Lecture notes on linear algebra and geometry

Andrea Ferraguti

August 27, 2024

Disclaimer: If you find any mistake and/or typo in these lecture notes you can let me know at and.ferraguti@gmail.com.

Contents

Chapter 0: Basics

0.1 Sets

Throughout these lecture notes, a *set* will be an unordered collection of objects, without repetitions. The objects contained in a set are called *elements*. Elements of a set will be enclosed between curly brackets.

Example 0.1.1. $\{1, 2, \heartsuit, w\}$ is the set whose elements are $1, 2, \heartsuit$ and w. This is the same as $\{2, 1, w, \heartsuit\}$, because sets are *unordered* collections of objects, and it is the same as $\{1, 2, 2, w, w, w, \heartsuit\}$, because repetitions do not matter.

There is a special set, called *empty set*, that is a collection of zero objects. This is denoted by $\emptyset$.

Elements of a set can be listed one by one, as in the example above, or they can be described by a property that characterizes them.

Example 0.1.2. The *set of natural numbers* will be denoted by $\mathbb{N}$, and it is the set $\{0, 1, 2, \ldots\}$. The *set of integers* will be denoted by $\mathbb{Z}$, and it is the set $\{0, 1, -1, 2, -2, 3, -3, \ldots\}$. The *set of rational numbers* will be denoted by $\mathbb{Q}$, and it can be described as $\{a/b\colon a, b \in \mathbb{Z} \text{ and } b \neq 0\}$. The colons in the description of $\mathbb{Q}$ shall be read as "such as".

If s is an element of a set S, we write $s \in S$, and we say that s *belongs* to S. If this is not the case, namely if s is *not* an element of S, we write $s \notin S$.

The following symbols are fundamental standard notation in mathematics.

- The symbol $\forall$ means "for all";
- The symbol $\exists$ means "there exists".
- The symbol $\exists!$ means "there exists a unique".
- The symbol $\nexists$ means "it does not exist".
- The symbol $\iff$ means "if and only if". If P, Q are propositions, we write $P \iff Q$ to say that if P holds true, then so does Q and if Q holds true, then so does P.

Example 0.1.3. The following propositions hold true.

- $\forall x \in \mathbb{Z}$, $\exists\, y \in \mathbb{Z}$ such that $x + y > 0$.
- $\forall x \in \mathbb{Z}$, $\exists!\, y \in \mathbb{Z}$ such that $x + y = 0$.
- $\nexists x \in \mathbb{N}$ such that $x^2 = 2$.
- $\forall x \in \mathbb{Z}$, $x^2 \leq 4 \iff -2 \leq x \leq 2$

If S, T are sets, we say that S is a *subset* of T, and we write $S \subseteq T$, if every element of S is an element of T as well. For instance, $\mathbb{N} \subseteq \mathbb{Z}$. If, on the other hand, there exists an element of S that does *not* belong to T, we write $S \not\subseteq T$. For instance, $\mathbb{Q} \not\subseteq \mathbb{Z}$.

Remark 0.1.4. Every set S has at least two subsets: the empty set and S itself.

Definition 0.1.5. Two sets S, T are *equal* if $S \subseteq T$ and $T \subseteq S$. If this is the case, we write $S = T$.

For S, T sets, the following operations are allowed and produce a new set.

- The *intersection* of S, T is the set:

$$S \cap T \coloneqq \{s \colon s \in S \text{ and } s \in T\}.$$

  If $S \cap T = \emptyset$, we say that S and T are *disjoint*.

- The *union* of S and T is the set:

$$S \cup T \coloneqq \{s \colon s \in S \text{ or } s \in T\}.$$

- The *difference* of S and T is the set:

$$S \setminus T \coloneqq \{s \colon s \in S \text{ and } s \notin T\}.$$

Remark 0.1.6. Intersection and union are *commutative* operations, that is, $S \cap T = T \cap S$ and $S \cup T = T \cup S$. On the other hand, the difference is not commutative. For example, you can try to show that $\mathbb{Q} \setminus \mathbb{Z}$ and $\mathbb{Z} \setminus \mathbb{Q}$

are not equal.

Lemma 0.1.7. If S, T, U are sets, the following hold true.

1. $S \cap S = S \cup S = S$;
2. $S \cap \emptyset = \emptyset$;
3. $S \cup \emptyset = S$;
4. $(S \cap T) \cap U = S \cap (T \cap U)$;
5. $(S \cup T) \cup U = S \cup (T \cup U)$;
6. $S \subseteq T \iff S \cap T = S \iff S \cup T = T$;
7. $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$;
8. $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$.

Definition 0.1.8. Given two sets S, T, the *cartesian product* of S and T is the set $S \times T$ formed by all ordered pairs (s, t) such that $s \in S$ and $t \in T$. In symbols,

$$S \times T \coloneqq \{(s, t) \colon s \in S,\, t \in T\}.$$

Example 0.1.9. If $S = \{a, b\}$ and $T = \{1, 2, 3\}$ then

$$S \times T = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}.$$

If S, T, U are sets, the following properties hold true.

- $S \times \emptyset = \emptyset \times S = \emptyset$;
- If S and T are both nonempty, $S \times T = T \times S \iff S = T$;
- $S \times (T \cup U) = (S \times T) \cup (S \times U)$;
- $S \times (T \cap U) = (S \times T) \cap (S \times U)$.

It is possible to construct the cartesian product of more than two sets. Namely, if $n \geq 1$ is any natural number and $S_1, \dots, S_n$ are sets, we let:

$$S_1 \times S_2 \times \dots \times S_n \coloneqq \{(s_1, s_2, \dots, s_n) \colon s_i \in S_i \ \forall i \in \{1, 2, \dots, n\}\}.$$

If the n sets $S_1, S_2, \ldots, S_n$ are all equal to a set S, we write S^n for the cartesian product $S_1 \times \ldots \times S_n$.

0.2 Functions

Let S, T be sets.

Definition 0.2.1. A *correspondence* between S and T is a subset of $S \times T$. A *function* (or *map*) between S and T is a correspondence f between S and T such that for every $s \in S$ there exists a unique $t \in T$ such that $(s,t) \in f$.

Example 0.2.2. If $S = \{0,1\}$ and $T = \{a, \spadesuit, \sqrt{7}\}$, the following are correspondences between S and T:

1. $S \times T$;
2. $\emptyset$;
3. $\{(0,\spadesuit),(1,\spadesuit)\}$;
4. $\{(0,\spadesuit),(1,\sqrt{7}),(1,a)\}$.

However, only 3. is a function between S and T.

If $f \in S \times T$ is a function, we know that for every $s \in S$ there is a unique $t \in T$ with $(s,t) \in f$. Since such t only depends on s, we can write $t = f(s)$. Hence the function f coincides with the set $\{(s, f(s)) \colon s \in S\}$. With this picture in mind, we will write

$$f \colon S \to T$$

to denote that f is a function between S and T. In layman's terms, f is a "rule" that assigns to every s in S a unique element $t \in T$. Such element is referred to as the *image* of s via f, and we denote it by $f(s)$.

Note:-

In order to define a function between two sets S, T it is enough, by the above considerations, to describe the image of every element $S \in s$. This will be done by using the notation $s \mapsto f(s)$. For example, writing:

$$f \colon \mathbb{Z} \to \mathbb{N}$$

$$x \mapsto x^2$$

means that f is the function between $\mathbb{Z}$ and $\mathbb{N}$ that associates to every integer x then natural number x^2.

Definition 0.2.3. Let $f\colon S \to T$ be a function.

1. The set S is called *domain* of f, while the set T is called *codomain*.
2. f is called *injective* if for every $s_1, s_2 \in S$ with $s_1 \neq s_2$ we have $f(s_1) \neq f(s_2)$.
3. f is called *surjective* if for every $t \in T$ there exists $s \in S$ with $f(s) = t$.
4. f is called *bijective* if it is both injective and surjective.
5. If $S' \subseteq S$, the *image* of S' is the set $f(S') \coloneqq \{f(s)\colon s \in S'\}$.
6. If $T' \subseteq T$, the *preimage* of T' is the set $f^{-1}(T') = \{s \in S\colon f(s) \in T'\}$.

Example 0.2.4.

- The function $f\colon \mathbb{Z} \to \mathbb{Z}$ that sends $x \mapsto x^2$ is neither injective nor surjective.
- The function $f\colon \mathbb{Z} \to \mathbb{Z}$ that sends $x \mapsto x^3$ is injective but not surjective.
- The function $f\colon \mathbb{Q} \to \mathbb{Q}$ that sends $x \mapsto x/2$ is bijective.

If S is a set, a *sequence* of element of S is a function $a\colon \mathbb{N} \to S$. Images of elements in the domain, instead of being denoted by $a(0), a(1), a(2), \dots$ are often denoted by $a_0, a_1, a_2, \dots$.

A set is *infinite* if there exists an injective sequence $f\colon \mathbb{N} \to S$. If this is not the case, then S is *finite*.

Definition 0.2.5. If S is a set and $n \in \mathbb{N}$, an *n-tuple* of elements of S is a function $a\colon \{1, 2, \dots, n\} \to S$.

Once again if a is an n-tuple of elements of S, images of the elements in the domain are denoted by $a_1, a_2, \ldots, a_n$. Conversely, writing down n elements of S, say $(b_1, \ldots, b_n)$ automatically defines an n-tuple, that is the function $b\colon \{1, \ldots, n\} \to S$ that maps $i \mapsto b_i$. From now on, n-tuples of elements of a set S will be denoted by $(a_1, \ldots, a_n)$. Notice that order matters. For example, if $S = \mathbb{N}$ the triple $(12, 27, 32)$ differs from the triple $(27, 12, 32)$, because the first one is a function $\{1, 2, 3\} \to \mathbb{N}$ that maps 1 to 12, while the second one is a function $\{1, 2, 3\} \to \mathbb{N}$ that maps 1 to 27.

If S is finite and nonempty, then there exists a natural number $n \geq 1$ and a bijective function $f\colon \{1, 2, \ldots, n\} \to S$. The number n is called *cardinality* of the set S, and we write $|S| = n$.

Proposition 0.2.6 (Inclusion-exclusion principle)**.** Let $S_1, S_2, \ldots, S_n$ be finite sets. Then :

$$|S_1 \cup S_2 \cup \ldots \cup S_n| = \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} |S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_k}| \right)$$

Note:-

What Proposition 0.2.6 says is that in order to compute the cardinality of a union of finite sets, you must sum the cardinality of each single set, then subtract the cardinality of all intersections of two of them, then add the cardinality of all intersections of three of them, and so on. For example, if $n = 2$ then:

$$|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|,$$

and if $n = 3$ then

$$|S_1 \cup S_2 \cup S_3| =$$

$$= |S_1| + |S_2| + |S_3| - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| + |S_1 \cap S_2 \cap S_3|.$$

If $S_1, \ldots, S_n$ are pairwise disjoint, then $|S_1 \cup \ldots \cup S_n| = |S_1| + |S_2| + \ldots + |S_n|$.

Given two functions $f\colon S \to T$ and $g\colon T \to U$, one can create a third function, called *composition* of f and g. This is denoted by $g \circ f$ and it is defined as

$$g \circ f\colon S \to U$$
$$s \mapsto g(f(s))$$

Proposition 0.2.7. Let $f\colon S \to T$, $g\colon T \to U$ and $h\colon U \to W$ be functions. Then:

$$h \circ (g \circ f) = (h \circ g) \circ f,$$

that is, composition of functions is associative.

If S is a set, there always exists a function from S to itself, called *identity function*. This is defined by

$$\mathrm{id}_S\colon S \to S$$
$$s \mapsto s$$

We say that a function $f\colon S \to T$ is *invertible* if there exists a function $g\colon T \to S$ such that $g \circ f = \mathrm{id}_S$ and $f \circ g = \mathrm{id}_T$. We call g an *inverse function* for f.

Proposition 0.2.8. A function is invertible if and only if it is bijective. Moreover, the inverse function is unique.

We denote the inverse of a function f by f^{-1}.

0.3 The induction principle

The induction principle is a tool that can be used to prove propositions involving natural numbers. This works as follows. Suppose we want to prove a proposition $P(n)$ on the n-th natural number. If we can prove the following two facts:

1. $P(0)$ holds true;
2. if $P(k)$ holds true for a natural number k, then $P(k+1)$ holds true,

then it follows that $P(n)$ is true for *every* natural number n. We will now illustrate this principle with three very classical examples.

Proposition 0.3.1. Let n be a natural number. Then $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Proof. The proposition $P(n)$ that we want to prove is:

$$P(n)\colon \sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

We therefore need to prove two facts. The first one is that $P(0)$ holds true, i.e. we need to show that

$$\sum_{i=0}^{0} i = \frac{0(0+1)}{2}.$$

This is clearly true.

Next, we need to prove that if $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$ for some integer k then $\sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2}$. That is, our hypothesis is $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$ (we call this *inductive hypothesis*) and our thesis is $\sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2}$.

So let us assume the inductive hypothesis and let us look at $\sum_{i=0}^{k+1} i$. We can split this sum in two pieces, writing $\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + k + 1$. But now we can use our inductive hypothesis, and get

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + k + 1 = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2},$$

which is exactly what we needed to prove. □

Proposition 0.3.2. Let n be a natural number. Then $2^{2n} - 1$ is divisible by 3.

Proof. The proposition we want to prove is: $P(n)$: $2^{2n} - 1$ is divisible by 3.

Once again, we need to prove two things. The first one is that $2^{2\cdot 0} - 1$ is divisible by 3. This is obviously true. The second one is that if $2^{2k} - 1$ is divisible by 3 for some integer k (inductive hypothesis), then $2^{2(k+1)} - 1$ is also divisible by 3. So let us assume the inductive hypothesis and look at $2^{2(k+1)} - 1$. We have:

$$2^{2(k+1)} - 1 = 4 \cdot 2^{2k} - 1 = 4 \cdot (2^{2k} - 1 + 1) - 1 = 4 \cdot (2^{2k} - 1) + 3.$$

Now the inductive hypothesis implies that $4 \cdot (2^{2k} - 1)$ is a multiple of 3, and therefore also $4 \cdot (2^{2k} - 1) + 3$ is a multiple of 3. This is exactly what we needed to prove. □

Proposition 0.3.3. Let S be a finite set with $|S| = n$. Then S has exactly 2^n subsets.

Proof. When $n = 0$, S is a set with 0 elements, and hence it is the empty set $\emptyset$. The only subset of $\emptyset$ is $\emptyset$ itself, so S has $1 = 2^0$ subsetes.

Now we need to show that if a set of cardinality k has 2^k subsets (inductive hypothesis), then a set of cardinality $k+1$ has 2^{k+1} subsets. Let S be a set with $|S| = k+1$, and let $\mathcal{P}(S)$ be the set of all subsets of S. Now fix an element $s \in S$ (notice that this exists since S is not empty, since its cardinality is at least 1). Elements of $\mathcal{P}(S)$ are of two types: either they contain s or they do not. So we can write $\mathcal{P}(S) = T \cup T'$, where

$$T = \{U \subseteq S \colon s \in U\}$$

and

$$T' = \{U \subseteq S \colon s \notin U\}.$$

The elements of T' are precisely the subsets of $S \setminus \{s\}$. Since $|S \setminus \{s\}| = k$, we can use our inductive hypothesis: there are exactly 2^k subsets of $|S \setminus \{s\}| = k$, so $|T'| = 2^k$. On the other hand, there exists a bijection $T' \to T$, that is the map sending $U \mapsto U \cup \{s\}$. It follows that $|T| = |T'| = 2^k$. Now since $T \cap T' = \emptyset$, by Proposition 0.2.6 we get that $|\mathcal{P}(S)| = |T| + |T'| = 2^{k+1}$. □

0.4 Real and complex numbers

The *set of real numbers*, denoted by $\mathbb{R}$, is the set of all numbers of the form $a_0, a_1a_2a_3\ldots$, where $a_0 \in \mathbb{Z}$ and $a_i \in \{0, \ldots, 9\}$ for every $i \geq 1$. We refer to this form as *decimal expansion*. The set $\mathbb{R}$ can be defined in a formal way starting from $\mathbb{Q}$, but we are not interested in such construction in these notes.

Clearly $\mathbb{R}$ contains $\mathbb{Z}$; integers are real numbers of the form $a_0, a_1a_2\ldots$ with $a_i = 0$ for every $i \geq 1$. Moreover, $\mathbb{R}$ contains $\mathbb{Q}$. Rational numbers are exactly those with an eventually periodic decimal expansion, namely they are exactly the ones whose decimal expansion has the form $a_0, a_1 \ldots a_n\overline{a_{n+1}\ldots a_{n+t}}$ for some $n \geq 0$, $t \geq 1$. This means that the block of digits $a_{n+1}\ldots a_{n+t}$ keeps repeating itself, i.e. for every $m > n$ we have $a_m = a_{m+t}$.

Note:-

Although every real number has a decimal expansion, the representation of a real number as $a_0, a_1a_2a_3\ldots$ is *not* unique. In fact, for example, the two expressions $0, \overline{9}$ and $1, \overline{0}$ are different, but they represent the same real number.

The set of *complex numbers*, denoted by $\mathbb{C}$, is the set $\{a + bi \colon a, b \in \mathbb{R}\}$,

where i is a symbol such that $i^2 = -1$. Of course $\mathbb{C}$ contains $\mathbb{R}$; the latter is simply the subset $\{a + 0i \colon a \in \mathbb{R}\}$.

Note:-

The representation of a complex number as $a + bi$ for some reals a, b is unique. That is, $a + bi = c + di$ if and only if $a = c$ and $b = d$.

Complex numbers can be added and multiplied according to the following rules:

- $(a + bi) + (c + di) = (a + c) + (b + d)i$.
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

One can verify that addition and multiplication are commutative and associative.

There is a bijective map, called *conjugation*, defined as follows:

$$\bar{\cdot} \colon \mathbb{C} \to \mathbb{C}$$

$$a + bi \mapsto \overline{a + bi} \coloneqq a - bi$$

Conjugation has the property that $\overline{x + y} = \overline{x} + \overline{y}$ and $\overline{xy} = \overline{x} \cdot \overline{y}$ for every $x, y \in \mathbb{C}$. Moreover,

$$\mathbb{R} = \{x \in \mathbb{C} \colon \overline{x} = x\}. \tag{1}$$

0.5 Polynomials

Let K be a field (for the definition of field, see Definition 1.1.13). If you are not familiar yet with the concept of field, just think of K as to one among $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. A *polynomial* with coefficients in K is an expression of the form

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

where $a_i \in K$ for every $i \in \{0, \ldots, n\}$.

The *degree* of $p(x)$, denoted by $\deg p(x)$, is the largest index i such that $a_i \neq 0$. If there is no such index, then $p(x) = 0$, and we set by convention $\deg p(x) = -\infty$.

Note:-

Polynomials of degree 0 are non-zero constants, i.e. they are simply elements of K different from 0.

The set of all polynomials with coefficients in K will be denoted by $K[x]$.

Polynomials can be added and multiplied. Let $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{j=0}^{m} b_j x^j$ be two polynomials with coefficients in K. Now suppose that $n > m$ (the case $m > n$ is symmetric); then you can write $q(x) = \sum_{j=0}^{n} b_j x^j$, where $b_j = 0$ if $j \in \{m+1, \dots, n\}$. Then:

$$p(x) + q(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

and

$$p(x)q(x) = \sum_{k=0}^{2n} \left(\sum_{i,j\colon i+j=k} a_i b_j \right) x^k.$$

When we add up two polynomials, the degree of the sum is at most the largest degree between the two, namely

$$\deg(p(x) + q(x)) \leq \max\{\deg p(x), \deg q(x)\},$$

and equality holds if $\deg p(x) \neq \deg q(x)$. When we multiply two polyomials, their degrees add up:

$$\deg(p(x)q(x)) = \deg p(x) + \deg q(x).$$

If $p(x)$ is a polynomial with coefficients in K and $z \in K$, we can evaluate $p(x)$ at $x = z$. This simply means computing

$$p(z) \coloneqq a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n,$$

that is an element of K. Notice that if $p(x), q(x) \in K[x]$ and $z \in K$ then:

$$(p(x) + q(x))(z) = p(z) + q(z) \quad \text{and} \quad (p(x)q(x))(z) = p(z)q(z).$$

We say that z is a *root* of $p(x)$ if $p(z) = 0$. Polynomials of degree 0 have no roots.

Theorem 0.5.1. Let $p(x) \in K[x]$ have degree $n \geq 1$. If $z \in K$ is a root of $p(x)$, then there exists a unique integer $k \geq 1$ and a unique polynomial $q(x)$ of degree $n - k$ such that $q(z) \neq 0$ and $p(x) = (x - z)^k q(x)$.

The positive integer k whose existence is granted by Theorem 0.5.1 is called *multiplicity* of the root z.

Corollary 0.5.2. If $\deg p(x) = n \geq 1$ and $z_1, \ldots, z_r \in K$ are roots of $p(x)$, with multiplicities $k_1, \ldots, k_r$, respectively, then $k_1 + \ldots + k_r \leq n$. In particular, $r \leq n$.

In other words, a polynomial of degree n has at most n roots in K, even when each root is counted with its multiplicity.

Theorem 0.5.3 (Fundamental theorem of algebra)**.** Let $p(x) \in \mathbb{C}[x]$ be a polynomial of degree n. Then there exists unique complex numbers $z_1, \ldots, z_r$ and unique positive integers $k_1, \ldots, k_r$ such that

$$p(x) = (x - z_1)^{k_1} \ldots (x - z_r)^{k_r}.$$

In other words, a polynomial with complex coefficients of degree n has exactly n roots, when each is counted with its multiplicity.

Notice that since $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, then every degree n polynomial with coefficients in $\mathbb{Q}$ or in $\mathbb{R}$ has exactly n complex roots, when each is counted with its multiplicty.

Lemma 0.5.4. Let $p(x) \in \mathbb{R}[x]$ be a polynomial. If $\lambda \in \mathbb{C}$ is a root of p, then $\overline{\lambda}$ is a root of p as well.

0.6 Matrices

Let K be a field (for the definition of field, see Definition 1.1.13). If you are not familiar yet with the concept of field, just think of K as to one among $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Let $m, n \geq 1$ be integers.

Definition 0.6.1. An $m \times n$ matrix with coefficients in K is a function

$$A \colon \{1, \ldots, m\} \times \{1, \ldots, n\} \to K.$$

The image of a pair $(i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\}$ will be denoted by a_{ij}.

For practical purposes, we identify a matrix with its image, and we arrange the values of the function defining the matrix in a rectangular table with m rows and n columns. That is, an $m \times n$ matrix A is a table of the following

form:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

To ease the notation, we sometimes will write $A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$ to say that A is an $m \times n$ matrix whose entry in row i and column j is a_{ij}.

The set of all $m \times n$ matrices with coefficients in K is denoted by $M_{m\times n}(K)$. If $m = n$, we shorten the notation by just writing $M_n(K)$. Matrices belonging to $M_n(K)$ are called *square matrices of size n*.

Any two elements of $M_{m\times n}(K)$ can be added, as follows. Given

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \text{ and } B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix}$$

we let

$$A + B \coloneqq \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}.$$

Matrices could, in principle, be multiplied entry-by-entry, similarly to the way we add them. However, this multiplication will <u>not</u> be used anywhere in these lecture notes. On the other hand, we will now define a matrix multiplication that can be performed <u>only</u> between an $m \times n$ and an $n \times p$ matrix, where m, n and p are positive integers. If $A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}} \in M_{m\times n}(K)$ and $B = (b_{ij})_{\substack{i=1,\dots,n \\ j=1,\dots,p}} \in M_{n\times p}(K)$, the matrix AB is the matrix $(c_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,p}} \in M_{m\times p}(K)$ where for every $i \in \{1, \dots, m\}$ and every $j \in \{1, \dots, p\}$:

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

In other words, to find the entry in row i and column j of the matrix AB, we need to take the i-th row of A (that has n entries) and the n-th column of B

(that also has n entries), multiply the corresponding entries (the entry in the i-th row and k-th column of A must be multiplied with the entry in the k-th row and j-th column of B), and add up all the results.

Note:-

Given matrices A and B, the product AB makes sense only when the number of columns of A equals the number of rows of B.

Example 0.6.2.

- Let $A \coloneqq \begin{pmatrix} 2 & 3 & 1 \\ -1 & 0 & 1 \end{pmatrix} \in M_{2\times 3}(\mathbb{R})$ and $B \coloneqq \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} \in M_{3\times 1}(\mathbb{R})$.

  Then $AB = \begin{pmatrix} 10 \\ 1 \end{pmatrix} \in M_{2\times 1}(\mathbb{R})$.

- Let $A \coloneqq \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Q})$ and $B \coloneqq \begin{pmatrix} 1 & 1 & -1 \\ 0 & 0 & 3 \end{pmatrix} \in M_{2\times 3}(\mathbb{Q})$.

  Then $AB = \begin{pmatrix} 2 & 2 & 4 \\ 0 & 0 & 0 \end{pmatrix} \in M_{2\times 3}(\mathbb{Q})$.

- The matrices $A \coloneqq \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{C})$ and $B \coloneqq \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} \in M_{3\times 1}(\mathbb{C})$

  cannot be multiplied, since A has two columns and B has 3 rows.

Remark 0.6.3. If $A, B \in M_n(K)$, then both products AB and BA make sense. However, in general, the two results are different from each other. That is, multiplication of matrices is not commutative.

We close this section with a few definitions that will be used later on.

Definition 0.6.4. Let K be a field and $n \geq 1$ an integer.

1. The *identity matrix* is the matrix $I_n = (a_{ij})_{i,j} \in M_n(K)$ defined by $a_{ij} = 1$ if $i = j$ and 0 otherwise.
2. $A = (a_{ij}) \in M_n(K)$ is a *diagonal matrix* if $a_{ij} = 0$ whenever $i \neq j$.
3. $A = (a_{ij}) \in M_n(K)$ is *upper triangular* if $a_{ij} = 0$ whenever $i > j$.
4. $A = (a_{ij}) \in M_n(K)$ is *lower triangular* if $a_{ij} = 0$ whenever $i < j$.

Example 0.6.5.

- The identity matrix $I_3 \in M_3(K)$ is:

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

- The matrix

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -\sqrt{2} \end{pmatrix}$$

  is diagonal.

- The matrix

$$A \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & -1 \end{pmatrix}$$

  is upper triangular.

- The matrix
$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ -7 & 3 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ \pi & 0 & 22 & 0 \end{pmatrix}$$
is lower triangular.

Remark 0.6.6. If $A \in M_n(K)$, then $AI_n = I_nA = A$.

Definition 0.6.7. Let K be a field.

1. Let $A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}} \in M_{m\times n}(K)$. The *transpose matrix* is the matrix ${}^tA = (b_{ji})_{\substack{j=1,\dots,n \\ i=1,\dots,m}} \in M_{n\times m}(K)$ defined by $b_{ji} = a_{ij}$ for every $i \in \{1,\dots,m\}$ and $j \in \{1,\dots,n\}$.
2. Let $A \in M_n(K)$ be a square matrix. A is called *symmetric* if $A = {}^tA$, and is called *antisymmetric* if $A = -{}^tA$.

Example 0.6.8.

- Let
$$A \coloneqq \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 7 \end{pmatrix}.$$
Then
$${}^tA = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ -3 & 7 \end{pmatrix}.$$
- Let
$$A \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}.$$

Then

$$ {}^tA = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}. $$

- Let

$$ A \coloneqq \begin{pmatrix} 1 & 2 & 0 \\ 5 & 6 & 7 \\ \pi & 8 & \sqrt{6} \end{pmatrix}. $$

Then

$$ {}^tA = \begin{pmatrix} 1 & 5 & \pi \\ 2 & 6 & 8 \\ 0 & 7 & \sqrt{6} \end{pmatrix}. $$

- The matrix

$$ \begin{pmatrix} 1 & 0 & -2 \\ 0 & 2 & -3 \\ -2 & -3 & 0 \end{pmatrix} $$

is symmetric.

Remark 0.6.9.

1. If $A \in M_{m\times n}(K)$, then ${}^t({}^tA) = A$.
2. If $A, B \in M_{m\times n}(K)$, then ${}^t(A+B) = {}^tA + {}^tB$.
3. if $A \in M_{m\times n}(K)$ and $B \in M_{n\times p}(K)$, then ${}^t(AB) = {}^tB{}^tA$.

Chapter 1: Vector spaces

In this chapter we will introduce the fundamental objects of linear algebra, namely vector spaces.

1.1 Groups and fields

Let S be a set.

Definition 1.1.1. An *operation* on S is a function $\star\colon S \times S \to S$. An operation $\star$ on S is called:

1. *associative* if for every $a, b, c \in S$ we have $(a \star b) \star c = a \star (b \star c)$;
2. *commutative* if for every $a, b \in S$ we have $a \star b = b \star a$.

Example 1.1.2.

- Addition is an associative and commutative operation on $\mathbb{N}$. Subtraction is not an operation on $\mathbb{N}$, because the difference of two natural numbers is not always a natural number.
- Subtraction is an operation on $\mathbb{Z}$, but it is not associative (for example, $1 - (2 - 2) \neq (1 - 2) - 2$) nor commutative (for example, $1 - 2 \neq 2 - 1$).

Definition 1.1.3. Let S be a set and $\star$ be an operation on S. An element $e \in S$ is called a *neutral element* for $\star$ if $a \star e = e \star a = a$ for every $a \in S$.

Example 1.1.4. 0 is a neutral element for the operation $+$ on $\mathbb{Q}$. 1 is a neutral element for the operation $\cdot$ on $\mathbb{R}$.

Lemma 1.1.5. Let S be a set and $\star$ an operation on S. A neutral element for $\star$, if it exists, is unique.

Proof. Let e, e' be neutral elements for $\star$. Then $e \star e' = e$ since e' is neutral, but also $e \star e' = e'$ since e is neutral. Hence $e = e'$. □

Definition 1.1.6. Let S be a set and $\star$ be an operation on S with neutral element e. Let $a \in S$. We say that an element $b \in S$ is an *inverse* of a if $a \star b = b \star a = e$.

Lemma 1.1.7. Let S be a set and $\star$ be an associative operation on S with neutral element e. Let $a \in S$. If there exists an inverse of a, then it is unique.

Proof. Let $b, b' \in S$ be such that $a \star b = e = a \star b'$. Multiplying both sides of this equality by b we get that $b \star (a \star b) = b \star (a \star b')$. Since $\star$ is associative, it follows that $(b \star a) \star b = (b \star a) \star b'$. Since b is an inverse of a, we have $b \star a = e$ and hence $e \star b = e \star b'$. Since e is neutral, $b = b'$ follows. □

Example 1.1.8. Addition is an associative and commutative operation on $\mathbb{C}$. The neutral element is 0, and every element $a + bi$ has the unique inverse $-a - bi$.

Definition 1.1.9. A *group* is a pair $(G, \star)$ where G is a nonempty set and $\star$ is an operation on G that satisfies the following properties:

1. $\star$ is associative;
2. there exists a neutral element e;
3. every element in G has an inverse.

If, in addition, $\star$ is commutative we say that the group $(G, \star)$ is *abelian*. If $\star$ is not commutative, we say that $(G, \star)$ is *non-abelian*.

Example 1.1.10.

- The pair $(\mathbb{Q}, +)$ is an abelian group. The set $(\mathbb{Q}, \cdot)$ is not an abelian group, because 0 does not possess an inverse.
- The pair $(\mathbb{C} \setminus \{0\}, \cdot)$ is an abelian group. In fact, every non-zero complex number $a + bi$ has the multiplicative inverse $\frac{a-bi}{a^2+b^2}$.

- If S is a finite set, the set

$$\{f\colon S \to S \text{ s.t. } f \text{ is bijective}\}$$

is a non-abelian group, when endowed with the operation "composition of functions". In fact, the composition of two bijective functions is bijective, composition is associative by Proposition 0.2.7, the identity function is the neutral element, and every element is invertible by Proposition 0.2.8.

Remark 1.1.11. The fact that an operation $\star$ on G is associative implies that we can omit brackets when we apply it several times in a row. Namely, the writing

$$g_1 \star g_2 \star \ldots \star g_n$$

makes sense because we can compute the operations in the order we prefer, and the result does not change. For example,

$$g_1 \star (g_2 \star (g_3 \star g_4))) = (g_1 \star g_2) \star (g_3 \star g_4).$$

Lemma 1.1.12. Let $(G, \star)$ be a group and let $a, b, c \in G$. If $a \star b = a \star c$, then $b = c$.

Proof. Let a' be the inverse of a. Since $a \star b = a \star c$, it follows that $a' \star (a \star b) = a' \star (a \star c)$. Since $\star$ is associative, we get $(a' \star a) \star b = (a' \star a) \star c$, and since $a' \star a$ is the neutral element, it follows $b = c$. □

From now on, we will denote by $+$ or $\cdot$ operations on groups, where $+$ will only be used in abelian groups while $\cdot$ can be used in both settings. When the operation is denoted by $+$, we denote by 0 the neutral element and by $-a$ the inverse of a. When the operation is denoted by $\cdot$ we denote by 1 the neutral element and by a^{-1} the inverse of a.

Definition 1.1.13. A *field* is a triple $(K, +, \cdot)$, where K is a nonempty set and $+, \cdot$ are two operations on K that satisfy the following properties:

1. $(K, +)$ is an abelian group;
2. $(K \setminus \{0\}, \cdot)$ is an abelian group;

3. for every $a, b, c \in K$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example 1.1.14. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields with the usual operations of sum and multiplication. $\mathbb{Z}$ is not a field with respect to the usual sum and multiplication because elements different from ± 1 do not have a multiplicative inverse.

The set $\mathbb{F}_2 \coloneqq \{0, 1\}$ is a field when endowed with the following two operations:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Remark 1.1.15. If $(K, +, \cdot)$ is a field, then K must contain at least the neutral element for the operation $+$, that we denote by 0, and the neutral element for the operation $\cdot$, that we denote by 1. These two elements cannot coincide, because the definition of field requires $(K \setminus \{0\}, \cdot)$ to be an abelian group, and groups are nonempty sets. Therefore, a field always contains at least two distinct elements, 0 and 1. The field $\mathbb{F}_2$ described in the above example is therefore the smallest possible example of a field.

From now on, we will denote fields just by the letter K, tacitly implying that the operations on K are $+$ and $\cdot$. Moreover, we will frequently drop the multiplication sign in fields. That is, if $a, b \in K$ we will write ab instead of $a \cdot b$.

Note:-

When K is a field, we denote by 0 the neutral element with respect to the operation $+$ and by 1 the neutral element with respect to the operation $\cdot$.

