, F^m)$, where $\mathrm{Hom}_F(M, N)$ is the space of homomorphisms from $M$ to $N$, where $M$ and $N$ can be vector spaces over $F$. Any linear transformation is a homomorphism, and any matrix defines a linear transformation. In general, we do not require $F$ to be a field for $\mathrm{Hom}_F$ to be defined. It can be a (not necessarily commutative) ring (usually with 1). In this case, $M$ is called an F-*module*.

**Question 5.** *Let $v_1, v_2, v_3$ be three linearly independent vectors in an $\mathbb{R}$-vector space $V$. Show that the vectors $v_1+v_2, v_2+v_3, v_3+v_1$ are also linearly independent. What if the field $\mathbb{R}$ is replaced by the field $\mathbb{Z}_2$ in this question?*

**Solution** To show linear independence, let $\alpha_i \in \mathbb{R}$ and consider

$$\begin{aligned} 0 &= \alpha_1(v_1 + v_2) + \alpha_2(v_2 + v_3) + \alpha_3(v_1 + v_3) \\ &= (\alpha_1 + \alpha_3)v_1 + (\alpha_1 + \alpha_2)v_2 + (\alpha_2 + \alpha_3)v_3. \end{aligned}$$

Since $\{v_1, v_2, v_3\}$ is a set of linearly independent vectors, we have

$$\begin{array}{rrrl} \alpha_1 & & + \alpha_3 & = 0 \\ \alpha_1 & + \alpha_2 & & = 0 \\ & \alpha_2 & + \alpha_3 & = 0 \end{array} \qquad \Rightarrow \quad \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \mathbf{x} = \mathbf{0}$$

which has only the trivial solution since the given matrix is invertible over $\mathbb{R}$. On the other hand, over $\mathbb{Z}_2$, $(1, 1, 1)$ is a non-trivial solution to the homogenous equation, and so the vectors $\{v_1 + v_2, v_2 + v_3, v_1 + v_3\}$ are not linearly independent.

**Question 6.** *Let $V$ be the $\mathbb{R}$-vector space of all infinitely differentiable functions on the real line. Show that the function $T : V \to V$ defined by $T(f) = f'$ (where $f'$ denotes as usual the derivative of $f$) is a linear transformation from $V$ to itself. Show that $T$ is not injective, and compute its kernel. Show that $T$ is surjective. Conclude that $V$ is not finite dimensional.*

**Solution** To see that $T$ is linear, apply the familiar rules of differentiation: for $f, g \in V$ and $a, b \in \mathbb{R}$ we have

$$T(af + bg) = (af + bg)' = af' + bg' = aT(f) + bT(g).$$

Now a handy fact about linear transformations (more generally, group homomorphisms) is that they are injective if and only if their kernel is trivial (this means the only vector mapped to 0 is 0), so to compute the kernel of $T$ we solve the (trivially easy) differential equation $f' = 0$, getting $f = c$ for some constant $c \in \mathbb{R}$. Thus the kernel of $T$ is composed of the constant functions (since constant functions are certainly infinitely differentiable), and this set is bigger than just 0, so $T$ is not injective. For a solution that does not rely on the handy fact referenced above, consider the functions $f(x) = x$ and $g(x) = x + 1$, which are both infinitely differentiable. $T(f) = f'(x) = 1$ and $T(g) = g'(x) = 1$ so $T(f) = T(g)$ but $f \neq g$, giving a different proof that $T$ is not injective.

To prove surjectivity, we need to show that for any $f \in V$ there exists $g \in V$ with $g' = f$. The fundamental theorem of calculus gives us what we need, since it says the function

$$g(x) = \int_0^x f(t)dt$$

is differentiable, and its derivative is $g'(x) = f(x)$. This shows us that our chosen $g$ is once-differentiable, but since $f$ is infinitely differentiable (since it is in $V$ by assumption), the rest of the derivatives of $g$ agree with those of $f$ so they exist too.

