Sheet 33: Vector spaces

Miklós Abért

Let R be a set endoved with two functions:

$$+ : R \times R \to R$$

and

$$\cdot : R \times R \to R$$

Instead of using function notation we will denote

$$a + b = +((a, b))$$

the *sum* of a and b ($a, b \in R$) and

$$a \cdot b = \cdot((a, b))$$

the *product* of a and b ($a, b \in R$).

So far this could be any weird structure since we did not make any restrictions on the sum and product functions. To make sense, we need some rules.

A1: Commutativity of Addition. For all $a, b \in R$ we have

$$a + b = b + a$$

A2: Associativity of Addition. For all $a, b, c \in R$ we have

$$a + (b + c) = (a + b) + c$$

A3: Additive Identity. There is $0 \in R$ such that for all $a \in R$ we have

$$a + 0 = 0 + a = a$$

A4: Additive Inverse. For all $a \in R$ there exists $-a \in R$ such that

$$a + (-a) = (-a) + a = 0$$

M1: Commutativity of Multiplication. For all $a, b \in R$ we have

$$a \cdot b = b \cdot a$$

M2: Associativity of Multiplication. For all $a, b, c \in R$ we have

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

M3: Multiplicative Identity. There is $1 \in R$ such that for all $a \in R$ we have

$$a \cdot 1 = 1 \cdot a = a$$

M4: Multiplicative Inverse. For all $0 \neq a \in R$ there exists $a^{-1} \in R$ such that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

D: Distributivity. For all $a, b, c \in R$ we have

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

If $R(+, \cdot)$ satisfies all but M4, we call it a *commutative ring* (with unit). Examples: $\mathbb{Z}$ (integers), $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers), $\mathbb{C}$ (complex numbers), $\mathbb{Z}[x]$ (polynomials) all with the usual addition and multiplication.

If $R(+, \cdot)$ satisfies all the above, we call it a *field*. From the above, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields but $\mathbb{Z}$ is not.

If we only defined $+$ then we say that $R(+)$ is an *Abelian group* if it satisfies A1-A4.

For vector spaces, one first needs a field K (called the ground field). Elements of K are called *scalars*. For this definition, we will be very punctual with notation; then we shall ease up.

Let $K(+_K, \cdot_K)$ be a field. Let V be a set endoved with two functions:

$$+_V : V \times V \to V$$

and

$$\cdot_V : K \times V \to V.$$

Note that $\cdot_V$ always multiplies a scalar with a vector! We will never attempt to multiply two vectors in a vector space.

DEFINITION. The structure $(V, K, +_K, \cdot_K, +_V, \cdot_V)$ is a *vector space*, if:

V1: $K(+_K, \cdot_K)$ is a field

V2: $(V, +_V)$ satisfies A1-A4 (that is, it is an Abelian group)

V3: For all $\alpha, \beta \in K$ and $v \in V$ we have

$$(\alpha \cdot_K \beta) \cdot_V v = \alpha \cdot_V (\beta \cdot_V v)$$

V4: For all $\alpha, \beta \in K$ and $v \in V$ we have

$$(\alpha +_K \beta) \cdot_V v = (\alpha \cdot_V v) +_V (\beta \cdot_V v)$$

V5: For all $\alpha \in K$ and $v, w \in V$ we have

$$\alpha \cdot_V (v +_V w) = (\alpha \cdot_V v) +_V (\alpha \cdot_V w)$$

V6: For all $v \in V$ we have

$$1 \cdot_V v = v$$

where 1 is the multiplicative identity of K.

Exercise 1 *Show that for all* $\alpha \in K, v \in V$ *we have*

$$\alpha \cdot_V 0 = 0 \cdot_V v = 0$$

and if $\alpha \cdot_V v = 0$ *then* $a = 0$ *or* $v = 0$.

Here 0 means two things of course: either the additive identity in V or in K. They are never equal, since one is in V and the other is in K. It is time to omit the subscripts in $\cdot_V$and so altogether, since it will be always clear which operator we are using. Also, after a while we will just write αv instead of $\alpha \cdot v$.

In the following, V is always a vector space over the field K.

Definition 2 (Linear Combination) *Let* $v_1, \ldots, v_n \in V$ *and let* $\alpha_1, \ldots, \alpha_n \in K$. *Then the* linear combination *of* v_i *with coefficients* α_i *is defined as*

$$\sum_{i=1}^{n} \alpha_i \cdot v_i$$

The linear comination is non-trivial, *if not all the* α_i *are* 0.

Definition 3 (Linearly Dependent Set) *Let* X *be a subset of* V. *Then* X *is* linearly dependent, *if there are distinct elements* $v_1, \ldots, v_n \in X$ *such that a non-trivial linear combination of the* v_i *equals zero.*

Definition 4 ((In)dependence from a Set) *Let* X *be a subset of* V *and let* $v \in V$. *Then* v *is* depends on X, *if it can be written as a linear combination of elements of* X. *Otherwise, it is* independent of X.

Some basic stuff.

Exercise 5 X *is linearly dependent if and only if there exists* $x \in X$ *that depends on* $X \setminus x$.

Exercise 6 *Let* X *be a linearly independent subset. Then* $v \in V$ *depends on* X *if and only if* $X \cup \{v\}$ *is linearly dependent.*

Definition 7 (Subspace) *A subset* $U \subseteq V$ *is a* subspace *if* U *is not empty and for all* $u, v \in U$ *and* $\alpha \in K$ *we have* $u + v \in U$ *and* $\alpha u \in U$.

Exercise 8 *The intersection of (an arbitrary number of) subspaces is a subspace.*

Definition 9 (Spanned subspace) *For a subset $X \subseteq V$ let the* subspace spanned by X *be defined as*

$$\langle X \rangle = \bigcap_{\substack{U \text{ subspace in } V \\ X \subseteq U}} U$$

the smallest subspace that contains X.

Exercise 10 *For any subset $X \subseteq V$ we have*

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} \alpha_i v_i \mid n \in N,\, \alpha_i \in K,\, v_i \in X \right\}$$

Definition 11 (Spanning subset) *A subset $X \subseteq V$* spans V *if $\langle X \rangle = V$. The vector space V is* finitely generated *if it has a finite spanning subset.*

Definition 12 (Basis) *A subset $X \subseteq V$ is a* basis *if it is linearly independent and spans V.*

Exercise 13 *A subset $X \subseteq V$ is a* basis *if and only if every element of V can be obtained as a unique linear combination of elements of X.*

Exercise 14 *The following are equivalent for a subset $X \subseteq V$:*
1) X is a basis;
2) X is a maximal independent subset;
3) X is a minimal spanning subset.

It is not clear at all, that every vector space has a basis! Actually, this is equvalent to the Axiom of Choice.

Exercise 15 *Let $X \subseteq V$ be a finite linearly independent subset and let $Y \subseteq V$ be a finite spanning subset. Then $|X| \leq |Y|$.*

Exercise 16 *If V is finitely generated, then it has a basis, and every basis has the same number of elements.*

Definition 17 (Dimension) *The* dimension *of V, $\dim_K(V)$ is the number of elements in a basis of V.*

Exercise 18 *Assume that V is finitely generated. Then any linearly independent subset of V can be extended to be a basis and any spanning subset of V contains a basis.*