Definition 1.1.16. Let K be a field. A *vector space over* K or a *K-vector space* is an abelian group $(V, +)$ endowed with a map

$$*\colon K \times V \to V$$

that satisfies the following properties:

1. for every $\alpha \in K$ and every $v, w \in V$, $\alpha * (v + w) = \alpha * v + \alpha * w$;
2. for every $\alpha, \beta \in K$ and every $v \in V$, $(\alpha\beta) * v = \alpha * (\beta * v)$.
3. for every $\alpha, \beta \in K$ and every $v \in V$, $(\alpha + \beta) * v = \alpha * v + \beta * v$;
4. for every $v \in V$, $1 * v = v$.

Elements of V are called *vectors*, and will be denoted by underlined letters, such as $\underline{v}, \underline{w}, \underline{u}$. In particular, the neutral element of $(V, +)$ is denoted by $\underline{0}$ and is called *zero vector*. Elements of K are called *scalars*.

Note:-

Addition in K and addition in V are both denoted by $+$. However, beware of the fact that these are different operations, since one is a function $K \times K \to K$ and the other one is a function $V \times V \to V$. Therefore, an expression of the form $\alpha + \underline{v}$, where $\alpha \in K$ and $\underline{v} \in V$, does not make any sense.

Note:-

While $\underline{0}$ denotes the zero vector, namely the neutral element of the group $(V, +)$, we denote by 0 the neutral element of the group $(K, +)$. Hence these are two very different objects, do not confuse them!

Example 1.1.17. Let $V = \{\underline{0}\}$ be the abelian group that possesses only one element, the neutral element with respect to the operation $+$ on V. This is a K-vector space over any field K, the operation $*$ being defined by $\alpha * \underline{0} = \underline{0}$ for every $\alpha \in K$. This is the simplest possible vector space, although not a very interesting one.

There are several important examples of vector spaces, but for the sake of these lecture notes the most important is by far the following one.

Example 1.1.18. We let K be any field, n be a positive integer and $V := K^n$, that is, V is the set of all n-tuples of elements of K. V is an abelian group with respect to the following operation:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

Now we define the following operation:

$$*\colon K \times V \to V$$

$$(\alpha, (a_1, \dots, a_n)) \mapsto (\alpha a_1, \dots, \alpha a_n)$$

Let us check that, for example, property 1. of the definition of a vector space is indeed satisfied. In order to do that, we need to take an arbitrary $\alpha \in K$ and two vectors $\underline{v} = (v_1, \dots, v_n)$ and $\underline{w} = (w_1, \dots, w_n)$ in V and prove that $\alpha * (\underline{v} + \underline{w}) = \alpha * \underline{v} + \alpha * \underline{w}$. Now

$$\underline{v} + \underline{w} = (v_1 + w_1, v_2 + w_2, \dots, v_n + w_n)$$

and hence

$$\alpha * (\underline{v} + \underline{w}) = (\alpha(v_1 + w_1), \alpha(v_2 + w_2), \dots, \alpha(v_n + w_n)) =$$

$$= (\alpha v_1 + \alpha w_1, \alpha v_2 + \alpha w_2, \dots, \alpha v_n + \alpha w_n).$$

On the other hand,

$$\alpha * \underline{v} = (\alpha v_1, \alpha v_2, \dots, \alpha v_n) \text{ and } \alpha * \underline{w} = (\alpha w_1, \alpha w_2, \dots, \alpha w_n).$$

Hence

$$\alpha \underline{v} + \alpha \underline{w} = (\alpha v_1 + \alpha w_1, \alpha v_2 + \alpha w_2, \dots, \alpha v_n + \alpha w_n) = \alpha * (\underline{v} + \underline{w}),$$

as desired. It is a very useful exercise for the reader to verify that properties 2., 3. and 4. are satisfied as well.

Notice that when $n = 1$ we have $V = K$. When this happens, operation $*$ coincides with multiplication in K. Therefore, every field K, seen as an abelian group with respect to the sum, is a vector space over K.

Example 1.1.19. Let $n \geq 1$ be an integer and K be a field. Let

$$K[x]_{\leq n} = \{p(x) \in K[x] \colon \deg p(x) \leq n\}.$$

This is the set of all polynomials with coefficients in K of degree at most n. The set $K[x]_{\leq n}$ is an abelian group with respect to addition of poly-

nomials, and it is a vector space over K with respect to the operation

$$*\colon K \times K[x]_{\leq n} \to K[x]_{\leq n}$$

$$\left(\alpha, \sum_{i=0}^{n} a_i x^i\right) \mapsto \sum_{i=0}^{n} (\alpha a_i) x^i$$

Example 1.1.20. Let $n \geq 1$ be an integer and K be a field. The set $M_n(K)$ of all $n \times n$ matrices with coefficients in K is an abelian group with respect to the sum of matrices. The group $(M_n(K), +)$ can be given a structure of vector space over K via the following operation:

$$*\colon K \times M_n(K) \to M_n(K)$$

$$(\alpha, (a_{ij})_{i,j=1,\dots,n}) \mapsto (\alpha a_{ij})_{i,j=1,\dots,n}.$$

Theorem 1.1.21. Let V be a vector space over a field K. Let $\alpha \in K$ and $\underline{v} \in V$. Then $\alpha * \underline{v} = \underline{0}$ if and only if $\underline{v} = \underline{0}$ or $\alpha = 0$.

Proof. First, we show that if $\alpha = 0$ or $\underline{v} = \underline{0}$ then $\alpha * \underline{v} = \underline{0}$. Let us start by assuming that $\alpha = 0$. Since $0 + 0 = 0$ (because 0 is the neutral element with respect to the sum in K), we have that

$$0 * \underline{v} = (0 + 0) * \underline{v} = 0 * \underline{v} + 0 * \underline{v},$$

using property 3. of Definition 1.1.16.

Now $0 * \underline{v} = 0 * \underline{v} + \underline{0}$, and therefore we can rewrite the above equality as:

$$0 * \underline{v} + \underline{0} = 0 * \underline{v} + 0 * \underline{v}.$$

Now we can apply Lemma 1.1.12 in the group $(V, +)$ and conclude that $0 * \underline{v} = \underline{0}$.

Next, suppose that $\underline{v} = \underline{0}$. Since $\underline{0} + \underline{0} = \underline{0}$ (because $\underline{0}$ is the neutral element with respect to the sum in V), we have that

$$\alpha * \underline{0} = \alpha * (\underline{0} + \underline{0}) = \alpha * \underline{0} + \alpha * \underline{0},$$

using property 1. of Definition 1.1.16.

Since $\alpha * \underline{0} = \alpha * \underline{0} + \underline{0}$, the above equality becomes

$$\alpha * \underline{0} + \underline{0} = \alpha * \underline{0} + \alpha * \underline{0},$$

and we can apply Lemma 1.1.12 and conclude that $\alpha * \underline{0} = \underline{0}$.

Conversely, we must show that if $\alpha * \underline{v} = \underline{0}$ then $\alpha = 0$ or $\underline{v} = \underline{0}$. So suppose that $\alpha \neq 0$; we will show that $\underline{v} = \underline{0}$. In fact, since $\alpha \neq 0$ then there exists a multiplicative inverse α^{-1} of α. Starting from the equality $\alpha * \underline{v} = \underline{0}$, we get:

$$\alpha^{-1} * (\alpha * \underline{v}) = \alpha^{-1} * \underline{0}.$$

Now on the one hand in the first part of the proof we proved that $\alpha^{-1} * \underline{0} = \underline{0}$. On the ohter hand we can use properties of vector spaces given by Definition 1.1.16, and get:

$$\underline{0} = \alpha^{-1} * \underline{0} = \alpha^{-1} * (\alpha * \underline{v}) = (\alpha^{-1}\alpha) * \underline{v} = 1 * \underline{v} = \underline{v},$$

that is, $\underline{v} = \underline{0}$. □

Corollary 1.1.22. If K is a field and $a, b \in K$ are such that $ab = 0$, then $a = 0$ or $b = 0$.

Proof. As noticed in Example 1.1.18, every field is a vector space over itself, with the operation $*$ coinciding with multiplication in K. Hence it is enough to apply Theorem 1.1.21 to such setting. □

Corollary 1.1.23. Let V be a K-vector space. Then for every $\underline{v} \in V$ we have $(-1) * \underline{v} = -\underline{v}$.

Proof. By Theorem 1.1.21 and the properties of vector spaces, we have that:

$$\underline{0} = 0 * \underline{v} = (1 - 1) * \underline{v} = 1 * \underline{v} + (-1) * \underline{v} = \underline{v} + (-1) * \underline{v},$$

that is, $(-1) * \underline{v} = -\underline{v}$. □

From now on, when V is a vector space over a field K with respect to some operation $*\colon K \times V \to V$, we will denote by $\cdot$ multiplication between scalars and vectors, and we will often drop the multiplication sign. That is, if $\alpha \in K$ and $\underline{v} \in V$, we will write $\alpha \cdot \underline{v}$ or $\alpha\underline{v}$ instead of $\alpha * \underline{v}$.

1.2 Linear combinations and subspaces

Definition 1.2.1. Let V be a vector space over a field K. Let $\underline{v}_1, \dots, \underline{v}_n \in V$ and $\alpha_1, \dots, \alpha_n \in K$. The *linear combination of* $\underline{v}_1, \dots, \underline{v}_n$ *with coefficients* $\alpha_1, \dots, \alpha_n$ is the vector:

$$\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_n \underline{v}_n \in V.$$

Example 1.2.2. Let $V = \mathbb{R}^2$, let $\underline{v}_1 = (0,1)$, $\underline{v}_2 = (1,-1)$ and $\underline{v}_3 = (2,2)$ be vectors. Let $\alpha_1 = 1$, $\alpha_2 = 2$, $\alpha_3 = 0$ be scalars. The linear combination of $\underline{v}_1, \underline{v}_2, \underline{v}_3$ with coefficients $\alpha_1, \alpha_2, \alpha_3$ is the vector

$$1 \cdot (0,1) + 2 \cdot (1,-1) + 0 \cdot (2,2) = (2,-1) \in V.$$

Definition 1.2.3. Let $(V, +)$ be an abelian group.

1. Let $W \subseteq V$ be a nonempty subset. W is called a *subgroup* of V if $(W, +)$ is an abelian group.
2. Let K be a field and let $*\colon K \times V \to V$ be an operation that makes V into a vector space over K. A subset $W \subseteq V$ is called a *vector subspace* of V if:
   (a) $(W, +)$ is an abelian group;
   (b) W is a K-vector space with respect to the operation $*$.

Example 1.2.4.

- Let $(V, +) := (\mathbb{Z}, +)$. The subset

  $$2\mathbb{Z} := \{n \in \mathbb{Z} \colon 2 \text{ divides } n\}$$

  is a subgroup of $\mathbb{Z}$. In fact, the sum of two multiples of 2 is a multiple of 2, there is a neutral element, namely 0, and the inverse of a multiple of 2 is a multiple of 2.

  On the other hand, the subset $2\mathbb{Z}+1 = \{n \in \mathbb{Z} \colon 2 \text{ does not divide } n\}$

is not a subgroup of $\mathbb{Z}$, since $+$ is not an operation on $2\mathbb{Z}+1$: the sum of two odd numbers is even.

- Let $(V,+) \coloneqq (K^2,+)$, with the sum being defined coordinatewise. As we have seen in Example 1.1.18, this is a K-vector space. The subset $W = \{(x,x)\colon x \in K\} \subseteq K^2$ is a vector subspace of V. Let us first verify that $(W,+)$ is a subgroup of $(V,+)$. If $(x,x),(y,y) \in W$, then $(x,x)+(y,y) = (x+y,x+y)$, that is an element of W since its two entries coincide. Hence $+$ is an operation on W. Clearly since $+$ is associative on V it is also associative on W. The neutral element for the sum on V is $(0,0)$, that belongs to W. Hence it is the neutral element for the sum on W. Finally, the inverse of an element $(x,x) \in W$ is $(-x,-x)$, that belongs again to W.

  Next, $\lambda(x,x) = (\lambda x, \lambda x) \in K^2$ for every $\lambda \in K$ and $(x,x) \in W$. Hence the operation $K \times V \to V$ given by $(\lambda,(x,y)) \mapsto (\lambda x, \lambda y)$ restricts to an operation on W that makes the latter into a K-vector space.

  On the other hand, the subset $U = \{(x,1)\colon x \in K\} \subseteq V$ is not a vector subspace of V, since $(U,+)$ is not a subgroup of $(V,+)$: in fact, it has no neutral element.

Lemma 1.2.5. Let $(G,\cdot)$ be a group, and let $H \subseteq G$. Then $(H,\cdot)$ is a subgroup if and only if for every $g,h \in H$ we have $g \cdot h^{-1} \in H$.

Proof. First, if H is a subgroup then given $g,h \in H$, the inverse of h, that is h^{-1}, must also belong to H, and the product $g \cdot h^{-1}$ must belong to H as well, since $\cdot$ is an operation on H.

Conversely, suppose that for every $g,h \in H$ the product $g \cdot h^{-1}$ belongs to H. We need to prove that $\cdot$ is an operation on H, that the neutral element 1 is in H and that if $h \in H$, then $h^{-1} \in H$. Notice that the fact that $\cdot$ is associative is obvious, since it is associative on G. If $g \in H$, then the hypothesis guarantees that $1 = g \cdot g^{-1} \in H$, and therefore H contains the neutral element. Therefore, if $h \in H$ then the same hypothesis guarantees that $h^{-1} = 1 \cdot h^{-1} \in H$, so H contains inverses of every element. Finally, if $g,h \in H$ then we have just proved that $h^{-1} \in H$ and so $g \cdot h = g \cdot (h^{-1})^{-1} \in H$ by the hypothesis, completing the proof. □

Theorem 1.2.6. Let V be a vector space over a field K and let $W \subseteq V$ be a non-empty subset. Then W is a vector subspace of V if and only if for every $\underline{v}_1, \underline{v}_2 \in W$ and every $\alpha_1, \alpha_2 \in K$ we have:

$$\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 \in W.$$

Proof. First, suppose that W is a subspace of V. Let $\underline{v}_1, \underline{v}_2 \in V$ and $\alpha_1, \alpha_2 \in K$. We need to prove that $\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 \in W$. Since W is a vector space with respect to the same operation that makes V into a K-vector space, we have that $\alpha_1 \underline{v}_1 \in W$ and $\alpha_2 \underline{v}_2 \in W$. On the other hand $(W, +)$ is a subgroup of $(V, +)$, and therefore for every $\underline{w}_1, \underline{w}_2 \in W$ we have that $\underline{w}_1 + \underline{w}_2 \in W$. If we pick $\underline{w}_1 = \alpha_1 \underline{v}_1$ and $\underline{w}_2 = \alpha_2 \underline{v}_2$, we get precisely that $\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 \in W$.

Conversely, suppose that for every $\underline{v}_1, \underline{v}_2 \in W$ and every $\alpha_1, \alpha_2 \in K$ we have $\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 \in W$. We need to prove that W is a subspace of V. This amounts to proving that $(W, +)$ is a subgroup of $(V, +)$ and that multiplication by scalars of K makes W into a K-vector space. We start by proving that $(W, +)$ is a subgroup of $(V, +)$. By Lemma 1.2.5, it is enough to show that for every $\underline{w}_1, \underline{w}_2 \in W$ we have $\underline{w}_1 - \underline{w}_2 \in W$. By hypothesis, given $\underline{w}_1, \underline{w}_2 \in W$, if we let $\alpha_1 = 1$ and $\alpha_2 = -1$ we have $\alpha_1 \underline{w}_1 + \alpha_2 \underline{w}_2 = \underline{w}_1 + (-1)\underline{w}_2 \in W$. By Corollary 1.1.23, it follows that $\underline{w}_1 - \underline{w}_2 \in W$. Hence $(W, +)$ is a subgroup of $(V, +)$. In order to prove that W is a vector space, we only need to prove that for every $\alpha \in K$ and every $\underline{w} \in W$ the vector $\alpha \underline{w}$ belongs to W. In fact, properties $1., \ldots, 4.$ of Definition 1.1.16 are automatically satisfied for W, since they are satisfied for V by hypothesis. Now if $\alpha \in K$ and $\underline{w} \in W$, the hypothesis guarantees that $\alpha \underline{w} = \alpha \cdot \underline{w} + 0 \cdot \underline{w} \in W$, as we needed to prove. □

Corollary 1.2.7. If W is a vector subspace of a K-vector space V, then for every $n \geq 1$, every $\alpha_1, \ldots, \alpha_n \in K$ and every $\underline{v}_1, \ldots, \underline{v}_n \in W$ we have:

$$\alpha_1 \underline{v}_1 + \ldots + \alpha_n \underline{v}_n \in W.$$

Proof. We use induction on n. For $n = 1$, the statement is true because $\alpha_1 \underline{v}_1 = \alpha_1 \underline{v}_1 + 0 \cdot \underline{v}_1$, and the latter belongs to W by Theorem 1.2.6. Now suppose that the claim is true for $n - 1$ vectors, and let $\alpha_1, \ldots, \alpha_n \in K$

and $\underline{v}_1, \dots, \underline{v}_n \in V$. Then

$$\alpha_1\underline{v}_1 + \dots + \alpha_n\underline{v}_n = (\alpha_1\underline{v}_1 + \dots + \alpha_{n-1}\underline{v}_{n-1}) + \alpha_n\underline{v}_n.$$

Now $\alpha_1\underline{v}_1 + \dots + \alpha_{n-1}\underline{v}_{n-1} \in W$ by the inductive hypothesis, and hence there exists $\underline{w} \in W$ such that $\alpha_1\underline{v}_1 + \dots + \alpha_{n-1}\underline{v}_{n-1} = \underline{w}$. Hence

$$\alpha_1\underline{v}_1 + \dots + \alpha_n\underline{v}_n = \underline{w} + \alpha_n\underline{v}_n,$$

and $\underline{w} + \alpha_n\underline{w}_n = 1 \cdot \underline{w} + \alpha_n\underline{v}_n$ belongs to W thanks to Theorem 1.2.6. □

Note:-

If V is a K-vector space and $W \subseteq V$ is a vector subspace, then $\underline{0} \in W$. In fact, in particular W is a subgroup of $(V, +)$ and therefore it must contain the neutral element for the sum on V. Hence, if $W \subseteq V$ is a subset with $\underline{0} \notin W$, then W is <u>not</u> a vector subspace of V.

Example 1.2.8. Using Theorem 1.2.6 it is easy to give examples of vector subspaces.

- Let K be a field and $V \coloneqq K^3$. Let

  $$W = \{(x, y, z) \in V : x + y + z = 0\}.$$

  Then W is a vector subspace of V. In fact, if $\alpha, \beta \in K$ and $(x, y, z), (x', y', z') \in W$, then $x + y + z = x' + y' + z' = 0$ and since

  $$\alpha(x, y, z) + \beta(x', y', z') = (\alpha x + \beta x', \alpha y + \beta y', \alpha z + \beta z')$$

  we get that

  $$\alpha x + \beta x' + \alpha y + \beta y' + \alpha z + \beta z' = \alpha(x + y + z) + \beta(x' + y' + z') = 0,$$

  so that $\alpha(x, y, z) + \beta(x', y', z') \in W$. Hence W is a vector subspace of V.

- Let K be a field, $n \geq 1$ be an integer and $V \coloneqq K[x]_{\leq n}$. The set

  $$W = \{p(x) \in V : p(0) = 0\}$$

is a vector subspace. In fact, if $p(x), q(x) \in W$ and $\alpha, \beta \in K$ then $(\alpha p(x) + \beta q(x))(0) = \alpha p(0) + \beta q(0) = 0 + 0 = 0$, and hence $\alpha p(x) + \beta q(x) \in W$. It follows that W is a vector subspace of V.

- Let K be a field, $n \geq 1$ and $M_n(K)$ the K-vector space of $n \times n$ matrices with entries in K. The subset $T \subseteq V$ of upper triangular matrices (see Definition 0.6.4) is a vector subspace. In fact, let $M = (a_{ij})_{i,j=1,\dots,n}$ and $M' = (a'_{ij})_{i,j=1,\dots,n}$ be elements of T. Then $a_{ij} = a'_{ij} = 0$ for every $i > j$. If $\alpha, \beta \in K$, the matrices αM and $\beta M'$ are still upper triangular, as $\alpha M = (\alpha a_{ij})_{i,j=1,\dots,n}$ and $\beta M' = (\beta a'_{ij})_{i,j=1,\dots,n}$. On the other hand, the sum of two upper triangular matrices is clearly upper triangular, and hence $\alpha M + \beta M' \in T$. Similarly, the set of lower triangular matrices and the set of diagonal matrices are vector subspaces of $M_n(K)$.

Definition 1.2.9. Let V be a K-vector space and let $A \subseteq V$ be a nonempty subset. The *span* of A is the set

$$\langle A \rangle := \left\{ \sum_{i=1}^{n} \alpha_i \underline{v}_i \colon n \in \mathbb{N}, \alpha_i \in K, \underline{v}_i \in A \right\}.$$

In other words, the span of A is the set of all linear combinations of all elements of A.

Remark 1.2.10. Clearly $A \subseteq \langle A \rangle$. In fact, every $\underline{v} \in \mathbb{A}$ can be seen as the linear combination $1 \cdot \underline{v}$, and being a linear combination of elements of A (in this case just one element), it belongs to $\langle A \rangle$.

Theorem 1.2.11. Let $A \subseteq V$ be a nonempty subset. Then $\langle A \rangle$ is a vector subspace of V.

Proof. Let $\sum_{i=1}^{n} \alpha_i \underline{v}_i$ and $\sum_{j=1}^{m} \beta_j \underline{w}_j$ be two elements of $\langle A \rangle$, so that $\underline{v}_i, \underline{w}_j \in A$ and $\alpha_i, \beta_j \in K$ for every i, j. Let $\lambda, \mu \in K$. Then

$$\lambda \sum_{i=1}^{n} \alpha_i \underline{v}_i + \mu \sum_{j=1}^{m} \beta_j \underline{w}_j = (\lambda\alpha_1)\underline{v}_1 + \ldots + (\lambda\alpha_n)\underline{v}_n + (\mu\beta_1)\underline{w}_1 + \ldots + (\mu\beta_m)\underline{w}_m,$$

that is again a linear combination of vectors of A, and therefore it is by definition an element of $\langle A \rangle$. It follows by Theorem 1.2.6 that $\langle A \rangle$ is a subspace of V. □

Proposition 1.2.12. Let V be a K-vector space and $A \subseteq V$. Then

$$\langle A \rangle = \bigcap_{\substack{W \subseteq V \text{ subsp.} \\ A \subseteq W}} W.$$

In other words, the span of A is the intersection of all vector subspaces of V that contain A.

Proof. In order to prove that two sets are equal, we need to prove that each is contained in the other one.

So first, suppose that $\underline{v} \in \langle A \rangle$. We need to show that if W is a subspace that contains A, then $\underline{v} \in W$. By definition, $\underline{v} = \sum_{i=1}^{n} \alpha_i \underline{v}_i$ for some $\underline{v}_1, \dots, \underline{v}_n \in A$ and $\alpha_1, \dots, \alpha_n \in K$. If $A \subseteq W$, then $\underline{v}_1, \dots, \underline{v}_n \in W$ and since subspaces are closed with respect to linear combinations (see Corollary 1.2.7), it follows that $\underline{v} \in W$.

Conversely, let $\underline{v}$ be a vector belonging to every subspace of V that contains A. Since $\langle A \rangle$ is a vector subspace of V by Theorem 1.2.11, and it contains A by Remark 1.2.10, it follows that $\underline{v} \in \langle A \rangle$. □

What Proposition 1.2.12 says is that the span of a subset $A \subseteq V$ is the smallest vector subspace of V that contains A.

Proposition 1.2.13. Let V be a K-vector space and let $A, B \subseteq V$ be non-empty subsets.

1. If $A \subseteq B$, then $\langle A \rangle \subseteq \langle B \rangle$.
2. $A = \langle A \rangle$ if and only if A is a vector subspace of V.

Proof. 1. The set $\langle B \rangle$ is a vector subspace of V, and therefore it is closed under linear combinations of elements of B. Since $A \subseteq B$ and $B \subseteq \langle B \rangle$, it follows that $\langle B \rangle$ must contain all linear combinations of elements of A, as well. That is, $\langle A \rangle \subseteq \langle B \rangle$.

2. If $A = \langle A \rangle$, since the right hand side is a vector subspace by Theorem 1.2.11, then so is the left hand side.

Conversely, if A is a vector subspace then it is closed under linear combinations of its elements, and hence it contains $\langle A \rangle$. □

Definition 1.2.14. Let V be a K-vector space and let $W \subseteq V$ be a subspace. A subset $A \subseteq W$ is called a *system of generators* for W if $\langle A \rangle = W$. The space V is said to be *finitely generated* (f.g. for short) if there exists a finite system of generators for V.

In other words, A is a system of generators for W if every vector in W can be written as a linear combination of vectors in A.

Example 1.2.15.

- The vector space K^n is finitely generated, and the set

$$\{(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}$$

  is a set of generators. In fact, for every $\underline{v} = (a_1, \dots, a_n) \in K^n$ we can write:

$$\underline{v} = a_1(1, 0, \dots, 0) + a_2(0, 1, 0, \dots, 0) + \dots + a_n(0, \dots, 0, 1),$$

  i.e. every vector of V is a linear combination of

$$(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1).$$

- The vector space $K[x]_{\leq n}$ of polynomials of degree $\leq n$ is finitely generated. In fact, if $p(x) = \sum_{i=0}^{n} a_i x^i$ then $p(x)$ is a linear combination of the $n+1$ polynomials $1, x, x^2, \dots, x^n$ with coefficients $a_0, \dots, a_{n+1}$.

- The vector space $K[x]$ of all polynomials with coefficients in K is not finitely generated. In fact, suppose $A = \{p_1(x), \dots, p_n(x)\}$ is a set of generators. Then every polynomial of $K[x]$ would be a linear combination of the $p_i(x)$'s. But the degree of a linear combination of elements of A is at most the maximum of the degrees of the elements of A, since $\deg(\alpha p(x) + \beta q(x)) \leq \max\{\deg p(x), \deg q(x)\}$. Hence if $f(x) \in K[x]$ is a polynomial of degree larger than $\max\{\deg p_i(x)\}$ then $f(x)$ cannot be a linear combination of elements of A.

Proposition 1.2.16. Let V be a K-vector space. Let $W \subseteq V$ be a finitely generated vector subspace, and let $\{\underline{w}_1, \dots, \underline{w}_n\} \subseteq W$ be a system of generators for W. Let $\underline{v}_0 \in V$ and

$$U \coloneqq \{\underline{v}_0 + \underline{w} \colon \underline{w} \in W\}$$

be the translated of W by $\underline{v}_0$. Then $\langle U \rangle = \langle \underline{v}_0, \underline{w}_1, \dots, \underline{w}_n \rangle$.

Proof. Let $\underline{u} \in \langle U \rangle$. By definition of span there exist an integer $m \geq 1$, scalars $\alpha_1, \dots, \alpha_m \in K$ and vectors $\underline{u}_1, \dots, \underline{u}_m \in U$ such that $\underline{u} = \sum_{i=1}^{m} \alpha_i \underline{u}_i$. Now by definition of U, every $\underline{u}_i$ has the form $\underline{v}_0 + \underline{v}_i$ for some $\underline{v}_i \in W$. Hence,

$$\underline{u} = (\alpha_1 + \ldots + \alpha_m)\underline{v}_0 + \sum_{i=1}^{m} \alpha_i \underline{v}_i. \tag{2}$$

On the other hand, W is spanned by $\underline{w}_1, \dots, \underline{w}_n$, and therefore for every $i \in \{1, \dots, m\}$ there exist $\beta_{i1}, \dots, \beta_{in}$ such that $\underline{v}_i = \sum_{j=1}^{n} \beta_{ij} \underline{w}_j$. Substituting in (2), we get that:

$$\underline{u} = (\alpha_1 + \ldots + \alpha_m)\underline{v}_0 + \sum_{j=1}^{n} \left(\sum_{i=1}^{m} \alpha_i \beta_{ij} \right) \underline{w}_j,$$

so that $\underline{u}$ is an element of $\langle \underline{v}_0, \underline{w}_1, \dots, \underline{w}_n \rangle$.

Conversely, let $\underline{u} = \alpha_0 \underline{v}_0 + \sum_{i=1}^{n} \alpha_i \underline{w}_i \in \langle \underline{v}_0, \underline{w}_1, \dots, \underline{w}_n \rangle$. Notice that $\underline{v}_0 \in U$, because we can write $\underline{v}_0$ as $\underline{v}_0 + \underline{0}$, that is in U by definition. Moreover, for every $\underline{w} \in W$ we have $-\underline{w} \in W$ and hence $\underline{v}_0 - \underline{w} \in W$. Therefore, for every $\underline{w} \in W$ we have that:

$$\underline{w} = \underline{v}_0 - (\underline{v}_0 - \underline{w}) \in \langle U \rangle,$$

because vector subspaces are closed under linear combinations. It follows that every $\underline{w}_i$ is in $\langle U \rangle$, and since the latter is a vector subspace then $\sum_{i=1}^{n} \alpha_i \underline{w}_i \in \langle U \rangle$ and $\alpha_0 \underline{v}_0 \in \langle U \rangle$. This implies that $\underline{u} = \alpha_0 \underline{v}_0 + \sum_{i=1}^{n} \alpha_i \underline{w}_i \in \langle U \rangle$. □

1.3 Linear dependence and linear independence

Definition 1.3.1. Let K be a field and V be a K-vector space. Let $\underline{v}_1, \dots, \underline{v}_n \in V$.

1. We say that the vectors $\underline{v}_1, \dots, \underline{v}_n$ are *linearly dependent* if there exist $\alpha_1, \dots, \alpha_n \in K$ with at least one α_i different from 0 such that:
$$\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_n \underline{v}_n = \underline{0}.$$
2. We say that the vectors $\underline{v}_1, \dots, \underline{v}_n$ are *linearly independent* if given $\alpha_1, \dots, \alpha_n \in K$, the equality $\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_n \underline{v}_n = \underline{0}$ implies that $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$.

In other words, n vectors $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent if the only linear combination of them that yields the zero vector is $0\underline{v}_1 + 0\underline{v}_2 + \dots + 0\underline{v}_n$. They are linearly dependent if there exists a linear combination of them that yields the zero vector with not all the coefficients equal to 0. Therefore, $\underline{v}_1, \dots, \underline{v}_n$ are either linearly dependent or linearly independent, they cannot be both dependent and independent at the same time.

Example 1.3.2. Let $V = \mathbb{R}^3$. The vectors $\underline{v}_1 = (1,0,0)$, $\underline{v}_2 = (0,1,0)$ and $\underline{v}_3 = (1,1,0)$ are linearly dependent. In fact, the linear combination $1 \cdot \underline{v}_1 + 1 \cdot \underline{v}_2 + (-1) \cdot \underline{v}_3$ equals the zero vector. The vectors $\underline{v}_1$ and $\underline{v}_2$, on the other hand, are linearly independent. In fact, suppose that $\alpha, \beta \in K$ are such that $\alpha \underline{v}_1 + \beta \underline{v}_2 = \underline{0}$. Since $\alpha \underline{v}_1 = (\alpha, 0, 0)$ and $\beta \underline{v}_2 = (0, \beta, 0)$, we must have that $(\alpha, \beta, 0) = \underline{0} = (0,0,0)$. This implies clearly that $\alpha = \beta = 0$. Hence, the only linear combination of $\underline{v}_1$ and $\underline{v}_2$ that yields the zero vector is that with both coefficients equal to 0.

Remark 1.3.3.

1. A single vector $\underline{v} \in V$ is linearly dependent if and only if it is the zero vector. In fact, if $\underline{v} = \underline{0}$ then the linear combination $1 \cdot \underline{v}$ equals $\underline{0}$, and its coefficient is not zero, and therefore $\underline{v}$ is linearly dependent. Conversely, if $\underline{v}$ is linearly dependent then by definition there exists $\alpha \in K$ with $\alpha \neq 0$ such that $\alpha \underline{v} = \underline{0}$. By Theorem 1.1.21, it follows that $\underline{v} = \underline{0}$.
2. Of course the notion of linear dependence/independence does not de-

pend on the order of the vectors. That is, if for example $\underline{v}_1, \underline{v}_2, \underline{v}_3$ are linearly dependent then so are $\underline{v}_2, \underline{v}_3, \underline{v}_1$. Formally, if $\underline{v}_1, \dots, \underline{v}_n \in V$ and $\sigma \colon \{1, \dots, n\} \to \{1, \dots, n\}$ is a bijection, then $\underline{v}_1, \dots, \underline{v}_n$ are linearly dependent if and only if $\underline{v}_{\sigma(1)}, \dots, \underline{v}_{\sigma(n)}$ are linearly dependent.

Proposition 1.3.4. Let V be a K-vector space and $\underline{v}_1, \dots, \underline{v}_n \in V$. Then the following hold.

1. If $\underline{v}_i = \underline{0}$ for some $i \in \{1, \dots, n\}$, then $\underline{v}_1, \dots, \underline{v}_n$ are linearly dependent.
2. If there exist $i, j \in \{1, \dots, n\}$ with $i \neq j$ and $\alpha \in K$ such that $\underline{v}_i = \alpha \underline{v}_j$, then $\underline{v}_1, \dots, \underline{v}_n$ are linearly dependent.
3. $\underline{v}_1, \dots, \underline{v}_n$ are linearly dependent if and only if there exists $i \in \{1, \dots, n\}$ and $\alpha_1, \dots, \alpha_{i-1}, \alpha_{i+1}, \dots, \alpha_n \in K$ such that
$$\underline{v}_i = \alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_{i-1} \underline{v}_{i-1} + \alpha_{i+1} \underline{v}_{i+1} + \dots + \alpha_n \underline{v}_n.$$
4. If $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent and $\underline{v} \in V$, then $\underline{v}_1, \dots, \underline{v}_n, \underline{v}$ are linearly dependent if and only if there exist $\alpha_1, \dots, \alpha_n \in K$ such that
$$\underline{v} = \alpha_1 \underline{v}_1 + \dots + \alpha_n \underline{v}_n.$$
5. If $\underline{v}_1, \dots, \underline{v}_n$ are linearly dependent, then given any other m vectors $\underline{w}_1, \dots, \underline{w}_m \in V$, the vectors $\underline{v}_1, \dots, \underline{v}_n, \underline{w}_1, \dots, \underline{w}_m$ are linearly dependent.
6. If $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent, then for every choice of indexes $i_1 < i_2 < \dots < i_m \subseteq \{1, \dots, n\}$, the vectors $\underline{v}_{i_1}, \dots, \underline{v}_{i_m}$ are linearly independent.

