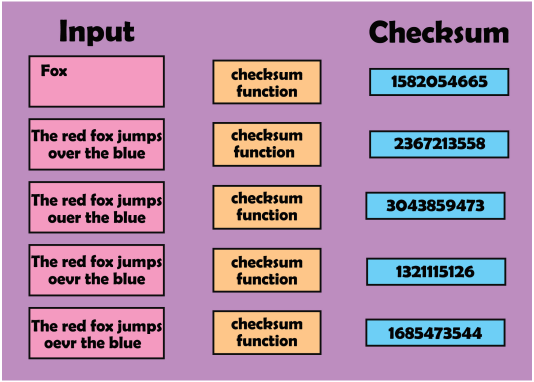
Course 6

Dimension

Prof. dr. Septimiu Crivei

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



Steinitz Theorem

Theorem (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.

In Steinitz Theorem not necessarily the first m vectors of Y can be replaced by the m vectors of X!

Theorem

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 $m \leq n$ by Steinitz Theorem. Since B is a system of generators for V and B' is linearly independent in V, we have $n \leq m$ by Steinitz Theorem. Hence $m = n$. $\square$

Definition

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 $\dim V$.

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

Examples I

(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 $m, n \in \mathbb{N}$, $m, n \geq 2$, then $\dim M_{m,n}(K) = m \cdot n$.

(e) Consider the subspace

$$S = \{(x, y, z) \in \mathbb{R}^3 \mid x - y - z = 0\} = \langle (1, 1, 0), (1, 0, 1) \rangle$$

of the canonical real vector space $\mathbb{R}^3$. 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 $\dim_{\mathbb{R}} \mathbb{C} = 2$.

Characterization of dimension

Theorem

Let V be a vector space over K. The following are equivalent:
(i) $\dim V = n$.
(ii) The maximum no. of linearly independent vectors in V is n.
(iii) The minimum no. of generators for V is n.

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

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

$(i) \Longleftrightarrow (iii)$ Homework.

When linear independence = system of generators I

Theorem

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

$$X \text{ is linearly independent} \iff X \text{ is a system of generators}.$$

Proof. Let $B = (v_1, \ldots, v_n)$ 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 Steinitz Theorem 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 $\exists j \in \{1, \ldots, n\}$ 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

$V = \langle X \rangle = \langle u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n \rangle$. But the minimum number of generators for V is n, which is a contradiction. Therefore, X is linearly independent. $\square$

Corollary

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 they are linearly independent 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 $\dim_K K^n = n$, the vectors are also a system of generators, and thus a basis of K^n. $\square$

Theorem

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 Steinitz Theorem 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 this must also linearly independent in V and consequently a basis of V. $\square$

Corollary

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) $\dim S = \dim V \iff S = V$.

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 the previous theorem.

(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, because $\dim V = n$. Thus, if $v \in V$, then $v = k_1 u_1 + \dots + k_n u_n$ for some $k_1, \dots, k_n \in K$, hence $v \in S$. Therefore, $S = V$. $\square$

Example

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

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. For instance, we may take $v_3 = (1, 1, 1)$, since the determinant consisting of the components of the three vectors is non-zero.

Decomposition theorem I

Theorem

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 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

$$v = \sum_{i=1}^{m} k_i u_i + \sum_{i=m+1}^{n} k_i v_i \in S + \overline{S},$$

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

Decomposition theorem II

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

$$v = \sum_{i=1}^{m} k_i u_i = \sum_{i=m+1}^{n} k_i v_i \,,$$

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

$$\sum_{i=1}^{m} k_i u_i - \sum_{i=m+1}^{n} k_i v_i = 0 \,,$$

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

Remark

This is an important property of a vector space, allowing to split it in "smaller" subspaces, that can be studied easier and are used to derive information about the entire vector space.

Definition

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*.

Note that a subspace may have more than one complement.

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.

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 the above theorem, a complement in V of the subspace $S = \langle e_1, e_2 \rangle$ is $\langle e_3 \rangle$ or $\langle v_3 \rangle$.

Theorem

Let V and V' be vector spaces over K. Then

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

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 $v = k_1 v_1 + \cdots + k_n v_n \in V$ (where $k_1, \ldots, k_n \in K$ are uniquely determined), define

$$f(v) = k_1 v_1' + \cdots + k_n v_n'.$$

Let us first prove that f is a K-linear map. Let $\alpha, \beta \in K$ and $v, w \in V$. Then $v = k_1 v_1 + \cdots + k_n v_n$ and $w = l_1 v_1 + \cdots + l_n v_n$ for some unique $k_1, \ldots, k_n, l_1, \ldots, l_n \in K$. It follows that

$$\begin{aligned} f(\alpha v + \beta w) &= f((\alpha k_1 + \beta l_1)v_1 + \cdots + (\alpha k_n + \beta l_n)v_n) \\ &= (\alpha k_1 + \beta l_1)v_1' + \cdots + (\alpha k_n + \beta l_n)v_n' \\ &= \alpha(k_1 v_1' + \cdots + k_n v_n') + \beta(l_1 v_1' + \cdots + l_n v_n') \\ &= \alpha f(v) + \beta f(w). \end{aligned}$$

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

Now let us prove that f is bijective. Let $v' = k_1'v_1' + \cdots + k_n'v_n' \in V'$ (where $k_1', \ldots, k_n' \in K$ are uniquely determined). Using the fact that $f(v_i) = v_i'$ for every $i \in \{1, \ldots, n\}$, it follows that

$$v' = k_1'f(v_1) + \cdots + k_n'f(v_n) = f(k_1'v_1 + \cdots + k_n'v_n),$$

where the vector $k_1'v_1 + \cdots + k_n'v_n \in V$ is uniquely determined. Hence f is bijective, and thus f is a K-isomorphism. $\square$

Uniqueness of n-dimensional vector spaces up to isomorphism

We may immediately deduce the following result.

Theorem

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

This result 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.

First Dimension Theorem

Definition

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 (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 (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

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 I

Definition

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

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

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

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

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.