Course 6

2.7 Dimension

Recall that we consider only finitely generated vector spaces. Let us begin with a very useful lemma, that will be often implicitly used.

Lemma 2.7.1 *Let V be a vector space over K and let $Y = \langle y_1, \dots, y_n, z\rangle$. If $z \in \langle y_1, \dots, y_n\rangle$, then $Y = \langle y_1, \dots, y_n\rangle$.*

Proof. The generated subspace Y is the set of all linear combinations of the vectors $y_1, \dots, y_n, z$. Since $z \in \langle y_1, \dots, y_n\rangle$, z is a linear combination of the vectors $y_1, \dots, y_n$. It follows that every vector in Y can be written as a linear combination only of the vectors $y_1, \dots, y_n$. Consequently, $Y = \langle y_1, \dots, y_n\rangle$. □

The following result is a key theorem for proving that any two bases of a vector space have the same number of elements. But it is worth mentioning that it has a much broader importance in Linear Algebra.

Theorem 2.7.2 (Steinitz Theorem, Exchange Theorem) *Let V be a vector space over K, $X = (x_1, \dots, x_m)$ a linearly independent list of vectors of V and $Y = (y_1, \dots, y_n)$ a system of generators of V. Then:*
(i) $m \leq n$.
(ii) m vectors of Y can be replaced by the vectors of X obtaining again a system of generators for V.

Proof. We prove this result by induction on m.

The first step is to check it for $m = 1$. Then clearly $m \leq n$. Since Y is a system of generators for V, we have $x_1 = \sum_{i=1}^{n} k_i y_i$ for some $k_1, \dots, k_n \in K$. The list $X = \{x_1\}$ is linearly independent, hence $x_1 \neq 0$. It follows that $\exists j \in \{1, \dots, n\}$ such that $k_j \neq 0$. Then

$$y_j = k_j^{-1} x_1 - \sum_{\substack{i=1\\ i\neq j}}^{n} k_j^{-1} k_i y_i \,,$$

that is, y_j is a linear combination of the vectors $y_1, \dots, y_{j-1}, x_1, y_{j+1}, \dots, y_n$. Hence, in any linear combination of $y_1, \dots, y_n$, the vector y_j can be expressed as a linear combination of the other vectors and x_1. Therefore, we have

$$V = \langle y_1, \dots, y_n\rangle = \langle y_1, \dots, y_{j-1}, x_1, y_{j+1}, \dots, y_n\rangle \,.$$

Thus, we have obtained again a system of n generators for V containing x_1.

Let us now move on to the second step of the induction. We suppose the conclusion is true for $m-1$ and prove it for m. Let $X = (x_1, \dots, x_m)$ be a linearly independent list in V. Then $(x_1, \dots, x_{m-1})$ must be also linearly independent in V. By the induction hypothesis, we have $m-1 \leq n$ and, after a renumbering,

$$V = \langle x_1, \dots, x_{m-1}, y_m, \dots, y_n\rangle \,.$$

If $m-1 = n$, then $V = \langle x_1, \dots, x_{m-1}\rangle$, whence it follows that $x_m \in \langle x_1, \dots, x_{m-1}\rangle$, which contradicts the fact that X is linearly independent in V. Thus $m-1 < n$, so that $m \leq n$.

We have $x_m \in V = \langle x_1, \dots, x_{m-1}, y_m, \dots, y_n\rangle$, whence

$$x_m = \sum_{i=1}^{m-1} k_i x_i + \sum_{i=m}^{n} k_i y_i$$

for some $k_1, \dots, k_n \in K$. The list X being linearly independent in V, it follows that $\exists m \leq j \leq n$ such that $k_j \neq 0$ (otherwise, $x_m = \sum_{i=1}^{m-1} k_i x_i$ and the list X would be linearly dependent in V). For simplicity of writing, assume that $j = m$. It follows that

$$y_m = k_m^{-1} x_m - \sum_{i=1}^{m-1} k_m^{-1} k_i x_i - \sum_{i=m+1}^{n} k_m^{-1} k_i y_i \,.$$

Thus, y_m is a linear combination of the vectors $x_1, \dots, x_m, y_{m+1}, \dots, y_n$, that is, we have $y_m \in \langle x_1, \dots, x_m, y_{m+1}, \dots, y_n \rangle$. Therefore, it follows that

$$V = \langle x_1, \dots, x_{m-1}, y_m, \dots, y_n \rangle = \langle x_1, \dots, x_m, y_{m+1}, \dots, y_n \rangle .$$

Thus, we have obtained again a system of generators for V, where m vectors of the list Y have been replaced by the vectors of the list X. This completes the proof. □

Remark 2.7.3 Let us point out that in Steinitz Theorem not necessarily the first m vectors of Y can be replaced by the m vectors of X.