Proof. 1. We have
$$0 \cdot \underline{v}_1 + 0 \cdot \underline{v}_2 + \dots + 0 \cdot \underline{v}_{i-1} + 1 \cdot \underline{v}_i + 0 \cdot \underline{v}_{i+1} + \dots + 0 \cdot \underline{v}_n = \underline{0},$$
and hence there is a linear combination of the vectors that gives $\underline{0}$ without all coefficients being 0.

2. By hypothesis, we have $1 \cdot \underline{v}_i + (-\alpha)\underline{v}_j = \underline{0}$. Therefore,

$$1 \cdot \underline{v}_i + (-\alpha)\underline{v}_j + \sum_{\substack{k=1 \\ k \neq i,j}}^{n} 0 \cdot \underline{v}_k = \underline{0}$$

is a linear combination of the vectors yielding $\underline{0}$ whose coefficients are not all 0.

3. Suppose that $\underline{v}_1, \dots, \underline{v}_n$ are linearly dependent. This means that there exist $\alpha_1, \dots, \alpha_n \in K$ not all zero such that $\sum_{j=1}^{n} \alpha_j \underline{v}_j = \underline{0}$. Let $i \in \{1, \dots, n\}$ be an index such that $\alpha_i \neq 0$. Then

$$\alpha_i \underline{v}_i = -\alpha_1 \underline{v}_1 - \dots - \alpha_{i-1}\underline{v}_{i-1} - \alpha_{i+1}\underline{v}_{i+1} - \dots - \alpha_n \underline{v}_n,$$

and multiplying both sides by α_i^{-1} we obtain:

$$\underline{v}_i = -(\alpha_i^{-1}\alpha_1)\underline{v}_1 - \dots - (\alpha_i^{-1}\alpha_{i-1})\underline{v}_{i-1} - (\alpha_i^{-1}\alpha_{i+1})\underline{v}_{i+1} - \dots - (\alpha_i^{-1}\alpha_n)\underline{v}_n.$$

Conversely, if

$$\underline{v}_i = \alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_{i-1}\underline{v}_{i-1} + \alpha_{i+1}\underline{v}_{i+1} + \dots + \alpha_n \underline{v}_n$$

for some $\alpha_1, \dots, \alpha_n \in K$ then

$$\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 + \dots + \alpha_{i-1}\underline{v}_{i-1} + (-1) \cdot \underline{v}_i + \alpha_{i+1}\underline{v}_{i+1} + \dots + \alpha_n \underline{v}_n = \underline{0}$$

is a linear combination of the $\underline{v}_i$'s yielding the zero vector without all coefficients being 0 (since the coefficient of $\underline{v}_i$ is -1).

4. First, suppose that $\underline{v}_1, \dots, \underline{v}_n, \underline{v}$ are linearly dependent. Then we have:

$$\sum_{i=1}^{n} \alpha_i \underline{v}_i + \beta \underline{v} = \underline{0} \tag{3}$$

for some $\alpha_1, \dots, \alpha_n, \beta \in K$ not all zero. Now if it was $\beta = 0$, then at least one α_i would be non-zero, and hence (3) would imply that $\underline{v}_1, \dots, \underline{v}_n$ are linearly dependent, contradicting the hypothesis. Hence, $\beta \neq 0$. Then (3) implies that:

$$\underline{v} = -(\beta^{-1}\alpha_1)\underline{v}_1 - \dots - (\beta^{-1}\alpha_n)\underline{v}_n,$$

proving the claim.

Conversely, if there exist $\alpha_1, \dots, \alpha_n$ such that $\underline{v} = \sum_{i=1}^{n} \alpha_i \underline{v}_i$, then by point 3. the vectors $\underline{v}_1, \dots, \underline{v}_n, \underline{v}$ are linearly dependent.

5. Let $\alpha_1, \dots, \alpha_n \in K$ be not all zero and such that $\sum_{i=1}^n \alpha_i \underline{v}_i = \underline{0}$. Then

$$\sum_{i=1}^{n} \alpha_i \underline{v}_i + 0 \cdot \underline{w}_1 + \dots + 0 \cdot \underline{w}_m = \underline{0},$$

proving that $\underline{v}_1, \dots, \underline{v}_n, \underline{w}_1, \dots, \underline{w}_m$ are linearly dependent.

6. Suppose by contradiction that there are vectors $\underline{v}_{i_1}, \dots, \underline{v}_{i_m}$, with $i_1 < \dots < i_m$ that are linearly dependent. Then there exist $\beta_{i_1}, \dots, \beta_{i_m} \in K$ not all zero such that $\sum_{j=1}^m \beta_{i_j} \underline{v}_{i_j} = \underline{0}$. Now for every $i \in \{1, \dots, n\}$ let

$$\alpha_i = \begin{cases} 0 & \text{if } i \notin \{i_1, \dots, i_m\} \\ \beta_{i_j} & \text{if } i = i_j \text{ for some } j \in \{1, \dots, m\} \end{cases}$$

and consider the linear combination $\sum_{i=1}^n \alpha_i \underline{v}_i$. This clearly yields the zero vector, since it can be written as $\sum_{j=1}^m \beta_{i_j} \underline{v}_{i_j} + \sum_{i \notin \{i_1, \dots, i_m\}} 0 \cdot \underline{v}_i$, and its coefficients are not all zero, since at least one of the β_{i_j} is nonzero. It follows that $\underline{v}_1, \dots, \underline{v}_n$ are linearly dependent, contradicting the hypothesis. □

Remark 1.3.5. Point 4. of Proposition 1.3.4 implies the following: if $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent and $\underline{w} \notin \langle \underline{v}_1, \dots, \underline{v}_n \rangle$, then $\underline{v}_1, \dots, \underline{v}_n, \underline{w}$ are linearly independent as well. In fact if they were not then by 4. it would follow $\underline{w} = \sum_{i=1}^n \alpha_i \underline{v}_i$ for some $\alpha_1, \dots, \alpha_n \in K$, so that $\underline{w} \in \langle \underline{v}_1, \dots, \underline{v}_n \rangle$.

1.4 Bases and dimension

Definition 1.4.1. Let V be a f.g. K-vector space. A *basis* of V is an n-tuple of vectors of V that are linearly independent and generate V.

Note:-

Bases are ordered, and therefore will be wrapped in round brackets. That is, if $(\underline{v}_1, \underline{v}_2, \underline{v}_3)$ is a basis of a vector space V, then $(\underline{v}_2, \underline{v}_1, \underline{v}_3)$ is still a basis, since the concepts of linear dependence and of generation do not depend on the order, but it is a different basis.

We will now prove that every finitely generated vector space has a basis, and any two bases have the same cardinality. This requires some preliminary results.

Lemma 1.4.2. Let V be a f.g. K-vector space. Let $\{\underline{v}_1, \dots, \underline{v}_n\}$ be a system of generators for V. If $\underline{v}_n$ is a linear combination of $\underline{v}_1, \dots, \underline{v}_{n-1}$, then $\{\underline{v}_1, \dots, \underline{v}_{n-1}\}$ is a system of generators for V.

Proof. Let $\alpha_1, \dots, \alpha_{n-1} \in K$ be such that

$$\underline{v}_n = \sum_{i=1}^{n-1} \alpha_i \underline{v}_i. \tag{4}$$

Now let $\underline{v} \in V$. Since $\{\underline{v}_1, \dots, \underline{v}_n\}$ is a system of generators for V, there exist $\beta_1, \dots, \beta_n \in K$ such that $\underline{v} = \sum_{i=1}^{n} \beta_i \underline{v}_i$. Substituting (4) into this relation, we obtain that:

$$\underline{v} = \beta_1 \underline{v}_1 + \dots + \beta_{n-1} \underline{v}_{n-1} + \beta_n \left(\sum_{i=1}^{n-1} \alpha_i \underline{v}_i \right) =$$

$$= (\beta_1 + \beta_n \alpha_1) \underline{v}_1 + (\beta_2 + \beta_n \alpha_2) \underline{v}_2 + \dots + (\beta_{n-1} + \beta_n \alpha_{n-1}) \underline{v}_{n-1},$$

so that $\underline{v}$ is a linear combination of $\underline{v}_1, \dots, \underline{v}_{n-1}$. This means precisely that $\{\underline{v}_1, \dots, \underline{v}_{n-1}\}$ is a system of generators for V. □

Lemma 1.4.3. Let V be a f.g. K-vector space with $V \neq \{\underline{0}\}$. Let $A = \{\underline{v}_1, \dots, \underline{v}_n\} \subseteq V$ be a system of generators for V. Then there exists a subset $B \subseteq A$ that is a linearly independent system of generators for V.

Proof. By induction on n. If $n = 1$ then $A = \{\underline{v}_1\}$ and it cannot be $\underline{v}_1 = \underline{0}$ because $V \neq \{\underline{0}\}$. Hence $\underline{v} \neq \underline{0}$, and by Remark 1.3.3, it follows that $\underline{v}$ is linearly independent. Hence A is a linearly independent set of generators.

Now suppose that the claim is true for $n-1$, and let $A = \{\underline{v}_1, \dots, \underline{v}_n\}$ be a set of generators for V. If A is linearly independent, there is nothing to prove. Otherwise, A is linearly dependent, and therefore by Proposition 1.3.4 one of the vectors in A is a linear combination of the others. Up to permuting the elements of A, we can assume that $\underline{v}_n$ is a linear combination of $\underline{v}_1, \dots, \underline{v}_{n-1}$. By Lemma 1.4.2, the set $A' = \{\underline{v}_1, \dots, \underline{v}_{n-1}\}$ is a system of generators for V. Since it has $n-1$ elements, by the inductive hypothesis it contains a linearly independent system of generators B. But $B \subseteq A$, and hence we are done. □

Corollary 1.4.4. Let V be a f.g. K-vector space. Then V has a basis.

Proof. Since V is f.g., there exists a finite system of generators $\{\underline{v}_1, \dots, \underline{v}_n\}$. By Lemma 1.4.3 this contains a linearly independent system of generators, i.e. a basis. □

Lemma 1.4.5 (Steinitz lemma)**.** Let V be a f.g. K-vector space with $V \neq \{\underline{0}\}$ and let $A = \{\underline{v}_1, \dots, \underline{v}_n\}$ be a system of generators for V. If $B = \{\underline{w}_1, \dots, \underline{w}_m\} \subseteq V$ is a set of linearly independent vectors, then $m \leq n$.

Proof. By contradiction, suppose that $m > n$. Since A generates V, there exist $\alpha_1, \dots, \alpha_n$ such that

$$\underline{w}_1 = \sum_{i=1}^{n} \alpha_i \underline{v}_i. \tag{5}$$

Since B is a set of linearly independent vectors, it cannot contain the zero vector by Proposition 1.3.4. Therefore, the α_i's cannot be all equal to zero. Up to permuting the $\underline{v}_i$'s, we can assume that $\alpha_1 \neq 0$. Then by (5) we get:

$$\underline{v}_1 = -\alpha_1^{-1}\underline{w}_1 - (\alpha_1^{-1}\alpha_2)\underline{v}_2 - \dots - (\alpha_1^{-1}\alpha_n)\underline{v}_n.$$

In other words, $\underline{v}_1$ is a linear combination of the vectors $\underline{w}_1, \underline{v}_2, \dots, \underline{v}_n$. Now since A generates V, then so does $A \cup \{\underline{w}_1\}$. But then by Lemma 1.4.2 the set $\{\underline{w}_1, \underline{v}_2, \dots, \underline{v}_n\}$ is a system of generators for V.

Since $\{\underline{w}_1, \underline{v}_2, \dots, \underline{v}_n\}$ generates V, the vector $\underline{w}_2$ is a linear combination of $\underline{w}_1, \underline{v}_2, \dots, \underline{v}_n$. Hence there exist $\alpha_1, \dots, \alpha_n$ such that

$$\underline{w}_2 = \alpha_1\underline{w}_1 + \alpha_2\underline{v}_2 + \dots + \alpha_n\underline{v}_n.$$

Now if it was $\alpha_2 = \alpha_3 = \dots = \alpha_n = 0$ then we would have $\underline{w}_2 = \alpha_1\underline{w}_1$ and by Proposition 1.3.4 the set B would be linearly dependent, yielding a contradiction. Hence, at least one among $\alpha_2, \dots, \alpha_n$ must be non-zero. Again without loss of generality we can assume that $\alpha_2 \neq 0$. Then, reasoning as above, we get

$$\underline{v}_2 = -\alpha_2^{-1}\alpha_1\underline{w}_1 + \alpha_2^{-1}\underline{w}_2 - \alpha_2^{-1}\alpha_3\underline{v}_3 + \dots + \alpha_2^{-1}\alpha_n\underline{v}_n,$$

and it follows that $\{\underline{w}_1, \underline{w}_2, \underline{v}_3, \dots, \underline{v}_n\}$ is a system of generators for V. Repeating this argument for $\underline{w}_3, \dots, \underline{w}_n$ we end up proving that $\{\underline{w}_1, \dots, \underline{w}_n\}$ generates V. Since we are assuming that $m > n$, the vector $\underline{w}_{n+1}$ is a linear combination of $\underline{w}_1, \dots, \underline{w}_n$, and hence the vectors $\underline{w}_1, \dots, \underline{w}_{n+1}$ are linearly dependent by Proposition 1.3.4, and consequently so are $\underline{w}_1, \dots, \underline{w}_m$. This contradicts the hypothesis, and therefore it must be $m \leq n$. □

Corollary 1.4.6. Let V be a f.g. K-vector space. Let $\mathcal{B}$ and $\mathcal{B}'$ be two bases of V. Then $|\mathcal{B}| = |\mathcal{B}'|$.

Proof. Let $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_n)$ and $\mathcal{B}' = (\underline{w}_1, \dots, \underline{w}_m)$. By the definition of basis, $\{\underline{v}_1, \dots, \underline{v}_n\}$ is a system of generators and $\underline{w}_1, \dots, \underline{w}_m$ are linearly independent. By Steinitz Lemma, it must be $m \leq n$. But one can argue symmetrically: $\{\underline{w}_1, \dots, \underline{w}_m\}$ is a system of generators and the vectors $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent. By Steinitz lemma then we have $n \leq m$, and hence $n = m$. □

Note:-

It can be proven that any vector space, not necessarily finitely generated, has a basis, and that any two bases have the same cardinality. However, the proof requires the axiom of choice, and is beyond the goal of these lecture notes.

Definition 1.4.7. Let V be a f.g. K-vector space with $V \neq \{\underline{0}\}$. The *dimension* of V is the cardinality of any basis of V. If V has dimension n we write $\dim V = n$.

Note:-

By convention, we say that the trivial vector space $\{\underline{0}\}$ has dimension 0. Vector spaces different from this always have dimension ≥ 1.

Example 1.4.8.

- Let $V = K^n$. The sequence $(\underline{e}_1, \underline{e}_2, \dots, \underline{e}_n)$ is a basis of V, where $\underline{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$ is the vector whose i-th entry is 1 and whose other entries are 0. In fact, as we have seen in Example

1.2.15 the $\underline{e}_i$'s generate V. Moreover, they are linearly independent, because $\sum_{i=1}^n \alpha_i \underline{e}_i = (\alpha_1, \dots, \alpha_n)$, and hence if the latter is the zero vector, then clearly $\alpha_i = 0$ for every i. It follows that

$$\dim K^n = n.$$

However, this is not the only basis of K^n; in fact if K is infinite there are infinitely many bases. For example, when $K = \mathbb{R}$ and $n = 3$ then the sequence $(\underline{v}_1, \underline{v}_2, \underline{v}_3)$ with $\underline{v}_1 = (1, 1, 0)$, $\underline{v}_2 = (0, 1, 1)$, $\underline{v}_3 = (1, 0, 0)$ is a basis of $\mathbb{R}^3$.

- Let $V = \mathbb{R}^2$. The set $\{\underline{v}_1, \underline{v}_2, \underline{v}_3\}$, where $\underline{v}_1 = (1, 1)$, $\underline{v}_2 = (1, 0)$ and $\underline{v}_3 = (-1, 1)$, is a system of generators for V but it is not a basis. In fact, since $\dim V = 2$ a basis must have 2 elements, and by Steinitz Lemma three vectors must be linearly dependent. A linear dependence relation between them is, for example, $\underline{v}_1 - 2\underline{v}_2 - \underline{v}_3 = \underline{0}$.

- Let $V = K[x]_{\leq n}$. As we have seen in Example 1.2.15, the set $\{1, x, \dots, x^n\}$ is a system of generators for V. It is easy to see that the sequence $(1, x, \dots, x^n)$ is in fact a basis of V, since these vectors are linearly independent; if $\sum_{i=1}^n \alpha_i x^i = 0$, we must have $\alpha_i = 0$ for every i: a polynomial is 0 if and only if all of its coefficients are 0. Hence
$$\dim V = n + 1.$$

- Let $V = M_{m\times n}(K)$. A basis of V is given by the sequence
$$(E_{11}, E_{12}, \dots, E_{1n}, E_{21}, E_{22}, \dots, E_{mn}),$$
where E_{ij} is the matrix whose entry in row i and column j is 1 and all other entries are 0. It follows that
$$\dim V = mn.$$

Definition 1.4.9. In the vector space K^n, the *canonical basis* is the basis $(\underline{e}_1, \dots, \underline{e}_n)$ introduced in Example 1.4.8.

Remark 1.4.10. The K-vector spaces $M_{n\times 1}(K)$ and $M_{1\times n}(K)$ of $n \times 1$ and $1 \times n$ matrices, respectively, naturally behave like K^n (this claim

can be made formal, but it goes beyond the scope of these notes). In layman's terms, a matrix of the form $\begin{pmatrix} a_1 \\ \dots \\ a_n \end{pmatrix}$ or $\begin{pmatrix} a_1 & \dots & a_n \end{pmatrix}$ can be seen as the element $(a_1, \dots, a_n)$ of K^n. This makes also evident the fact that $\dim K^n = \dim M_{n\times 1}(K) = \dim M_{1\times n}(K) = n$, and that a canonical basis should also exist for the latter two spaces. We call *canonical basis* of $M_{1\times n}(K)$ the basis $(\underline{e}_1, \dots, \underline{e}_n)$ where $\underline{e}_i = \begin{pmatrix} 0 & \dots & 1 & \dots & 0 \end{pmatrix}$ is the matrix with a 1 in position $(1, i)$ and 0 elsewhere. We call *canonical basis* of $M_{n\times 1}(K)$ the basis constituted of the transpose of the vectors of the canonical basis of $M_{1\times n}(K)$.

The following theorem is of the utmost importance.

Theorem 1.4.11. Let V be a f.g. K-vector space of dimension $n \geq 1$. An n-tuple $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_n)$ of vectors of V is a basis if and only if for every $\underline{v} \in V$ there exist a unique n-tuple $(\alpha_1, \dots, \alpha_n) \in K^n$ such that $\underline{v} = \sum_{i=1}^n \alpha_i \underline{v}_i$.

Proof. First, suppose that $\mathcal{B}$ is a basis. Let $\underline{v} \in V$. Since $\mathcal{B}$ generates V, there exist $\alpha_1, \dots, \alpha_n \in K$ such that $\underline{v} = \sum_{i=1}^n \alpha_i \underline{v}_i$. We only need to prove that the sequence $(\alpha_1, \dots, \alpha_n)$ is unique. Suppose that there is a second one, say $(\beta_1, \dots, \beta_n)$. Since $\underline{v} = \sum_{i=1}^n \beta_i \underline{v}_i$, we get that

$$\sum_{i=1}^n \alpha_i \underline{v}_i = \sum_{i=1}^n \beta_i \underline{v}_i,$$

and hence

$$\sum_{i=1}^n (\alpha_i - \beta_i)\underline{v}_i = \underline{0}.$$

But $\mathcal{B}$ is linearly independent, and hence a linear combination of its vectors that gives the zero vector must have all coefficients equal to 0, i.e. $\alpha_i = \beta_i$ for every $i \in \{1, \dots, n\}$.

Conversely, suppose that every vector of V can be written in a unique way as a linear combination of the $\underline{v}_i$'s. To prove that $\mathcal{B}$ is a basis, we need to prove that it generates V and that is linearly independent. That it generates V is obvious by hypothesis, since every element of V is a

linear combination of elements of $\mathcal{B}$. If $\sum_{i=1}^{n} \alpha_i \underline{v}_i = \underline{0}$, then observe that $\sum_{i=1}^{n} 0\underline{v}_i = \underline{0}$ by Theorem 1.1.21; since the representation of the vector $\underline{0} \in V$ as a linear combination of the $\underline{v}_i$'s is unique, it must be $\alpha_i = 0$ for every i. □

Theorem 1.4.11 allows us to give the following definition.

Definition 1.4.12. Let V be a K-vector space of dimension $n \geq 1$, and let $\mathcal{B} = \{\underline{v}_1, \dots, \underline{v}_n\}$ be a basis of V. If $\underline{v} \in V$, the *components* of $\underline{v}$ with respect to $\mathcal{B}$ are the unique $a_1, \dots, a_n \in K$ such that $\underline{v} = \sum_{i=1}^{n} a_i \underline{v}_i$.

Corollary 1.4.13. Let V be a K-vector space of dimension n. Let $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_n)$ be a basis of V. The function

$$\Phi_{\mathcal{B}} \colon V \to K^n$$

$$\underline{v} = \sum_{i=1}^{n} a_i \underline{v}_i \mapsto (a_1, \dots, a_n)$$

is a bijection.

Proof. By Theorem 1.4.11, if $\Phi_{\mathcal{B}}(\underline{v}) = \Phi_{\mathcal{B}}(\underline{w})$ then it must be $\underline{v} = \underline{w}$, because the representation of $\underline{v}$ and $\underline{w}$ with respect to the basis $\mathcal{B}$ is unique. Hence $\Phi_{\mathcal{B}}$ is injective. Surjectivity is obvious: if $(b_1, \dots, b_n) \in K^n$ then $(b_1, \dots, b_n) = \Phi_{\mathcal{B}}\left(\sum_{i=1}^{n} b_i \underline{v}_i\right)$. □

Note:-

The function $\Phi_{\mathcal{B}}$ is the unique function that associates to a vector the n-tuple of its components with respect to the basis $\mathcal{B}$.

Remark 1.4.14. The function $\Phi_{\mathcal{B}}$ defined above is not just bijective, it also has the property that for every $\alpha, \beta \in K$ and every $\underline{v}, \underline{w} \in V$ we have

$$\Phi_{\mathcal{B}}(\alpha\underline{v} + \beta\underline{w}) = \alpha\Phi_{\mathcal{B}}(\underline{v}) + \beta\Phi_{\mathcal{B}}(\underline{w}).$$

A map with all these properties is called an *isomorphism*. Being isomorphic vector spaces is an equivalence relation; what Corollary 1.4.13 says is that, in loose terms, all K-vector spaces of dimension n "behave" as K^n.

Corollary 1.4.15. Let V be a K-dimensional vector space of dimension $n \geq 1$.

1. Let $\underline{v}_1, \dots, \underline{v}_m \in V$ with $m > n$. Then $\underline{v}_1, \dots, \underline{v}_m$ are linearly dependent.
2. Let $\underline{v}_1, \dots, \underline{v}_m \in V$ with $m < n$. Then $\langle \underline{v}_1, \dots, \underline{v}_m \rangle \neq V$.
3. Let $\underline{v}_1, \dots, \underline{v}_n \in V$. Then the following are equivalent:
   (a) $\langle \underline{v}_1, \dots, \underline{v}_n \rangle = V$;
   (b) $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent;
   (c) $(\underline{v}_1, \dots, \underline{v}_n)$ is a basis of V.
4. For every $m \in \{0, \dots, n\}$, V has a vector subspace of dimension m. If $m = 0$ or $m = n$ such subspace is unique.
5. If $W \subseteq V$ is a vector subspace, then W is f.g. and $\dim W \leq \dim V$, with equality holding if and only if $W = V$.
6. Let $\underline{v}_1, \dots, \underline{v}_m \in V$. Then $\dim\langle \underline{v}_1, \dots, \underline{v}_m \rangle$ is the maximum number of linearly independent vectors in the set $\{\underline{v}_1, \dots, \underline{v}_m\}$.

Proof. 1. Since V is generated by n vectors, by Steinitz lemma $m > n$ vectors must be linearly dependent.

2. If it was, by contradiction, $\langle \underline{v}_1, \dots, \underline{v}_m \rangle = V$, then by Lemma 1.4.3 the set $\{\underline{v}_1, \dots, \underline{v}_m\}$ would contain a set of independent generators, i.e. a basis. But all bases have the same cardinality by Corollary 1.4.6, and this contradicts the assumption $m < n$.

3. We will prove that $(a) \Rightarrow (b)$, $(b) \Rightarrow (c)$ and $(c) \Rightarrow (a)$.

$(a) \Rightarrow (b)$. If $\underline{v}_1, \dots, \underline{v}_n$ were linearly dependent, by Lemma 1.4.3 the set $\{\underline{v}_1, \dots, \underline{v}_n\}$ would contain a basis with less than n elements, contradicting Corollary 1.4.6.

$(b) \Rightarrow (c)$ If it was $\langle \underline{v}_1, \dots, \underline{v}_n \rangle \neq V$, this would mean that at least a vector $\underline{w} \in V$ is not a linear combination of the $\underline{v}_i$'s. But then the vectors $\underline{v}_1, \dots, \underline{v}_n, \underline{w}$ are linearly independent. In fact, if $\sum_{i=1}^n \alpha_i \underline{v}_i + \beta \underline{w} = \underline{0}$ there are two cases: if $\beta = 0$ then all the α_i's must be 0 since $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent. If $\beta \neq 0$ then $\underline{w} = \sum_{i=1}^n (-\beta^{-1}\alpha_i)\underline{v}_i$, contradicting the fact that $\underline{w}$ is not a linear combination of the $\underline{v}_i$'s. Hence $\underline{v}_1, \dots, \underline{v}_n, \underline{w}$ are linearly independent, but this contradicts Steinitz lemma.

Hence $\langle \underline{v}_1, \dots, \underline{v}_n \rangle = V$.

$(c) \Rightarrow (a)$ Obvious by definition of basis.

4. The unique K-vector space of dimension 0 is $\{\underline{0}\} \subseteq V$. Next, V is a vector subspace of V of dimension n. Let us show that it is the only one. If $W \subseteq V$ is a vector subspace of dimension n, then it has a basis $\mathcal{B} = (\underline{w}_1, \dots, \underline{w}_n)$. But the $\underline{w}_i$'s belong to V and they are linearly independent since $\mathcal{B}$ is a basis of W. Then by point 3. they are a basis of V, and therefore $\langle \underline{w}_1, \dots, \underline{w}_n \rangle = W = V$.

Finally, if $m \in \{1, \dots, n-1\}$, let $(\underline{v}_1, \dots, \underline{v}_n)$ be a basis of V and define $W_m = \langle \underline{v}_1, \dots, \underline{v}_m \rangle$. This is a subspace of dimension m because $(\underline{v}_1, \dots, \underline{v}_m)$ is a basis of W_m: the vectors $\underline{v}_1, \dots, \underline{v}_m$ generate W_m by construction and they are linearly independent because they are elements of a basis of V.

5. Any $m > n$ vectors in W cannot be linearly independent, by point 1. Therefore there is a maximum number r of linearly independent vectors in W. Let $\underline{v}_1, \dots, \underline{v}_r \in W$ be linearly independent. If it was $\langle \underline{v}_1, \dots, \underline{v}_r \rangle \neq W$, there would exist some $\underline{w} \in W$ such that $\underline{w} \notin \langle \underline{v}_1, \dots, \underline{v}_r \rangle$. By Remark 1.3.5, this would imply that $\underline{v}_1, \dots, \underline{v}_r, \underline{w}$ are linearly independent. But this is impossible, since they are $r+1$ vectors. Therefore $\langle \underline{v}_1, \dots, \underline{v}_r \rangle = W$, and so W is f.g.

6. Let r be the maximum number of linearly independent vectors in the set $A = \{\underline{v}_1, \dots, \underline{v}_m\}$, and let $\underline{v}_{i_1}, \dots, \underline{v}_{i_r} \in A$ be linearly independent. Then, by definition of basis, $\mathcal{B} = (\underline{v}_{i_1}, \dots, \underline{v}_{i_r})$ is a basis of $\langle \underline{v}_{i_1}, \dots, \underline{v}_{i_r} \rangle$, which then has dimension r. Now if $\underline{v}_j \notin A$, the set $A \cup \{\underline{v}_j\}$ cannot be linearly independent, since otherwise it would contain $r+1$ linearly independent vectors, and this contradicts the fact that r is the maximum number of linearly independent vectors among the $\underline{v}_i$'s. Hence $\underline{v}_j$ must be a linear combination of $\underline{v}_{i_1}, \dots, \underline{v}_{i_r}$, and since this holds for every $\underline{v}_j \notin A$, it follows that $\langle A \rangle = \langle \mathcal{B} \rangle$, so that $\dim \langle A \rangle = r$. □

We end this section with a very important result on bases.

Theorem 1.4.16. Let V be a f.g. K-vector space of dimension n, and let $\mathcal{B}$ be a basis of V.

1. Let $A \subseteq V$. If $\mathcal{B} \subseteq \langle A \rangle$, then $\langle A \rangle = V$.
2. Let $\underline{v}_1, \dots, \underline{v}_m \in V$ be linearly independent, with $m < n$. Then there exist $\underline{v}_{m+1}, \dots, \underline{v}_n \in \mathcal{B}$ such that $(\underline{v}_1, \dots, \underline{v}_n)$ is a basis of V.

Proof. 1. By Proposition 1.2.13, since $\mathcal{B} \subseteq \langle A \rangle$ then $V = \langle \mathcal{B} \rangle \subseteq \langle A \rangle \subseteq V$. Hence it must be $\langle A \rangle = V$.

2. By Corollary 1.4.15 we must have $\langle \underline{v}_1, \dots, \underline{v}_m \rangle \neq V$. Therefore by point 1. we cannot have $\mathcal{B} \subseteq \langle \underline{v}_1, \dots, \underline{v}_m \rangle$. This means that there exists a vector $\underline{v}_{m+1} \in \mathcal{B}$ such that $\underline{v}_{m+1} \notin \langle \underline{v}_1, \dots, \underline{v}_m \rangle$, and therefore $\underline{v}_1, \dots, \underline{v}_{m+1}$ are linearly independent by Proposition 1.3.4. Now we repeat the same argument on the set $\{\underline{v}_1, \dots, \underline{v}_{m+1}\}$ until we get n linearly independent vectors; these must form a basis by Corollary 1.4.15. □

1.5 Sum and intersection of subspaces

Definition 1.5.1. Let V be a K-vector space and $U, W \subseteq V$ be subspaces. The *sum* of U and W is the set:

$$U + W = \{\underline{u} + \underline{w} \colon \underline{u} \in U, \underline{w} \in W\}.$$

We say that the sum $U + W$ is *direct* if for every $\underline{v} \in U + W$ there exist unique $\underline{u} \in U$ and $\underline{w} \in W$ such that $\underline{v} = \underline{u} + \underline{w}$. If the sum $U + W$ is direct, we write $U \oplus W$.

Remark 1.5.2. If $U, W \subseteq V$ are vector subspaces, the following hold true.

1. $U \cap W = U$ if and only if $U \subseteq W$, because this is true for sets in general.
2. $U, W \subseteq U + W$. In fact, if $\underline{u} \in U$ then $\underline{u} = \underline{u} + \underline{0} \in U + W$, and similarly for vectors of W.
3. $U + W = U$ if and only if $W \subseteq U$. In fact, if $W \subseteq U$ then for every $\underline{u} + \underline{w} \in U + W$ we have that $\underline{u} + \underline{w} \in U$, since both $\underline{u}$ and $\underline{w}$ belong to U. Hence $U + W \subseteq U$. On the other hand, by 2. we have that $U \subseteq U + W$, and therefore $U = U + W$. Conversely, if $U = U + W$ then for every $\underline{w} \in W$ we have that $\underline{w} = \underline{0} + \underline{w} \in U + W = U$, that means that $\underline{w} \in U$. Hence $W \subseteq U$.

Proposition 1.5.3. Let V be a K-vector space and U, W be subspaces of V. The sets $U \cap W$ and $U + W$ are vector subspaces of V.

Proof. First, let $\underline{u}, \underline{w} \in U \cap W$ and $\alpha, \beta \in K$. Since $\underline{u}, \underline{w} \in U$, that is a vector subspace of V, then $\alpha\underline{u} + \beta\underline{w} \in U$. But the same is true for W, since this is a vector subspace too. Then $\alpha\underline{u} + \beta\underline{w} \in W$, and it follows that $\alpha\underline{u} + \beta\underline{w} \in U \cap W$. Hence $U \cap W$ is a vector subspace by Theorem 1.2.6.

Next, let $\underline{u}_1 + \underline{w}_1, \underline{u}_2 + \underline{w}_2 \in U + W$, where $\underline{u}_1, \underline{u}_2 \in U$ and $\underline{w}_1, \underline{w}_2 \in W$. Let $\alpha_1, \alpha_2 \in K$. Then $\alpha_1(\underline{u}_1 + \underline{w}_1) + \alpha_2(\underline{u}_2 + \underline{w}_2) = (\alpha_1\underline{u}_1 + \alpha_2\underline{u}_2) + (\alpha_1\underline{w}_1 + \alpha_2\underline{w}_2)$, and since U and W are subspaces, we get that $\alpha_1\underline{u}_1 + \alpha_2\underline{u}_2 \in U$ and $\alpha_1\underline{w}_1 + \alpha_2\underline{w}_2 \in W$. It follows that $\alpha_1(\underline{u}_1 + \underline{w}_1) + \alpha_2(\underline{u}_2 + \underline{w}_2) \in U + W$, and hence the latter is a subspace by Theorem 1.2.6. □

Proposition 1.5.4. Let V be a vector space and U, W be vector subspaces of V. The sum $U + W$ is direct if and only if $U \cap W = \{\underline{0}\}$.

Proof. First, assume that the sum is direct. We want to show that $U \cap W = \{\underline{0}\}$. Let $\underline{v} \in U \cap W$. Since $\underline{v} \in U$, a way of expressing $\underline{v}$ as a sum of a vector of U and one of W is $\underline{v} = \underline{v} + \underline{0}$. On the other hand, $\underline{v} \in W$ as well, and hence we can also write $\underline{v} = \underline{0} + \underline{v}$, a sum of a vector of U, namely $\underline{0}$, and one of W. Since the sum of U and W is direct, there can be only one way of writing $\underline{v}$ as a sum of an element of U and one of W, and therefore it must be $\underline{v} = \underline{0}$. That is, $U \cap W = \{\underline{0}\}$.

