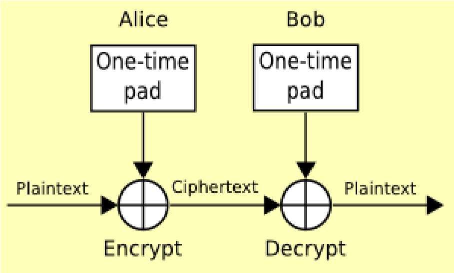
Course 3

Vector spaces, subspaces

Prof. dr. Septimiu Crivei

Application: Vernam cipher

Following [Klein], we describe an easy, but secure cipher on binary strings, based on vector spaces over $\mathbb{Z}_2$.



Vector spaces

Throughout the present chapter K will always denote a field.

Definition

A *vector space over* K (or a K*-vector space*) is an abelian group $(V, +)$ together with a so-called *external operation* or *scalar multiplication*

$$\cdot : K \times V \to V\,, \quad (k, v) \mapsto k \cdot v \quad (\text{or simply } kv)\,,$$

satisfying the following axioms:
(L_1) $k \cdot (v_1 + v_2) = k \cdot v_1 + k \cdot v_2$;
(L_2) $(k_1 + k_2) \cdot v = k_1 \cdot v + k_2 \cdot v$;
(L_3) $(k_1 \cdot k_2) \cdot v = k_1 \cdot (k_2 \cdot v)$;
(L_4) $1 \cdot v = v$,
for every $k, k_1, k_2 \in K$ and every $v, v_1, v_2 \in V$.
The elements of K are called *scalars* and the elements of V are called *vectors*.
Sometimes a vector space is also called a *linear space*.

Remarks

We usually denote a vector space V over K by ${}_K V$ or $(V, K, +, \cdot)$.

(1) In the definition of a vector space there are present four operations (3 by our definition), two denoted by the same symbol "$+$" and two denoted by the same symbol "$\cdot$". Of course, they are not the same, but we use the convention to denote them identically for the sake of simplicity of writing.

(2) The axioms (L_1) and (L_2) look like some distributive laws and the axiom (L_3) looks like an associative law, but they are not, since the involved elements are not taken from the same set.

(3) We have defined a *left vector space*. It is also possible to define a *right vector space* by considering an external operation

$$\cdot : V \times K \to V\,, \quad (v, k) \mapsto v \cdot k,$$

satisfying some similar axioms, but on the right hand side.

(a) Let V_2 be the set of all vectors (in the classical sense) in the plane with a fixed origin O. Then V_2 is a vector space over $\mathbb{R}$ (or a *real vector space*), where the addition is the usual addition of two vectors by the parallelogram rule and the external operation is the usual scalar multiplication of vectors by real scalars.

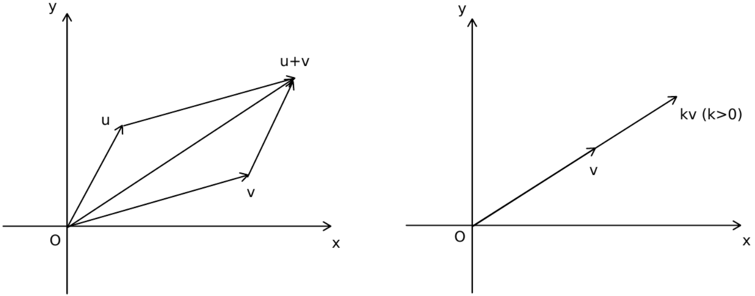


Figure: Vector addition and scalar multiplication.

Examples II

If we consider two coordinate axes Ox and Oy in the plane, each vector in V_2 is perfectly determined by the coordinates of its ending point. Therefore, the addition of vectors and the scalar multiplication of vectors by real numbers become:

$$\begin{aligned} (x, y) + (x', y') &= (x + x', y + y'), \\ k \cdot (x, y) &= (k \cdot x, k \cdot y), \end{aligned}$$

$\forall k \in \mathbb{R}$ and $\forall (x, y), (x', y') \in \mathbb{R} \times \mathbb{R}$. Thus, $(\mathbb{R}^2, \mathbb{R}, +, \cdot)$ is a vector space.