Theorem 2.7.4 *Any two bases of a vector space have the same number of elements.*

Proof. Let V be a vector space over K and let $B = (v_1, \dots, v_m)$ and $B' = (v'_1, \dots, v'_n)$ be bases of V. Since B is linearly independent in V and B' is a system of generators for V, we have $m \le n$ by Theorem 2.7.2. Since B is a system of generators for V and B' is linearly independent in V, we have $n \le m$ by the same Theorem 2.7.2. Hence $m = n$. □

Definition 2.7.5 Let V be a vector space over K. Then the number of elements of any of its bases is called the *dimension of* V and is denoted by $\dim_K V$ or simply by $\dim V$.

Remark 2.7.6 If $V = \{0\}$, then V has the basis $\emptyset$ and $\dim V = 0$.

Example 2.7.7 Using the examples of bases given in the previous section, one can easily determine the dimension of each of those vector spaces.

(a) Let K be a field and $n \in \mathbb{N}^*$. Then $\dim_K K^n = n$.

(b) We have seen that the subspaces of $\mathbb{R}^3$ are $\{(0,0,0)\}$, any line containing the origin, any plane containing the origin and $\mathbb{R}^3$. Their dimensions are 0, 1, 2 and 3 respectively.

(c) Let K be a field and $n \in \mathbb{N}$. Then $\dim K_n[X] = n + 1$.

(d) Let K be a field. Then $\dim M_2(K) = 4$.
More generally, if $m, n \in \mathbb{N}$, $m, n \ge 2$, then $\dim M_{m,n}(K) = m \cdot n$.

(e) Consider the subspace

$$S = \{(x, y, z) \in \mathbb{R}^3 \mid x - y - z = 0\}$$

of the canonical real vector space $\mathbb{R}^3$. We have seen that $S = \langle (1,1,0), (1,0,1) \rangle$. Since the vectors $(1,1,0)$ and $(1,0,1)$ are linearly independent, it follows that $B = ((1,1,0), (1,0,1))$ is a basis of S. Hence $\dim S = 2$.

(f) We have $\dim_{\mathbb{C}} \mathbb{C} = 1$ and $\dim_{\mathbb{R}} \mathbb{C} = 2$.

Theorem 2.7.8 *Let V be a vector space over K. Then the following statements are equivalent:*
(i) $\dim V = n$.
(ii) The maximum number of linearly independent vectors in V is n.
(iii) The minimum number of generators for V is n.

Proof. $(i) \Longrightarrow (ii)$ Assume that $\dim V = n$. Let $B = (v_1, \dots, v_n)$ be a basis of V. Then B is a list of n linearly independent vectors in V. Since B is a system of generators for V, any linearly independent list in V must have at most n elements by Theorem 2.7.2.

$(ii) \Longrightarrow (i)$ Assume (ii). Let $B = (v_1, \dots, v_m)$ be a basis of V and let $(u_1, \dots, u_n)$ be a linearly independent list in V. Since B is linearly independent, we have $m \le n$ by hypothesis. Since B is a system of generators for V, we have $n \le m$ by Theorem 2.7.2. Hence $m = n$ and consequently $\dim V = n$.

$(i) \Longrightarrow (iii)$ Assume that $\dim V = n$. Let $B = (v_1, \dots, v_n)$ be a basis of V. Then B is a system of n generators for V. Since B is a linearly independent list in V, any system of generators for V must have at least n elements by Theorem 2.7.2.

(iii) $\Longrightarrow$ *(i)* Assume *(iii)*. Let $B = (v_1, \dots, v_m)$ be a basis of V and let $(u_1, \dots, u_n)$ be a system of generators for V. Since B is a system of generators for V, we have $n \leq m$ by hypothesis. Since B is linearly independent, we have $m \leq n$ by Theorem 2.7.2. Hence $m = n$ and consequently $\dim V = n$. □

Theorem 2.7.9 *Let V be a vector space over K with $\dim V = n$ and $X = (u_1, \dots, u_n)$ a list of vectors in V. Then*

$$X \text{ is linearly independent in } V \Longleftrightarrow X \text{ is a system of generators for } V.$$

Proof. Let $B = (v_1, \dots, v_n)$ be a basis of V.

