

The dimension of a finitely generated vector space

Pierre-Yves Gaillard¹

There are, in the literature and on the web, hundreds (if not thousands) of proofs of the fact that the dimension of a finitely generated vector space is a well defined invariant. We give a short proof of this fact.

Let V be a K -vector space, and S a finite subset of V . We define the subspace *generated* (or *spanned*) by S in the usual way. We also define the condition that S is *linearly dependent* in the usual way. We say that V is *finitely generated* if it is generated by a finite subset, and we assume that such is the case. We define a *basis* of V as a (finite) linearly independent generating subset. Our aim is to prove:

Theorem 1. *Any finitely generated K -vector space admits a basis, and any two such basis have the same cardinality.*

Theorem 1 will follow from Propositions 2 and 3 below.

Proposition 2. *Let V be a K -vector space, and let F and G be two finite subsets of V such that F is linearly independent, G generates V , and $F \subset G$. Let B be also a subset of V . (We think of F and G as being “fixed”, and B being “variable”).*

- (a) *Assume that $F \subset B \subset G$, that B is linearly independent, and that B is maximal for these two conditions, then B generates V .*
- (b) *Assume that $F \subset B \subset G$, that B generates V , and that B is minimal for these two conditions, then B is linearly independent.*

(The notation F is supposed to suggest the word “free”.) Proposition 2 will follow from Lemmas 4 and 5 below.

Proposition 3. *Let V be a K -vector space, let G be a generating subset of V of finite cardinality $n \geq 0$, and let S be a subset of V of finite cardinality $m > n$. Then S is linearly dependent.*

It only remains to prove Propositions 2 and 3. If S is a finite subset of a vector space V , we denote by $\langle S \rangle$ the subspace spanned by S . The following “high school algebra fact” will be freely used:

(☺) Let n be an integer ≥ 2 and let v_1, \dots, v_n be vectors in V . Then

$$\begin{aligned} \langle v_2, \dots, v_n \rangle = \langle v_1, v_2, \dots, v_n \rangle &\iff v_1 \in \langle v_2, \dots, v_n \rangle \\ &\iff \text{there is a linear relation } \sum_{i=1}^n \lambda_i v_i = 0 \text{ with } \lambda_1 \neq 0. \end{aligned}$$

Lemma 4. *Let S be a finite linearly independent subset of a vector space V , and let v be in $V \setminus \langle S \rangle$. Then $S \cup \{v\}$ is again linearly independent.*

¹ORCID <https://orcid.org/0000-0002-7960-1698>

Proof. Let v_1, \dots, v_n (with $n \geq 0$) be the distinct elements of S . If $S \cup \{v\}$ was linearly dependent we would get $\lambda v + \sum \lambda_i v_i = 0$ with $(\lambda, \lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$. This would imply $\lambda \neq 0$, and thus $v \in \langle S \rangle$ by (\odot) . \square

Lemma 5. *If G is a finite nonempty linearly dependent generating subset of a vector space V , then there is a g in G such $G \setminus \{g\}$ is again generating.*

Proof. Let g_1, \dots, g_n (with $n \geq 1$) be the distinct elements of G . We have $\sum \lambda_i g_i = 0$ for some $(\lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$. We may assume $\lambda_n \neq 0$. Then g_n is a linear combination of g_1, \dots, g_{n-1} by (\odot) , and, thus, so is any vector in V . \square

Proof of Proposition 3. Writing $|X|$ for the cardinality of X , we assume by contradiction that F and G are two finite subsets of V such that F is linearly independent, G is generating, and we have $|F| = m > n = |G|$. We can assume that $k := |F \cap G|$ is maximum among *all* couples (F', G') of subsets of V such that $|F'| = m, |G'| = n$, F' is linearly independent and G' spans V . We clearly have $k < n$ (indeed, $k = n$ would imply that f_m is a linear combination of f_1, \dots, f_k , contradicting the linear independence of the f_i). Set

$$F = \{f_1, \dots, f_k, \dots, f_n, \dots, f_m\}, \quad G = \{g_1, \dots, g_k, \dots, g_n\},$$

with $f_1 = g_1, \dots, f_k = g_k$. Since G spans V , we have $f_m = \sum_{i=1}^n \lambda_i g_i$, or equivalently

$$-f_m + \sum_{i=1}^n \lambda_i g_i = 0 \tag{1}$$

for some $(\lambda_i)_{i=1}^n$. Since $f_m \notin \langle f_1, \dots, f_k \rangle = \langle g_1, \dots, g_k \rangle$, there is an r with $k+1 \leq r \leq n$ and $\lambda_r \neq 0$. Set $G' := (G \cup \{f_m\}) \setminus \{g_r\}$. By (1), the definition of r , and (\odot) we have $\langle G' \rangle = \langle G \cup \{f_m\} \rangle = V$. The equalities $|G'| = n$ and $|F \cap G'| = k+1$ being clear, Proposition 3 is proved. This completes the proof of Theorem 1. \square

We end with a short unrelated observation whose goal is to define the sign homomorphism from the symmetric group to $\{\pm 1\}$. Let n be an integer ≥ 3 , set $X := \{1, \dots, n\}$, let S_n be the group of permutations of X , let Y be the set of two-element subsets of X , and let σ be in S_n . For $y \in Y$ define $\sigma y \in Y$ by $\sigma\{i, j\} = \{\sigma i, \sigma j\}$. Let $1 \leq i < j \leq n$. Say that $\{i, j\}$ is an **inversion** for σ if $\sigma j < \sigma i$, let I_σ be the set of all such inversions, and define the map $\varepsilon : A_n \rightarrow \{\pm 1\}$ by $\varepsilon(\sigma) = (-1)^{|I_\sigma|}$. We claim

$$\varepsilon(\tau\sigma) = \varepsilon(\tau)\varepsilon(\sigma) \tag{2}$$

for $\tau, \sigma \in S_n$. Recall that the **symmetric difference** $A \Delta B$ of two sets A and B is the set $(A \cup B) \setminus (A \cap B)$. We clearly have

$$|A \Delta B| = |A| + |B| - 2|A \cap B| \tag{3}$$

if A and B are finite, as well as

$$I_{\tau\sigma} = I_\sigma \Delta \sigma^{-1}(I_\tau), \tag{4}$$

and (2) follows from (3) and (4). We also claim that half the members of S_n satisfy $\varepsilon(\sigma) = -1$. It suffices to show that at least one of them does. But the transposition (12) swapping 1 and 2 satisfies this condition (in fact we have $I_{(12)} = \{\{1, 2\}\}$).