Finally, to conclude that $V$ is not finite dimensional we can use another handy fact: in a finite dimensional vector space, if a linear transformation is surjective it is necessarily injective and vice versa. Suppose, then, that $V$ were finite dimensional; since we've exhibited a transformation that is surjective but not injective, we get a contradiction of our handy fact, so our assumption must fail. Hence $V$ is not finite dimensional.

**Question 7.** *A* generalised vector space *over a field $F$ is a* not necessarily commutative *group $V$ (so that the group operation is written using the multiplicative notation) equipped with a "scalar multiplication"*

$$F \times V \to V \qquad \textit{denoted} \qquad (\lambda, v) \mapsto v^{[\lambda]},$$

*satisfying the following axioms analogous to those of a usual vector space*

*M1* $(vw)^{[\lambda]} = v^{[\lambda]}w^{[\lambda]}$, *for all* $v, w \in V$ *and* $\lambda \in F$;

*M2* $v^{[\lambda_1+\lambda_2]} = v^{[\lambda_1]}v^{[\lambda_1]}$ *for all* $v \in V$ *and* $\lambda_1, \lambda_2 \in F$;

*M3* $\left(v^{[\lambda_1]}\right)^{[\lambda_2]} = v^{[\lambda_1\lambda_2]}$, *for all* $v \in V$ *and* $\lambda_1, \lambda_2 \in F$;

*M4* $v^{[1]} = v$, *for all* $v \in V$.

*Show that a generalised vector space is just an ordinary vector space; i.e., the group law on $V$ is necessarily commutative.*

**Solution** Sometimes when you're working with a group, a nice characterization of being abelian comes in handy: a group $G$ is abelian if and only if the map $G \to G$ defined by $g \mapsto g^{-1}$ is a homomorphism (We'll prove part of this here, so you can use it later!). In this particular case, it's just what we need. M1 tells us that for each $\lambda \in F$ the map $G \to G$ defined by $g \mapsto g^{[\lambda]}$ is a homomorphism, so our proof will hinge on the hint given: let's show that $v^{[-1]} = v^{-1}$. First we'll show that $v^{[0]} = e$, the group identity, for all $v \in V$. To see this, note that $v^{[0]}v^{[0]} = v^{[0+0]} = v^{[0]}$ by axiom M2. Multiplying by $\left(v^{[0]}\right)^{-1}$ on both sides gives $v^{[0]} = e$ as required. With this in hand, the rest is easy!

$$\begin{aligned} v^{[-1]}v &= v^{[-1]}v^{[1]} && \text{(Axiom M4)} \\ &= v^{[-1+1]} && \text{(Axiom M2)} \\ &= v^{[0]} \\ &= e && \text{(proven above)} \end{aligned}$$

so indeed $v^{[-1]} = v^{-1}$. Then for any $v, w \in V$ we have

$$vw = (w^{-1}v^{-1})^{-1} = (w^{-1}v^{-1})^{[-1]} = (w^{-1})^{[-1]}(v^{-1})^{[-1]} = wv$$

so the group law is indeed abelian (we've here shown the more general fact that if taking inverses is a homomorphism then the group is abelian).

**Question 8.** *Let $X$ be a set, and let $\mathcal{P}(X)$ denote the* power set *of $X$, i.e., the set of all subsets of $X$. Define the sum of two sets to be*

$$A + B := A \cup B - (A \cap B),$$

*and define a scalar multiplcation of $\mathbb{Z}_2$ on $\mathcal{P}(X)$ by the rule:*

$$0 \cdot A := \emptyset, \qquad 1 \cdot A = A.$$

*Show that $\mathcal{P}(X)$ with these operations is a vector space over $\mathbb{Z}_2$. What is its dimension?*

**Solution** Note that the "addition" operation defined here is called the *symmetric difference* of two sets: it consists of the elements that lie in exactly one of the two sets, but not both. The reason its used here (instead of adding two sets by just taking their union, say) is because it lets us have the distributive laws for vector spaces.