Conversely, assume that $U \cap W = \{\underline{0}\}$. Now let $\underline{v} \in U + W$, and let $\underline{u}_1, \underline{u}_2 \in U$, $\underline{w}_1, \underline{w}_2 \in W$ be such that $\underline{v} = \underline{u}_1 + \underline{w}_1 = \underline{u}_2 + \underline{w}_2$. Then $\underline{u}_1 - \underline{u}_2 = \underline{w}_1 - \underline{w}_2$. This implies that $\underline{u}_1 - \underline{u}_2$ is both an element of U, because U is a subspace, and an element of W, because it is equal to $\underline{w}_1 - \underline{w}_2$ that is an element of W. Hence $\underline{u}_1 - \underline{u}_2 \in U \cap W = \{\underline{0}\}$, so that $\underline{u}_1 = \underline{u}_2$. Therefore also $\underline{w}_1 - \underline{w}_2 = \underline{0}$, so that there is only one way of writing $\underline{v}$ as a sum of a vector in U and one in W. □

Proposition 1.5.5. Let U, W be f.g. subspaces of a K-vector space V.

1. $U \cap W$ is finitely generated.
2. Let $\mathcal{B} = (\underline{u}_1, \dots, \underline{u}_m)$ be a basis of U and $\mathcal{B}' = (\underline{w}_1, \dots, \underline{w}_n)$ be a basis of W. Then $U + W$ is finitely generated, and $\mathcal{B} \cup \mathcal{B}'$ is a system of generators.

Proof. 1. The space $U \cap W$ is a subspace of U, that is f.g., and hence it

is f.g. itself (see Corollary 1.4.15).

2. Let $\underline{v} \in U + W$, so that $\underline{v} = \underline{u} + \underline{w}$ for some $\underline{u} \in U$ and $\underline{w} \in W$. There exist $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \in K$ such that $\underline{u} = \sum_{i=1}^{m} \alpha_i \underline{u}_i$ and $\underline{w} = \sum_{j=1}^{n} \beta_j \underline{w}_j$. Then $\underline{v} = \sum_{i=1}^{m} \alpha_i \underline{u}_i + \sum_{j=1}^{n} \beta_j \underline{w}_j$. We have just proved that every vector of $U + W$ is a linear combination of elements of $\mathcal{B} \cup \mathcal{B}'$. Therefore $U + W = \langle \mathcal{B} \cup \mathcal{B}' \rangle$. □

Definition 1.5.6. Let V be a K-vector space and let $W \subseteq V$ be a subspace. A *direct complement* for W in V is a subspace $W' \subseteq V$ such that $W \oplus W' = V$.

Theorem 1.5.7. Let V be a f.g. K-vector space, and let $W \subseteq V$ be a vector subspace. Then there exists a direct complement W' for W.

Proof. If $W = V$ then just take $W' = \{\underline{0}\}$. If $W = \{\underline{0}\}$, take $W' = V$. Otherwise, let $n = \dim V$ and let $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_m)$ be a basis for W, with $m < n$, and $\mathcal{B}'$ a basis for V. By Theorem 1.4.16, there exist $\underline{v}_{m+1}, \dots, \underline{v}_n \in \mathcal{B}'$ such that $(\underline{v}_1, \dots, \underline{v}_n)$ is a basis of V. We claim that $W' = \langle \underline{v}_{m+1}, \dots, \underline{v}_n \rangle$ is a direct complement for W. We need to prove that $W + W' = V$ and that $W \cap W' = \{\underline{0}\}$.

The fact that $W + W' = V$ follows immediately from Proposition 1.5.5.

If $\underline{v} \in W \cap W'$, then $\underline{v} = \sum_{i=1}^{m} \alpha_i \underline{v}_i$ for some $\alpha_1, \dots, \alpha_m \in K$, since $\underline{v} \in W$, but also $\underline{v} = \sum_{i=m+1}^{n} \beta_i \underline{v}_i$ for some $\beta_{m+1}, \dots, \beta_n \in K$, since $\underline{v} \in W'$. Hence

$$\alpha_1 \underline{v}_1 + \dots + \alpha_m \underline{v}_m - \beta_{m+1} \underline{v}_{m+1} - \dots - \beta_n \underline{v}_n = \underline{0},$$

and since $(\underline{v}_1, \dots, \underline{v}_n)$ is a basis for V it follows that $\alpha_i = 0 = \beta_j$ for every i, j. Hence $W \cap W' = \{\underline{0}\}$. □

Remark 1.5.8. The proof of Theorem 1.5.7 shows clearly that a subspace does not have just one direct complement. For example, if $V = \mathbb{R}^2$ and $W = \langle (1, 0) \rangle$, then W has infinitely many direct complements. In fact, if $\underline{v} \in V \setminus W$ then $W' = \langle \underline{v} \rangle$ is a direct complement for W: by construction $W \cap W' = \{\underline{0}\}$ and $\dim(W \oplus W') = 2$ by Grassmann formula. It must then be $W \oplus W' = V$, since the unique subspace of V of dimension 2 is V itself (see Corollary 1.4.15).

Theorem 1.5.9 (Grassmann formula)**.** Let V be a K-vector space and let $U, W \subseteq V$ be f.g. vector subspaces. Then:

$$\dim(U+W) = \dim U + \dim W - \dim(U \cap W).$$

Proof. If $\dim U = 0$ or $\dim W = 0$ the formula is obvious since $\dim U \cap W = 0$. From now on, we let $\mathcal{B} = (\underline{u}_1, \dots, \underline{u}_m)$ be a basis of U and $\mathcal{B}' = (\underline{w}_1, \dots, \underline{w}_n)$ be a basis of W, so that $\dim U = m$ and $\dim W = n$ and $m, n \geq 1$.

Case 1: $U \cap W = \{\underline{0}\}$. If this happens, then $\dim(U \cap W) = 0$, and so we need to prove that

$$\dim(U+W) = \dim U + \dim W. \tag{6}$$

By Proposition 1.5.5, $\mathcal{B} \cup \mathcal{B}'$ generates $U+W$. If we can prove that $\underline{u}_1, \dots, \underline{u}_m, \underline{w}_1, \dots, \underline{w}_n$ are linearly independent, it will follow that $\mathcal{B} \cup \mathcal{B}'$ is a basis of $U+W$ with $m+n$ elements, and therefore $\dim(U+W) = m+n$ as we need.

Let $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \in K$ be such that

$$\alpha_1\underline{u}_1 + \dots + \alpha_m\underline{u}_m + \beta_1\underline{w}_1 + \dots + \beta_n\underline{w}_n = \underline{0}.$$

Then

$$\alpha_1\underline{u}_1 + \dots + \alpha_m\underline{u}_m = -\beta_1\underline{w}_1 - \dots - \beta_n\underline{w}_n. \tag{7}$$

The left hand side of the above equality is an element of U and it equals the right hand side that is a vector of W. It follows that $\alpha_1\underline{u}_1 + \dots + \alpha_m\underline{u}_m \in U \cap W = \{\underline{0}\}$. This means that

$$\alpha_1\underline{u}_1 + \dots + \alpha_m\underline{u}_m = \underline{0}.$$

But $\mathcal{B}$ is a basis, and therefore $\alpha_1 = \dots = \alpha_m = 0$. Substituting this in (7) it follows that

$$\beta_1\underline{w}_1 + \dots + \beta_n\underline{w}_n = \underline{0}.$$

But $\mathcal{B}'$ is also a basis, and hence $\beta_1 = \dots = \beta_n = 0$. We proved that the α_i's and the β_j's are all 0, and so that $\underline{u}_1, \dots, \underline{u}_m, \underline{w}_1, \dots, \underline{w}_n$ are linearly independent; it follows that $\mathcal{B} \cup \mathcal{B}'$ is a basis of $U+W$ of cardinality $m+n$, and (6) is proved.

Case 2: $U \cap W \neq \{\underline{0}\}$. By Proposition 1.5.5, the space $U \cap W$ is f.g., and hence it admits a basis $\mathcal{B}'' = \{\underline{v}_1, \dots, \underline{v}_p\}$, where $p = \dim(U \cap W) \geq 1$

and $p \leq \min\{m, n\}$. By Theorem 1.4.16, we can complete $\mathcal{B}''$ to a basis of U, using vectors of $\mathcal{B}$, and to a basis of W, using vectors of $\mathcal{B}'$. Up to permuting the elements of $\mathcal{B}$ and those of $\mathcal{B}'$, we can assume that $\widetilde{\mathcal{B}} = (\underline{v}_1, \dots, \underline{v}_p, \underline{u}_1, \dots, \underline{u}_{m-p})$ is a basis of U and $\widetilde{\mathcal{B}}' = (\underline{v}_1, \dots, \underline{v}_p, \underline{w}_1, \dots, \underline{u}_{n-p})$ is a basis of W. If $m - p = 0$ this means that $\dim U \cap W = \dim U$, and this in turn means that $U = U \cap W$, so that $U \subseteq W$. Then the formula we need to prove becomes $\dim(U + W) = \dim W$, which is certainly true since $U + W = W$. The case $n - p = 0$ is analogous. Hence we can assume that $m - p, n - p \geq 1$.

Now we claim that $\mathcal{C} = (\underline{v}_1, \dots, \underline{v}_p, \underline{u}_1, \dots, \underline{u}_{m-p}, \underline{w}_1, \dots, \underline{w}_{n-p})$ is a basis of $U + W$. This will conclude the proof, since then $U + W$ has a basis with $m + n - p$ elements, i.e. $\dim(U + W) = m + n - p$. We need to prove that $\mathcal{C}$ generates $U + W$ and that it consists of linearly independent vectors.

The first claim follows immediately by Proposition 1.5.5, because $\mathcal{C} = \widetilde{\mathcal{B}} \cup \widetilde{\mathcal{B}}'$.

Now let $\alpha_1, \dots, \alpha_{m-p}, \beta_1, \dots, \beta_{n-p}, \gamma_1, \dots, \gamma_p \in K$ be such that:

$$\alpha_1\underline{u}_1 + \dots + \alpha_{m-p}\underline{u}_{m-p} + \beta_1\underline{w}_1 + \dots + \beta_{n-p}\underline{w}_{n-p} + \gamma_1\underline{v}_1 + \dots + \gamma_p\underline{v}_p = \underline{0}. \quad (8)$$

Rewrite this as:

$$\alpha_1\underline{u}_1 + \dots + \alpha_{m-p}\underline{u}_{m-p} = -\beta_1\underline{w}_1 - \dots - \beta_{n-p}\underline{w}_{n-p} - \gamma_1\underline{v}_1 - \dots - \gamma_p\underline{v}_p.$$

The left hand side is a vector of U, and it equals the right hand side that is a vector of W. Hence the left hand side is a vector of $U \cap W$, and therefore it can be expressed in the basis $\mathcal{B}''$. This means that there exist $\delta_1, \dots, \delta_p \in K$ such that $\sum_{i=1}^{n-p} \alpha_i\underline{u}_i = \sum_{i=1}^{p} \delta_i\underline{v}_i$. Substituting this in (8), we get:

$$\beta_1\underline{w}_1 + \dots + \beta_{n-p}\underline{w}_{n-p} + (\gamma_1 + \delta_1)\underline{v}_1 + \dots + (\gamma_p + \delta_p)\underline{v}_p = \underline{0}.$$

Now remember that $\widetilde{\mathcal{B}}'$ is a basis; it must then be

$$\beta_1 = \dots = \beta_{n-p} = \gamma_1 + \delta_1 = \dots = \gamma_p + \delta_p = 0.$$

Since the β_i's are all 0, equation (8) becomes:

$$\alpha_1\underline{u}_1 + \dots + \alpha_{m-p}\underline{u}_{m-p} + \gamma_1\underline{v}_1 + \dots + \gamma_p\underline{v}_p = \underline{0}.$$

But now remember that also $\widetilde{\mathcal{B}}$ is a basis, and therefore

$$\alpha_1 = \ldots = \alpha_{m-p} = \gamma_1 = \ldots = \gamma_p = 0.$$

All in all, we have proved that all the α_i's, all the β_i's and all the γ_i's are 0, i.e. that the vectors of $\mathcal{C}$ are linearly independent. □

Chapter 2: Determinant and rank

2.1 Determinant

Definition 2.1.1. Let K be a field and $A \in M_{m\times n}(K)$ an $m \times n$ matrix with entries in K. A *submatrix* is a matrix obtained by erasing rows and/or columns of A.

Example 2.1.2. Let $A = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 2 \\ -1 & 6 & 7 \end{pmatrix} \in M_3(\mathbb{R})$.

Erasing the middle row, we obtain the submatrix $\begin{pmatrix} 1 & 2 & 4 \\ -1 & 6 & 7 \end{pmatrix}$.

Erasing the first two columns, we obtain the submatrix $\begin{pmatrix} 4 \\ 2 \\ 7 \end{pmatrix}$.

Erasing the first and third column and the third row, we obtain the submatrix $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$.

Definition 2.1.3. Let K be a field and $n \geq 1$ be an integer. Let $A = (a_{ij})_{i,j=1,\dots,n} \in M_n(K)$ be a square matrix. The *determinant* of A is the element of K that is defined in the following recursive way:

1. if $n = 1$ then $A = (a_{11})$ and the determinant of A is a_{11};
2. in general, the determinant of A is defined by:

$$\det A = \sum_{j=1}^{n} (-1)^{1+j} a_{1j} A_{1j},$$

where A_{1j} is the determinant of the submatrix obtained by erasing from A the first row and the j-th column.

Example 2.1.4.

- If $n = 2$ then $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Definition 2.1.3 yields:

$$\det A = a_{11} \det(a_{22}) - a_{12} \det(a_{21}) = a_{11}a_{22} - a_{12}a_{21}.$$

- If $n = 3$ then $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$. Definition 2.1.3 yields:

$$\det A = a_{11} \det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} - a_{12} \det \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13} \det \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}.$$

Now we can use the previous computation of the determinant of a 2×2 matrix and get:

$$\det A = a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}).$$

Definition 2.1.5. Given $A \in M_{m\times n}(K)$, a *minor* of A is the determinant of a square submatrix of A.

Theorem 2.1.6 (Laplace theorem)**.** Let K be a field and $A = (a_{ij})_{i,j=1,\dots,n} \in M_n(K)$. Fix an index $k \in \{1, \dots, n\}$. Then:

$$\det A = \sum_{j=1}^{n} (-1)^{k+j} a_{kj} A_{kj} = \sum_{i=1}^{n} (-1)^{i+k} a_{ik} A_{ik},$$

where $A_{\ell m}$ is the minor obtained by erasing the ℓ-th row and the m-th column from A.

In other words, Laplace theorem says that the determinant can be com-

puted starting from any row or column of A, by multiplying each entry of the row/column by the determinant of the corresponding submatrix and the appropriate sign, and then adding up the terms.

Example 2.1.7. Let $A = \begin{pmatrix} 1 & 2 & 0 \\ -1 & 0 & 1 \\ -1 & 1 & 1 \end{pmatrix} \in M_3(\mathbb{R})$. The determinant of A can be computed by its definition, namely using the first row:

$$\det A = 1 \cdot \det \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} - 2 \cdot \det \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} + 0 \cdot \det \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} =$$

$$= 1(0-1) - 2(-1+1) + 0(-1-0) = -1.$$

On the other hand, Laplace theorem says that we can also compute it using any row or column. For example, let us choose the second column:

$$\det A = -2 \cdot \det \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} + 0 \cdot \det \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} - 1 \cdot \det \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} =$$

$$= -2(-1+1) + 0(1-0) - 1(1-0) = -1.$$

Proposition 2.1.8. Let $A \in M_n(K)$. The determinant of A enjoys the following properties.

1. If A has a row or a column all of whose entries are 0, then $\det A = 0$.
2. $\det(A) = \det({}^tA)$.
3. If A' is the matrix obtained by swapping two adjacent rows or two adjacent columns of A, then $\det A = -\det A'$.
4. If two rows or columns of A are equal, then $\det A = 0$.

5. If $A = \begin{pmatrix} \frac{R_1}{} \\ \frac{R_2}{} \\ \frac{\dots}{} \\ \frac{R_k + R_k'}{} \\ \frac{\dots}{} \\ R_n \end{pmatrix}$, where $R_1, \dots, R_n$ are the rows of A, then:

$$\det A = \det \begin{pmatrix} \frac{R_1}{} \\ \frac{R_2}{} \\ \frac{\dots}{} \\ \frac{R_k}{} \\ \frac{\dots}{} \\ R_n \end{pmatrix} + \det \begin{pmatrix} \frac{R_1}{} \\ \frac{R_2}{} \\ \frac{\dots}{} \\ \frac{R_k'}{} \\ \frac{\dots}{} \\ R_n \end{pmatrix}.$$

Analogously, if $A = (C_1|\dots|C_k + C_k'|\dots|C_n)$ where $C_1, \dots, C_n$ are the columns of A, then:

$$\det A = \det(C_1|\dots|C_k|\dots|C_n) + \det(C_1|\dots|C_k'|\dots|C_n).$$

6. if A' is the matrix obtained by multiplying every entry of a row or a column of A by the same constant $\lambda \in K$, then $\det A' = \lambda \det A$.

7. if a row/column of A is a linear combination of other rows/columns of A, then $\det A = 0$.

8. if A' is the matrix obtained by adding to a row/column of A a linear combination of other rows/columns of A, then $\det A' = \det A$.

Proof. 1. This is clear by Laplace theorem, if we compute the determinant of A using a row or a column all of whose entries are 0.

2. Again clear by Laplace theorem: computing the determinant of A using the first row is the same as computing the determinant of ${}^tA$ using the first column.

Thanks to point 2., it suffices to prove all remaining points for rows, since the same statement for columns follows by considering the transpose matrix.

3. Let $A = (a_{ij})_{i,j=1,\dots,n}$ and suppose $A' = (b_{ij})_{i,j=1,\dots,n}$ is obtained by swapping the i-th row with the $(i+1)$-th row of A. By Laplace theorem,

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} A_{ij}$$

by computing the determinant using the i-th row. On the other hand,

$$\det A' = \sum_{j=1}^{n} (-1)^{i+1+j} b_{(i+1)j} A'_{(i+1)j}$$

by Laplace theorem, where we computed the determinant using the $(i+1)$-th row and $A'_{(i+1)j}$ is the minor of A' obtained by erasing the $(i+1)$-th row and the j-th column. Now just notice that $b_{(i+1)j} = a_{ij}$ for every $j \in \{1, \dots, n\}$, since we swapped row i and row $i+1$, and $A'_{(i+1)j} = A_{ij}$ for every $j \in \{1, \dots, n\}$: deleting the $(i+1)$-th row of A' has the same effect of deleting the i-th row of A. Hence

$$\det A' = \sum_{j=1}^{n} (-1)^{i+1+j} a_{ij} A_{ij} = -\sum_{j=1}^{n} (-1)^{i+j} a_{ij} A_{ij} = -\det A.$$

4. By induction on n. If $n = 2$ and two rows are equal, we necessarily have $A = \begin{pmatrix} a & b \\ a & b \end{pmatrix}$, so that $\det A = ab - ab = 0$. Now suppose that the claim is true for a square matrix of size $n-1$ and consider $A \in M_n(K)$, with $n \geq 3$. Suppose that two rows of A coincide, say $R_i = R_j$ and fix another row R_k, with $k \neq i, j$. By Laplace theorem,

$$\det A = \sum_{\ell=1}^{n} (-1)^{k+\ell} a_{k\ell} A_{k\ell},$$

where $A_{k\ell}$ is the minor of A obtained by erasing the k-th row and the ℓ-th column. Clearly, when we erase the k-th row and the ℓ-th column from A, the submatrix we obtain has two equal rows, because A had them and

we erased a different row. This means that $A_{k\ell} = 0$ for every ℓ, by the inductive hypothesis. It follows that $\det A = 0$.

5. Let $R_k = (a_{k1}, \dots, a_{kn})$ and $R'_k = (a'_{k1}, \dots, a'_{kn})$. Then by Laplace theorem using the k-th row we get:

$$\det A = \sum_{j=1}^{n} (-1)^{k+j} (a_{kj} + a'_{kj}) A_{kj} =$$

$$= \sum_{j=1}^{n} (-1)^{k+j} a_{kj} A_{kj} + \sum_{j=1}^{n} (-1)^{k+j} a'_{kj} A_{kj},$$

and by Laplace theorem these two terms are exactly the determinants of the matrices $\begin{pmatrix} R_1 \\ \hline R_2 \\ \hline \dots \\ \hline R_k \\ \hline \dots \\ \hline R_n \end{pmatrix}$ and $\begin{pmatrix} R_1 \\ \hline R_2 \\ \hline \dots \\ \hline R'_k \\ \hline \dots \\ \hline R_n \end{pmatrix}$.

6. Let $A = (a_{ij})_{i,j=1,\dots,n}$ and suppose A' is obtained by A by multiplying the k-th row by a constant $\lambda \in K$. By Laplace theorem we get:

$$\det A' = \sum_{j=1}^{n} (-1)^{k+j} (\lambda a_{kj}) A_{kj} = \lambda \sum_{j=1}^{n} (-1)^{k+j} a_{kj} A_{kj} = \lambda \det A.$$

7. Let $R_1, \dots, R_n$ be the rows of A and suppose that the k-th row R_k of A can be written as $\sum_{i \neq k} \lambda_i R_i$, for some $\lambda_i \in K$. By points 5. and 6.

we get that

$$\det A = \sum_{\substack{i=1,\dots,n \\ i\neq k}} \lambda_i \det \begin{pmatrix} \hline R_1 \\ \hline \dots \\ \hline R_i \\ \hline \dots \\ \hline R_i \\ \hline \dots \\ \hline R_n \end{pmatrix},$$

and each of the determinants in the right hand side is 0 by point 4.

8. Suppose A' is obtained from A by adding to the k-th row R_k a linear combination of the other rows, so that the k-th row of A' equals $R_k + \sum_{\substack{i=1,\dots,n \\ i\neq k}} \lambda_i R_i$. By point 5. we have

$$\det A' = \det \begin{pmatrix} \hline R_1 \\ \hline R_2 \\ \hline \dots \\ \hline R_k \\ \hline \dots \\ \hline R_n \end{pmatrix} + \det \begin{pmatrix} \hline R_1 \\ \hline R_2 \\ \hline \dots \\ \hline \sum \lambda_i R_i \\ \hline \dots \\ \hline R_n \end{pmatrix}.$$

Now the first term in the right hand side is exactly $\det A$ and the second term is 0 by point 7. □

Remark 2.1.9. If A is upper triangular or lower triangular, then the determinant of A equals the product of the elements on the diagonal. This can be shown by induction on the size n of the matrix. Of course it is enough to prove it for upper triangular matrices, since the transpose of a lower triangular matrix is upper triangular and has the same diagonal. If $n = 1$, the claim is obvious. Suppose it is true for upper triangular matrices of

size $n-1$ and let $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix}$ be upper triangular of size n. By Laplace theorem, using the first column, we get:

$$\det A = a_{11} \det \begin{pmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ 0 & a_{32} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix}.$$

In the right hand side of the equality we are computing the determinant of an upper triangular matrix of size $n-1$ and hence by the inductive hypothesis its determinant is $a_{22}a_{33}\dots a_{nn}$. It follows that

$$\det A = a_{11}a_{22}\dots a_{nn}.$$

Theorem 2.1.10 (Binet theorem)**.** Let $A, B \in M_n(K)$. Then:

$$\det(AB) = \det A \cdot \det B.$$

Definition 2.1.11. A matrix $A \in M_n(K)$ is *invertible* if there exists a matrix $B \in M_n(K)$ such that $AB = BA = I_n$.

Theorem 2.1.12. A matrix $A \in M_n(K)$ is invertible if and only if $\det A \neq 0$. If this is the case, the inverse matrix is unique, is denoted by A^{-1} and it is given by:

$$A^{-1} = \frac{1}{\det A} \cdot {}^t((-1)^{i+j}A_{ij})_{i,j=1,\dots,n},$$

where A_{ij} is the minor of A obtained by erasing the i-th row and the j-th column.

2.2 Change of basis

Let V be a f.g. K-vector space, and let $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_n)$ and $\mathcal{B}' = (\underline{v}'_1, \dots, \underline{v}'_n)$ be two bases for V. For every $j \in \{1, \dots, n\}$, let

$$\underline{v}'_j = \sum_{i=1}^{n} \lambda_{ij} \underline{v}_i$$

be the expression of the vectors of $\mathcal{B}'$ with respect to the basis $\mathcal{B}$.

Definition 2.2.1. The matrix $A = (\lambda_{ij})_{i,j=1,\dots,n}$ is called *change of basis matrix* from $\mathcal{B}'$ to $\mathcal{B}$.

Proposition 2.2.2. Let $\underline{v} = \sum_{i=1}^{n} a_i \underline{v}'_i$ and let $E = (a_1, \dots, a_n)$. Then $A \cdot {}^tE$ is the vector of the components of $\underline{v}$ with respect to the basis $\mathcal{B}$.

Proof. Let $\underline{v} = \sum_{j=1}^{n} a_j \underline{v}'_j$. Now substitute $\underline{v}'_j = \sum_{i=1}^{n} \lambda_{ij} \underline{v}_i$ so that

$$\underline{v} = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_j \lambda_{ij} \right) \underline{v}_i$$

is the expression of $\underline{v}$ with respect to the basis $\mathcal{B}$. Now it is just a matter of checking that

$$A \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} a_j \lambda_{1j} \\ \sum_{j=1}^{n} a_j \lambda_{2j} \\ \dots \\ \sum_{j=1}^{n} a_j \lambda_{nj} \end{pmatrix}.$$

□

Therefore once we have the change of basis matrix, in order to transform the expression of a vector in basis $\mathcal{B}'$ into the expression in basis $\mathcal{B}$ we just have to multiply the column vector of components by the matrix A.

Example 2.2.3. Let $V = \mathbb{R}^3$. The sequence

$$\mathcal{B} = ((1,1,1), (1,0,1), (-1,0,0))$$

is a basis of V, and so is

$$\mathcal{B}' = ((2,0,0),(0,1,1),(2,3,0)).$$

In order to write down the change of basis matrix, all we need to do is to express vectors of $\mathcal{B}'$ with respect to $\mathcal{B}$, and then writing the components by columns in a 3×3 matrix. We have:

$$(2,0,0) = -2 \cdot (-1,0,0)$$

$$(0,1,1) = 1 \cdot (1,1,1) + 1 \cdot (-1,0,0)$$

$$(2,3,0) = 3 \cdot (1,1,1) - 3 \cdot (1,0,1) - 2 \cdot (-1,0,0)$$

so that the change of basis matrix is:

$$A = \begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & -3 \\ -2 & 1 & -2 \end{pmatrix}.$$

Now if we take any vector of V and we write it with respect to the basis $\mathcal{B}'$, such as for example $(4,4,1) = 1 \cdot (2,0,0) + 1 \cdot (0,1,1) + 1 \cdot (2,3,0)$, in order to find its components with respect to $\mathcal{B}$ we just need to compute

$$\begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & -3 \\ -2 & 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ -3 \\ -3 \end{pmatrix}.$$

In fact,

$$(4,4,1) = 4 \cdot (1,1,1) - 3 \cdot (1,0,1) - 3 \cdot (-1,0,0).$$

Proposition 2.2.4. The change of basis matrix A from $\mathcal{B}'$ to $\mathcal{B}$ is invertible, and its inverse A^{-1} is the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$

Proof. Let A' be the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$. Then clearly for any $(a_1, \dots, a_n) \in K^n$ we have

$$A'A \cdot {}^t(a_1, \dots, a_n) = {}^t(a_1, \dots, a_n),$$

because $A \cdot {}^t(a_1, \dots, a_n)$ is the vector of components of the vector $\sum_{i=1}^n a_i \underline{v}_i'$ with respect to $\mathcal{B}$, and hence $A' \cdot (A \cdot {}^t(a_1, \dots, a_n))$ is the vector of components of $\sum_{i=1}^n a_i \underline{v}_i'$ in basis $\mathcal{B}'$, that is just ${}^t(a_1, \dots, a_n)$.

Then in particular when $(a_1, \dots, a_n) = (0, \dots, 0, 1, 0, \dots, 0)$, with the only 1 in position k, we see that $A'A^t(a_1, \dots, a_n)$ on the one hand is the k-th column of $A'A$, and on the other hand is ${}^t(0, \dots, 0, 1, 0, \dots, 0)$. This means precisely that $A'A = I_n$. On the other hand one can swap the role of $\mathcal{B}$ and $\mathcal{B}'$ and repeat the same argument; this leads to proving that $AA' = I_n$. Therefore A is invertible and A' is its inverse. □

2.3 Rank

Definition 2.3.1. Let $A \in M_{m\times n}(K)$ be a matrix. If B is a square submatrix of A, the *size* of B is the number of rows (or columns) of B.

The *rank* of A is the largest size of a square submatrix of A with nonzero determinant. If all square submatrices of A have determinant 0, then we say that A has rank 0. The rank of A is denoted by $\mathrm{rk}(A)$.

Remark 2.3.2.

1. A has rank 0 if and only if all of its entries are 0. In fact, if all of its entries are 0 then clearly there are no square submatrices with nonzero determinant, and conversely if all square submatrices of A have determinant 0 then in particular all submatrices of size 1 have determinant 0. But a square submatrix of size 1 is just an entry of A.

2. If $A \in M_n(K)$, then $\mathrm{rk}(A) = n$ if and only if $\det A \neq 0$. In fact, the unique square submatrix of A of size n is A itself.

3. If $A \in M_{m\times n}(K)$, then $\mathrm{rk}(A) \leq \min\{m, n\}$, since a square submatrix of A can have size at most $\min\{m, n\}$.

4. Since the determinant of a matrix equals the determinant of the transpose, we have that $\mathrm{rk}(A) = \mathrm{rk}({}^tA)$.

5. if B is a submatrix of a matrix A, then $\mathrm{rk}(A) \geq \mathrm{rk}(B)$.

Example 2.3.3.

- Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \end{pmatrix} \in M_{2\times 3}(\mathbb{R})$. Since A is not the zero matrix, $\operatorname{rk}(A) \geq 1$ and of course $\operatorname{rk}(A) \leq 2$. To decide whether $\operatorname{rk}(A) = 1$ or $\operatorname{rk}(A) = 2$ we need to decide if A has a submatrix of size 2 with non-zero determinant. The submatrices of size 2 of A are:

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 & 3 \\ 4 & 6 \end{pmatrix}.$$

  These all have determinant 0, so $\operatorname{rk} A = 1$

- Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 6 \end{pmatrix} \in M_{2\times 3}(\mathbb{R})$. The size 2 submatrix of A given by $\begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix}$ has determinant $4 \neq 0$. Therefore, $\operatorname{rk}(A) = 2$.

If $A \in M_{m\times n}(K)$ has a square submatrix of size r with non-zero determinant, then the rank of A is at least r, by definition. In order to prove that the rank is exactly r, one needs to prove that every square submatrix of A of size larger than r has zero determinant. However, it is enough to consider square submatrices of size $r+1$, as shown by the following proposition.

Proposition 2.3.4. Let $A \in M_{m\times n}(K)$ and let $r \leq \min\{m, n\}$. Suppose that every square submatrix of A of size $r+1$ has determinant 0. Then $\operatorname{rk}(A) \leq r$.

Proof. To prove that the rank of A is at most r, we need to prove that the determinant of every square submatrix of A of size $r+k$ is zero, for every $k = 1, \ldots, \min\{m, n\} - r$. We do this by induction on k.

The claim for $k = 1$ is true by hypothesis. Now suppose the claim is true for $k-1$, i.e. suppose that every square submatrix of A of size $r+k-1$ has determinant 0, and let $B = (b_{ij})_{i,j=1,\ldots,r+k}$ be a square submatrix of A of size $r+k$. Computing the determinant of B via Laplace theorem via

the first row of B yields:

$$\det B = \sum_{j=1}^{r+k} (-1)^{1+j} b_{1j} \det B_{1j}, \tag{9}$$

where B_{1j} is the submatrix obtained from B by erasing the first row and the j-th column of B. But now for every $j = 1, \dots, r+k$ the matrix B_{1j} is a square submatrix of B, and hence of A, of size $r+k-1$, and hence it has determinant 0 by the inductive hypothesis. It follows from (9) that $\det B = 0$. □

Corollary 2.3.5. Let $A \in M_{m\times n}(K)$ and suppose that A has a size r submatrix with non-zero determinant. If all submatrices of size $r+1$ have zero determinant, then $\mathrm{rk}(A) = r$

Proof. Since A has a size r submatrix with non-zero determinant, $\mathrm{rk}(A) \geq r$. On the other hand, by Proposition 2.3.4 we have $\mathrm{rk}(A) \leq r$, and therefore $\mathrm{rk}(A) = r$. □

Definition 2.3.6. Let V be a f.g. K-vector space and let $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_n)$ be a basis of V. Let $\underline{w}_1, \dots, \underline{w}_k \in V$ and write, for every $i \in \{1, \dots, k\}$, $\underline{w}_i = \sum_{j=1}^{n} \lambda_{ji} \underline{v}_j$ with $\lambda_{1i}, \dots, \lambda_{ni} \in K$. The matrix

$$A_{\mathcal{B}} = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \dots & \lambda_{1k} \\ \lambda_{21} & \lambda_{22} & \dots & \lambda_{2k} \\ \dots & \dots & \dots & \dots \\ \lambda_{n1} & \lambda_{n2} & \dots & \lambda_{nk} \end{pmatrix}$$

is called *component matrix* of the vectors $\underline{w}_1, \dots, \underline{w}_k$ with respect to the basis $\mathcal{B}$.

Example 2.3.7. Let $V = \mathbb{R}^3$ and let $\mathcal{B} = ((1,1,1), (1,0,1), (0,0,-1))$, that is a basis of V. Let $\underline{w}_1 = (2,1,0)$ and $\underline{w}_2 = (-1,0,0)$. We have that $\underline{w}_1 = (1,1,1) + (1,0,1) + 2(0,0,-1)$ and $\underline{w}_2 = -(1,0,1) - (0,0,-1)$.