Similarly, one can consider the real vector space V_3 of all vectors in the space with a fixed origin. Moreover, a further, but more algebraical, generalization is possible, as we may see in the following example.

(b) Let $n \in \mathbb{N}^*$. Define

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)\,,$$
$$k \cdot (x_1, \ldots, x_n) = (kx_1, \ldots, kx_n)\,,$$

$\forall (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$ and $\forall k \in K$. Then $(K^n, K, +, \cdot)$ is a vector space, called the *canonical vector space* (or *standard vector space*) over K.

For $K = \mathbb{Z}_2$, $\mathbb{Z}_2^n$ is a vector space over $\mathbb{Z}_2$. For $n = 1$, ${}_K K$ is a vector space. Hence ${}_{\mathbb{Q}}\mathbb{Q}$, ${}_{\mathbb{R}}\mathbb{R}$ and ${}_{\mathbb{C}}\mathbb{C}$ are vector spaces.

(c) If $V = \{e\}$ is a single element set, then we know that there is a unique structure of an abelian group for V, namely that one defined by $e + e = e$. Then we can define a unique scalar multiplication, namely $k \cdot e = e$, $\forall k \in K$. Thus, V is a vector space, called the *zero (null) vector space* and denoted by $\{0\}$.

Examples IV

(d) If A is a subfield of the field K, then K is a vector space over A, where the addition and the scalar multiplication are just the addition and the multiplication of elements in the field K.

In particular, ${}_{\mathbb{Q}}\mathbb{R}$, ${}_{\mathbb{Q}}\mathbb{C}$ and ${}_{\mathbb{R}}\mathbb{C}$ are vector spaces. Note that $\mathbb{R}$ may be viewed as a vector space over $\mathbb{Q}$ or $\mathbb{R}$, while $\mathbb{C}$ may be viewed as a vector space over any of the fields $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

(e) $(K[X], K, +, \cdot)$ is a vector space, where the addition is the usual addition of polynomials and the scalar multiplication is defined as follows: $\forall f = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$, $\forall k \in K$,

$$kf = (ka_0) + (ka_1)X + \cdots + (ka_n)X^n \,.$$

(f) Let $m, n \in \mathbb{N}$, $m, n \geq 2$. Then $(M_{m,n}(K), K, +, \cdot)$ is a vector space, where the operations are the usual addition and scalar multiplication of matrices.

(g) Let A be a non-empty set. Denote

$$K^A = \{f \mid f : A \to K\}\,.$$

Then $(K^A, K, +, \cdot)$ is a vector space, where the addition and the scalar multiplication are defined as follows: $\forall f, g \in K^A$, $\forall k \in K$, we have $f + g \in K^A$, $kf \in K^A$, where

$$(f+g)(x) = f(x) + g(x)\,,$$
$$(kf)(x) = kf(x)$$

$\forall x \in A$. As a particular case, we obtain the vector space $(\mathbb{R}^{\mathbb{R}}, \mathbb{R}, +, \cdot)$ of real functions of a real variable.

Examples VI

(h) Let V and V' be K-vector spaces. Then the cartesian product $V \times V'$ is a K-vector space, called the *direct product* of V and V', where the addition and the scalar multiplication are defined by:

$$(v_1, v_1') + (v_2, v_2') = (v_1 + v_2, v_1' + v_2'),$$
$$k(v_1, v_1') = (kv_1, kv_1')$$

$\forall (v_1, v_1'), (v_2, v_2') \in V \times V'$ and $\forall k \in K$.