i. The empty set is our zero element, since for any $A \in \mathcal{P}(X)$,

$$A + \emptyset = A \cup \emptyset - (A \cap \emptyset) = A - \emptyset = A.$$

ii. Each element is its own inverse, since for any $A \in \mathcal{P}(X)$,

$$A + A = A \cup A - (A \cap A) = A - A = \emptyset.$$

iii. Let's be honest, nobody has ever enjoyed showing that the symmetric difference of two sets is an associative operation because its an ugly process, but everybody has to do it at least once. It's a good exercise in keeping your thoughts in order and using lots of super basic rules of set theory. Also it helps a lot to draw pictures in a situation like this. First lets prove a "lemma" to clean up what is to come: given $A, B \in V$,

$$\begin{aligned}(A^c \cap B^c) \cup (A \cap B) &= (A^c \cup (A \cap B)) \cap (B^c \cup (A \cap B)) \\ &= ((A^c \cup A) \cap (A^c \cup B)) \cap ((B^c \cup A) \cap (B^c \cup B)) \\ &= (X \cap (A^c \cap B)) \cap ((A \cup B^c) \cap X) \\ &= (A^c \cup B) \cap (A \cup B^c).\end{aligned}$$

To see associativity of addition, let $A, B, C \in \mathcal{P}(X)$ be given. Then, by liberal applications of De Morgan's laws and the distributivity of

unions and intersections,

$$\begin{aligned}
(A+B)+C &= ((A\cup B)-(A\cap B))+C \\
&= (((A\cup B)-(A\cap B))\cup C)-(((A\cup B)-(A\cap B))\cap C) \\
&= (((A\cup B)\cap(A\cap B)^c)\cup C)\cap(((A\cup B)\cap(A\cap B)^c)\cap C)^c \\
&= (((A\cup B)\cap(A^c\cup B^c))\cup C)\cap(((A\cup B)\cap(A^c\cup B^c))\cap C)^c \\
&= (((A\cup B)\cap(A^c\cup B^c))\cup C)\cap(((A\cup B)\cap(A^c\cup B^c))^c\cup C^c) \\
&= (((A\cup B)\cap(A^c\cup B^c))\cup C)\cap(((A\cup B)^c\cup(A^c\cup B^c)^c)\cup C^c) \\
&= (((A\cup B)\cap(A^c\cup B^c))\cup C)\cap(((A^c\cap B^c)\cup(A\cap B))\cup C^c) \\
&= (((A\cup B)\cap(A^c\cup B^c))\cup C)\cap(((A^c\cup(A\cap B))\cap(B^c\cup(A\cap B)))\cup C^c) \\
&= (((A\cup B)\cap(A^c\cup B^c))\cup C)\cap((A^c\cup B)\cap(A\cup B^c))\cup C^c) \\
&= ((A\cup B\cup C)\cap(A^c\cup B^c\cup C))\cap((A^c\cup B\cup C^c)\cap(A\cup B^c\cup C^c)),
\end{aligned}$$

where the second last line follows from our "lemma". Note that the expression in that last line is symmetric; its just an intersection of four unions. Since union and intersection are commutative and associative operations, we get a sense here that the associativity will fall out. Basically we now need to change our brackets and work backwards until we get the expression we want, but this is arbitary-looking and feels unmotivated, so instead we'll just show that $A+(B+C)$ also equals the bottom line above.