$\boxed{\Longrightarrow}$ Assume that X is linearly independent. Since B is a system of generators for V, we know by Theorem 2.7.2 that n vectors of B, that is, all the vectors of B, can be replaced by the vectors of X and we get another system of generators for V. Hence $\langle X \rangle = V$. Thus, X is a system of generators for V.

$\boxed{\Longleftarrow}$ Assume that X is a system of generators for V. Suppose that X is linearly dependent. Then $\exists j \in \{1, \dots, n\}$ such that

$$u_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i u_i$$

for some $k_i \in K$. It follows that

$$V = \langle X \rangle = \langle u_1, \dots, u_{j-1}, u_{j+1}, \dots, u_n \rangle .$$

But the minimum number of generators for V is n by Theorem 2.7.8, which is a contradiction. Therefore, X is linearly independent. □

Corollary 2.7.10 *Let $n \in \mathbb{N}$, $n \geq 2$. Then n vectors in K^n form a basis of the canonical vector space K^n if and only if the determinant consisting of their components is non-zero.*

Proof. We have seen that n vectors in K^n are linearly independent if and only if the determinant consisting of their components is non-zero. But if this happens, then using the fact that $\dim_K K^n = n$ and Theorem 2.7.9, the vectors are also a system of generators, and thus a basis of K^n. □

Theorem 2.7.11 *Any linearly independent list of vectors in a vector space can be completed to a basis of the vector space.*

Proof. Let V be a vector space over K. Let $B = (v_1, \dots, v_n)$ be a basis of V and let $(u_1, \dots, u_m)$ be a linearly independent list in V. Since B is a system of generators for V, we know by Theorem 2.7.2 that $m \leq n$ and m vectors of B can be replaced by the vectors $(u_1, \dots, u_m)$ obtaining again a system of generators for V, say $(u_1, \dots, u_m, v_{m+1}, \dots, v_n)$. But by Theorem 2.7.9, this is also linearly independent in V and consequently a basis of V. □

Remark 2.7.12 The completion of a linearly independent list to a basis of the vector space is not unique.

Example 2.7.13 The list (e_1, e_2), where $e_1 = (1, 0, 0)$ and $e_2 = (0, 1, 0)$, is linearly independent in the canonical real vector space $\mathbb{R}^3$. It can be completed to the canonical basis of the space, namely (e_1, e_2, e_3), where $e_3 = (0, 0, 1)$. On the other hand, since $\dim_{\mathbb{R}} \mathbb{R}^3 = 3$, in order to obtain a basis of the space it is enough to add to our list a vector v_3 such that (e_1, e_2, v_3) is linearly independent (see Theorem 2.7.9). For instance, we may take $v_3 = (1, 1, 1)$, since the determinant consisting of the components of the three vectors is non-zero.

Corollary 2.7.14 *Let V be a vector space over K and $S \leq V$. Then:*
(i) Any basis of S is a part of a basis of V.
(ii) $\dim S \leq \dim V$.
(iii) $\dim S = \dim V \Longleftrightarrow S = V$.

Proof. (i) Let $(u_1, \dots, u_m)$ be a basis of S. Since the list is linearly independent, it can be completed to a basis $(u_1, \dots, u_m, v_{m+1}, \dots, v_n)$ of V by Theorem 2.7.11.

(ii) It follows by (i).

(iii) Assume that $\dim S = \dim V = n$. Let $(u_1, \dots, u_n)$ be a basis of S. Then it is linearly independent in V, hence it is a basis of V by Theorem 2.7.9. Thus, if $v \in V$, then $v = k_1u_1 + \dots + k_nu_n$ for some $k_1, \dots, k_n \in K$, hence $v \in S$. Therefore, $S = V$. $\square$

Theorem 2.7.15 *Let V be a vector space over K and let $S \leq V$. Then there exists $\overline{S} \leq V$ such that $V = S \oplus \overline{S}$. In particular,*

$$\dim V = \dim S + \dim \overline{S}.$$

Proof. Let $(u_1, \dots, u_m)$ be a basis of S. Then by Corollary 2.7.14, it can be completed to a basis $B = (u_1, \dots, u_m, v_{m+1}, \dots, v_n)$ of V. We consider

$$\overline{S} = \langle v_{m+1}, \dots, v_n \rangle$$

and we prove that $V = S \oplus \overline{S}$.