(i) We have seen that $V = K \times K$ has a canonical structure of vector space over K. Let us now see what happens if we change the addition or the scalar multiplication.
Let us first define them as follows:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, 2y_1 + 2y_2),$$
$$k \cdot (x_1, y_1) = (kx_1, ky_1)$$

$\forall (x_1, y_1), (x_2, y_2) \in V$ and $\forall k \in K$. Then V is still a vector space over K, with a different structure of vector space than the canonical one.
Now let us define them as follows:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$
$$k \cdot (x_1, y_1) = (kx_1, y_1)$$

$\forall (x_1, y_1), (x_2, y_2) \in V$ and $\forall k \in K$. In general, they do not define a structure of vector space for V over K, because the axiom (L_2) does not hold.

For instance, for $K = \mathbb{R}$, we have

$$(1+2)\cdot(3,4) = 3\cdot(3,4) = (9,4) \neq (9,8) = (3,4)+(6,4) = 1\cdot(3,4)+2\cdot(3,4).$$

Basic properties

We denote by 0 both the zero scalar and the zero vector.

Theorem

Let V be a vector space over K. Then $\forall k, k' \in K$ and $\forall v, v' \in V$:
(i) $k \cdot 0 = 0 \cdot v = 0$.
(ii) $k(-v) = (-k)v = -kv$.
(iii) $k(v - v') = kv - kv'$.
(iv) $(k - k')v = kv - k'v$.

Proof. We only prove (i) and (ii); the others are homework.

$$k \cdot 0 + k \cdot v = k(0 + v) = kv \Longrightarrow k \cdot 0 = 0,$$

$$0 \cdot v + k \cdot v = (0 + k)v = kv \Longrightarrow 0 \cdot v = 0.$$

$$kv + k(-v) = k(v - v) = k \cdot 0 = 0 \Longrightarrow k(-v) = -kv,$$

$$kv + (-k)v = (k - k)v = 0 \cdot v = 0 \Longrightarrow (-k)v = -kv.$$

Theorem

Let V be a vector space over K and let $k \in K$ and $v \in V$. Then:

$$kv = 0 \iff k = 0 \text{ or } v = 0\,.$$

Proof. $\boxed{\Longrightarrow}$ Assume that $kv = 0$. Suppose that $k \neq 0$. Then k is invertible in the field K and we have

$$kv = 0 \Longrightarrow kv = k \cdot 0 \Longrightarrow k^{-1}(kv) = k^{-1}(k \cdot 0)$$
$$\Longrightarrow (k^{-1}k)v = (k^{-1}k) \cdot 0 \Longrightarrow v = 0\,.$$

$\boxed{\Longleftarrow}$ This is true by the previous Theorem, part (i). □

Definition

Let V be a vector space over K and let $S \subseteq V$. Then S is a *subspace* of V if:
(i) $S \neq \emptyset$.
(ii) $\forall v_1, v_2 \in S$, $v_1 + v_2 \in S$.
(iii) $\forall k \in K$, $\forall v \in S$, $kv \in S$.

We usually denote by $S \leq_K V$, or simply by $S \leq V$, the fact that S is a subspace of the vector space V over K.

Notice that every subspace S of a vector space V over K is a subgroup of the additive group $(V, +)$, hence S must contain 0.

Characterization of subspaces

Theorem

Let V be a vector space over K and let $S \subseteq V$. Then

$$S \leq V \iff \begin{cases} S \neq \emptyset \quad (0 \in S) \\ \forall k_1, k_2 \in K\,,\ \forall v_1, v_2 \in S\,,\ k_1 v_1 + k_2 v_2 \in S\,. \end{cases}$$

Proof. $\boxed{\Longrightarrow}$ Taking $k = 0$ and $v_1 \in S \neq \emptyset$, we have $0 = 0 \cdot v_1 \in S$. Now let $k_1, k_2 \in K$ and $v_1, v_2 \in S$. Then we have $k_1 v_1, k_2 v_2 \in S$, and then $k_1 v_1 + k_2 v_2 \in S$.