$$\begin{aligned}
A+(B+C) &= A+((B\cup C)-(B\cap C)) \\
&= (A\cup((B\cup C)-(B\cap C)))-(A\cap((B\cup C)-(B\cap C))) \\
&= (A\cup((B\cup C)\cap(B\cap C)^c))\cap(A\cap((B\cup C)\cap(B\cap C)^c))^c \\
&= (A\cup((B\cup C)\cap(B^c\cup C^c)))\cap(A\cap((B\cup C)\cap(B^c\cup C^c)))^c \\
&= ((A\cup B\cup C)\cap(A\cup B^c\cup C^c))\cap(A^c\cup((B\cup C)\cap(B^c\cup C^c))^c) \\
&= ((A\cup B\cup C)\cap(A\cup B^c\cup C^c))\cap(A^c\cup((B\cup C)^c\cup(B^c\cup C^c)^c)) \\
&= ((A\cup B\cup C)\cap(A\cup B^c\cup C^c))\cap(A^c\cup((B^c\cap C^c)\cup(B\cap C))) \\
&= ((A\cup B\cup C)\cap(A\cup B^c\cup C^c))\cap(A^c\cup((B^c\cup C)\cap(B\cup C^c))) \qquad \text{(lemma)} \\
&= ((A\cup B\cup C)\cap(A\cup B^c\cup C^c))\cap(A^c\cup((B^c\cup C)\cap(B\cup C^c))) \\
&= ((A\cup B\cup C)\cap(A\cup B^c\cup C^c))\cap((A^c\cup B^c\cup C)\cap(A^c\cup B\cup C^c)) \\
&= ((A\cup B\cup C)\cap(A^c\cup B^c\cup C))\cap((A^c\cup B\cup C^c)\cap(A\cup B^c\cup C^c)) \\
&= (A+B)+C.
\end{aligned}$$

So the hard work is done. A *much* nicer way to see this is by using indicator functions, discussed below.

iv. Commutativity:

$$A+B=(A\cup B)-(A\cap B)=(B\cup A)-(B\cap A)=B+A$$

v. "Associativity" of scalar multiplication: If $a,b\in\mathbb{Z}_2$, since multiplication in a field is commutative we have three cases:

(a) $a = 0, b = 0$. For any $A \in V$,

$$0 \cdot (0 \cdot A) = 0 \cdot (\emptyset) = \emptyset = 0 \cdot A = (0 \cdot 0) \cdot A.$$

(b) $a = 0, b = 1$. For any $A \in V$,

$$0 \cdot (1 \cdot A) = 0 \cdot A = (0 \cdot 1) \cdot A.$$

(c) $a = 1, b = 1$. For any $A \in V$,

$$1 \cdot (1 \cdot A) = 1 \cdot A = (1 \cdot 1) \cdot A.$$

vi. Distributivity of scalars over vectors: If $a, b \in \mathbb{Z}_2$, since addition is commutative in a field, we have three cases:

(a) $a = 0, b = 0$. For any $A \in V$,

$$(0 + 0) \cdot A = 0 \cdot A = \emptyset = (\emptyset \cup \emptyset) - (\emptyset \cap \emptyset) = \emptyset + \emptyset = 0 \cdot A + 0 \cdot A.$$

(b) $a = 0, b = 1$. For any $A \in V$,

$$(0 + 1) \cdot A = 1 \cdot A = A = (\emptyset \cup A) - (\emptyset \cap A) = \emptyset + A = 0 \cdot A + 1 \cdot A.$$

(c) $a = 1, b = 1$. For any $A \in V$,

$$(1 + 1) \cdot A = 0 \cdot A = \emptyset = (A \cup A) - (A \cap A) = A + A = 1 \cdot A + 1 \cdot A.$$

vii. Distributivity of vectors over scalars: Let $A, B \in V$, $a \in \mathbb{Z}_2$ and consider the two cases:

(a) $a = 0$.

$$0 \cdot (A + B) = \emptyset = (\emptyset \cup \emptyset) - (\emptyset \cap \emptyset) = \emptyset + \emptyset = 0 \cdot A + 0 \cdot B.$$

(b) $a = 1$.

$$1 \cdot (A + B) = A + B = 1 \cdot A + 1 \cdot B.$$

viii. Finally we have $1 \cdot A = A$ for all $A \in V$ by definition.

