Vector Spaces

Definition 1. A vector space is an Abelian group \((V, +)\) (vectors), a field \(F\) (scalars), and a binary operation \(\cdot : F \times V \rightarrow V\) (scalar multiplication) satisfying the following properties for all scalars \(a, b \in F\) and vectors \(x, y \in V\):

\[(i) \quad a \cdot (x + y) = a \cdot x + a \cdot y;\]
\[(ii) \quad (a + b) \cdot x = a \cdot x + b \cdot x;\]
\[(iii) \quad (ab) \cdot x = a \cdot (b \cdot x);\]
\[(iv) \quad 1 \cdot x = x.\]

We say that \(V\) is a vector space over \(F\), or simply that \(V\) is a vector space.

Remark. The above properties are listed on page 7 of the textbook without using the terminology of groups. You can identify them as follows: VS 1=‘Abelian’, VS 2,3,4 are the group axioms, VS 7,8,6,5 are listed here as (i)-(iv).

Notations: Addition in \(F\) and in \(V\) are both denoted by +, multiplication in \(F\) and the scalar multiplication are both denoted by \(\cdot\) (the context makes it clear which one is used). Similarly, 0 stands for the identity for + and \(-x\) for the (additive) inverse of \(x\) both in \(F\) and in \(V\) (although in this handout I use bold face \(0\) for the ‘zero vector’). 1 is the multiplicative identity in \(F\), and \(x^{-1}\) is the multiplicative inverse of the non-zero element \(x \in F\). We often write \(ab\) and \(cx\) instead of \(a \cdot b\) and \(c \cdot x\).

The following properties are easily seen. They express that most standard rules of high-school algebra are valid for vector spaces:

For all \(a, b \in F\) and \(x, y \in V\):

- (a) \(a \cdot 0 = 0\)
- (b) \(0 \cdot x = 0\) \quad (Note the two different 0s!)
- (c) \((-a) \cdot x = -(a \cdot x) = a \cdot (-x)\)
- (d) \((-a) \cdot (-x) = a \cdot x\)
- (e) \((-1) \cdot x = -x\)
- (f) \(a \cdot (x - y) = a \cdot x - a \cdot y\)
- (g) \((a - b) \cdot x = a \cdot x - b \cdot x\)
- (h) \(a \cdot x = 0\) \quad \text{iff} \quad \text{either } a = 0 \text{ or } x = 0
Remark: Very formally (too formally perhaps) a vector space is a six-tuple $(V, F, \oplus, \odot, +, \cdot)$, where $\oplus : F \times F \to F$, $\odot : F \times F \to F$, $+: V \times V \to V$, $\cdot : F \times V \to V$, and the operations satisfy 17 properties: the 9 properties expressing that $(F, \oplus, \odot)$ is a field, the 4 properties expressing that $(V, +)$ is an Abelian group, and the above 4 properties connecting the scalar multiplication $\cdot$ with the other operations:

(i) $c \cdot (x + y) = c \cdot x + c \cdot y$;
(ii) $(a \oplus b) \cdot x = a \cdot x + b \cdot x$;
(iii) $(a \odot b) \cdot x = a \cdot (b \cdot x)$;
(iv) $1 \cdot x = x$.

We will use the first (sensible) notation, but keep in mind the dual roles of $+$, $-$, $\cdot$, and 0 (and also that we did not define multiplication of vectors).

A cautionary example:
Let $V = \mathbb{Z}$ and $F = \mathbb{Z}_2$. Define (vector-)addition on $\mathbb{Z}$ as ordinary addition of integers, and define scalar multiplication by the natural rules: $0 \cdot x = 0$ and $1 \cdot x = x$ for all $x \in \mathbb{Z}$. Is $V$ a vector space over $F$? The answer is NO.
Proof (indirect): Assume it is. Then we would have

$$10 = 5 + 5 = 1 \cdot 5 + 1 \cdot 5 = (1 + 1) \cdot 5 = 0 \cdot 5 = 0,$$

a contradiction. □

If you are confused about this, it would help a little to distinguish the different components: Let us write 0 and 1 for the elements of $F$, but $n$ for the “vectors” $n \in V = \mathbb{Z}$. Also, as above, we write $\oplus$ and $\odot$ for operations in $F$ (mod 2 operations) and $+$ for addition in $V$ (which is not mod 2, so $5 + 5$ is 10 and not 0), and $\cdot$ for scalar multiplication.
Then the above line will read as:

$$\overline{10} = \overline{5} + \overline{5} = 1 \cdot \overline{5} + 1 \cdot \overline{5} = (1 \oplus 1) \cdot \overline{5} = 0 \cdot \overline{5} = \overline{0}, \quad \text{a contradiction.}$$

The following general conclusion can be derived from this argument:

Theorem. Let $V$ be a non-trivial vector space over a field $F$. Then every non-zero vector in $V$ has the same order. The characteristic of $V$ can be defined as this common order if it is finite and 0 if the common order is infinite. With this definition, $\text{char}(V) = \text{char}(F)$. 