

(Due Friday, February 16)

Each problem will be graded out of 10 points.

1. How many distinct subspaces are there in \mathbb{Z}_2^2 ?

Five.

Proof. First of all, we have the trivial subspace with just the zero vector.

Then we have the whole space.

We also have the spaces spanned by $(1, 0)$, the space spanned by $(0, 1)$, and the space spanned by $(1, 1)$.

So that makes 5 subspaces in total.

□

If S_1 and S_2 are nonempty subsets of a vector space V , then the *sum* of S_1 and S_2 is the set

$$S_1 + S_2 := \{x + y : x \in S_1, y \in S_2\}.$$

A vector space V is called the *direct sum* of W_1 and W_2 if W_1 and W_2 are subspaces of V such that $W_1 \cap W_2 = \{0\}$ and $W_1 + W_2 = V$. We denote that V is the direct sum of W_1 and W_2 by writing

$$V = W_1 \oplus W_2.$$

2. Let W_1 and W_2 be subspaces of V .

(a) Prove that $W_1 + W_2$ is a subspace of V that contains both W_1 and W_2 .

Proof. Since both W_1 and W_2 are vector spaces, they contain the zero element. So we can set x or y to 0 in the definition of $W_1 + W_2$ to get all elements of W_1 and W_2 . \square

(b) Prove that any subspace of V that contains both W_1 and W_2 contains $W_1 + W_2$.

Proof. If $U \subseteq V$ is a vector space, then it is closed under linear combinations. Because it contains all elements from W_1 and W_2 , it contains all vectors that are linear combinations of those elements, which is exactly the vectors from $W_1 + W_2$. \square

3. Let V be a vector space and suppose $V = U \oplus W$. If $v \in V$, prove that there exist unique vectors $u \in U$ and $w \in W$ such that $v = u + w$.

Proof. By definition of V , there exist $u \in U, w \in W$ such that $v = u + w$. The hard part is proving that there exist a unique pair (u, w) .

Suppose by way of contradiction that $u_1 + w_1 = u_2 + w_2 = v$, where $u_1, u_2 \in U$ and $w_1, w_2 \in W$.

Subtracting $w_2 + u_1$ from both sides of the equality gives us

$$w_1 - w_2 = u_2 - u_1$$

.

Since U, W are both vector spaces and closed under linear combination, the left side is in W and the right in U . So $w_1 - w_2 = u_2 - u_1$ is in $U \cap W$. But this means that $0 = w_1 - w_2 = u_2 - u_1$ because by definition of the direct sum 0 is the only vector in the intersection. Hence $w_1 = w_2$ and $u_2 = u_1$. \square

Let W be a subspace of a vector space V over a field \mathbb{F} . For any $v \in V$, the set

$$v + W := \{v + w : w \in W\}$$

is called the *coset of W containing v* . Define $V/W := \{v + W : v \in V\}$, and define operations

$$(v_1 + W) + (v_2 + W) := (v_1 + v_2) + W,$$

$$a(v_1 + W) := (av_1) + W,$$

for all $a \in \mathbb{F}$ and $v_1, v_2 \in V$.

4. Prove that the operations defined above on V/W are well-defined; that is, if $a \in \mathbb{F}$, $v_1 + W = u_1 + W$, and $v_2 + W = u_2 + W$, then $(v_1 + W) + (v_2 + W) = (u_1 + W) + (u_2 + W)$ and $a(v_1 + W) = a(u_1 + W)$.

- Property 1

Proof. By definition of the coset-addition operator,

$$(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$$

and

$$(u_1 + W) + (u_2 + W) = (u_1 + u_2) + W$$

.

So now we want to show that the two right sides are equal.

$a + W = b + W$ for vectors $a, b \in V$ means that adding each element of W to a or b generates the same set. Because $0 \in W$ as W is a subspace, $b + W$ must contain $a + 0 = a$ and $a + W$ must contain $b + 0 = b$. So we know that $a + w = b$ for some vector $w \in W$ and vice versa, hence $a - b \in W$.

Now by specification, $v_1 - u_1 \in W$ and $v_2 - u_2 \in W$. Because W is a vector space closed under linear combination, $v_1 - u_1 + v_2 - u_2 \in W$, which means that $v_1 + v_2 = u_1 + u_2 + w$ for some $w \in W$.

But this means that $(v_1 + v_2) + W = (u_1 + u_2) + W$: $(v_1 + v_2) + W$ is a subset of $(u_1 + u_2) + W$ because for any $x \in W$, $v_1 + v_2 + x = u_1 + u_2 + w + x$, where $(w + x)$ is an element of W by closure. Switching over, $(u_1 + u_2) + W$ is a subset of $(v_1 + v_2) + W$ because for any $x \in W$, $(u_1 + u_2) + x = (v_1 + v_2) - w + x$, and $-w + x$ is an element of W by closure. Mutual containment establishes set equivalence, so the two are equal, proving the first property. \square

- Property 2

Proof. By definition of the operator,

$$a(v_1 + W) = (av_1) + W$$

and

$$a(u_1 + W) = (au_1) + W$$

.

Since $(u_1 + W) = (v_1 + W)$, we know that $u_1 = v_1 + w$ for some $w \in W$, which means that $au_1 = av_1 + aw$.

Again, we establish mutual containment to prove coset equivalence.

$(au_1) + W$ contains $(av_1) + W$ because for any $x \in W$, there exists a vector $y = -aw + x \in W$ (containment comes from closure and $aw, x \in W$) such that $au_1 + y = av_1 + x$.

$(av_1) + W$ contains $(au_1) + W$ because for any $x \in W$, there exists a vector $y = x + aw \in W$ (again, y is in W because W is closed under linear combination) such that $av_1 + y = au_1 + x$. □

5. Prove that V/W is a vector space over \mathbb{F} with the operations defined above.
(The vector space V/W is called the *quotient space of V modulo W* .)

Proof. Since V is a vector space, and since addition gets passed through the $+W$ operation, we have all the requisite properties plus the zero and the inverse: just as an example, the zero element is guaranteed by $0_W = 0_V + W$ because for any $v \in V$,
 $(v + W) + 0_W = (v + W) + (0_V + W) = (v + 0_V) + W = (v + W)$.

The operators involving scalar multiplication pass through the $+W$ operator similarly: for example, the multiplicative identity holds because $1 \cdot (v + W) = (1 \cdot v) + W = (v + W)$. \square

6. Let S be a linearly independent subset of a vector space V over a field \mathbb{F} . For any proper subset S' of S , prove that S' is linearly independent and $\text{span}(S') \subsetneq \text{span}(S)$.

Proof. S independent means that the coefficient $a_i \in \mathbb{F}$ satisfying the equation

$$\sum_{s_i \in S} a_i s_i = 0$$

are necessarily 0.

Removing one or more elements from S would not give the equation nonzero coefficients: the coefficients of the removed elements were 0 before they were gone, and when they are gone their terms just go away. If after removal some terms get nonzero coefficients, we can add the removed terms back with zero coefficients and say that S was never independent from the start because there are nonzero coefficients.

$\text{span}(S') \subsetneq \text{span}(S)$ because if we consider the elements in $S \setminus S'$, we can't get them as linear combinations of elements of S' or else this proves that S is not linearly independent.

□