So we've shown that $V$ is a vector space the long way. A method which is in some sense slicker is to put $V$ in bijective correspondence with a well-known vector space: $\{0, 1\}^X$, the space of all functions $X \to \mathbb{Z}_2$. So define $V \to \{0, 1\}^X$ by $A \mapsto \chi_A$, the characteristic or indicator function of $A$. Then the definitions of addition and scalar multiplication coincide, since for all $A \in V$, $\chi_{0 \cdot A} = \chi_\emptyset = 0 = 0 \cdot \chi_A$ and $\chi_{1 \cdot A} = \chi_A = 1 \cdot \chi_A$ and *furthermore* $\chi_A(x) + \chi_B(x)$ is 0 if $x$ is in neither $A$ nor $B$ or else if $x$ is in both (since $\chi_A(x) + \chi_B(x) = 1 + 1 = 0$ for such $x$); in other words $\chi_A + \chi_B = \chi_{A+B}$. After having established this association, all the axioms follow immediately.

The dimension of $\mathcal{P}(X)$ over $\mathbb{Z}_2$ is $|X|$, the cardinality of $X$, where if $X$ is infinite, $\mathcal{P}(X)$ is infinite-dimensional. We'll consider the finite and infinite cases separately.

1. $X$ finite: We claim the singleton sets $\{x_i\}$ form a basis for $X$. First we prove they span $X$: let $A = \{a_1, \ldots, a_n\}$ be any nonzero vector in

$\mathcal{P}(X)$ (i.e., a nonempty subset of $X$). We claim that $A = \sum_{i=1}^{n} \{a_i\}$ and we prove the claim by induction on $|A|$. If $|A| = 1$ then $A = \{a_1\}$ and the claim holds. Suppose inductively that every set of cardinality $k$ can be expressed as a sum as above. Let $A = \{a_1, \ldots, a_{k+1}\}$ be of cardinality $k+1$. Then $\{a_1, \ldots, a_k\} = \sum_{i=1}^{k} \{a_i\}$ by the inductive hypothesis, and

$$\begin{aligned} A = \{a_1, \ldots, a_k\} \cup \{a_{k+1}\} &= \{a_1, \ldots, a_k\} \cup \{a_{k+1}\} - \emptyset \\ &= \{a_1, \ldots, a_k\} \cup \{a_{k+1}\} - \{a_1, \ldots, a_k\} \cap \{a_{k+1}\} \\ &= \sum_{i=1}^{k} \{a_i\} + \{a_{k+1}\} \\ &= \sum_{i=1}^{k} \{a_i\}, \end{aligned}$$

proving the claim. To complete the proof that the singletons form a basis, we must show they are linearly independent, so suppose we have $a_1, \ldots, a_n \in \mathbb{Z}_2$ such that $\sum_{i=1}^{n} a_i \{x_i\} = \emptyset$. Then we have

$$\emptyset = \sum_{i=1}^{n} a_i \{x_i\} = \bigcup_{i : a_i = 1} \{x_i\},$$

and since the union on the right contains nonempty sets, it must be an empty union; that is, $a_i = 0$ for all $i$. Thus the singletons are independent, completing the proof that they form a basis (of cardinality $|X|$, hence the dimension of our vector space is $|X|$).

2. $X$ infinite: If $X$ is infinite, obviously $\mathcal{P}(X)$ will also be infinite. However, suppose $\mathcal{P}(X)$ were finite dimensional over $\mathbb{Z}_2$ and let $\{A_1, \ldots, A_n\}$ be a basis. Then we have a linear map $\mathcal{P}(X) \to (\mathbb{Z}_2)^n$ given by $\sum_{i=1}^{n} b_i A_i \mapsto (b_1, \ldots, b_n)$; this is clearly bijective, hence an isomorphism. But $|(\mathbb{Z}_2)^n| = 2^n < \infty$, contradicting our observation that $\mathcal{P}(X)$ is infinite. Thus in this case $\mathcal{P}(X)$ is infinite-dimensional. It is very important to note that this case *must* be treated separately: to claim that the singletons still form a basis in this case is incorrect, because the span of a set is defined to be the set of *finite* linear combinations of elements of the set, therefore the infinite subsets of $X$ will not be in the span of the singletons!