Hence the component matrix of $\underline{w}_1, \underline{w}_2$ with respect to $\mathcal{B}$ is:

$$\begin{pmatrix} 1 & 0 \\ 1 & -1 \\ 2 & -1 \end{pmatrix}.$$

Theorem 2.3.8. Let V be a f.g. K-vector space of dimension n, let $\mathcal{B}$ be a basis of V and let $\underline{v}_1, \dots, \underline{v}_k \in V$ be k vectors with $k \leq n$. Let $A_{\mathcal{B}} \in M_{n\times k}(K)$ be the component matrix of such vectors with respect to $\mathcal{B}$. Then $\underline{v}_1, \dots, \underline{v}_k$ are linearly independent if and only if $\mathrm{rk}(A_{\mathcal{B}}) = k$.

Proof. Let $A \coloneqq A_{\mathcal{B}} = (\lambda_{ij})_{\substack{i=1,\dots,n \\ j=1,\dots,k}}$ be the component matrix.

First, we prove that if $\underline{v}_1, \dots, \underline{v}_k$ are linearly dependent then $\mathrm{rk}(A) < k$. Hence assume that $\underline{v}_1, \dots, \underline{v}_k$ are linearly dependent. Then there are $\alpha_1, \dots, \alpha_k \in K$, not all 0, such that

$$\alpha_1 \underline{v}_1 + \dots + \alpha_k \underline{v}_k = \underline{0}. \tag{10}$$

Let $\mathcal{B} = (\underline{w}_1, \dots, \underline{w}_n)$ and let $\underline{v}_i = \sum_{j=1}^{n} \lambda_{ji} \underline{w}_j$ for every i. Substituting in (10), we get that

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{k} \alpha_j \lambda_{ij} \right) \underline{w}_i = 0.$$

Since $\mathcal{B}$ is a basis, it follows that for every row index $i \in \{1, \dots, n\}$ we have

$$\alpha_1 \lambda_{i1} + \dots + \alpha_k \lambda_{ik} = 0. \tag{11}$$

Notice that the j-th column C_j of A is given by $\begin{pmatrix} \lambda_{1j} \\ \lambda_{2j} \\ \dots \\ \lambda_{nj} \end{pmatrix}$, and therefore relation (11) implies that $\sum_{j=1}^{k} \alpha_j C_j = \underline{0}$.

Now if we erase any $n - k$ rows from A, obtaining a square submatrix $\widetilde{A}$ of size k, relation (11) will still hold on every row of $\widetilde{A}$, of course. But this means precisely that the columns of $\widetilde{A}$, when thought as vectors in

$M_{k\times 1}(K)$, are linearly dependent. Hence, by Proposition 2.1.8, $\det(\widetilde{A}) = 0$. Since this holds for every square submatrix of A of size k, by Proposition 2.3.4 it follows that $\mathrm{rk}(A) < k$.

Conversely, we prove that if $\underline{v}_1, \dots, \underline{v}_k$ are linearly independent then $\mathrm{rk}(A) = k$. Assume then that $\underline{v}_1, \dots, \underline{v}_k$ are linearly independent. By Theorem 1.4.16, there exist $\underline{v}_{k+1}, \dots, \underline{v}_n \in \mathcal{B}$ such that $\mathcal{B}' = (\underline{v}_1, \dots, \underline{v}_n)$ is a basis of V. Now let H be the change of basis matrix from $\mathcal{B}'$ to $\mathcal{B}$. In order to obtain it, we need to express the vectors of $\mathcal{B}'$ in the basis $\mathcal{B}$. When doing this process on $\underline{v}_1, \dots, \underline{v}_k$, we obtain precisely the columns of A, by definition. On the other hand the vectors $\underline{v}_{k+1}, \dots, \underline{v}_n$ are already expressed with respect to the basis $\mathcal{B}$, as they are simply elements of such basis. Hence the corresponding columns of the change of basis matrix will have all entries equal to 0 except for one entry equal to 1. All in all, the matrix H will look like $(A|A')$, where

$$A' = \begin{pmatrix} \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & 1 \\ 1 & \dots & \dots & \dots \\ \dots & 1 & \dots & \dots \end{pmatrix}$$

is an $n \times (n-k)$ matrix whose columns have one entry equal to 1 and all the remaining ones equal to 0. Moreover, since $\underline{v}_{k+1}, \dots, \underline{v}_n$ are all different, if C, C' are two columns of A' then the entry 1 will be in two different positions.

Now the matrix H has non-zero determinant by Proposition 2.2.4. On the other hand, we can compute $\det H$ by Laplace theorem using the last column of A'. This has only one non-zero entry that is 1 in position i, so erasing the corresponding row of H we get that the determinant of H is (up to sign) that of $(\widetilde{A}|\widetilde{A}')$, where $\widetilde{A}$ is the submatrix obtained from A by erasing the i-th row and $\widetilde{A}'$ is the submatrix obtained from A' by erasing the i-th row and the last column. Now we can repeat this process using the last column of $\widetilde{A}'$; notice that such column will have exactly one non-zero entry 1, since when we erased the i-th row from A' we did not erased any other non-zero entry from A': this happens because the 1's in such matrix are all in different positions. Repeating this process until we use up all columns of A' we end up seeing that the determinant of H is, up to sign, that of a square submatrix of A obtained by erasing $n-k$ rows.

Since $\det H \neq 0$, this means that A has a square submatrix of size k with non-zero determinant, and hence $\mathrm{rk}(A) = k$. □

Corollary 2.3.9. Let V be a f.g. K-vector space of dimension n. Let $\underline{v}_1, \dots, \underline{v}_k \in V$ and let $\mathcal{B}$ be a basis of V. Then $\underline{v}_1, \dots, \underline{v}_k$ are linearly dependent if and only if in the component matrix $A_{\mathcal{B}}$ every square submatrix of size k has determinant 0.

Proof. By Theorem 2.3.8, $\underline{v}_1, \dots, \underline{v}_k$ are linearly dependent if and only if $A_{\mathcal{B}}$ has rank $< k$, and this happens precisely when every submatrix of size k has determinant 0, by the definition of rank. □

Corollary 2.3.10. Let V be a f.g. K-vector space of dimension n. Let $\underline{v}_1, \dots, \underline{v}_n \in V$ and let $\mathcal{B}$ be a basis of V. Then $(\underline{v}_1, \dots, \underline{v}_n)$ is a basis of V if and only if the component matrix of $\underline{v}_1, \dots, \underline{v}_n$ with respect to $\mathcal{B}$ has non-zero determinant.

Proof. By Corollary 1.4.15, $(\underline{v}_1, \dots, \underline{v}_n)$ is a basis if and only if $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent. By Theorem 2.3.8, this happens if and only if the component matrix $A_{\mathcal{B}}$ of $\underline{v}_1, \dots, \underline{v}_n$ with respect to $\mathcal{B}$ has rank n. Since this is an $n \times n$ matrix, it has rank n if and only if its determinant is non-zero, by Remark 2.3.2. □

Example 2.3.11.

- Let $V = \mathbb{R}^3$ and let $\underline{v}_1 = (1, 1, 0)$, $\underline{v}_2 = (-1, 0, 1)$ and $\underline{v}_3 = (2, 2, 2)$. In order to decide whether $(\underline{v}_1, \underline{v}_2, \underline{v}_3)$ is a basis of V or not, we can apply Corollary 2.3.10. That is, we choose a basis $\mathcal{B}$ of V, we write down the component matrix of $(\underline{v}_1, \underline{v}_2, \underline{v}_3)$ with respect to V and then we compute its determinant: this is non-zero if and only if $(\underline{v}_1, \underline{v}_2, \underline{v}_3)$ is a basis. Clearly the easiest choice for $\mathcal{B}$ is the canonical basis $\mathcal{B} = (\underline{e}_1, \underline{e}_2, \underline{e}_3)$; the component matrix is

$$A_{\mathcal{B}} = \begin{pmatrix} 1 & -1 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}$$

and its determinant is 2. Therefore $(\underline{v}_1, \underline{v}_2, \underline{v}_3)$ is a basis of V.

- Let $V = \mathbb{R}[x]_{\leq 3}$. Consider the vectors $\underline{v}_1 = 2 - x + 3x^2$, $\underline{v}_2 = 1 - x - x^2 - x^3$ and $\underline{v}_3 = -x - 5x^2 - 2x^3$. In order to decide whether they are linearly independent or not, we can apply Theorem 2.3.8. So first we choose a convenient basis of V, such as, for example, $\mathcal{B} = (1, x, x^2, x^3)$. Next, we write the component matrix of $(\underline{v}_1, \underline{v}_2, \underline{v}_3)$ with respect to $\mathcal{B}$. This is:

$$A_{\mathcal{B}} = \begin{pmatrix} 2 & 1 & 0 \\ -1 & -1 & -1 \\ 3 & -1 & -5 \\ 0 & -1 & -2 \end{pmatrix}.$$

Theorem 2.3.8 says that the vectors are linearly independent if and only if $\mathrm{rk}(A_{\mathcal{B}}) = 3$. The four submatrices of $A_{\mathcal{B}}$ of size 3 are:

$$\begin{pmatrix} 2 & 1 & 0 \\ -1 & -1 & -1 \\ 3 & -1 & -5 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 0 \\ -1 & -1 & -1 \\ 0 & -1 & -2 \end{pmatrix},$$

$$\begin{pmatrix} 2 & 1 & 0 \\ 3 & -1 & -5 \\ 0 & -1 & -2 \end{pmatrix}, \begin{pmatrix} -1 & -1 & -1 \\ 3 & -1 & -5 \\ 0 & -1 & -2 \end{pmatrix},$$

and they all have determinant 0. Therefore $\mathrm{rk}(A_{\mathcal{B}}) < 3$ and the three vectors are linearly dependent.

- Let $V = M_2(\mathbb{R})$, and consider the vectors

$$\underline{v}_1 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \underline{v}_2 = \begin{pmatrix} -1 & -1 \\ 0 & 0 \end{pmatrix}, \underline{v}_3 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \underline{v}_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Let $\mathcal{B}$ be the following basis of V:

$$\left(\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right).$$

The component matrix of $(\underline{v}_1, \underline{v}_2, \underline{v}_3, \underline{v}_4)$ with respect to $\mathcal{B}$ is:

$$A_{\mathcal{B}} = \begin{pmatrix}2 & -1 & 0 & 1\\ 0 & -1 & 1 & 1\\ 0 & 0 & 0 & 1\\ 1 & 0 & 1 & 1\end{pmatrix}.$$

The determinant of $A_{\mathcal{B}}$ is

$$\det A_{\mathcal{B}} = -\det\begin{pmatrix}2 & -1 & 0\\ 0 & -1 & 1\\ 1 & 0 & 1\end{pmatrix} = -2\det\begin{pmatrix}-1 & 1\\ 0 & 1\end{pmatrix} - \det\begin{pmatrix}-1 & 0\\ -1 & 1\end{pmatrix} =$$

$$= 2 + 1 = 3 \neq 0,$$

and therefore $(\underline{v}_1, \underline{v}_2, \underline{v}_3, \underline{v}_4)$ is a basis of V by Corollary 2.3.10.

Let $A \in M_{m\times n}(K)$. The rows of A can be thought as elements of K^n, since they are n-tuples of elements of K. Analogously, the columns of A can be thought as elements of K^m.

Example 2.3.12. Let

$$A = \begin{pmatrix}1 & 2 & 3\\ 4 & \sqrt{2} & -1\end{pmatrix} \in M_{2\times 3}(\mathbb{R}).$$

The two rows of A can be seen as the vectors $(1, 2, 3)$ and $(4, \sqrt{2}, -1)$ in $\mathbb{R}^3$. The three columns of A can be seen as the vectors $(1, 4), (2, \sqrt{2})$ and $(3, -1)$ in $\mathbb{R}^2$.

Remark 2.3.13. Every matrix $A \in M_{m\times n}$ can be read as the component matrix of its column vectors, with respect to the canonical basis of K^m. In fact, if $C_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \dots \\ a_{mj} \end{pmatrix}$ is a column of A then we can identify C_j with the vector $(a_{1j}, a_{2j}, \dots, a_{mj}) \in K^m$, and one writes this vector as $a_{1j}\underline{e}_1 + a_{2j}\underline{e}_2 + \dots + a_{mj}\underline{e}_m$, where $(ue_1, \dots, \underline{e}_m)$ is the canonical basis of K^m. Hence A is the component matrix of the vectors $C_1, \dots, C_n$ with respect to the canonical basis.

Lemma 2.3.14. Let $A \in M_{m\times n}(K)$. Then the rank of A is equal to the maximum number of linearly independent columns of A.

Proof. By Remark 2.3.13, the matrix A is the component matrix of its column vectors $C_1, \dots, C_n$ with respect to the canonical basis of K^m. Let r be the maximum number of linearly independent columns of A, and let $C_{i_1}, \dots, C_{i_r}$ be linearly independent. By Theorem 2.3.8, the submatrix of A given by $(C_{i_1}|C_{i_2}|\dots|C_{i_r})$ has rank r. Hence $\mathrm{rk}(A) \geq r$. On the other hand, if it was $\mathrm{rk}(A) = s > r$, the would be a size s submatrix A' of A with non-zero determinant. The submatrix A' is formed by selecting s columns $C_{i_1}, \dots, C_{i_s}$ and s rows of A. Now consider the matrix $A'' = (C_{i_1}|C_{i_2}|\dots|C_{i_s})$. This is an $m \times s$ matrix that contains A' as a submatrix; since the latter has rank s, then $\mathrm{rk}(A'') = s$. But then by Theorem 2.3.8 the columns of A'' are linearly independent, and since they are also columns of A, this means that there are s linearly independent columns in A. Since $s > r$, we obtain a contradiction, because r was the maximum number of linearly independent columns. Hence it must be $s \leq r$, and it follows that $\mathrm{rk}(A) = r$. □

Corollary 2.3.15. The rank of $A \in M_{m\times n}(K)$ equals the maximum number of linearly independent rows of A.

Proof. By lemma 2.3.14 applied to ${}^tA$ we get that $\mathrm{rk}({}^tA)$ is the maximum number of linearly independent columns of ${}^tA$. On the other hand, the columns of ${}^tA$ are the rows of A, and $\mathrm{rk}(A) = \mathrm{rk}({}^tA)$. □

Definition 2.3.16. Let $A \in M_{m\times n}(K)$. The *space of rows* of A, denoted by $\mathcal{R}(A)$, is the subspace of K^n generated by the rows of A. The *space of columns* of A, denoted by $\mathcal{C}(A)$, is the subspace of K^m generated by the columns of A.

Example 2.3.17. If A is the matrix of example 2.3.12, the space of rows of A is the subspace of $\mathbb{R}^3$ generated by $(1,2,3)$ and $(4,\sqrt{2},-1)$. These are linearly independent vectors, so such subspace has dimension 2.

The space of columns of A is the subspace of $\mathbb{R}^2$ generated by the vectors $(1,4),(2,\sqrt{2})$ and $(3,-1)$. Notice that $(1,4)$ and $(2,\sqrt{2})$ are linearly independent, while

$$(3,-1) = \frac{3+\sqrt{2}}{1-4\sqrt{2}}(1,4) + \frac{13\sqrt{2}}{8\sqrt{2}-2}(2,\sqrt{2}),$$

so that $(1,4),(2,\sqrt{2}),(3,-1)$ are linearly dependent. Hence the space of columns has dimension 2, too.

Theorem 2.3.18 (Kronecker theorem). Let $A \in M_{m\times n}(K)$. Then

$$\operatorname{rk}(A) = \dim \mathcal{R}(A) = \dim \mathcal{C}(A).$$

Proof. By Lemma 2.3.14 and Corollary 2.3.15, $\operatorname{rk}(A)$ is the maximum number of linearly independent columns (maximum number of linearly independent rows) of A. By Corollary 1.4.15, this equals the dimension of $\mathcal{C}(A)$ (dimension of $\mathcal{R}(A)$). □

Corollary 2.3.19.

1. Let $A \in M_{m\times n}(K)$. The rank of A is the maximum number of linearly independent rows or linearly independent columns of A.
2. Let $A \in M_n(K)$. Then the following are equivalent:
   (a) $\det A \neq 0$;
   (b) A is invertible;
   (c) $\operatorname{rk}(A) = n$;

(d) the rows (columns) of A are linearly independent, when seen as vectors in K^n;

(e) the rows (columns) of A are a basis of K^n.

Proof. 1. It follows by Theorem 2.3.18 and Corollary 1.4.15.

2. The equivalence $(a) \iff (b)$ follows from Theorem 2.1.12.

The equivalence $(a) \iff (c)$ follows from the definition of rank.

The equivalence $(c) \iff (d)$ follows from Theorem 2.3.18 theorem, together with Corollary 1.4.15.

The equivalence $(d) \iff (e)$ follows from Corollary 1.4.15. □

Kronecker's theorem yields an easier way to compute the rank of a matrix. By Corollary 2.3.5, if $A \in M_{m\times n}(K)$ is a matrix, in order to prove that A has rank r we need to find a size r square submatrix of A with non-zero determinant and then show that every square submatrix of A of size $r+1$ has determinant 0. However, this can result in a large number of operations. The next theorem yields a simpler criterion.

Theorem 2.3.20. Let $A \in M_{m\times n}(K)$ be a matrix. Suppose that A has a square submatrix B of size r with nonzero determinant and that every square submatrix of A of size $r+1$ containing B has determinant 0. Then $\mathrm{rk}(A) = r$.

Proof. The submatrix B is formed by taking r columns $C_{i_1}, \dots, C_{i_r}$ and r rows from A, where $i_1 < i_2 < \dots < i_r$. Now consider the matrix $\widetilde{B} = (C_{i_1}|\dots|C_{i_r}) \in M_{m\times r}(K)$; this has B as a size r square submatrix with non-zero determinant, and therefore it has rank r. By Theorem 2.3.8, the columns $C_{i_1}, \dots, C_{i_r}$ are therefore linearly independent when seen as vectors of K^m.

We now claim that if C is a column of A different from $C_{i_1}, \dots, C_{i_r}$, then $C_{i_1}, \dots, C_{i_r}, C$ are linearly dependent vectors of K^m. Notice that this implies that the columns $C_{i_1}, \dots, C_{i_r}$ span the space of columns $\mathcal{C}(A)$, and since they are linearly independent then by Theorem 2.3.18 we have $\mathrm{rk}(A) = r$.

Let C be a column of A different from $C_{i_1}, \dots, C_{i_r}$, and consider the $m \times (r+1)$ submatrix $\widetilde{B}'$ of A formed by taking the columns $C_{i_1}, \dots, C_{i_r}$ and C. This has B as a submatrix, formed by taking the r columns $C_{i_1}, \dots, C_{i_r}$ and r rows $R_{j_1}, \dots, R_{j_r}$. Now consider the matrix $\widetilde{B}''$ formed only by the r rows $R_{j_1}, \dots, R_{j_r}$ of $\widetilde{B}'$. This is an $r \times (r+1)$ matrix that

has B as a size r square submatrix with non-zero determinant; hence it has rank r. By Theorem 2.3.18, this implies that $R_{j_1}, \dots, R_{j_r}$ are linearly independent when seen as vectors of K^{r+1}. Now let R' be a row of $\widetilde{B}'$ different from $R_{j_1}, \dots, R_{j_r}$. The matrix formed by $R', R_{j_1}, \dots, R_{j_r}$ is an $(r+1)\times(r+1)$ submatrix of A that contains B, and hence it has determinant 0 by hypothesis. Therefore, $R', R_{j_1}, \dots, R_{j_r}$ are linearly dependent vectors of K^{r+1}. Since this holds for every row of $\widetilde{B}'$, it follows that $R_{j_1}, \dots, R_{j_r}$ span $R(\widetilde{B}')$, and hence the matrix $\widetilde{B}'$ has rank r by Theorem 2.3.18. But then, again by Theorem 2.3.18, the $r+1$ columns of $\widetilde{B}'$ must be linearly dependent, as desired. □

Example 2.3.21. Let $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & -1 & 6 & 7 \\ 7 & -4 & 3 & 2 \end{pmatrix} \in M_{3\times 4}(\mathbb{R})$. The submatrix $B = \begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix}$ has determinant $-11 \neq 0$, so $\mathrm{rk}(A) \geq 2$. The 3×3 submatrices of A that contain B are:

$$\begin{pmatrix} 1 & 2 & 3 \\ 5 & -1 & 6 \\ 7 & -4 & 3 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 4 \\ 5 & -1 & 7 \\ 7 & -4 & 2 \end{pmatrix},$$

and they both have determinant 0. Hence $\mathrm{rk}(A) = 2$ by Theorem 2.3.20. Notice that A has four different square submatrices of size 3, but thanks to Theorem 2.3.20 we only need to look at two of them.

Alternatively, one can notice that the first two rows R_1, R_2 of A are linearly independent, while $R_3 = -3R_1 + 2R_2$, so that $\mathrm{rk}(A) = 2$ by Kronecker theorem.

Chapter 3: Linear systems

3.1 Compatibility of linear systems

Definition 3.1.1. Let K be a field, let $m, n \geq 1$ be integers. A *linear system of m equations in n variables* with coefficients in K is a system of equations of the following form:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots \\ a_{m1}x_1 + a_{m2} + \ldots + a_{mn}x_n = b_m \end{cases}, \tag{12}$$

where the elements a_{ij}, b_k are in K and $x_1, \ldots, x_n$ are variables.

The *matrix associated to the linear system* is the matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \in M_{m\times n}(K).$$

If we let

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_1 \\ b_2 \\ \ldots \\ b_m \end{pmatrix},$$

we can write linear system (12) in its *matrix form*

$$AX = B, \tag{13}$$

where AX is the usual matrix multiplication.

Definition 3.1.2. A column vector $\overline{X} = \begin{pmatrix} \overline{x}_1 \\ \overline{x}_2 \\ \dots \\ \overline{x}_n \end{pmatrix} \in M_{n\times 1}(K)$ is a *solution* to system (12) if $A\overline{X} = B$.

A linear system is *compatible* if it admits at least one solution.

Note:-

Notice that there is a big difference between the matrix form of a linear system (13) and the identity $A\overline{X} = B$ for some $\overline{X} \in M_{n\times 1}(K)$. In fact, the former is a formal way of expressing (12), that is a system of equations, while the latter is an identity between matrices with coefficients in K.

When the number of variables is low, typically less than 5, instead of labeling them as $x_1, \dots, x_n$ we will label them as x, y, z, t.

Example 3.1.3.

- The system
$$\begin{cases} 2x + 3z = 1 \\ y - z = -1 \end{cases}$$
is a linear system of 2 equations and 3 variables with coefficients in $\mathbb{R}$. The matrix associated to the system is
$$A = \begin{pmatrix} 2 & 0 & 3 \\ 0 & 1 & -1 \end{pmatrix},$$
and if we let $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ and $B = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ then the matrix form of the system is $AX = B$.

A solution is, for example, the vector $\begin{pmatrix} -4 \\ 2 \\ 3 \end{pmatrix}$, and therefore the system is compatible. Another one is $\begin{pmatrix} -7 \\ 4 \\ 5 \end{pmatrix}$. We will see later on that this system has infinitely many solutions.

- The system of 3 equations in 2 variables

$$\begin{cases} x + y = 1 \\ x - y = 3 \\ 2x - 2y = 4 \end{cases},$$

when considered as a linear system over $\mathbb{R}$, has no solutions, since clearly the second and the third equations cannot hold true at the same time for any pair of real numbers (x, y). This system is therefore not compatible.

Now let $A \in M_{m\times n}(K)$, $\overline{X} \in M_{n\times 1}(K)$ and $B \in M_{m\times 1}(K)$. The key observation that allows to relate linear systems to vector spaces is the following: if $C_1, \dots, C_n$ are the columns of A, so that $A = (C_1|C_2|\dots|C_n)$, and $\overline{X} = \begin{pmatrix} \overline{x}_1 \\ \overline{x}_2 \\ \dots \\ \overline{x}_n \end{pmatrix}$, then

$$A\overline{X} = \overline{x}_1 C_1 + \overline{x}_2 C_2 + \dots + \overline{x}_n C_n.$$

Namely, multiplying A by $\overline{X}$ means taking the linear combination of the columns of A with coefficients $\overline{x}_1, \dots, \overline{x}_n$.

Note:-

If $AX = B$ is a linear system, we will denote by $(A|B)$ the matrix obtained

by adjoining the column B to the matrix A. For example, if $A = \begin{pmatrix} 2 & 2 \\ 1 & -3 \end{pmatrix}$ and $B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, the matrix $(A|B)$ is $\begin{pmatrix} 2 & 2 & 1 \\ 1 & -3 & 0 \end{pmatrix}$.

Theorem 3.1.4 (Rouché-Capelli). Let K be a field, $A \in M_{m\times n}(K)$, $X = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}$ and $B \in M_{m\times 1}(K)$. The system $AX = B$ is compatible if and only if $\mathrm{rk}(A) = \mathrm{rk}(A|B)$.

Proof. The system is compatible if and only if there exists $\overline{X} \in M_{n\times 1}(K)$ such that $A\overline{X} = B$. By what we observed above, this is equivalent to the existence of coefficients $\overline{x}_1, \dots, \overline{x}_n \in K$ such that

$$\overline{x}_1 C_1 + \overline{x}_2 C_2 + \dots + \overline{x}_n C_n = B,$$

where $C_1, \dots, C_n$ are the columns of A. This is equivalent to saying that $B \in \langle C_1, \dots, C_n \rangle$, which in turn is equivalent to saying that

$$\dim\langle C_1, \dots, C_n \rangle = \dim\langle C_1, \dots, C_n, B \rangle.$$

By Kronecker theorem, this is equivalent to asking that $\mathrm{rk}(A) = \mathrm{rk}(A|B)$. □

A particular case of Rouché-Capelli theorem is that where $m = n$, i.e. where the number of equations equals the number of variables.

Theorem 3.1.5 (Cramer). Let $AX = B$ be a linear system over a field K, where $A \in M_n(K)$. If $\det A \neq 0$, then the system is compatible and has a

unique solution, given by

$$\overline{X} = \begin{pmatrix} \frac{\det(B_1)}{\det(A)} \\ \frac{\det(B_2)}{\det(A)} \\ \cdots \\ \frac{\det(B_n)}{\det(A)} \end{pmatrix}.$$

Here B_i is the matrix obtained from A by replacing the i-th column with B.

Proof. First, since $\det A \neq 0$ then by Corollary 2.3.19 we have $\mathrm{rk}(A) = n$. Now $(A|B)$ is an $n \times (n+1)$ matrix, so that its rank is at most n. Since A is a submatrix of size n of $(A|B)$ with non-zero determinant, it follows that $\mathrm{rk}(A|B) = n$ and hence by Theorem 3.1.4 the system is compatible.

Now suppose that $X_1, X_2 \in M_{n\times 1}(K)$ are two solutions of the system, so that $AX_1 = AX_2$. Since $\det A \neq 0$ then A is invertible, so we can multiply both sides of the expression by A^{-1}, obtaining

$$A^{-1}(AX_1) = A^{-1}(AX_2).$$

Since matrix multiplication is associative, we get $(AA^{-1})X_1 = (AA^{-1})X_2$, and since $AA^{-1} = I_n$ it follows that $X_1 = X_2$. Hence the solution of the system is unique.

Notice that the vector $\overline{X} = A^{-1}B$ is a solution, because $A(A^{-1}B) = (AA^{-1})B = B$, and therefore it is the unique solution. To end the proof, we just need to show that this vector has the form claimed in the state-

ment. Let $B = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix}$. Recall that

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} A_{11} & -A_{21} & \dots & (-1)^{n+1}A_{n1} \\ -A_{12} & A_{22} & \dots & (-1)^{n+2}A_{n2} \\ \dots & \dots & \dots & \dots \\ (-1)^{1+n}A_{1n} & (-1)^{2+n}A_{2n} & \dots & A_{nn} \end{pmatrix},$$

where A_{ij} is the determinant of the $(n-1) \times (n-1)$ submatrix of A obtained by erasing the i-th row and the j-th column. Therefore we have:

$$A^{-1}B = \frac{1}{\det(A)} \begin{pmatrix} \sum_{i=1}^n b_i(-1)^{i+1}A_{i1} \\ \sum_{i=1}^n b_i(-1)^{i+2}A_{i2} \\ \dots \\ \sum_{i=1}^n b_i(-1)^{i+n}A_{in} \end{pmatrix}.$$

A moment of reflection, using Laplace theorem on the j-th column, shows that $\sum_{i=1}^n b_i(-1)^{i+j}A_{ij}$ is exactly the determinant of the matrix $B_j = (C_1|\dots|C_{j-1}|B|C_{j+1}|\dots|C_n)$, where $C_1, \dots, C_n$ are the columns of A. □

Example 3.1.6. Let $A = \begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ 0 & 0 & 3 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ and $B = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$, where all coefficients are real. Using Laplace theorem on the last row of A we see that $\det A = -6 \neq 0$, so by Theorem 3.1.5 the system has a

unique solution. In the notation of the theorem we have:

$$B_1 = \begin{pmatrix} 2 & 1 & -1 \\ 0 & -1 & 1 \\ 1 & 0 & 3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 3 \end{pmatrix}, \quad B_3 = \begin{pmatrix} 1 & 1 & 2 \\ 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

so that $\det B_1 = -6$, $\det B_2 = -8$, $\det B_3 = -2$. This yields

$$\overline{X} = \begin{pmatrix} 1 \\ 4/3 \\ 1/3 \end{pmatrix}$$

as the unique solution to the system.

3.2 The rank-nullity theorem

The next step in the theory of linear system is to describe, in a precise sense, how many solutions a compatible linear system has.

Example 3.2.1.

- Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M_2(\mathbb{R})$. The system $AX = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ has a unique solution, by Theorem 3.1.5.
- Let $A = \begin{pmatrix} 1 & 2 \end{pmatrix} \in M_{1\times 2}(\mathbb{R})$. The system $AX = 0$ has infinitely many solutions, since all vectors of the form $\begin{pmatrix} -2x \\ x \end{pmatrix}$, with $x \in \mathbb{R}$, are solutions.
- Let $A = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \in M_{2\times 1}(\mathbb{R})$. The system $AX = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ has no solutions, since if $x \in \mathbb{R} = M_1(\mathbb{R})$ is a solution, then the two equations $x = 1$ and $2x = 1$ should hold true at the same time.

Definition 3.2.2. A linear system $AX = B$ is *homogeneous* if B is the zero vector.

Remark 3.2.3. A homogeneous linear system is always compatible, as it admits the zero vector as a solution. Namely, if $A \in M_{m\times n}(K)$ and $\overline{X} = \begin{pmatrix} 0 \\ \dots \\ 0 \end{pmatrix} \in M_{n\times 1}(K)$ then $A\overline{X} = \begin{pmatrix} 0 \\ \dots \\ 0 \end{pmatrix} \in M_{m\times 1}(K)$. We will denote by $\underline{0}$ the $m \times 1$ or $n \times 1$ zero matrix, so that a homogeneous linear system will be written as $AX = \underline{0}$.

If A is a square matrix with non-zero determinant, the system $AX = \underline{0}$ only has $X = \underline{0}$ as a solution, by Theorem 3.1.5.

Definition 3.2.4. Let K be a field and $A \in M_{m\times n}(K)$. The *kernel* of A is the set of solutions of the homogeneous linear system $AX = \underline{0}$. The kernel of A will be denoted by $\ker A$.

A solution of the system $AX = \underline{0}$ is called *nontrivial* if it is different from $\underline{0}$.

Remark 3.2.5. Let $A \in M_{m\times n}(K)$. Then $\ker A$ is a vector subspace of $M_{n\times 1}(K)$. In fact, if $\overline{X}, \overline{Y} \in \ker A$ and $\alpha, \beta \in K$ then

$$A(\alpha\overline{X} + \beta\overline{Y}) = A(\alpha\overline{X}) + A(\beta\overline{Y}) = \alpha(A\overline{X}) + \beta(A\overline{Y}) = \underline{0} + \underline{0} = \underline{0},$$

so that $\alpha\overline{X} + \beta\overline{Y} \in \ker A$.

Lemma 3.2.6. Let K be a field and $A \in M_{m\times n}(K)$. Let $p \in \{1, \dots, n\}$ be a natural number. Let $\underline{e}_{i_1}, \dots, \underline{e}_{i_p}$ be vectors of the canonical basis of $M_{n\times 1}(K)$, with $1 \leq i_1 < i_2 < \dots < i_p \leq n$. Let $C_1, \dots, C_n$ be the columns of A. Then $C_{i_1}, \dots, C_{i_p}$ are linearly independent if and only if $\ker A \cap \langle \underline{e}_{i_1}, \dots, \underline{e}_{i_p} \rangle = \{\underline{0}\}$.

Proof. Start by noticing that $\langle \underline{e}_{i_1}, \dots, \underline{e}_{i_p} \rangle$ coincides with the set of $n \times 1$ matrices $(a_{i1})_{i=1\dots,n} \in M_{n\times 1}(K)$ with the property that $a_{j1} = 0$ for every

$j \notin \{i_1, \dots, i_p\}$. It follows that the set $\{A\overline{X} : \overline{X} \in \langle \underline{e}_{i_1}, \dots, \underline{e}_{i_p} \rangle\}$ coincides with the set of all linear combinations of $C_{i_1}, \dots, C_{i_p}$: if $\alpha_1, \dots, \alpha_p \in K$, the linear combination $\sum_{j=1}^{p} \alpha_j C_{i_j}$ corresponds to $A(\sum_{j=1}^{p} \alpha_j \underline{e}_{i_j})$.

The condition $\ker A \cap \langle \underline{e}_{i_1}, \dots, \underline{e}_{i_p} \rangle = \{\underline{0}\}$ means that no non-zero vectors in $\langle \underline{e}_{i_1}, \dots, \underline{e}_{i_p} \rangle$ are solutions to the system $AX = \underline{0}$. By what we said above, this means precisely that no linear combination of $C_{i_1}, \dots, C_{i_p}$ with not all coefficients being zero gives the zero vector; in other words, $C_{i_1}, \dots, C_{i_p}$ are linearly independent. □

Theorem 3.2.7 (Rank-nullity theorem)**.** Let K be a field and $A \in M_{m \times n}(K)$. Then

$$\dim(\ker A) = n - \mathrm{rk}(A).$$

Proof. Let $r = \mathrm{rk}(A)$ and $p = \dim(\ker A)$. We need to prove that $p = n - r$. Since $\mathrm{rk}(A) = r$, by Theorem 2.3.18 there are r linearly independent columns $C_{i_1}, \dots, C_{i_r}$ in A. By Lemma 3.2.6, it follows that $\ker A \cap \langle \underline{e}_{i_1}, \dots, \underline{e}_{i_r} \rangle = \{\underline{0}\}$. Therefore, by Grassmann formula we have:

$$\dim(\langle \underline{e}_{i_1}, \dots, \underline{e}_{i_r} \rangle + \ker A) = r + p \leq n,$$

so that $p \leq n - r$. Now we have to prove the converse inequality.