Let $v \in V$. Then

$$v = \sum_{i=1}^{m} k_iu_i + \sum_{i=m+1}^{n} k_iv_i \in S + \overline{S}\,,$$

for some $k_1, \dots, k_n \in K$. Hence $V = S + \overline{S}$.

Now let $v \in S \cap \overline{S}$. Then

$$v = \sum_{i=1}^{m} k_iu_i = \sum_{i=m+1}^{n} k_iv_i\,,$$

for some $k_1, \dots, k_n \in K$. Hence

$$\sum_{i=1}^{m} k_iu_i - \sum_{i=m+1}^{n} k_iv_i = 0\,,$$

whence $k_i = 0$, $\forall i \in \{1, \dots, n\}$, because B is a basis. Thus, $v = 0$ and $S \cap \overline{S} = \{0\}$.

Therefore, $V = S \oplus \overline{S}$. $\square$

Remark 2.7.16 This is an extremely important property of a vector space, that allows us to split it in "smaller" subspaces, that can be studied much easier and then to use that information to get information about the entire vector space.

Definition 2.7.17 Let V be a vector space over K and $S \leq V$. Then a subspace $\overline{S}$ of V such that

$$V = S \oplus \overline{S}$$

is called a *complement of S in V*.

Remark 2.7.18 A subspace of a vector space may have more than one complement (see also the remark following Theorem 2.7.11).

Example 2.7.19 Consider the subspace $S = \langle e_1, e_2 \rangle$ of the canonical real vector space $\mathbb{R}^3$, where $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$. Then clearly (e_1, e_2) is a basis of S. Now by Example 2.7.13, it can be completed to a basis of $\mathbb{R}^3$, with the vector $e_3 = (0, 0, 1)$ or with the vector $v_3 = (1, 1, 1)$. Following the proof of Theorem 2.7.15, a complement in V of the subspace $S = \langle e_1, e_2 \rangle$ is $\langle e_3 \rangle$ or $\langle v_3 \rangle$.

2.8 Dimension theorems

Theorem 2.8.1 *Let V and V' be vector spaces over K. Then*

$$V \simeq V' \iff \dim V = \dim V'.$$

Proof. $\boxed{\Longrightarrow}$ Let $f : V \to V'$ be a K-isomorphism and let $B = (v_1, \dots, v_n)$ be a basis of V. Note that, since f is injective, we have $f(v_i) \neq f(v_j)$ for every $i, j \in \{1, \dots, n\}$ with $i \neq j$. Hence the list

$$B' = f(B) = (f(v_1), \dots, f(v_n))$$

has n elements. Then B' is a basis of V'. Now it follows that $\dim V = \dim V'$.

$\boxed{\Longleftarrow}$ Assume that $\dim V = \dim V' = n$. Let $B = (v_1, \dots, v_n)$ and $B' = (v'_1, \dots, v'_n)$ be bases of V and V' respectively. Define a function $f : V \to V'$ in the following way. For every $v = k_1v_1 + \dots + k_nv_n \in V$ (where $k_1, \dots, k_n \in K$ are uniquely determined), define

$$f(v) = k_1v'_1 + \dots + k_nv'_n.$$

Let us first prove that f is a K-linear map. Let $\alpha, \beta \in K$ and $v, w \in V$. Then $v = k_1v_1 + \dots + k_nv_n$ and $w = l_1v_1 + \dots + l_nv_n$ for some unique $k_1, \dots, k_n, l_1, \dots, l_n \in K$. It follows that

$$\begin{aligned} f(\alpha v + \beta w) &= f((\alpha k_1 + \beta l_1)v_1 + \dots + (\alpha k_n + \beta l_n)v_n) \\ &= (\alpha k_1 + \beta l_1)v'_1 + \dots + (\alpha k_n + \beta l_n)v'_n \\ &= \alpha(k_1v'_1 + \dots + k_nv'_n) + \beta(l_1v'_1 + \dots + l_nv'_n) \\ &= \alpha f(v) + \beta f(w). \end{aligned}$$

Hence f is a K-linear map. In particular, we have $f(v_i) = v'_i$ for every $i \in \{1, \dots, n\}$.

Now let us prove that f is bijective. Let $v' = k'_1v'_1 + \dots + k'_nv'_n \in V'$ (where $k'_1, \dots, k'_n \in K$ are uniquely determined). Using the fact that $f(v_i) = v'_i$ for every $i \in \{1, \dots, n\}$, it follows that

$$v' = k'_1f(v_1) + \dots + k'_nfv_n) = f(k'_1v_1 + \dots + k'_nv_n),$$

where the vector $k'_1v_1 + \dots + k'_nv_n \in V$ is uniquely determined. Hence f is bijective, and thus f is a K-isomorphism. □

We may immediately deduce the following result.

