Spaces of n-tuples and their subspaces

The linear subspaces of a vector space have a regular structure. There purpose of this note is to show some irregularities that can arise with the analogues of linear subspaces of $\mathbb{Z}_m^n$ when m is composite. We begin by reviewing the regularity in two cases of vector spaces and then exhibit the irregularities in the case of $\mathbb{Z}_m^n$.

1 The space of n-tuples over $\mathbb{R}$

Consider the space of all 3-tuples over $\mathbb{R}$, which is denoted as $\mathbb{R}^3$. A *linear subspace* of this is a subset that closed under taking linear combinations. In other words, a subspace is a subset $S \subseteq \mathbb{R}^3$ such that, for any $v_1, \ldots, v_k \in S$ and any scalars $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$, the linear combination $\lambda_1 v_1 + \cdots + \lambda_k v_k$ is also contained in S.

Since $\mathbb{R}^3$ is a *vector space* over the field $\mathbb{R}$, *all* of its linear subspaces are of one of these forms:

- 0-dimensional, if $S = \{0\}$.
- 1-dimensional, if $S = \text{span}(v) = \{\lambda v : \text{for all } \lambda \in \mathbb{R}\}$, for some non-zero $v \in \mathbb{R}^3$.
- 2-dimensional, if $S = \text{span}(v_1, v_2) = \{\lambda_1 v_1 + \lambda_2 v_2 : \text{for all } \lambda_1, \lambda_2 \in \mathbb{R}\}$, for some linearly independent $v_1, v_2 \in \mathbb{R}^3$.
- 3-dimensional, if $S = \mathbb{R}^3$.

2 The space of n-tuples over $\mathbb{Z}_p$, when p is prime

When the modulus is prime, $\mathbb{Z}_p$ is a field, and the space of n-tuples is also a vector space. The linear subspaces have a similar regular form. For example, for the space of all 3-tuples over $\mathbb{Z}_p$ (denoted as $\mathbb{Z}_p^3$), *all* of its linear subspaces are of one of these forms:

- 0-dimensional, if $S = \{0\}$.
- 1-dimensional, if $S = \text{span}(v) = \{\lambda v : \text{for all } \lambda \in \mathbb{Z}_p\}$, for a non-zero $v \in \mathbb{Z}_p^3$.
- 2-dimensional, if $S = \text{span}(v_1, v_2) = \{\lambda_1 v_1 + \lambda_2 v_2 : \text{for all } \lambda_1, \lambda_2 \in \mathbb{Z}_p\}$, for linearly independent $v_1, v_2 \in \mathbb{Z}_p^3$.
- 3-dimensional, if $S = \mathbb{Z}_p^3$.

Moreover, every linear subspace of dimension d has exactly p^d elements in it.

3 The space of n-tuples over $\mathbb{Z}_m$, when m is composite

When the modulus m is composite, $\mathbb{Z}_m$ is not a field and the space of n-tuples is technically not a vector space. We can still consider linear subspaces (subsets that are closed under linear combinations over $\mathbb{Z}_m$); however, these subspaces no longer have the regular form that arises in vector spaces.

As an illustrative example, consider the case of $\mathbb{Z}_6^2$ (2-tuples over $\mathbb{Z}_6$). Each of the following subsets is certainly a subspace

$$\text{span}\{(1,0)\} = \{(0,0),\ (1,0),\ (2,0),\ (3,0),\ (4,0),\ (5,0)\} \tag{1}$$
$$\text{span}\{(0,1)\} = \{(0,0),\ (0,1),\ (0,2),\ (0,3),\ (0,4),\ (0,5)\} \tag{2}$$
$$\text{span}\{(1,1)\} = \{(0,0),\ (1,1),\ (2,2),\ (3,3),\ (4,4),\ (5,5)\} \tag{3}$$
$$\text{span}\{(2,0)\} = \{(0,0),\ (2,0),\ (4,0)\} \tag{4}$$
$$\text{span}\{(3,0)\} = \{(0,0),\ (3,0)\} \tag{5}$$

but notice that the sets are not all the same size! So if we think of them as 1-dimensional subspaces then the property that all 1-dimensional spaces have the same size does not hold.

Furthermore, notice that the set

$$\text{span}\{(2,0),\ (0,3)\} = \{(0,0),\ (2,0),\ (4,0),\ (0,3),\ (2,3),\ (4,3)\} \tag{6}$$

is the same as the set

$$\text{span}\{(2,3)\} = \{(0,0),\ (2,3),\ (4,0),\ (0,3),\ (2,0),\ (4,3)\}. \tag{7}$$

So the same linear subspace can be expressed either as the span of two independent vectors or the span of just one single vector. Therefore, the notion of *dimension* is not clearly defined.