$\boxed{\Longleftarrow}$ Choose $k_1 = k_2 = 1$ and then $k_2 = 0$ and to show that S is a subspace. $\square$

(a) Every non-zero vector space V over K has two subspaces, namely $\{0\}$ and V. They are called the *trivial subspaces*.

(b) Let us show that

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

are subspaces of the canonical real vector space $\mathbb{R}^3$ [...].
Note that S is a plane passing through the origin. For instance, the plane

$$\{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 1\}$$

is not a subspace of $\mathbb{R}^3$ over $\mathbb{R}$.
Note that T is a line passing through the origin.

(c) More generally, the only subspaces of $\mathbb{R}^3$ are $\{(0, 0, 0)\}$, any line containing the origin, any plane containing the origin and $\mathbb{R}^3$.

(d) Let $n \in \mathbb{N}$ and let

$$K_n[X] = \{f \in K[X] \mid \mathrm{degree}(f) \leq n\}.$$

Then $K_n[X]$ is a subspace of the polynomial vector space $K[X]$ over K. Note that the set $\{f \in K[X] \mid \mathrm{degree}(f) = n\}$ is not a subspace of $K[X]$ over K.

(e) Let $I \subseteq \mathbb{R}$ be an interval. We have seen that

$$\mathbb{R}^I = \{f \mid f : I \to \mathbb{R}\}$$

is a real vector space, where the addition and the scalar multiplication are defined as follows: $\forall f, g : I \to \mathbb{R}$, $\forall k \in K$, we have $f + g : I \to \mathbb{R}$, $kf : I \to \mathbb{R}$, where

$$\begin{aligned}(f+g)(x) &= f(x) + g(x)\,,\\ (kf)(x) &= kf(x)\,, \forall x \in I\,.\end{aligned}$$

Examples III

The subsets

$$C(I,\mathbb{R}) = \{f \in \mathbb{R}^I \mid f \text{ continuous on } I\},$$
$$D(I,\mathbb{R}) = \{f \in \mathbb{R}^I \mid f \text{ derivable on } I\}$$

are subspaces of $\mathbb{R}^I$, because they are nonempty and we have:

$$\forall k_1, k_2 \in \mathbb{R}, \forall f, g \in C(I,\mathbb{R}),\ k_1 f + k_2 g \in C(I,\mathbb{R}),$$

$$\forall k_1, k_2 \in \mathbb{R}, \forall f, g \in D(I,\mathbb{R}),\ k_1 f + k_2 g \in D(I,\mathbb{R}).$$

Extra: Vernam cipher I

Let $n \in \mathbb{N}^*$ and consider the canonical vector space $V = \mathbb{Z}_2^n$ over $\mathbb{Z}_2$. The vectors of V may be identified with n-bit binary strings.

Suppose that Alice needs to send an n-bit plaintext $p \in \mathbb{Z}_2^n$ to Bob.

Vernam cipher:

1. (*Key establishment*) Alice and Bob randomly choose a vector $k \in \mathbb{Z}_2^n$ as a key.
2. (*Encryption*) Alice computes the ciphertext c according to the formula $c = p + k$, where the sum is a vector in $\mathbb{Z}_2^n$.
3. (*Decryption*) Bob computes the plaintext p according to the formula $p = c - k = c + k$, where the sum is a vector in $\mathbb{Z}_2^n$.

The system satisfies perfect secrecy, but the key k must be distributed in advance.

Extra: Vernam cipher II

Example

Alice wants to send to Bob the message

$$p = (0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \in \mathbb{Z}_2^{10}.$$

Alice and Bob agree on the following vector as the key

$$k = (0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \in \mathbb{Z}_2^{10}.$$

Alice encrypts the message by computing the ciphertext c as:

$$c = p + k = (0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \in \mathbb{Z}_2^{10}.$$

Bob decrypts the message by computing the plaintext p as:

$$p = c + k = (0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \in \mathbb{Z}_2^{10}.$$