Theorem 2.8.2 *Any vector space V over K with $\dim V = n$ is isomorphic to the canonical vector space K^n over K.*

Remark 2.8.3 Theorem 2.8.2 is a very important structure theorem, saying that, up to an isomorphism, *any finite dimensional vector space over K is, in fact, the canonical vector space K^n over K*. For instance, we have the K-isomorphisms $K_n[X] \simeq K^{n+1}$ and $M_{m,n}(K) \simeq K^{mn}$. Now we have an explanation why we have used so often the canonical vector spaces: not only because the operations are very nice and easily defined, but they are, up to an isomorphism, the only types of finite dimensional vector spaces.

Definition 2.8.4 Let $f : V \to V'$ be a K-linear map. Then:
(1) $\dim(\mathrm{Ker} f)$ is called the *nullity* of f, and is denoted by $\mathrm{null}(f)$.
(2) $\dim(\mathrm{Im} f)$ is called the *rank* of f, and is denoted by $\mathrm{rank}(f)$.

Next we present an important theorem relating the nullity and the rank of a linear map.

Theorem 2.8.5 (First Dimension Theorem) *Let $f : V \to V'$ be a K-linear map. Then*

$$\dim V = \dim(\mathrm{Ker} f) + \dim(\mathrm{Im} f).$$

In other words, $\dim V = \mathrm{null}(f) + \mathrm{rank}(f)$.

Theorem 2.8.6 (Second Dimension Theorem) *Let V be a vector space over K and let S, T be subspaces of V. Then*

$$\dim S + \dim T = \dim(S \cap T) + \dim(S + T)\,.$$

Corollary 2.8.7 *Let V be a vector space over K, and let S and T be subspaces of V such that $V = S \oplus T$. Then*

$$\dim V = \dim S + \dim T\,.$$

Extra: Checksum function

Following [Klein], we present a checksum function for detecting corrupted files.

Definition 2.8.8 Let $u = (x_1, \dots, x_n), v = (y_1, \dots, y_n) \in K^n$. Then the *dot-product* (or *scalar product*) of u and v is the scalar

$$u \cdot v = x_1 y_1 + \cdots + x_n y_n \in K.$$

Example 2.8.9 We give an example of a checksum function which may detect accidental random corruption of a file during transmission or storage.
Let $a_1, \dots, a_{64} \in \mathbb{Z}_2^n$ and let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^{64}$ be the $\mathbb{Z}_2$-linear map defined by

$$f(v) = (a_1 \cdot v, \dots, a_{64} \cdot v).$$

Suppose that v is a "file". We model corruption as the addition of a random vector $e \in \mathbb{Z}_2^n$ (the error), so the corrupted version of the file is $v + e$. We look for a formula for the probability that the corrupted file has the same checksum as the original file.
The checksum of the original file v is taken to be $f(v)$, hence the checksum of the corrupted file $v + e$ is $f(v + e)$. The original file and the corrupted file have the same checksum if and only if $f(v) = f(v + e)$ if and only if $f(e) = 0$ if and only if $e \in \operatorname{Ker} f$.
Every vector space V over the field $\mathbb{Z}_2$ with $\dim V = n$ is isomorphic to $\mathbb{Z}_2^n$, hence it has 2^n vectors. In particular, $\operatorname{Ker} f$ has 2^k vectors, where $k = \dim(\operatorname{Ker} f)$.
If the error is chosen according to the uniform distribution, the probability that $v + e$ has the same checksum as v is the following:

$$P = \frac{\text{number of vectors in } \operatorname{Ker} f}{\text{number of vectors in } \mathbb{Z}_2^n} = \frac{2^k}{2^n}.$$

One may show that $\dim(\operatorname{Im} f)$ is close to $\min(n, 64)$. So if we choose $n \geq 64$, we may assume that $\dim(\operatorname{Im} f) = 64$. By the First Dimension Theorem, we have

$$k = \dim(\operatorname{Ker} f) = \dim \mathbb{Z}_2^n - \dim(\operatorname{Im} f) = n - 64.$$

Hence

$$P = \frac{2^{n-64}}{2^n} = \frac{1}{2^{64}},$$

and thus there is only a very tiny chance that the change is undetected.