

§ 30 Vector spaces

Recall from linear algebra: a (real) vector space is a collection of "vectors" $v, w, \dots$

- scalar multiplication av ($a \in \mathbb{R}$)
 - vector addition $v+w$
- } give another vector

like $\mathbb{R}^n$, subspaces $V \subset \mathbb{R}^n, \dots$

We generalize coefficient system from $\mathbb{R}$ to other fields $\mathbb{Q}, \mathbb{C}, \mathbb{Z}_n$ (prime n), $\dots$

Def. F : field ; a vector space over F (or F -vector space) is given by

- commutative group V ; $v+w, -v$ make sense
- binary operation $F \times V \rightarrow V$; av for $a \in F$
 $v \in V$ make sense in V

satisfying

- associativity $(ab)v = a(bv)$ $a, b \in F, v \in V$
- distributive law $(a+b)v = av + bv$
 $a(v+w) = av + aw$
- unit constraint $1v = v$ for mult. ident. $1 \in F$

Remark: this is a particular case of module (Apr. 1)

In this lecture we are mainly interested in:

extension field E of $F \hookrightarrow E$ as a vec. sp. / F

Def. V : vec. sp. over F

- a subset $S \subset V$ spans V (over F) when any $v \in V$ can be written as

$$v = a_1 w_1 + \dots + a_k w_k \quad a_i \in F, w_i \in S \quad k=0,1,2,\dots$$

- S is linearly independent (over F)

(cont.) if $a_1 w_1 + \dots + a_k w_k = 0$ ($a_i \in F, w_i \in S$)
only if $a_i = 0$ for all i

($\Leftrightarrow$) $a_1 w_1 + \dots + a_k w_k = b_1 w_1 + \dots + b_k w_k$
only if $a_i = b_i$ for all i)

Example E ext. field of F , $\alpha \in E$ algebraic over F

$\leadsto S = \{1, \alpha, \dots, \alpha^{n-1}\}$ n : deg. of min. poly.
of α

spans E , is lin. indep. over F

Def. $S \subset V$ is a basis over F if it is both
spanning V and lin. indep.

The "size" of a vector space is given by
 $\dim V =$ number of basis vectors ($|S|$ for $\begin{smallmatrix} a \\ \uparrow \\ \text{basis} \\ S \subset V \end{smallmatrix}$)

Is this well-defined? i.e., if $S, T \subset V$ are both
basis, do we have $|S| = |T|$?

Th'm (cf. 30. ~~18~~ ^{and 19}) $S, T \subset V$; suppose

- S is linearly indep.
- $S \cup T$ spans V

Then $\exists$ subset $T' \subset T$ s.t. $S \cup T'$ is a basis

Proof. Informally: keep finding vectors $w_1, w_2, \dots$ in T
such that $S \cup \{w_1, \dots, w_k\}$ lin. indep.

Continue until we cannot do this; $T' = \{w_1, \dots, w_n\}$

Formally: the collection $F = \{T'' \subset T \mid S \cup T'' \text{ lin. ind.}\}$
satisfies the assumption of Zorn's lemma

$\leadsto \exists$ maximal elem $T' \in F$

$S \cup T'$ should span V ; otherwise we can make

T' bigger and still be in F

□

Thm (30.19, second part) $S \subset V$ lin indep,

$T \subset V$ basis $\leadsto |S| \leq |T|$

Proof write $S = \{v_1, \dots, v_r\}$, $T = \{w_1, \dots, w_n\}$

We want $r \leq n$

Set $S^{(k)} = \{v_1, \dots, v_k\}$ for $k=1, \dots, r$

Step 1. $S^{(1)} \cup T$ spans $V \leadsto \exists T^{(1)} \subsetneq T$ s.t.
but not lin. indep.

$S^{(1)} \cup T^{(1)}$ is a basis of V

Step 2. $S^{(2)} \cup T^{(1)}$ spans V , not lin. indep.

$\leadsto \exists T^{(2)} \subsetneq T^{(1)}$ s.t. $S^{(2)} \cup T^{(2)}$ basis

... $S^{(r)} \cup T^{(r)}$ basis of V for

$T \supsetneq T^{(1)} \supsetneq T^{(2)} \supsetneq \dots \supsetneq T^{(r)}$ i.e. $|T^{(r)}| \leq n-r$ $\square$

Cor. Either

- V has a finite basis ; then any basis has same size
- V has an infinite basis ; again any basis is infinite