Let $\mathcal{B}$ be a basis of $\ker A$ in $M_{n \times 1}(K)$. By Theorem 1.4.16, the basis $\mathcal{B}$ can be completed to a basis $\mathcal{B}'$ of $M_{n \times 1}(K)$ using vectors of the canonical basis. Thus there are $\underline{e}_{i_1}, \dots, \underline{e}_{i_{n-p}}$ in the canonical basis such that $\mathcal{B} \cup (\underline{e}_{i_1}, \dots, \underline{e}_{i_{n-p}})$ is a basis of $M_{n \times 1}(K)$. Since the latter set is a basis, we must have, by Grassmann formula, that

$$\ker A \cap \langle \underline{e}_{i_1}, \dots, \underline{e}_{i_{n-p}} \rangle = \{\underline{0}\}.$$

By Lemma 3.2.6, it follows that the columns $C_{i_1}, \dots, C_{i_{n-p}}$ are linearly independent. By Theorem 2.3.18, this implies that $r \geq n - p$, i.e. $p \geq n - r$. □

Corollary 3.2.8. Let K be a field and $A \in M_{m \times n}(K)$. The homogeneous system $AX = \underline{0}$ has a nontrivial solution if and only if $\mathrm{rk}(A) < n$. In particular:

1. if $m < n$, the homogeneous system $AX = \underline{0}$ always has a nontrivial solution.

2. if $m = n$, the homogeneous system $AX = \underline{0}$ has a nontrivial solution if and only if $\det A = 0$.

Proof. The system $AX = \underline{0}$ has a nontrivial solution if and only if $\ker A \neq \{\underline{0}\}$, that is, if and only if $\dim \ker A > 0$. By Theorem 3.2.7, this is equivalent to asking that $n > \mathrm{rk}(A)$.

If $m < n$ then $\mathrm{rk}(A) \leq m < n$, since $\mathrm{rk}\, A \leq \min\{m, n\}$, and hence the system has a nontrivial solution.

If $m = n$ then the condition $\mathrm{rk}(A) < n$ is equivalent to $\det A = 0$ by Corollary 2.3.19. □

Proposition 3.2.9. Let K be a field, $A \in M_{m\times n}(K)$ and $B \in M_{m\times 1}(K)$. Suppose that the system $AX = B$ is compatible and let $\overline{X} \in M_{n\times 1}(K)$ be a solution. Then the set S of all solutions of the system $AX = B$ is given by:

$$\{\overline{X} + Z \colon Z \in \ker A\}.$$

Proof. Let $\overline{S} = \{\overline{X} + Z \colon Z \in \ker A\}$. We need to prove that $S = \overline{S}$. First, let $\overline{Y} \in S$, so that $A\overline{Y} = B$. Since $A\overline{X} = B$ as well, subtracting these two equations term by term we get that

$$A(\overline{Y} - \overline{X}) = B - B = \underline{0}.$$

This means exactly that $\overline{Y} - \overline{X} \in \ker A$, or, in other words, that there exists $Z \in \ker A$ such that $\overline{Y} - \overline{X} = Z$. Hence $\overline{Y} = \overline{X} + Z$, that is, $\overline{Y} \in \overline{S}$.

Conversely, let $\overline{Y} \in \overline{S}$, so that there exists $Z \in \ker A$ such that $\overline{Y} = \overline{X} + Z$. Then

$$A\overline{Y} = A(\overline{X} + Z) = A\overline{X} + AZ = B + \underline{0} = B,$$

so that $\overline{Y} \in S$. □

Proposition 3.2.9 completely describes all solutions of a compatible linear system $AX = B$: once we find one solution $\overline{X}$ of the system, all solutions are of the form $\overline{X} + Z$, where Z is any element of the kernel of A.

Remark 3.2.10. When $K = \mathbb{R}$, if a system of m equations in n variables is compatible, we will say that it has $\infty^{n-\mathrm{rk}(A)}$ solutions. When $n = \mathrm{rk}(A)$, the system has a unique solution.

3.3 How do I solve a linear system?

To conclude this chapter, we have to explain how to solve a linear system. Thanks to Theorem 3.2.7 and Proposition 3.2.9, we know the structure of the set of solutions. Now all remains to do is to actually find the solutions.

We begin by proving a lemma that allows to reduce a linear system to a smaller one with the same solutions.

Lemma 3.3.1. Let K be a field, $A \in M_{m\times n}(K)$ and $B = \begin{pmatrix} b_1 \\ \dots \\ b_m \end{pmatrix} \in M_{m\times 1}(K)$. Let the linear system $AX = B$ be compatible and let $r = \mathrm{rk}(A) = \mathrm{rk}(A|B)$. Let $R_1, \dots, R_m$ be the rows of A and $\widetilde{R}_1, \dots, \widetilde{R}_m$ be the rows of $(A|B)$, so that deleting the last entry of $\widetilde{R}_i$ one obtains R_i. Let $1 \leq i_1 < i_2 < \dots < i_r \leq m$ be such that $\mathrm{rk}\left(\begin{array}{c} R_{i_1} \\ \hline R_{i_2} \\ \hline \dots \\ \hline R_{i_r} \end{array}\right) = r$, let $A' = \left(\begin{array}{c} R_{i_1} \\ \hline R_{i_2} \\ \hline \dots \\ \hline R_{i_r} \end{array}\right)$ and $B' = \left(\begin{array}{c} b_{i_1} \\ \hline b_{i_2} \\ \hline \dots \\ \hline b_{i_r} \end{array}\right)$. Then the following hold:

1. $\mathrm{rk}(A'|B') = r$.
2. An element $\overline{X} \in M_{n\times 1}(K)$ is a solution of the system $AX = B$ if and only if it is a solution of $A'X = B'$.

Proof. 1. The matrix $(A'|B')$ is obtained from A' by adding a final column, whose entries are the $i_1, i_2, \dots, i_r$-th entries of B. Hence $(A'|B')$ is a submatrix of $(A|B)$, and since A' is a submatrix of $(A'|B')$ of rank r and $(A|B)$ has rank r, too, we must have that $\mathrm{rk}(A'|B') = r$ by Remark 2.3.2.

2. An element $\overline{X} \in M_{n\times 1}(K)$ is a solution of $AX = B$ if and only if:

$$R_i\overline{X} = b_i \text{ for every } i = 1, \dots, m, \tag{14}$$

where $R_i\overline{X}$ is the usual matrix multiplication between the i-th row of A and $\overline{X}$. On the other hand, $\overline{X}$ is a solution to $A'X = B'$ if and only if $R_{i_j}\overline{X} = b_{i_j}$ for every $j = 1, \dots, r$. Hence it is obvious that if $\overline{X}$ is a solution of $AX = B$ then it is also a solution of $A'X = B'$.

Conversely, suppose that $\overline{X}$ is a solution of $A'X = B'$. This means that:

$$R_{i_j}\overline{X} = b_{i_j} \text{ for every } j = 1, \dots, r. \tag{15}$$

Since $\mathrm{rk}(A'|B') = \mathrm{rk}(A') = \mathrm{rk}(A) = \mathrm{rk}(A|B) = r$, we have by Kronecker theorem that

$$\langle \widetilde{R}_{i_1}, \dots, \widetilde{R}_{i_r} \rangle = \langle \widetilde{R}_1, \dots, \widetilde{R}_m \rangle,$$

or, in other words, that $\widetilde{R}_{i_1}, \dots, \widetilde{R}_{i_r}$ generate the space of rows of $(A|B)$. Hence for every $k \in \{1, \dots, m\}$ there exist $\lambda_1, \dots, \lambda_r \in K$ such that $\sum_{j=1}^{r} \lambda_j \widetilde{R}_{i_j} = \widetilde{R}_k$. This means, in particular, that:

$$\sum_{j=1}^{r} \lambda_j R_{i_j} = R_k \text{ and } \sum_{j=1}^{r} \lambda_j b_{i_j} = b_k. \tag{16}$$

From (15) and (16) we get that

$$R_k\overline{X} = \left(\sum_{j=1}^{k} \lambda_j R_{i_j}\right)\overline{X} = \sum_{j=1}^{k} (\lambda_j R_{i_j}\overline{X}) = \sum_{j=1}^{k} (\lambda_j b_{i_j}) = b_k.$$

Since this holds true for every $k \in \{1, \dots, m\}$, we have by (14) that $\overline{X}$ is a solution to $AX = B$. □

What Lemma 3.3.1 is saying is that once we have a compatible linear system, in order to solve it we can erase equations that are linearly dependent from the others.

Example 3.3.2. Let $K = \mathbb{R}$. Let $A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & -2 & 2 & -1 \\ 2 & -1 & 2 & 0 \\ 1 & 4 & -2 & 3 \end{pmatrix}$ and $B = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix}$. Let $R_1, \dots, R_4$ be the rows of A and $\widetilde{R}_1, \dots, \widetilde{R}_4$ be the rows of $(A|B)$. Since R_1, R_3 are linearly independent, while $R_2 = R_3 - R_1$ and $R_4 = 3R_1 - R_3$, we have $\mathrm{rk}(A) = 2$. Moreover, $\widetilde{R}_2 = \widetilde{R}_3 - \widetilde{R}_1$ and $\widetilde{R}_4 = 3\widetilde{R}_1 - \widetilde{R}_3$, so that $\mathrm{rk}(A|B) = 2$ and the system is compatible. By Lemma 3.3.1, in order to solve the system we can disregard the second and the fourth equation, i.e. it is enough to solve the system:

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & -1 & 2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

In consequence of Lemma 3.3.1, we can just look at systems of the form $AX = B$ with $A \in M_{m\times n}(K)$ and $\mathrm{rk}(A) = \mathrm{rk}(A|B) = m$. In fact, if the system is compatible then $\mathrm{rk}(A) = \mathrm{rk}(A|B) \leq m$, and we can erase equations until we get a basis of the space of rows of $(A|B)$.

Hence suppose that $A \in M_{m\times n}(K)$ is such that $\mathrm{rk}(A) = m$ and the system $AX = B$ is compatible. Clearly if $n = m$ then Theorem 3.1.5 already tells us how to solve it. In principle, this theorem can be always used, even when $n > m$, in view of the following observation. Since $\mathrm{rk}(A) = m$, the matrix A has m linearly independent columns, say $C_{i_1}, \dots, C_{i_m}$. Now consider the variables x_k, with $k \notin \{i_1, \dots, i_m\}$. However we fix values $\overline{x}_k \in K$ for such

variables, the system

$$\begin{cases} a_{1i_1}x_{i_1} + \ldots + a_{1i_m}x_{i_m} = b_1 - \sum_{k\notin\{i_1,\ldots,i_m\}} a_{1k}\overline{x}_k \\ a_{2i_1}x_{i_1} + \ldots + a_{2i_m}x_{i_m} = b_2 - \sum_{k\notin\{i_1,\ldots,i_m\}} a_{2k}\overline{x}_k \\ \ldots \\ a_{mi_1}x_{i_1} + \ldots + a_{mi_m}x_{i_m} = b_m - \sum_{k\notin\{i_1,\ldots,i_m\}} a_{mk}\overline{x}_k \end{cases}$$

is compatible, because the matrix that represents it is a square matrix of full rank, by construction. Therefore, we can just apply Theorem 3.1.5 to the system

$$\begin{cases} a_{1i_1}x_{i_1} + \ldots + a_{1i_m}x_{i_m} = b_1 - \sum_{k\notin\{i_1,\ldots,i_m\}} a_{1k}x_k \\ a_{2i_1}x_{i_1} + \ldots + a_{2i_m}x_{i_m} = b_2 - \sum_{k\notin\{i_1,\ldots,i_m\}} a_{2k}x_k \\ \ldots \\ a_{mi_1}x_{i_1} + \ldots + a_{mi_m}x_{i_m} = b_m - \sum_{k\notin\{i_1,\ldots,i_m\}} a_{mk}x_k \end{cases}, \tag{17}$$

where the variables x_k with $k \notin \{i_1, \ldots, i_m\}$ will be treated as parameters. Applying Theorem 3.1.5 we will obtain an expression of the form:

$$\begin{cases} x_{i_1} = d_1 + \sum_{k\notin\{i_1,\ldots,i_m\}} c_{1k}x_k \\ x_{i_2} = d_2 + \sum_{k\notin\{i_1,\ldots,i_m\}} c_{2k}x_k \\ \ldots \\ x_{i_m} = d_m + \sum_{k\notin\{i_1,\ldots,i_m\}} c_{mk}x_k \end{cases},$$

where the coefficients c_{ij} and d_ℓ are elements of k. This means that to obtain all solutions to our linear system, we have to let all variables x_k with $k \notin \{i_1, \ldots, i_m\}$ vary over K, and the values of the remaining variables are determined by the values of the former ones.

Note:-

Formally, solutions of a linear system $AX = B$ are vectors of $M_{n\times 1}(K)$, so they should be written as column vectors. However, this is annoying in practice, so we will often write solutions as vectors in K^n, namely as row vectors.

Example 3.3.3. Let us go back to the system of Example 3.3.2. We have

seen, thanks to Lemma 3.3.1, that it is enough to solve

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & -1 & 2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \tag{18}$$

Now, the matrix $A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & -1 & 2 & 0 \end{pmatrix}$ has rank 2. Let us choose two linearly independent columns: the first and the second one. These correspond to the variables x and y; treating the other two variables as parameters we can rewrite the system as:

$$\begin{cases} x + y = 1 - t \\ 2x - y = 1 - 2z \end{cases}.$$

Now this can be seen as a system of 2 equations in 2 variables, namely x and y, that is represented by the matrix $A' = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}$, that has determinant -3. Applying Theorem 3.1.5, we get the solutions:

$$x = -\frac{1}{3} \det \begin{pmatrix} 1-t & 1 \\ 1-2z & -1 \end{pmatrix} = -\frac{1}{3}(2z + t - 2)$$

$$y = -\frac{1}{3} \det \begin{pmatrix} 1 & 1-t \\ 2 & 1-2z \end{pmatrix} = -\frac{1}{3}(2t - 2z - 1).$$

This means that the set S of solutions of (18) is:

$$S = \left\{ \left(-\frac{1}{3}(2z + t - 2), -\frac{1}{3}(2t - 2z - 1), z, t \right) : z, t \in \mathbb{R} \right\}.$$

Notice how this has exactly the shape predicted by Proposition 3.2.9: a specific solution of the system is $(2/3, 1/3, 0, 0)$, and the kernel of the

matrix A is given by:

$$\left\{\left(-\frac{1}{3}(2z+t), -\frac{1}{3}(2t-2z), z, t\right) : z, t \in \mathbb{R}\right\},$$

that is a 2-dimensional subspace of $\mathbb{R}^4$.

Note:-

One is not obliged to use Theorem 3.1.5 to solve the system

$$\begin{cases} x + y = 1 - t \\ 2x - y = 1 - 2z \end{cases}.$$

For example, here one can also notice that adding up the two equation the relation

$$3x = 2 - t - 2z$$

must hold, so that $x = \frac{1}{3}(2 - t - 2z)$, and substituting this for x in any of the two equations gives the value of y.
Moreover, one can choose any two linearly independent columns from the matrix A. For example, a smarter choice here would be to choose the third and the fourth column, so that the system to be solved becomes:

$$\begin{cases} t = 1 - x - y \\ 2z = 1 - 2x + y \end{cases},$$

whose solution in t and z is obvious, and yields the following equivalent form of the set of solutions S of the system (18):

$$S = \left\{\left(x, y, \frac{1}{2}(1 - 2x + y), 1 - x - y\right) : x, y \in \mathbb{R}\right\}.$$

This is exactly the same set we found in Example 3.3.3, but written in a different way.

We end the section by illustrating another way of solving a system in the form (17). This is called *Gauss elimination method*, and it is based on the following observations.

1. Let $A \in M_m(K)$, $\overline{X} \in M_{n\times 1}(K)$, $B \in M_{m\times 1}(K)$ and $U \in \mathrm{GL}_m(K)$ be an invertible matrix. Then $A\overline{X} = B$ if and only if $(UA)\overline{X} = UB$. In fact, if $A\overline{X} = B$ then multiplying both sides by U one gets $(UA)\overline{X} = UB$,

and conversely if $(UA)\overline{X} = UB$ then multiplying both sides by U^{-1} one gets $A\overline{X} = B$.

2. Let $AX = B$ be a linear system, with $A \in M_{m\times n}(K)$ and $B \in M_{m\times 1}(K)$. Let $i, j \in \{1, \dots, m\}$ be two distinct indices. If A', B' are the matrices obtained from A, B, respectively, by swapping row i and row j, then $\overline{X}$ is a solution of $AX = B$ if and only if it is a solution of $A'X = B'$.

3. Let $A \in M_{m\times n}(K)$ and let $R_1, \dots, R_m$ be the rows of A. Let $i, j \in \{1, \dots, m\}$ with $j < i$ and let $c \in K$. Finally, let

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & c & \dots & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & 0 & 1 \end{pmatrix} \in M_m(K),$$

namely the $m \times m$ matrix that differs from the identity matrix just by the (i, j)-th entry, that is equal to c. Then U is invertible, since it is lower triangular and the entries on the diagonal are all 1, and UA is an $m \times n$ matrix that coincides with A, except for the fact that the i-throw is replaced by $cR_j + R_i$.

Given a square matrix A of size m, by applying the three operations described above, multiple times if necessary, we can find a matrix $U \in \mathrm{GL}_m(K)$ such that UA is upper triangular. Notice that we do not really need to compute U, we can just perform the following two types of operations on A: swapping two rows, or replacing a row R_i with $R_i + cR_j$, for some other row R_j and some $c \in K$.

Now let us go back to the linear system (17). In order to ease the notation, we assume that $\{i_1, \dots, i_m\} = \{1, \dots, m\}$, but the argument works in any case. Let $A' = (a_{ij})_{i,j=1,\dots,m} \in M_m(K)$ be the matrix of the coefficients of the system and write the system as $A'X = B'$. By our preliminary reductions, $\det A' \neq 0$. Now let $U \in \mathrm{GL}_m(K)$ be such that UA' is upper triangular. The system $UA' = UB'$, that has the same solutions as the original system by

point 1., has the form:

$$\begin{cases} a'_{11}x_1 + a'_{12}x_2 + \ldots + a'_{1n}x_n = d'_1 + \sum_{k=m+1}^{n} c'_{1k}x_k \\ a'_{22}x_2 + a'_{23}x_3 + \ldots + a'_{2n}x_n = d'_2 + \sum_{k=m+1}^{n} c'_{2k}x_k \\ a'_{33}x_3 + a'_{34}x_4 + \ldots + a'_{3n}x_n = d'_3 + \sum_{k=m+1}^{n} c'_{3k}x_k \\ \ldots \\ a'_{mm}x_m = d'_m + \sum_{k=m+1}^{n} c'_{mk}x_k \end{cases}.$$

That is, the last equation directly gives us the value of x_m. Substituting this into the $m-1$-th equation we immediately get the value of x_{m-1}. Substituting these values into the $(m-2)$-th equation we get the value of x_{m-2}, and so on. Notice that the fact that $\det A \neq 0$ is crucial, since it ensures that $a'_{ii} \neq 0$ for every $i = 1, \ldots, m$. Let us show how this algorithm works with two examples.

Example 3.3.4. Consider the linear system with real coefficients:

$$\begin{cases} 3x + 2y + z = 1 \\ x - y + z = 0 \\ x - z = 2 \end{cases},$$

whose associated matrices are:

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 1 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}.$$

The matrix A is square and has nonzero determinant, so we are already in the form of (17). Moreover, by Theorem 3.1.5 we know that the system has a unique solution. Let us bring A into upper triangular form. Let R_1, R_2, R_3 be the rows of A. As a first step, we replace R_2 with $R_2 - 1/3R_1$ and R_3 with $R_3 - 1/3R_1$, and we do the same on B. We end up with the

matrices:

$$A_1 = \begin{pmatrix} 3 & 2 & 1 \\ 0 & -5/3 & 2/3 \\ 0 & -2/3 & -4/3 \end{pmatrix}, \qquad B_1 = \begin{pmatrix} 1 \\ -1/3 \\ 5/3 \end{pmatrix}.$$

Next, if R'_1, R'_2, R'_3 are the rows of A_1, we replace R'_3 with $R'_3 - 2/5R'_2$, and we do the same on B_1. We end up with:

$$A_2 = \begin{pmatrix} 3 & 2 & 1 \\ 0 & -5/3 & 2/3 \\ 0 & 0 & -24/15 \end{pmatrix}, \qquad B_1 = \begin{pmatrix} 1 \\ -1/3 \\ 27/15 \end{pmatrix}.$$

The system $A_2X = B_2$ is:

$$\begin{cases} 3x + 2y + z = 1 \\ -5y + 2z = -1 \\ -8z = 9 \end{cases},$$

that easily gives $x = 7/8$, $y = -1/4$ and $z = -9/8$.

Example 3.3.5. Consider the system $AX = B$ over $\mathbb{R}$, where:

$$A = \begin{pmatrix} 1 & 1 & 2 & 0 & 0 \\ 1 & 0 & 1 & -1 & -1 \\ 0 & 1 & 1 & -1 & -1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}, \quad B = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \\ 2 \end{pmatrix}.$$

One checks that $R_2 = R_1 - R_5$ and $R_3 = R_1 - R_4$, where $R_1, \dots, R_5$ are the rows of $(A|B)$ while first, fourth and fifth rows of A are linearly independent. Hence $\mathrm{rk}(A) = \mathrm{rk}(A|B) = 3$, and by Theorem 3.2.7 the system is compatible and has ∞^2 solutions.

By Lemma 3.3.1, it is enough to consider the system given by the first,

fourth and fifth equations, namely the system:

$$\begin{cases} x_1 + x_2 + 2x_3 = 1 \\ x_1 + x_3 + x_4 + x_5 = 0 \\ x_2 + x_3 + x_4 + x_5 = 2 \end{cases} \tag{19}$$

whose associated matrices are:

$$A' = \begin{pmatrix} 1 & 1 & 2 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad \text{and} \qquad B' = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}.$$

The matrix A' has rank 3, by construction. The next step is to select three linearly independent columns of A'. For example, we can select the first, the second and the fourth. Now in system (19) we move the third and the fifth variables, namely the ones not corresponding to the selected columns, to the right side of the equalities, getting the system:

$$\begin{cases} x_1 + x_2 = 1 - 2x_3 \\ x_1 + x_4 = -x_3 - x_5 \\ x_2 + x_4 = 2 - x_3 - x_5 \end{cases}. \tag{20}$$

Now all we need to do is to solve for x_1, x_2, x_4. This is easy and can be done by substitution, or via Cramer's theorem 3.1.5. However, let us show how to use Gauss' elimination. The matrices associated to system (20) are:

$$A'' = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad \text{and} \qquad B'' = \begin{pmatrix} 1 - 2x_3 \\ -x_3 - x_5 \\ 2 - x_3 - x_5 \end{pmatrix}.$$

In order to bring A'' to upper triangular form, the first step is to replace its second row R_2 with $R_2 - R_1$, and to perform the same operation on

B''. This yields:

$$A_1'' = \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad \text{and} \qquad B_1'' = \begin{pmatrix} 1 - 2x_3 \\ -1 + x_3 - x_5 \\ 2 - x_3 - x_5 \end{pmatrix}.$$

Now the second and last step is to replace the third row R_3 of A_1'' with $R_3 + R_2$, and do the same on B_1''. We get:

$$A_1'' = \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \qquad \text{and} \qquad B_1'' = \begin{pmatrix} 1 - 2x_3 \\ -1 + x_3 - x_5 \\ 1 - 2x_5 \end{pmatrix}.$$

This corresponds to the system:

$$\begin{cases} x_1 + x_2 = 1 - 2x_3 \\ -x_2 + x_4 = -1 + x_3 - x_5 \\ 2x_4 = 1 - 2x_5 \end{cases}. \tag{21}$$

System (21) is easy to solve: the third equation tells us that $x_4 = 1/2 - x_5$; substituting into the second one we get that $x_2 = 3/2 - x_3$, and substituting the latter into the first tells us that $x_1 = -1/2 - x_3$. This means that the set of solutions to (21), and thus to (19), is

$$S = \{(-1/2 - x_3, 3/2 - x_3, x_3, 1/2 - x_5, x_5) \colon x_3, x_5 \in \mathbb{R}\}.$$

Once again, we can see how the set S matches the prediction of Proposition 3.2.9. A specific solution to the system is $(-1/2, 3/2, 0, 1/2, 0)$, while

$$\ker A = \langle (-1, -1, 1, 0, 0), (0, 0, 0, -1, 1) \rangle,$$

that is a two-dimensional subspace of $\mathbb{R}^5$, so that the set S can be written as

$$A = \{(-1/2, 3/2, 0, 1/2, 0) + Z \colon Z \in \ker A\}.$$

Chapter 4: Scalar products and orthogonality

4.1 Bilinear forms and scalar products

Definition 4.1.1. Let K be a field and V be a K-vector space. A *bilinear form* on V is a function

$$*\colon V \times V \to K$$

that satisfies the following properties:

1. for every $\underline{u}, \underline{v}, \underline{w} \in V$,
$$(\underline{u} + \underline{v}) * \underline{w} = \underline{u} * \underline{w} + \underline{v} * \underline{w};$$
2. for every $\underline{u}, \underline{v}, \underline{w} \in V$,
$$\underline{u} * (\underline{v} + \underline{w}) = \underline{u} * \underline{v} + \underline{u} * \underline{w};$$
3. for every $\underline{v}, \underline{w} \in V$ and every $\lambda \in K$,
$$\lambda(\underline{v} * \underline{w}) = (\lambda \underline{v}) * \underline{w} = \underline{v} * (\lambda \underline{w}).$$

If, in addition, for every $\underline{v}, \underline{w} \in V$ we have that

$$\underline{v} * \underline{w} = \underline{w} * \underline{v},$$

then $*$ is called a *symmetric bilinear form* or, alternatively, a *scalar product*.

Example 4.1.2.

- Let $V = \mathbb{C}^3$. The function
$$*\colon V \times V \to \mathbb{C}$$
$$((x_1, x_2, x_3), (y_1, y_2, y_3)) \mapsto x_1 y_1 + x_1 y_2 + x_2 y_2 + x_3 y_3$$
is a bilinear form. You can check, as an exercise, that properties 1., 2., 3. are satisfied. However, this is not a scalar product, since for example $(1, 1, 0) * (1, 0, 0) = 1$ while $(1, 0, 0) * (1, 1, 0) = 2$.

- Let $V = \mathbb{R}^2$. The function

$$*\colon V \times V \to \mathbb{R}$$

$$((x_1, x_2), (y_1, y_2)) \mapsto x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2$$

is a scalar product.

Definition 4.1.3. Let V be a K-vector space with a scalar product $*$. Two vectors $\underline{v}, \underline{w} \in V$ are *orthogonal* if $\underline{v} * \underline{w} = 0$.

Remark 4.1.4.

- Let V be a K-vector space and $*$ be a scalar product on V. Then the zero vector is orthogonal to every vector $\underline{v}$. In fact, $(\underline{0}+\underline{0}) * \underline{v} = 2(\underline{0} * \underline{v})$ by property 1. of bilinear forms, but on the other hand $(\underline{0}+\underline{0}) * \underline{v} = \underline{0} * \underline{v}$, so that $\underline{0} * \underline{v} = 2(\underline{0} * \underline{v})$. This implies that $\underline{0} * \underline{v} = 0$, and since a scalar product is a symmetric bilinear form, it follows that $\underline{v} * \underline{0} = 0$.
- It might happen that $\underline{v} * \underline{v} = 0$ even if $\underline{v}$ is not the zero vector. For example, in $V = \mathbb{R}^2$ consider the scalar product given by:

$$(x_1, x_2) * (y_1, y_2) = x_1y_1 - x_2y_1 - x_1y_2 + x_2y_2.$$

Then $(1, 1) * (1, 1) = 0$.

- If $\underline{v} * \underline{w} = 0$ then for every $\alpha, \beta \in K$ we have:

$$(\alpha\underline{v}) * (\beta\underline{w}) = (\alpha\beta)(\underline{v} * \underline{w}) = 0.$$

Definition 4.1.5. Let V be a K-vector space with a scalar product $*$. Let $A \subseteq V$ be a non-empty subset. The *orthogonal complement* of A in V is the set:

$$A^{\perp} = \{\underline{v} \in V \colon \underline{w} * \underline{v} = 0, \ \ \forall \underline{w} \in A\}.$$

Proposition 4.1.6. Let V be a K-vector space, let $*$ be a scalar product on V and let $A \subseteq V$ be a non-empty subset.

1. $A^\perp$ is a vector subspace of V.
2. If $A \subseteq B \subseteq V$, then $B^\perp \subseteq A^\perp$.
3. $A^\perp = \langle A \rangle^\perp$.
4. $\langle A \rangle \subseteq (A^\perp)^\perp$.
5. Let $U \subseteq V$ be a vector subspace and let $\mathcal{B}$ be a basis for U. Then $\mathcal{B}^\perp = U^\perp$.

Proof. 1. Let $\underline{v}_1, \underline{v}_2 \in A^\perp$, let $\alpha_1, \alpha_2 \in K$ and let $\underline{w} \in A$. Then

$$(\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2) * \underline{w} = \alpha_1(\underline{v}_1 * \underline{w}) + \alpha_2(\underline{v}_2 * \underline{w}) = 0 + 0 = 0,$$

so that $\alpha_1 \underline{v}_1 + \alpha_2 \underline{v}_2 \in A^\perp$.

2. If $\underline{v} \in B^\perp$, then $\underline{v} * \underline{w} = 0$ for every $\underline{w} \in B$. Since $A \subseteq B$, it follows in particular that $\underline{v} * \underline{w} = 0$ for every $\underline{w} \in A$, and therefore $\underline{v} \in A^\perp$.

3. Since $A \subseteq \langle A \rangle$, by 2. it follows that $\langle A \rangle^\perp \subseteq A^\perp$. Conversely, suppose that $\underline{v} \in A^\perp$. Let $\underline{w} \in \langle A \rangle$. Then, by definition of span, there exist $\alpha_1, \dots, \alpha_n \in K$ and $\underline{v}_1, \dots, \underline{v}_n \in A$ such that $\underline{w} = \sum_{i=1}^n \alpha_i \underline{v}_i$. Then:

$$\underline{v} * \underline{w} = \underline{v} * \left(\sum_{i=1}^n \alpha_i \underline{v}_i \right) = \sum_{i=1}^n \alpha_i (\underline{v} * \underline{v}_i) = 0$$

since $\underline{v} * \underline{v}_i = 0$ for every i, because $\underline{v}_i \in A$ and $\underline{v} \in A^\perp$.

4. We have that $(A^\perp)^\perp = \{\underline{v} \in V : \underline{v} * \underline{w} = 0 \ \forall \underline{w} \in A^\perp\}$, by definition. However, by point 3. we have that $A^\perp = \langle A \rangle^\perp$, so that

$$(A^\perp)^\perp = \{\underline{v} \in V : \underline{v} * \underline{w} = 0 \ \forall \underline{w} \in \langle A \rangle^\perp\}.$$

Now if $\underline{v} \in \langle A \rangle$ then by definition $\underline{v} * \underline{w} = 0$ for every $\underline{w} \in \langle A \rangle^\perp$, and therefore $\underline{v} \in (A^\perp)^\perp$.

5. Follows immediately from 3. by setting $A = \mathcal{B}$. □

4.2 Positive definite scalar products

Until the end of this chapter, we will only consider vector spaces over the field $\mathbb{R}$ of real numbers.

Definition 4.2.1. Let V be an $\mathbb{R}$-vector space and let $*$ be a scalar product on V. The product $*$ is *positive definite* if:

1. for every $\underline{v} \in V$ we have $\underline{v} * \underline{v} \geq 0$;
2. $\underline{v} * \underline{v} = 0$ if and only if $\underline{v} = \underline{0}$.

Positive definite scalar products will be denoted using a dot: $\cdot$.

Example 4.2.2. The most important example of positive definite scalar product is the usual scalar product on $V = \mathbb{R}^n$. That is, the function

$$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$$

$$((x_1, \dots, x_n), (y_1, \dots, y_n)) \mapsto \sum_{i=1}^{n} x_i y_i.$$

This will be called the *standard* or *euclidean* scalar product on $\mathbb{R}^n$.

However, there are many other examples. For instance, the function

$$\mathbb{R}^2 \times \mathbb{R}^2 \mapsto \mathbb{R}$$

$$((x_1, x_2), (y_1, y_2)) \mapsto 3x_1x_2 - x_2y_1 - x_1y_2 + 3y_1y_2$$

is a positive definite scalar product.

Definition 4.2.3. Let V be an $\mathbb{R}$-vector space and $\cdot$ a positive definite scalar product on V. The *norm* of a vector $\underline{v} \in V$ is defined as:

$$\|\underline{v}\| = \sqrt{\underline{v} \cdot \underline{v}}.$$

A vector $\underline{v} \in V$ is called *versor* if $\|\underline{v}\| = 1$. If $\underline{v} \in V$ is a non-zero vector, the *versor associated to* $\underline{v}$ is the vector $\frac{1}{\|\underline{v}\|}\underline{v}$.

Proposition 4.2.4. Let V be an $\mathbb{R}$-vector space with a positive definite scalar product $\cdot$. For every $\alpha \in \mathbb{R}$ and every $\underline{v} \in V$ we have:

$$\|\alpha \underline{v}\| = |\alpha| \|\underline{v}\|.$$

Consequently, if $\underline{v} \in V$ then the versor associated to $\underline{v}$ has norm 1.

Proof.
$$\|\alpha\underline{v}\| = \sqrt{(\alpha\underline{v}) \cdot (\alpha\underline{v})} = \sqrt{\alpha^2(\underline{v} \cdot \underline{v})} = |\alpha|\|\underline{v}\|.$$
□

Proposition 4.2.5 (Cauchy-Schwarz inequality)**.** Let V be an $\mathbb{R}$-vector space with a positive definite scalar product $\cdot$. Let $\underline{u}, \underline{v} \in V$. Then we have:
$$|\underline{u} \cdot \underline{v}| \leq \|\underline{u}\|\|\underline{v}\|,$$
and equality holds if and only if $\underline{u}, \underline{v}$ are linearly dependent.

Proof. If $\underline{u}, \underline{v}$ are linearly dependent, there exists $\alpha \in \mathbb{R}$ such that $\alpha\underline{u} = \underline{v}$, so that
$$|\underline{u} \cdot \underline{v}| = |(\alpha\underline{u}) \cdot \underline{u}| = |\alpha|\|\underline{u}\|^2 = |\alpha|\|\underline{u}\|\|\underline{u}\| = \|\underline{u}\|\|\underline{v}\|,$$
using Proposition 4.2.4, as desired. Hence we can assume that $\underline{u}, \underline{v}$ are linearly independent. This is equivalent to say that for every $\alpha \in \mathbb{R}$ we have $\alpha\underline{u} + \underline{v} \neq \underline{0}$. Therefore, for every $\alpha \in \mathbb{R}$ we have:
$$0 < (\alpha\underline{u} + \underline{v}) \cdot (\alpha\underline{u} + \underline{v}) = \alpha^2\|\underline{u}\|^2 + 2\alpha(\underline{u} \cdot \underline{v}) + \|\underline{v}\|^2.$$
This means that the degree 2 polynomial with real coefficients:
$$x^2\|\underline{u}\|^2 + 2x(\underline{u} \cdot \underline{v}) + \|\underline{v}\|^2$$
only assumes positive values. Hence, its discriminant must be negative, i.e.
$$(\underline{u} \cdot \underline{v})^2 - \|\underline{u}\|^2\|\underline{v}\|^2 < 0,$$
which is precisely the desired inequality. □

Definition 4.2.6. Let V be an $\mathbb{R}$-vector space with a positive definite scalar product $\cdot$. A subset $A = \{\underline{v}_1, \ldots, \underline{v}_n\} \subseteq V$ is called an *orthogonal system* if $\underline{v}_i \cdot \underline{v}_j = 0$ for every $i \neq j$. If in addition every $\underline{v}_i$ is a versor, the set is called an *orthonormal system*.

If, in addition, A is a basis then it will be referred to as an *orthogonal basis* or an *orthonormal basis*, respectively.

Theorem 4.2.7. Let $\{\underline{v}_1, \dots, \underline{v}_n\} \subseteq V$ be an orthogonal system not containing $\underline{0}$. Then $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent.

Proof. Suppose that $\alpha_1\underline{v}_1 + \dots + \alpha_n\underline{v}_n = \underline{0}$ for some $\alpha_1, \dots, \alpha_n \in \mathbb{R}$. For every $i \in \{1, \dots, n\}$, taking the scalar product with $\underline{v}_i$ on both sides of such equality we get:

$$0 = \underline{0} \cdot \underline{v}_i = (\alpha_1\underline{v}_1 + \dots + \alpha_n\underline{v}_n) \cdot \underline{v}_i = \sum_{j=1}^{n} \alpha_j(\underline{v}_j \cdot \underline{v}_i) = \alpha_i\|\underline{v}_i\|^2,$$

because $\underline{v}_i \cdot \underline{v}_j = 0$ whenever $i \neq j$. Now since $\underline{v}_i \neq \underline{0}$ and $\cdot$ is positive definite, we have that $\|\underline{v}_i\|^2 \neq 0$, and therefore it must be $\alpha_i = 0$. Since this is true for every i, the vectors $\underline{v}_1, \dots, \underline{v}_n$ are linearly independent. □

The next fundamental theorem to prove is that every f.g. $\mathbb{R}$-vector space endowed with a positive definite scalar product has an orthonormal basis. The proof is based on the following lemma.

Lemma 4.2.8. Let V be an $\mathbb{R}$-vector space endowed with a positive definite scalar product $\cdot$. Suppose that $\{\underline{v}_1, \dots, \underline{v}_n\}$ is an orthogonal system not containing $\underline{0}$ and let $\underline{w} \in V$ be such that $\underline{w} \notin \langle \underline{v}_1, \dots, \underline{v}_n \rangle$. Let

$$\underline{v}_{n+1} = \underline{w} - \sum_{i=1}^{n} \frac{\underline{w} \cdot \underline{v}_i}{\|\underline{v}_i\|^2}\underline{v}_i.$$

Then $\{\underline{v}_1, \dots, \underline{v}_{n+1}\}$ is an orthogonal system not containing $\underline{0}$.

Proof. To prove that $\{\underline{v}_1, \dots, \underline{v}_{n+1}\}$ is an orthogonal system we only need to prove that $\underline{v}_j \cdot \underline{v}_{n+1} = 0$ for every $j \in \{1, \dots, n\}$, since $\{\underline{v}_1, \dots, \underline{v}_n\}$ is already orthogonal by hypothesis. This holds true because

$$\underline{v}_{n+1} \cdot \underline{v}_j = \underline{w} \cdot \underline{v}_j - \sum_{i=1}^{n} \frac{\underline{w} \cdot \underline{v}_i}{\|\underline{v}_i\|^2}(\underline{v}_i \cdot \underline{v}_j) = \underline{w} \cdot \underline{v}_j - \frac{\underline{w} \cdot \underline{v}_j}{\|\underline{v}_j\|^2}(\underline{v}_j \cdot \underline{v}_j) = \underline{w} \cdot \underline{v}_j - \underline{w} \cdot \underline{v}_j = 0,$$

using the fact that $\{\underline{v}_1, \dots, \underline{v}_n\}$ is orthogonal.

Now we need to prove that $\{\underline{v}_1, \dots, \underline{v}_{n+1}\}$ does not contain $\underline{0}$. Suppose by contradiction it does; then necessarily $\underline{v}_{n+1} = \underline{0}$, since $\{\underline{v}_1, \dots, \underline{v}_n\}$ does

not contain $\underline{0}$ by hypothesis. However, if $\underline{v}_{n+1} = \underline{0}$ then:

$$\underline{w} = \sum_{i=1}^{n} \frac{\underline{w} \cdot \underline{v}_i}{\|\underline{v}_i\|^2} \underline{v}_i,$$

which is impossible since by hypothesis $\underline{w} \notin \langle \underline{v}_1, \dots, \underline{v}_n \rangle$. □

Remark 4.2.9. In the hypotheses of Lemma 4.2.8, if $\underline{w}$ is orthogonal to every $\underline{v}_i$, then

$$\underline{v}_{n+1} = \underline{w} - \sum_{i=1}^{n} \frac{\underline{w} \cdot \underline{v}_i}{\|\underline{v}_i\|^2} \underline{v}_i = \underline{w}.$$

In other words, the vector $\underline{w}$ stays the same.

Theorem 4.2.10 (Gram-Schmidt orthonormalization algorithm)**.** Let V be a f.g. $\mathbb{R}$-vector space endowed with a positive definite scalar product $\cdot$. Then there exists an orthonormal basis for V.

Proof. Let $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_n)$ be any basis for V. Define $\underline{v}'_1 = \underline{v}_1$ and recursively, for every $j = 2, \dots, n$, let:

$$\underline{v}'_j = \underline{v}_j - \sum_{i=1}^{j-1} \frac{\underline{v}_j \cdot \underline{v}'_i}{\|\underline{v}'_i\|^2} \underline{v}'_i.$$

We claim that $\{\underline{v}'_1, \dots, \underline{v}'_n\}$ is an orthogonal basis for V. To see this, first notice that $\{\underline{v}'_1\}$ is an orthogonal system not containing $\underline{0}$. Since $\{\underline{v}_1, \dots, \underline{v}_n\}$ is a basis, it follows, in particular, that $\underline{v}_2 \notin \langle \underline{v}_1 \rangle$, and therefore by Lemma 4.2.8 we have that $\{\underline{v}'_1, \underline{v}'_2\}$ is an orthogonal system not containing $\underline{0}$. Now again $\underline{v}_3 \notin \langle \underline{v}_1, \underline{v}_2 \rangle$, and since $\underline{v}'_1$ and $\underline{v}'_2$ are both linear combinations of $\underline{v}_1$ and $\underline{v}_2$, they both belong to $\langle \underline{v}_1, \underline{v}_2 \rangle$, so that $\underline{v}_3 \notin \langle \underline{v}'_1, \underline{v}'_2 \rangle$. Hence $\{\underline{v}'_1, \underline{v}'_2, \underline{v}'_3\}$ is an orthogonal system not containing $\underline{0}$. Iterating this process, we find that $\{\underline{v}'_1, \dots, \underline{v}'_n\}$ is an orthogonal system not containing $\underline{0}$. Now by Theorem 4.2.7 such set is linearly independent, and since $\dim V = n$, it follows that $(\underline{v}'_1, \dots, \underline{v}'_n)$ is a basis.

To conclude, just replace each $\underline{v}'_i$ with its associated versor; this way we obtain, by Remark 4.1.4, a sequence of n versors that are still pairwise orthogonal or, in other words, an orthonormal basis. □

Example 4.2.11.

- Let $V = \mathbb{R}^3$, endowed with the standard scalar product. The sequence $\mathcal{B} = ((1,1,1),(1,0,1),(0,0,2))$ is a basis of V. Let us see how to obtain from $\mathcal{B}$ an orthonormal basis using Theorem 4.2.10. We start by setting $\underline{v}_1 = (1,1,1), \underline{v}_2 = (1,0,1), \underline{v}_3 = (0,0,2)$. The first step is simply to let

$$\underline{v}'_1 = \underline{v}_1 = (1,1,1).$$

Next, we let

$$\underline{v}'_2 = \underline{v}_2 - \frac{\underline{v}_2 \cdot \underline{v}'_1}{\|\underline{v}'_1\|^2}\underline{v}'_1 = (1,0,1) - \frac{2}{3}(1,1,1) = (1/3, -2/3, 1/3).$$

Finally, we let

$$\underline{v}'_3 = \underline{v}_3 - \frac{\underline{v}_3 \cdot \underline{v}'_2}{\|\underline{v}'_2\|^2}\underline{v}'_2 - \frac{\underline{v}_3 \cdot \underline{v}'_1}{\|\underline{v}'_1\|^2}\underline{v}'_1 =$$

$$= (0,0,2) - \frac{2/3}{2/3}(1/3, -2/3, 1/3) - \frac{2}{3}(1,1,1) = (-1,0,1).$$

The sequence $((1,1,1),(1/3,-2/3,1/3),(-1,0,1))$ is then an orthogonal basis of V. In order to obtain an orthonormal basis, we just need to divide every vector by its norm. This yields:

$$\mathcal{B}' = \left(\left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right), \left(\frac{1}{\sqrt{6}}, -\frac{\sqrt{2}}{\sqrt{3}}, \frac{1}{\sqrt{6}}\right), \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)\right).$$

- Let again $V = \mathbb{R}^3$, but this time let it be endowed with a different positive definite scalar product, namely the function

$$\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$$

$$(x_1, x_2, x_3) \cdot (y_1, y_2, y_3)) =$$

$$= 2x_1y_1 + x_1y_2 + x_2y_1 + 4x_2y_2 + x_2y_3 + x_3y_2 + 2x_3y_3.$$

The reader can verify as an exercise that this is indeed a positive definite scalar product. Now consider the canonical basis $\mathcal{B} =$

$((1,0,0),(0,1,0),(0,0,1))$. This is of course an orthonormal basis with respect to the standard scalar product on V, but it is no longer orthonormal (and neither orthogonal) with respect to the above scalar product. Hence, we can apply Gram-Schmidt algorithm and obtain an orthonormal one. First, we set

$$\underline{v}_1 = (1,0,0), \quad \underline{v}_2 = (0,1,0), \quad \underline{v}_3 = (0,0,1).$$

Next, we let

$$\underline{v}_1' = \underline{v}_1 = (1,0,0).$$

Notice that $\|\underline{v}_1'\|^2 = 2$. Next, we let:

$$\underline{v}_2' = \underline{v}_2 - \frac{\underline{v}_2 \cdot \underline{v}_1'}{\|\underline{v}_1'\|^2}\underline{v}_1' = (0,1,0) - \frac{1}{2}(1,0,0) = (-1/2,1,0).$$

Notice that $\|\underline{v}_2'\|^2 = 7/2$ Finally,

$$\underline{v}_3' = \underline{v}_3 - \frac{\underline{v}_3 \cdot \underline{v}_2'}{\|\underline{v}_2'\|^2}\underline{v}_2' - \frac{\underline{v}_3 \cdot \underline{v}_1'}{\|\underline{v}_1'\|^2}\underline{v}_1' =$$

$$(0,0,1) - \frac{1}{7/2}(-1/2,1,0) - \frac{0}{2}(1,0,0) = (1/7,-2/7,1),$$

so that $\|\underline{v}_3'\|^2 = 12/7$. Hence an orthonormal basis for this scalar product is:

$$\left(\left(\frac{1}{\sqrt{2}},0,0\right),\left(-\frac{1}{\sqrt{14}},\frac{2}{\sqrt{14}},0\right),\left(\frac{1}{\sqrt{84}},-\frac{2}{\sqrt{84}},\frac{7}{\sqrt{84}}\right)\right).$$

Theorem 4.2.12. Let V be an $\mathbb{R}$-vector space of dimension n endowed with a positive definite scalar product. Let $\{\underline{v}_1,\dots,\underline{v}_k\} \subseteq V$ be a subset of orthogonal vectors not containing the zero vector. Then there exist $\underline{v}_{k+1},\dots,\underline{v}_n$ such that $(\underline{v}_1,\dots,\underline{v}_n)$ is an orthogonal basis for V.

Proof. By Theorem 4.2.7, the vectors $\underline{v}_1,\dots,\underline{v}_k$ are linearly independent. Therefore we can apply Theorem 1.4.16, and find vectors $\underline{w}_{k+1},\dots,\underline{w}_n$ such that $\mathcal{B} = (\underline{v}_1,\dots,\underline{v}_k,\underline{w}_{k+1},\dots,\underline{w}_n)$ is a basis of V. Now we can apply Gram-Schmidt algorithm to the basis $\mathcal{B}$. In order to do that, we

first have to let, for every $i \in \{1, \dots, k\}$:

$$\underline{v}'_i = \underline{v}_i - \sum_{j=1}^{i-1} \frac{\underline{v}_i \cdot \underline{v}'_j}{\|\underline{v}'_j\|^2} \underline{v}'_j.$$

However, as noticed in Remark 4.2.9, when we apply the above operation to a vector that is already orthogonal to the previous ones, we are not actually doing anything. That is, when performing the Gram-Schmidt algorithm to $\mathcal{B}$ we obtain a basis of the form $(\underline{v}_1, \dots, \underline{v}_k, \underline{w}'_{k+1}, \dots, \underline{w}'_n)$, as required. □

Theorem 4.2.13. Let V be an $\mathbb{R}$-vector space of dimension n endowed with a positive definite scalar product. Let $A \subseteq V$ be a non-empty subset. Then:

$$V = \langle A \rangle \oplus A^\perp.$$

Proof. First, we need to show that $\langle A \rangle \cap A^\perp = \{\underline{0}\}$. This is easy: first recall that, by Proposition 4.1.6, $A^\perp = \langle A \rangle^\perp$. Hence if $\underline{v} \in \langle A \rangle \cap A^\perp = \langle A \rangle \cap \langle A \rangle^\perp$ then we must have $\underline{v} \cdot \underline{v} = 0$. But $\underline{v} \cdot \underline{v} = \|\underline{v}\|^2$, and hence $\|\underline{v}\|^2 = 0$. Since the scalar product is positive definite, this implies that $\underline{v} = \underline{0}$.

Next, let $m = \dim A$. To conclude the proof, we need to show that $\dim A^\perp = n - m$. By Grassmann formula, we have:

$$\dim(\langle A \rangle \oplus A^\perp) = m + \dim A^\perp,$$

and since $\langle A \rangle \oplus A^\perp \subseteq V$, we must have

$$\dim A^\perp \leq n - m.$$

Now let $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_m)$ be an orthogonal basis of $\langle A \rangle$. By Theorem 4.2.12, there exist $\underline{v}_{m+1}, \dots, \underline{v}_n \in V$ such that $(\underline{v}_1, \dots, \underline{v}_n)$ is an orthogonal basis of V. Since $\underline{v}_{m+1}, \dots, \underline{v}_n$ are orthogonal to $\underline{v}_1, \dots, \underline{v}_m$, they must belong to $A^\perp$, since $A^\perp = \mathcal{B}^\perp$. It follows that $\langle \underline{v}_{m+1}, \dots, \underline{v}_n \rangle \subseteq A^\perp$. Since $\underline{v}_{m+1}, \dots, \underline{v}_n$ are part of a basis then they are linearly independent, and hence their span has dimension $n - m$. It follows that

$$\dim A^\perp \geq n - m,$$

concluding the proof. □

Corollary 4.2.14. Let V be an $\mathbb{R}$-vector space of dimension n endowed with a positive definite scalar product. Let $U \subseteq V$ be a subspace. Then:

$$(U^\perp)^\perp = U$$

Proof. Let $m = \dim U$. By Theorem 4.2.13, $\dim U^\perp = n-m$. By the same theorem, $\dim(U^\perp)^\perp = n - (n-m) = m$. On the other hand, $U \subseteq (U^\perp)^\perp$ by Proposition 4.1.6, and since both spaces have the same dimension m, equality must hold. □

Chapter 5: Eigenspaces and diagonalization

5.1 Eigenvalues,eigenvectors and eigenspaces

Definition 5.1.1. Let K be a field and $A \in M_n(K)$. The *characteristic polynomial* of the matrix A is the expression:

$$p_A(x) = \det(A - xI_n) \in K[x].$$

The *eigenvalues* of the matrix A are the roots of the characteristic polynomial.

Remark 5.1.2. By developing the expression $\det(A - xI_n)$ with Laplace theorem, one sees easily that $\deg p_A(x) = n$.

Example 5.1.3.

- Let $A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{R})$. Then

$$p_A(x) = \det \begin{pmatrix} 1-x & 2 \\ 1 & -x \end{pmatrix} = x^2 - x - 2.$$

- Let $A = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ -1 & -1 & 0 \end{pmatrix} \in M_3(\mathbb{R})$. Then

$$p_A(x) = \det \begin{pmatrix} 1-x & 0 & -1 \\ 0 & 1-x & -1 \\ -1 & -1 & -x \end{pmatrix} = x^3 - 3x^2 - x + 2$$

Notice that if $\lambda \in K$ is an eigenvalue of A, then $\det(A - \lambda I_n) = 0$. This means that $\dim \ker(A - \lambda I_n) \geq 1$, because of Theorem 3.2.7. Hence, there exists a

non-zero $X \in M_{n\times 1}(K)$ such that $(A - \lambda I_n)X = \underline{0}$, i.e.

$$AX = \lambda X.$$

Definition 5.1.4. Let $\lambda \in K$ be an eigenvalue of A. The *eigenspace* relative to λ is the space

$$V_\lambda = \ker(A - \lambda I_n).$$

The *eigenvectors* relative to λ are the non-zero elements of V_λ.

Note:-

Technically, an eigenspace is a subspace of $M_{n\times 1}(K)$, so eigenvectors will be column vectors. However, since practically it is easier to write rows instead of columns, we will think of eigenspace as subspaces of K^n, i.e. we will write eigenvectors as n-tuples of elements of K.

Definition 5.1.5. Two matrices $A, B \in M_n(K)$ are *similar* if there exists an invertible matrix $P \in \mathrm{GL}_n(K)$ such that $P^{-1}AP = B$.

A matrix $A \in M_n(K)$ is *diagonalizable* if it is similar to a diagonal matrix. If this is the case, and $P^{-1}AP$ is diagonal for some $P \in \mathrm{GL}_n(K)$, the matrix P is called a *diagonalizing matrix* for A.

Remark 5.1.6. If $D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \lambda_n \end{pmatrix} \in M_n(K)$ is a diagonal matrix then

$$p_D(x) = \det(D - xI_n) = \det \begin{pmatrix} \lambda_1 - x & 0 & \dots & 0 \\ 0 & \lambda_2 - x & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \lambda_n - x \end{pmatrix} = \prod_{i=1}^{n} (\lambda_i - x).$$

Therefore, the eigenvalues of D are precisely the elements on the diagonal.

Lemma 5.1.7. if $A, B \in M_n(K)$ are similar, then $p_A(x) = p_B(x)$.

Proof. Let $P \in \mathrm{GL}_n(K)$ be such that $P^{-1}AP = B$. Then:

$$p_B(x) = \det(B - xI_n) = \det(P^{-1}AP - xI_n) = \det(P^{-1}AP - xP^{-1}P) =$$
$$= \det(P^{-1}(A - xI_n)P) = \det P^{-1} \cdot p_A(x) \cdot \det P =$$
$$= (\det P)^{-1} \cdot \det P \cdot p_A(x) = p_A(x).$$

□

Theorem 5.1.8. A matrix $A \in M_n(K)$ is diagonalizable if and only if the vector space K^n has a basis entirely consisting of eigenvectors of A.

Proof. First, suppose that A is diagonalizable. Let $P \in \mathrm{GL}_n(K)$ be such that $P^{-1}AP = D$ with $D \in M_n(K)$ a diagonal matrix. Multiplying on both sides by D, we get that

$$AP = PD.$$

Now write $P = (P_1|P_2|\dots|P_n)$ with $P_1, \dots, P_n$ the columns of P. Then:

$$AP = (AP_1|AP_2|\dots|AP_n),$$

that is, the columns of the matrix AP are $AP_1, \dots, AP_n$. On the other hand, if $D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}$ then

$$PD = (\lambda_1 P_1|\lambda_2 P_2|\dots|\lambda_n P_n),$$

that is, the columns of PD are $\lambda_1 P_1, \dots, \lambda_n P_n$. Since the two matrices are equal, it follows that $AP_i = \lambda_i P_i$ for every $i = 1, \dots, n$. This means precisely that every P_i is an eigenvector of A (notice that no P_i can be

the zero vector since P is invertible). Moreover, since $\det P \neq 0$ then the columns of P are a basis of K^n.

Conversely, let $P_1, \dots, P_n$ be a basis of K^n consisting of eigenvectors of A. Let $P = (P_1|\dots|P_n)$. Since $AP = (AP_1|\dots|AP_n)$ and the P_i's are eigenvectors, there exist $\lambda_1, \dots, \lambda_n \in K$ such that $AP_i = \lambda_i P_i$ for every $i = 1, \dots, n$. Therefore,

$$AP = (\lambda_1 P_1|\dots|\lambda_n P_n) = DP,$$

where $D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}$. Since $(P_1, \dots, P_n)$ is a basis of K^n, the matrix P is invertible and therefore

$$P^{-1}AP = D,$$

so that A is diagonalizable. □

Remark 5.1.9. The proof of Theorem 5.1.8 shows how to find a diagonalizing matrix for a diagonalizable matrix $A \in M_n(K)$: it sufficies to find a basis $(P_1, \dots, P_n)$ of K^n consisting of eigenvectors of A and then set $P = (P_1|P_2|\dots|P_n)$. The matrix P is a diagonalizing matrix for A.

Example 5.1.10.

- Let $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in M_2(\mathbb{R})$. The characteristic polynomial of A is:

$$P_A(x) = \det \begin{pmatrix} 1-x & 2 \\ 2 & 1-x \end{pmatrix} = (1-x)^2 - 4,$$

so that the eigenvalues of A are $\lambda_1 = -1$, $\lambda_2 = 3$. Let us compute

the eigenspaces. We have:

$$V_{-1} = \ker(A + I_2) = \ker \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix},$$

and it is immediate to see that this is the subspace

$$\{(\alpha, -\alpha) \colon \alpha \in \mathbb{R}\} \subseteq \mathbb{R}^2.$$

Next,

$$V_3 = \ker(A - 3I_2) = \ker \begin{pmatrix} -2 & 2 \\ 2 & -2 \end{pmatrix} = \{(\alpha, \alpha) \colon \alpha \in \mathbb{R}\}.$$

Thus both eigenspaces are 1-dimensional. A basis of V_{-1} is $((1, -1))$, while a basis of V_3 is $((1, 1))$. Since $(1, -1)$ and $(1, 1)$ are linearly independent, they together constitute a basis of $\mathbb{R}^2$. This means that $((1, -1), (1, 1))$ is a basis of $\mathbb{R}^2$ consisting of eigenvectors of A. Hence the matrix

$$P = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

is a diagonalizing matrix for A. In fact one can verify that:

$$P^{-1}AP = \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix}.$$

- Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$. We have $p_A(x) = (1 - x)^2$, so that the unique eigenvalue of A is $\lambda = 1$. The relative eigenspace is $\ker(A - I_2) = \ker \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, that is a 1-dimensional subspace of $\mathbb{R}^2$. Therefore, $\mathbb{R}^2$ cannot have a basis consisting of eigenvectors of A; it follows that A is <u>not</u> diagonalizable.

- Let A be the second matrix in Example 5.1.3, so that

$$p_A(x) = x^3 - 3x^2 - x + 2 = (x+1)(x-1)(x-2).$$

The eigenvalues are therefore: $\lambda_1 = -1$, $\lambda_2 = 1$ and $\lambda_3 = 2$. Hence

$$V_{-1} = \ker(A + I_3) = \ker \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 1 \end{pmatrix}.$$

To find such kernel, we need to solve the homogeneous linear system

$$\begin{cases} 2x - z = 0 \\ 2y - z = 0 \\ -x - y + z = 0 \end{cases}.$$

The associated matrix is of course $A + I_2$, that has rank 2. The first two rows are linearly independent, so we can disregard the third equation and solve the system

$$\begin{cases} 2x - z = 0 \\ 2y - z = 0 \end{cases},$$

whose set of solutions is

$$V_{-1} = \{(\alpha, \alpha, 2\alpha) \colon \alpha \in \mathbb{R}\} = \langle (1,1,2) \rangle.$$

Next,

$$V_1 = \ker(A - I_2) = \ker \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ -1 & -1 & -1 \end{pmatrix},$$

so that

$$V_1 = \{(\alpha, -\alpha, 0) \colon \alpha \in \mathbb{R}\} = \langle (1,-1,0) \rangle.$$

Finally,

$$V_2 = \ker(A - 2I_2) = \ker \begin{pmatrix} -1 & 0 & -1 \\ 0 & -1 & -1 \\ -1 & -1 & -2 \end{pmatrix}$$

so that

$$V_2 = \{(\alpha, \alpha, -\alpha) \colon \alpha \in \mathbb{R}\} = \langle (1, 1, -1) \rangle.$$

The sequence $((1, 1, 2), (1, -1, 0), (1, 1, -1))$ is a basis of $\mathbb{R}^3$, and therefore the matrix A is diagonalizable. If $P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 0 & -1 \end{pmatrix}$ then

$$P^{-1}AP = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Definition 5.1.11. Let $A \in M_n(K)$ and let $\lambda \in K$ be an eigenvalue of A. The *algebraic multiplicity* a_λ of λ is the multiplicity of λ as a root of the characteristic polynomial of A.

The *geometric multiplicity* g_λ of λ is the dimension of the eigenspace relative to λ.

Remark 5.1.12. We have that $a_\lambda, g_\lambda \geq 1$. In fact, this is obvious by definition for the algebraic multiplicity, and since $g_\lambda = \dim(\ker(A - \lambda I_n))$ and $\det(A - \lambda I_n) = 0$ we have that $g_\lambda \geq 1$ by Theorem 3.2.7.

Theorem 5.1.13. Let $A \in M_n(K)$ and let $\lambda \in K$ be an eigenvalue of A. Then:

$$g_\lambda \leq a_\lambda.$$

Proof. Let V_λ be the eigenspace relative to λ. Let $P_1, \dots, P_m$ be a basis of V_λ, so that $m = g_\lambda$. Let us fix a basis $\mathcal{B} = (P_1, \dots, P_m, P_{m+1}, \dots, P_n)$ of K^n, thanks to Theorem 1.4.16, and let $P = (P_1|P_2|\dots|P_m)$, where we

think of the P_i's as column vectors. Then:

$$P^{-1}AP = (P^{-1}AP_1|P^{-1}AP_2|\dots|P^{-1}AP_n),$$

and since $P_1, \dots, P_m \in V_\lambda$ we have $AP_i = \lambda P_i$ for every $i \in \{1, \dots, m\}$. Hence:

$$P^{-1}AP = (P^{-1}\lambda P_1|P^{-1}AP_2|\dots|P^{-1}\lambda P_m|P^{-1}AP_{m+1}|\dots|P^{-1}AP_n) =$$

$$(\lambda P^{-1}P_1|\lambda P^{-1}P_2|\dots|\lambda P^{-1}P_m|P^{-1}AP_{m+1}|\dots|P^{-1}AP_n).$$

Now notice that $P^{-1}P_i$ is simply the i-th vector of the canonical basis, since

$$I_n = P^{-1}P = (P^{-1}P_1|P^{-1}P_2|\dots|P^{-1}P_n).$$

Therefore, the first m columns of $P^{-1}AP$ are $\lambda \underline{e}_1, \lambda \underline{e}_2, \dots, \lambda \underline{e}_m$. It follows that when we compute the characteristic polynomial of $P^{-1}AP$ we will obtain $(\lambda - x)^m q(x)$, for some polynomial $q(x) \in K[x]$. In other words, $(\lambda - x)^m$ is a factor of the characteristic polynomial of $P^{-1}AP$. But this equals $p_A(x)$, thanks to Lemma 5.1.7. Hence the algebraic multiplicity of λ is at least m, as desired. □

Definition 5.1.14. An eigenvalue λ of a matrix $A \in M_n(K)$ is called *regular* if $a_\lambda = g_\lambda$.

Remark 5.1.15. If $a_\lambda = 1$ then λ is regular, by Remark 5.1.12 and Theorem 5.1.13.

Proposition 5.1.16. Let $A \in M_n(K)$ and let $\lambda_1, \dots, \lambda_m \in K$ be distinct eigenvalues. Then the sum $V_{\lambda_1} + V_{\lambda_2} + \dots + V_{\lambda_m}$ is direct.

Proof. By induction on m. For $m = 1$ there is nothing to prove. Now assume that the claim is true for $m - 1$. Let $X \in V_{\lambda_1} + V_{\lambda_2} + \dots + V_{\lambda_m}$. We need to show that this can be written in a unique way as a sum of eigenvectors belonging to different eigenspaces. Suppose then that:

$$X = X_1 + X_2 + \dots + X_m = Y_1 + Y_2 + \dots + Y_m$$

where $X_i, Y_i \in V_{\lambda_i}$ for every $i = 1, \dots, m$. Subtracting the two expressions

we get:

$$(X_1 - Y_1) + (X_2 - Y_2) + \ldots + (X_m - Y_m) = \underline{0}. \tag{22}$$

Multiplying by A on the left both sides of (22) we get:

$$\lambda_1(X_1 - Y_1) + \lambda_2(X_2 - Y_2) + \ldots + \lambda_m(X_m - Y_m) = \underline{0}, \tag{23}$$

since $X_i - Y_i$ is an eigenvector relative to λ_i, for every i. On the other hand, we can multiply both sides of (22) by λ_m and get:

$$\lambda_m(X_1 - Y_1) + \lambda_m(X_2 - Y_2) + \ldots + \lambda_m(X_m - Y_m) = \underline{0}. \tag{24}$$

Subtracting (24) from (23), we get:

$$(\lambda_1 - \lambda_m)(X_1 - Y_1) + \ldots + (\lambda_{m-1} - \lambda_m)(X_{m-1} - Y_{m-1}) = \underline{0}$$

or, in other words:

$$(\lambda_1 - \lambda_m)X_1 + \ldots + (\lambda_{m-1} - \lambda_m)X_{m-1} = (\lambda_1 - \lambda_m)Y_1 + \ldots + (\lambda_{m-1} - \lambda_m)Y_{m-1}.$$

We have therefore written a vector of $V_{\lambda_1} + \ldots + V_{\lambda_{m-1}}$ in two ways; by the inductive hypothesis these two ways must coincide. That is, for every $i \in \{1, \ldots, m-1\}$ we must have:

$$(\lambda_i - \lambda_m)X_i = (\lambda_i - \lambda_m)Y_i.$$

Since the λ_i's are all distinct, the coefficient $\lambda_i - \lambda_m$ is non-zero, and therefore we get:

$$X_i = Y_i \text{ for every } i \in \{1, \ldots, m-1\}.$$

Substituting in (22), we get that $X_m = Y_m$, too, and the proof is complete. □

Theorem 5.1.17. Let $A \in M_n(K)$. Then A is diagonalizable if and only if all eigenvalues belong to K and they are all regular.

Proof. First, suppose that A is diagonalizable. By Theorem 5.1.8, the space K^n has a basis $\mathcal{B}$ consisting of eigenvectors of A. Since such eigenvectors must belong to certain eigenspaces, there exist pairwise distinct eigenvalues $\lambda_1, \ldots, \lambda_m \in K$ of A such that $\mathcal{B} \subseteq V_{\lambda_1} + V_{\lambda_2} + \ldots + V_{\lambda_m}$. By

Proposition 5.1.16, the latter sum is direct and hence

$$\mathcal{B} \subseteq V_{\lambda_1} \oplus V_{\lambda_2} \oplus \ldots \oplus V_{\lambda_m}.$$

Since $\langle \mathcal{B} \rangle = V$, we must have $V_{\lambda_1} \oplus V_{\lambda_2} \oplus \ldots \oplus V_{\lambda_m} = K^n$. Therefore, by Grassmann formula,

$$n = g_{\lambda_1} + \ldots + g_{\lambda_m}.$$

On the other hand, $g_{\lambda_i} \leq a_{\lambda_i}$ for every i by Theorem 5.1.13, and of course $a_{\lambda_1} + \ldots + a_{\lambda_m} \leq n$ by the fundamental theorem of algebra 0.5.3. It follows that:

$$n = g_{\lambda_1} + \ldots + g_{\lambda_m} \leq a_{\lambda_1} + \ldots + a_{\lambda_m} \leq n,$$

and hence equality must hold everywhere. In particular, $a_{\lambda_1} + \ldots + a_{\lambda_m} = n$, so that $\lambda_1, \ldots, \lambda_m$ are all the eigenvalues of A, and so they all belong to K, and $g_{\lambda_i} = a_{\lambda_i}$ for every i, so that all eigenvalues are regular.

Conversely, suppose that all eigenvalues of A belong to K and they are all regular. Let such eigenvalues be $\lambda_1, \ldots, \lambda_m$. Since $a_{\lambda_i} = g_{\lambda_i}$ for every i, we have that $g_{\lambda_1} + \ldots + g_{\lambda_m} = n$ because, as we explained above, $a_{\lambda_1} + \ldots + a_{\lambda_m} = n$ by the fundamental theorem of algebra. On the other hand,

$$\dim(V_{\lambda_1} + \ldots + V_{\lambda_m}) = \dim(V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_m})$$

by Proposition 5.1.16. Altogether, these observations imply that

$$V_{\lambda_1} \oplus \ldots \oplus V_{\lambda_m} = K^n.$$

Hence if $\mathcal{B}_i$ is a basis of V_{λ_i} for every i, we have, by Proposition 1.5.5, that $\mathcal{B}_1 \cup \mathcal{B}_2 \cup \ldots \cup \mathcal{B}_m$ is a basis of K^n consisting of eigenvectors of A, and it follows that A is diagonalizable by Theorem 5.1.8. □

Example 5.1.18.

- We have seen in Example 5.1.10 that the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$$

is not diagonalizable. In fact, such matrix does not satisfy the hy-

potheses of Theorem 5.1.17, since 1 is a non-regular eigenvalue: it has algebraic multiplicity 2 but geometric multiplicity 1.

- The matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{R})$ is not diagonalizable for a different reason: its characteristic polynomial is $x^2 + 1$, that has no roots in $\mathbb{R}$. So this matrix has no real eigenvalues, and again it does not satisfy the hypotheses of Theorem 5.1.17. However, if we think of A as an element of $M_2(\mathbb{C})$ rather than an element of $M_2(\mathbb{R})$, then the eigenvalues belong to the base field $\mathbb{C}$, since they are $\pm i$, and they are both regular, since they have algebraic multiplicity 1. Hence the matrix A is diagonalizable over $\mathbb{C}$. In fact if $P = \begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}$ then one can verify that:

$$P^{-1}AP = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

5.2 Real symmetric matrices

Definition 5.2.1. We recall that a square matrix $A \in M_n(K)$ is called *symmetric* if $A = {}^tA$.

If $X \in \mathbb{C}^n$, we denote by $\overline{X}$ the vector whose entries are the complex conjugates of the entries of X. Namely, if $X = (x_1, \dots, x_n)$ then:

$$\overline{X} = (\overline{x}_1, \dots, \overline{x}_n).$$

Notice that if $X = (x_1, \dots, x_n) \in \mathbb{C}^n$ is non-zero then

$$\overline{X}^t X = \sum_{i=1}^{n} |x_i|^2 > 0. \tag{25}$$

Theorem 5.2.2. Let $A \in M_n(\mathbb{R})$ be a symmetric matrix. Then its eigenvalues are all real.

Proof. Let $p_A(x) \in \mathbb{R}[x]$ be the characteristic polynomial of A. If $\lambda \in \mathbb{C}$ is an eigenvalue of A, namely a root of $p_A(x)$, then also $\overline{\lambda}$ is an eigenvalue of A (cf. Lemma 0.5.4). Moreover, if X is an eigenvector of A relative to λ then

$$AX = \lambda X,$$

and taking conjugates we get:

$$A\overline{X} = \overline{AX} = \overline{\lambda X} = \overline{\lambda} \cdot \overline{X}, \tag{26}$$

using the fact that $\overline{A} = A$ since A has real entries. This means that $\overline{X}$ is an eigenvector of A relative to the eigenvalue $\overline{\lambda}$. Using (26) together with the fact that $A = {}^tA$ we get:

$$\lambda({}^tX \cdot \overline{X}) = {}^t(\lambda X) \cdot \overline{X} = {}^t(AX) \cdot \overline{X} = {}^tX\,{}^tA\overline{X} =$$

$$= {}^tX(A\overline{X}) = {}^tX\overline{\lambda X} = \overline{\lambda}({}^tX\overline{X}).$$

Equating the first and the last terms of the above chain of equalities we see that $\lambda({}^tX \cdot \overline{X}) = \overline{\lambda}({}^tX \cdot \overline{X})$, namely

$$(\lambda - \overline{\lambda})({}^tX \cdot \overline{X}) = 0.$$

Since X is an eigenvector, it is not the zero vector, and therefore by (25) we have ${}^tX \cdot \overline{X} \neq 0$. It follows that $\lambda = \overline{\lambda}$, or, in other words, that $\lambda \in \mathbb{R}$. □

The standard scalar product $\cdot\colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ can be extended to a scalar product

$$\bullet\colon \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$$

$$((x_1, \dots, x_n), (y_1, \dots, y_n)) \mapsto \sum_{i=1}^{n} x_i y_i.$$

Note:-

The standard scalar product $\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ defined above is <u>not</u> positive definite; in fact it makes no sense to talk about *positive* complex numbers. Moreover, it is not even true that $(x_1, \dots, x_n) \bullet (x_1, \dots, x_n) = 0$ if and only if $(x_1, \dots, x_n) = 0$. For example, $(1, i) \bullet (1, i) = 1 - 1 = 0$.

Proposition 5.2.3. Let $A \in M_n(\mathbb{R})$ be a symmetric matrix. Let $\lambda, \mu \in \mathbb{R}$ be distinct eigenvalues of A. Let X be an eigenvector relative to λ and Y an eigenvector relative to μ. Then $X \bullet Y = 0$.

Proof. By hypothesis, $AX = \lambda X$ and $AY = \mu Y$. Hence

$$\lambda(X \bullet Y) = \lambda({}^tX \cdot Y) = {}^t(\lambda X) \cdot Y =$$
$$= {}^t(AX) \cdot Y = ({}^tX\,{}^tA)Y = {}^tXAY =$$
$$= {}^tX\mu Y = \mu(X \bullet Y),$$

so that

$$(\lambda - \mu)(X \bullet Y) = 0.$$

Since by hypothesis $\lambda \neq \mu$, we get that $X \bullet Y = 0$. □

Definition 5.2.4. A matrix $A \in M_n(\mathbb{R})$ is *orthogonal* if its rows form an orthonormal basis of $\mathbb{R}^n$ and its columns form an orthonormal basis of $\mathbb{R}^n$.

Example 5.2.5. The matrix $A = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \in M_2(\mathbb{R})$ is orthogonal, since $((1/\sqrt{2}, 1/\sqrt{2}), (1/\sqrt{2}, -1/\sqrt{2}))$ is an orthonormal basis of $\mathbb{R}^2$.

Remark 5.2.6. An orthogonal matrix is necessarily invertible, since its rows/columns are linearly independent.

Lemma 5.2.7. A matrix $A \in M_n(\mathbb{R})$ is orthogonal if and only if ${}^tA = A^{-1}$.

Proof. Let $R_1, \ldots, R_n$ be the rows of A and $C_1, \ldots, C_n$ be the columns of A. If A is orthogonal, then by definition the following conditions hold:

1. $R_i \bullet R_j = 0$ for every $i \neq j$;
2. $R_i \bullet R_i = 1$ for every i;

3. $C_i \bullet C_j = 0$ for every $i \neq j$;
4. $C_i \bullet C_i = 1$ for every i.

On the other hand, ${}^tA = A^{-1}$ if and only if the following conditions hold:

(a) $A \cdot {}^tA = I_n$;

(b) ${}^tA \cdot A = I_n$.

To conclude the proof, it is enough to look at how the products $A \cdot {}^tA$ and ${}^tA \cdot A$ are computed. The matrix A^tA is given by $(a_{ij})_{i,j\in\{1,\dots,n\}}$ where $a_{ij} = R_i \bullet R_j$ for every i, j. Hence such matrix equals I_n precisely if conditions 1. and 2. hold true. Similarly, we have

$$ {}^tA \cdot A = (C_i \bullet C_j)_{i,j\in\{1,\dots,n\}},$$

so that ${}^tA \cdot A = I_n$ if and only if conditions 3. and 4. hold true. □

Remark 5.2.8. If $A, B \in M_n(\mathbb{R})$ are orthogonal, then AB is orthogonal, since

$$(AB)^{-1} = B^{-1}A^{-1} = {}^tB{}^tA = (AB)^t.$$

In fact, the set of all orthogonal matrices in $\mathrm{GL}_n(\mathbb{R})$ is a group, with the operation being the usual multiplication of matrices.

Definition 5.2.9. A matrix $A \in M_n(\mathbb{R})$ is *orthogonally diagonalizable* if there exists an orthogonal matrix $O \in \mathrm{GL}_n(\mathbb{R})$ such that $O^{-1}AO$ is diagonal.

Theorem 5.2.10 (Spectral theorem)**.** A matrix $A \in M_n(\mathbb{R})$ is orthogonally diagonalizable if and only if it is symmetric.

Proof. First, suppose that A is orthogonally diagonalizable, and let $O \in \mathrm{GL}_n(\mathbb{R})$ be an orthogonal matrix such that $O^{-1}AO = D$, with $D \in M_n(\mathbb{R})$ diagonal. By Lemma 5.2.7, we have that $O^{-1} = {}^tO$, and hence ${}^tOAO = D$. On the other hand, a diagonal matrix is symmetric, so that $D = {}^tD$. Hence

$$ {}^tOAO = D = {}^tD = {}^t({}^tOAO) = {}^tO{}^tAO,$$

so that ${}^tOAO = {}^tO{}^tAO$. Multiplying this equality on the left by O and on the right by ${}^tO$ yields $A = {}^tA$, i.e. that A is symmetric.

Conversely, suppose that A is symmetric. We will prove the claim by induction on n. For $n = 1$, there is nothing to do because A is itself diagonal and equals $1 \times A \times 1$, with 1 being an orthogonal (1×1)-matrix. Now suppose that the claim is true for all square matrices of size $n-1$ and consider our matrix $A \in M_n(\mathbb{R})$. Let $\lambda \in \mathbb{R}$ be an eigenvalue (that exists thanks to Theorem 5.2.2), and let X be an eigenvector relative to λ, normalized so that $X \bullet X = 1$. Now choose an orthonormal basis $\mathcal{B} = (X, X_2, \dots, X_n)$ of $\mathbb{R}^n$ and let $P = (X|X_2|\dots|X_n)$ be the matrix whose columns are the vectors in $\mathcal{B}$. Then

$$ {}^tPAP = {}^tP(AX|AX_2|\dots|AX_n) = {}^tP(\lambda X|AX_2|\dots|AX_n). $$

Now notice that since $\mathcal{B}$ is an orthonormal basis, when we compute the product ${}^tP(\lambda X)$ we obtain the columns vector ${}^t(\lambda, 0, 0, \dots, 0)$, and therefore

$$ {}^tPAP = \left(\begin{array}{c|c} \lambda & \underline{v} \\ \hline {}^t\underline{0} & C \end{array}\right), \tag{27} $$

where $\underline{v} \in \mathbb{R}^{n-1}$, ${}^t\underline{0}$ is the column vector of size $n-1$ with only 0 entries and $C \in M_{n-1}(\mathbb{R})$. Since the matrix A is symmetric, then so is ${}^tPAP$, and hence expression (27) implies that $\underline{v}$ is the zero vector in $\mathbb{R}^{n-1}$ and $C = {}^tC$. Now we can use the inductive hypothesis: $C \in M_{n-1}(\mathbb{R})$ is symmetric, and hence orthogonally diagonalizable. Let $Q \in \mathrm{GL}_{n-1}(\mathbb{R})$ be an orthogonal matrix such that ${}^tQCQ = D$, with D diagonal. Now let

$$ P' = \left(\begin{array}{c|c} 1 & \underline{0} \\ \hline {}^t\underline{0} & Q \end{array}\right); $$

this is orthogonal because Q is orthogonal and $O = PP'$ is orthogonal since both P and P' are (see Remark 5.2.8). All in all, we have that:

$$ {}^tOAO = {}^t(PP')A(PP') = {}^tP'({}^tPAP)P' = $$

$$ = {}^tP' \left(\begin{array}{c|c} \lambda & \underline{0} \\ \hline {}^t\underline{0} & C \end{array}\right) P' = \left(\begin{array}{c|c} \lambda & \underline{0} \\ \hline {}^t\underline{0} & D \end{array}\right), $$

that is diagonal, ending the proof. □

Chapter 6: Affine geometry

6.1 Affine spaces

Definition 6.1.1. An *affine space* of dimension n over a field K is a triple (A, V, f) where:

- A is a non-empty set, whose elements are called *points* of the affine space;
- V is a K-vector space of dimension n;
- $f\colon A \times A \to V$ is a function with the following properties:
  - (i) For every $P \in A$ and every $\underline{v} \in V$, there exists a unique $Q \in A$ such that $f(P, Q) = \underline{v}$.
  - (ii) If $P, Q, R \in V$ are such that $f(P, Q) = \underline{v}$ and $f(Q, R) = \underline{w}$, then $f(P, R) = \underline{v} + \underline{w}$.

One shall think of A as the set of points in the affine space, while elements of V are vectors that represent the "difference" between two points. The following examples are the keys to understanding the concept of affine space.

Example 6.1.2. Let $K = \mathbb{R}$, let $A = \mathbb{R}^2$, seen as the well-known set of points in the cartesian plane, and let V be the vector space $\mathbb{R}^2$. Given two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ in A, we define

$$f(P, Q) \coloneqq (x_Q - x_P, y_Q - y_P) \in V.$$

Let us check that the triple (A, V, f) is an affine space of $\mathbb{R}$ of dimension 2. First, given a point $(x_P, y_P) \in A$ and a vector $\underline{v} \in V$, we can write $\underline{v} = (v_1, v_2)$ for some $v_1, v_2 \in \mathbb{R}$. Hence if we let $Q \coloneqq (v_1 + x_P, v_2 + y_P)$ then $f(P, Q) = (v_1 + x_P - x_P, v_2 + y_P - y_P) = \underline{v}$, and it is easy to check that Q is the unique point of A with this property. Therefore property (i) holds true. Moreover, if $P, Q, R \in A$ are such that $f(P, Q) = \underline{v}$ and $f(Q, R) = \underline{w}$, then writing $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ and $R = (x_R, y_R)$ we get that $\underline{v} = (x_Q - x_P, y_Q - y_P)$ and $\underline{w} = (x_R - x_Q, y_R - y_Q)$, so that

$\underline{v} + \underline{w} = (x_R - x_P, y_R - x_R)$. On the other hand, by definition

$$f(P, R) = (x_R - x_P, y_R - y_P),$$

so that $f(P, R) = f(P, Q) + f(Q, R)$ and (ii) holds true as well.

Example 6.1.2 is nothing else than the well-known cartesian plane. The points of the space are given by pairs of real numbers, and for every pair of points P, Q in the plane there is a vector connecting them. This vector can be visualized by drawing a straight arrow from P to Q pointing at Q. However, one needs to be careful using this graphic representation because vectors with the same length, direction and verse are the same element of the underlying vector space V. For example, the vector connecting the points $(0, 0)$ and $(1, 0)$ is the same vector that connects $(0, 1)$ and $(1, 1)$, although graphically we represent the two vectors as two separate objects.

The function f of example 6.1.2 is nothing else that the function that associates to a pair of points P, Q the vector of $V = \mathbb{R}^2$ that connects them. Property (i) then just says that given a point P and a vector $\underline{v}$, one can "translate" the point P by $\underline{v}$ in a unique way, obtaining a new point Q. For example, if one is given the point $P = (1, 1)$ and the vector $\underline{v} = (-2, 0)$, the unique translate of P by $\underline{v}$ is the point $Q = (-1, 1)$. Finally, property (ii) simply says that if Q is the translate of P by a vector $\underline{v}$ and R is the translate of Q by a vector $\underline{w}$ then R is the translate of P by the vector $\underline{v} + \underline{w}$.

Example 6.1.2 can of course be generalized to any dimension and any field. We will see later on that this is, in a way, the only relevant example.

Example 6.1.3. Let $n \geq 1$ be an integer, K a field, $A = K^n$, seen as a set of points, and $V = K^n$ seen as an n-dimensional K-vector space. Let $f \colon A \times A \to V$ be the function defined by

$$((x_1, \dots, x_n), (y_1, \dots, y_n)) \mapsto (y_1 - x_1, \dots, y_n - x_n).$$

Then the triple (A, f, V) is an affine space of dimension n over the field K. Of course when $n = 2$ and $K = \mathbb{R}$ we recover Example 6.1.2. When $n = 3$ and $K = \mathbb{R}$ this is also a well-known object: it is nothing else that the 3-dimensional space, where every point is identified uniquely by a triple of real numbers, usually referred to as "coordinates". Once again, given two points in the space it is possible to connect them by a unique vector, represented as a straight arrow starting at the first point and pointing at

the second one.

The case $n > 3$ and $K = \mathbb{R}$ cannot be drawn on paper of course, since our world is only 3-dimensional, but it works exactly in the same way: a point is identified with an n-tuple of real numbers, and there is a unique vector connecting two distinct points.

When $n = 1$ and $K = \mathbb{R}$ the affine space above is simply the real line: its points are real numbers, and the vector connecting two real numbers is just their difference.

Definition 6.1.4. The affine space defined in Example 6.1.3 will be denoted by $\mathbb{A}^n(K)$.

From now on, when (A, V, f) is an affine space and $P, Q \in A$, we will denote by $\overrightarrow{PQ}$ the vector $f(P, Q)$.

Proposition 6.1.5. Let (A, V, f) be an affine space over a field K, and let $P, Q, R, S \in A$. The following hold true.

1. $\overrightarrow{PQ} = \overrightarrow{PR}$ if and only if $Q = R$;
2. $\overrightarrow{PQ} = \underline{0}$ if and only if $P = Q$;
3. if $\underline{v} = \overrightarrow{PQ}$, then $-\underline{v} = \overrightarrow{QP}$;
4. $\overrightarrow{PQ} = \overrightarrow{RS}$ if and only if $\overrightarrow{PR} = \overrightarrow{QS}$.

Proof. 1. Of course if $Q = R$ then $\overrightarrow{PQ} = \overrightarrow{PR}$. Conversely, let $\underline{v} := \overrightarrow{PQ}$. By property (i) of the function f, there exists a unique point $X \in A$ such that $\overrightarrow{PX} = \underline{v}$. Therefore that point must be Q, and hence if $\overrightarrow{PR} = \underline{v}$ then necessarily $R = Q$.

2. By property (ii) of the function f, we have $\overrightarrow{PP} = \overrightarrow{PP} + \overrightarrow{PP}$, and therefore $\overrightarrow{PP} = \underline{0}$. Conversely, if $\overrightarrow{PQ} = \underline{0}$, then $\overrightarrow{PQ} = \overrightarrow{PP}$, and therefore $Q = P$ by point 1.

3. By property (ii) of the function f, we have $\overrightarrow{PP} = \overrightarrow{PQ} + \overrightarrow{QP}$. By point 2., this implies that $\overrightarrow{PQ} = -\overrightarrow{QP}$.

4. By property (ii) of f, we have $\overrightarrow{PQ} + \overrightarrow{QS} = \overrightarrow{PS} = \overrightarrow{PR} + \overrightarrow{RS}$. The claim follows immediately. □

Definition 6.1.6. Let (A, V, f) be an affine space of dimension n over a field K. Let $P \in A$ and $\underline{v} \in V$. The *translate* of P by $\underline{v}$, denoted by $t_{\underline{v}}(P)$, is the unique point $Q \in A$ such that $\overrightarrow{PQ} = \underline{v}$.

Given a vector $\underline{v} \in V$, the *translation map* associated to $\underline{v}$ is the map

$$t_{\underline{v}} \colon A \to A$$

$$P \mapsto t_{\underline{v}}(P)$$

Note:-

The existence of the translate of P by $\underline{v}$ is granted by property 1. of the function f associated to an affine space.

Corollary 6.1.7. The translation map $t_{\underline{v}} \colon A \to A$ is a bijection.

Proof. Suppose $t_{\underline{v}}(P) = t_{\underline{v}}(Q) = R$. This is the same as saying that $\overrightarrow{PR} = \underline{v} = \overrightarrow{QR}$. By Proposition 6.1.5, it follows that $\overrightarrow{RP} = -\underline{v} = \overrightarrow{RQ}$ and in turn that $P = Q$. Hence $t_{\underline{v}}$ is injective.

If $Q \in A$, by the definition of affine space there exists a unique $P \in A$ such that $\overrightarrow{QP} = -\underline{v}$. By Proposition 6.1.5 it follows that $\overrightarrow{PQ} = \underline{v}$, namely we have $t_{\underline{v}}(P) = Q$. This shows that $t_{\underline{v}}$ is surjective. □

6.2 Linear subspaces

Definition 6.2.1. Let (A, V, f) be an affine space of dimension n over a field K. Let $O \in A$ and $W \subseteq V$ be a vector subspace of dimension m. The *linear subspace* associated to O and W is the set

$$[O, W] \coloneqq \{t_{\underline{v}}(O) \colon \underline{v} \in W\}.$$

The vector subspace W is called *translation space* of $[O, W]$. The point O is called *origin* of $[O, W]$.

In other words, a linear subspace of an affine space is the set of all translates of a point via vectors that lie in a vector subspace of V.

Example 6.2.2. Let $\mathbb{A}^2(\mathbb{R})$ be the affine space of Example 6.1.2. Let $W \subseteq V$ be the subspace generated by the vector $(1,1)$ and let $O = (0,0) \in \mathbb{A}^2(\mathbb{R})$. The linear subspace $[O,W]$ is the set of all points in the plane that are translates of $(0,0)$ via a multiple of $(1,1)$. Depicting $\mathbb{A}^2(\mathbb{R})$ as the usual cartesian plane, $[O,W]$ is nothing else than the bisector of the first quadrant.

Similarly, let $\mathbb{A}^3(\mathbb{R})$ be the affine space of Example 6.1.3 with $n = 3$ and $K = \mathbb{R}$. Let $O = (1,1,1) \in \mathbb{A}^3(\mathbb{R})$ and let $W = \langle (1,0,0), (0,1,0) \rangle \subseteq V$. Depicting $\mathbb{A}^3(\mathbb{R})$ in the usual way, the linear subspace $[O,W]$ is the plane passing by $(1,1,1)$ and parallel to the xy-plane.

In general, we will see that linear subspaces in $\mathbb{A}^n(K)$ are nothing else than sets of solutions of linear systems!

Proposition 6.2.3. Let (A,V,f) be an affine space of dimension n over a field K, and let $[O,W]$ be a linear subspace. Then the triple

$$([O,W], W, f|_{[O,W]\times[O,W]})$$

is an affine space of dimension m.

Proof. In order to ease the notation, we will write $f|_{[O,W]}$ in place of $f|_{[O,W]\times[O,W]}$.

First, we need to show that $f|_{[O,W]}$ takes values in W. In other words, we need to show that if $P,Q \in [O,W]$ then $f(P,Q) \in W$. Since $P,Q \in [O,W]$ then by definition there exist $\underline{v}, \underline{w} \in W$ such that $f(O,P) = \underline{v}$ and $f(O,Q) = \underline{w}$. Then by Proposition 6.1.5 we have that $f(P,O) = -\underline{v}$ and since (A,V,f) is a vector space we have

$$-\underline{v} + \underline{w} = f(P,O) + f(O,Q) = f(P,Q).$$

It follows that $f(P,Q) = \underline{w} - \underline{v}$, and since W is a vector subspace the latter difference belongs to W. Hence $f|_{[O,W]}$ takes values in W.

Next, we need to show that $f|_{[O,W]}$ satisfies properties 1. and 2. of Definition 6.1.1. Let then $P \in [O,W]$ and $\underline{v} \in W$. Since (A,V,f) is an affine space, there exists a unique $Q \in A$ such that $f(P,Q) = \underline{v}$. Showing that $Q \in [O,W]$ is equivalent then to proving that property 1. holds for $f|_{[O,W]}$. Since $P \in [O,W]$, by definition of linear subspace there is a

$\underline{w} \in W$ such that $f(O,P) = \underline{w}$. Then

$$f(O,Q) = f(O,P) + f(P,Q) = \underline{w} + \underline{v},$$

so that $f(O,Q) \in W$. But this means precisely that Q is a translate of O via a vector of W, namely that $Q \in [O,W]$.

Finally, let $P,Q,R \in [O,W]$. Then $f(P,Q) + f(Q,R) = f(P,R)$ because (A,V,f) is an affine space. On the other hand of course $f(P,Q)$ equals $f|_{[O,W]}(P,Q)$, and the same holds true for $f(Q,R)$ and $f(P,R)$. Property 2. then holds true for $f|_{[O,W]}$. □

Remark 6.2.4. One can prove that if (A,V,f) is an affine space, $B \subseteq A$ is a non-empty subset and $W \subseteq V$ is a vector subspace such that $(B,W,f|_{B\times B})$ is an affine space, then for every $O \in B$ the set $\{t_{\underline{w}}(O) \colon \underline{w} \in W\}$ is a linear subspace of (A,V,f).

Proposition 6.2.5. Let (A,V,f) be an affine space of dimension n over a field K, and let $[O,W]$ be a linear subspace. Then we have:

$$[O,W] = [O',W] \text{ for every } O' \in [O,W].$$

In other words, every point of a linear subspace can be taken as origin of the subspace.

Proof. Let $O' \in [O,W]$. First, we prove that $[O,W] \subseteq [O',W]$. Let $Q \in [O,W]$. Then there exists $\underline{w} \in W$ such that $\underline{w} = \overrightarrow{OQ}$. On the other hand $O' \in [O,W]$ as well, and therefore there exists $\underline{w}' \in [O,W]$ such that $\underline{w}' = \overrightarrow{OO'}$. It follows that

$$\overrightarrow{O'Q} = \overrightarrow{O'O} + \overrightarrow{OQ} = \underline{w} - \underline{w}' \in W,$$

and therefore $Q \in [O',W]$, by definition.

To conclude the proof we need to show that $[O',W] \subseteq [O,W]$. So let $Q \in [O',W]$. Then there is some $\underline{w} \in W$ such that $\overrightarrow{O'Q} = \underline{w}$. Since $O' \in [O,W]$, there is also some $\underline{v} \in W$ such that $\overrightarrow{OO'} = \underline{v}$. It follows that

$$\overrightarrow{OQ} = \overrightarrow{OO'} + \overrightarrow{O'Q} = \underline{v} + \underline{w} \in W,$$

so that $Q \in [O, W]$. □

Proposition 6.2.6. Let (A, V, f) be an affine space over a field K and let $[O, W]$ and $[O', W']$ be two linear subspaces.

1. If $P \in [O, W] \cap [O', W']$, then
$$[O, W] \cap [O', W'] = [P, W \cap W'].$$
2. $[O, W] \subseteq [O', W']$ if and only if $[O, W] \cap [O', W'] \neq \emptyset$ and $W \subseteq W'$

Proof. 1. Since $P \in [O, W] \cap [O', W']$, by Proposition 6.2.5 we can write $[O, W] = [P, W]$ and $[O', W'] = [P, W']$. Therefore it is enough to show that $[P, W] \cap [P, W'] = [P, W \cap W']$.

First, we show that $[P, W \cap W'] \subseteq [P, W] \cap [P, W']$. Let then $Q \in [P, W \cap W']$, and write $\underline{w} = \overrightarrow{PQ}$ with $\underline{w} \in W \cap W'$. Since $\underline{w} \in W$, it follows that $Q \in [P, W]$, and since $\underline{w} \in W'$, it follows that $Q \in [P, W']$. Hence $Q \in [P, W] \cap [P, W']$.

Conversely, we need to show that $[P, W] \cap [P, W'] \subseteq [P, W \cap W']$. Let $Q \in [P, W] \cap [P, W']$. Then there are vectors $\underline{w} \in W$ and $\underline{w}' \in W'$ such that $\overrightarrow{PQ} = \underline{w}$ and $\overrightarrow{PQ} = \underline{w}'$. But then $\underline{w} = \underline{w}'$, hence $\underline{w} \in W \cap W'$ and it follows that $Q \in [P, W \cap W']$.

2. First assume that $[O, W] \subseteq [O', W']$. It is then obvious that $[O, W] \cap [O', W'] \neq \emptyset$. Moreover, since $O \in [O', W']$ then by Proposition 6.2.5 we have $[O', W'] = [O, W']$. Now we have to show that $W \subseteq W'$. If $\underline{w} \in W$, then $Q \coloneqq t_{\underline{w}}(O) \in [O, W']$, but by definition of $[O, W']$ we must also have $Q = t_{\underline{w}'}(O)$ for some $\underline{w}' \in W'$. It follows that $\underline{w} = \overrightarrow{OQ} = \underline{w}'$, and so $\underline{w} \in W'$. This shows that $W \subseteq W'$.

Conversely, assume that $[O, W] \cap [O', W'] \neq \emptyset$ and $W \subseteq W'$. By point 1. we have that $[O, W] \cap [O', W'] = [P, W \cap W']$ for some $P \in [O, W] \cap [O', W']$. Since $W \subseteq W'$, it follows that $[O, W] \cap [O', W'] = [P, W]$. Since $P \in [O, W]$, we have that $\overrightarrow{OP} \in W$, and hence $\overrightarrow{PO} \in W$ by Proposition 6.1.5. Hence $O \in [P, W]$ and by Proposition 6.2.5 it follows that
$$[O, W] \cap [O', W'] = [O, W].$$
This implies obviously that $[O, W] \subseteq [O', W']$. □

Definition 6.2.7. Two linear subspaces $[O, W]$ and $[O', W']$ of an affine space (A, V, f) are called *parallel* if $W \subseteq W'$ or $W' \subseteq W$.

To denote parallel linear subspaces we write $[O, W] \parallel [O', W']$.

Proposition 6.2.8. If $[O, W]$ and $[O', W']$ are two parallel subspaces of an affine space (A, V, f), then one of the following hold true:

1. $[O, W] \subseteq [O', W']$;
2. $[O', W'] \subseteq [O, W]$;
3. $[O, W] \cap [O', W'] = \emptyset$.

In particular, if $\dim W = \dim W'$ then either $[O, W] = [O', W']$ or $[O, W] \cap [O', W'] = \emptyset$.

Proof. Follows immediately form Proposition 6.2.6. □

6.3 Relative position of linear subspaces

Definition 6.3.1. Let (A, V, f) be an affine space of dimension n, and let $[O, W]$ be a linear subspace.

- If $W = \{\underline{0}\}$, then $[O, W]$ is called *point*.
- If $\dim W = 1$, then $[O, W]$ is called *line*.
- If $\dim W = 2$, then $[O, W]$ is called *plane*.
- If $\dim W = n - 1$, then $[O, W]$ is called *hyperplane*.

Remark 6.3.2. Linear subspaces of dimension 0, namely points, are nothing else than elements of A. In fact by definition a point $[O, \{\underline{0}\}]$ is the set $\{t_{\underline{0}}(O)\} = \{O\}$.

Definition 6.3.3. Let $[O, W]$ and $[O', W']$ be two linear subspaces of an affine space. We say that $[O, W]$ *lies on* $[O', W']$ if $[O, W] \subseteq [O', W']$.

Proposition 6.3.4. Let (A, V, f) be an affine space of dimension 2, and let r, s be two lines. If $r \cap s = \emptyset$, then $r \parallel s$.

Proof. Let $r = [P, \langle \underline{v} \rangle]$ and $s = [Q, \langle \underline{w} \rangle]$ for some non-zero vectors $\underline{v}, \underline{w} \in V$. By contradiction, suppose that r and s are not parallel. Then $\underline{w} \notin \langle \underline{v} \rangle$, as otherwise we would have $\langle \underline{w} \rangle \subseteq \langle \underline{v} \rangle$. Hence $\underline{v}$ and $\underline{w}$ are linearly independent, and therefore $\dim \langle \underline{v}, \underline{w} \rangle = 2$. Since $\dim V = 2$, it follows that $V = \langle \underline{v}, \underline{w} \rangle$. Hence there exist $\alpha, \beta \in K$ such that $\overrightarrow{PQ} = \alpha \underline{v} + \beta \underline{w}$. Let $Q' \in s$ be such that $\overrightarrow{QQ'} = -\beta \underline{w}$. Then:

$$\overrightarrow{PQ'} = \overrightarrow{PQ} + \overrightarrow{QQ'} = \alpha \underline{v} + \beta \underline{w} - \beta \underline{w} = \alpha \underline{v}.$$

It follows that $Q' \in r$, but of course $Q' \in s$ by construction. Hence $r \cap s \neq \emptyset$, contradicting the hypothesis. □

Definition 6.3.5. Let (A, V, f) be an affine space of dimension $n \geq 3$. Two lines that are not parallel and have empty intersection are called *skew*. Two lines that lie on the same plane are called *coplanar*.

Proposition 6.3.6. Let (A, V, f) be an affine space of dimension $n \geq 3$.

1. Two lines r, s in (A, V, f) are skew if and only if they are not coplanar
2. There exist two skew lines in (A, V, f).
3. Two skew lines lie on parallel planes.

Proof. 1. First, assume that r, s are skew. Let $r = [P, \langle \underline{v} \rangle]$ and $s = [Q, \langle \underline{w} \rangle]$. Suppose by contradiction that they lie on a plane $\pi = [O, W]$, where $W \subseteq V$ is a subspace of dimension 2. By Proposition 6.2.3, π is an affine space of dimension 2. Since $r \cap s = \emptyset$, by Proposition 6.3.4 they are parallel, but this contradicts the hypothesis.

Conversely, assume that there is no plane containing r and s. Assume by contradiction that $r \cap s \neq \emptyset$. Let $P \in r \cap s$. Write $r = [P, \langle \underline{v} \rangle]$ and $s = [P, \langle \underline{w} \rangle]$ for some non-zero $\underline{v}, \underline{w} \in V$, thanks to Proposition 6.2.5. The space $\langle \underline{v}, \underline{w} \rangle$ is at most 2-dimensional, hence there exists a subspace $W \subseteq V$ such that $\dim W = 2$ and $\langle \underline{v}, \underline{w} \rangle \subseteq W$. Then the linear subspace $[P, W]$ is a plane that clearly contains both lines, contradicting the hypothesis.

Hence it must be $r \cap s = \emptyset$. Now suppose by contradiction that $r \parallel s$. Then there exists a non-zero vector $\underline{v} \in V$ such that $r = [P, \langle \underline{v} \rangle]$ and $s = [Q, \langle \underline{v} \rangle]$. Since $r \cap s = \emptyset$, it must be $r \neq s$ and hence we can assume that $Q \notin r$. Let $\pi = [P, \langle \overrightarrow{PQ}, \underline{v} \rangle]$. We claim that this is a plane containing both r and s. First, $\overrightarrow{PQ}$ cannot be proportional to $\underline{v}$ for as it was, then Q would be a translate of P via a multiple of $\underline{v}$, and hence it would lie on r, which is impossible. The line r lies on π by construction. Let now $R \in s$. Then $\overrightarrow{QR} = \alpha \underline{v}$ for some $\alpha \in K$. On the other hand Q lies on π by construction, since it is the translate of P via $\overrightarrow{PQ}$. Hence R lies on π as well, since it is the translate of Q via a multiple of $\underline{v}$. This shows that s lies on π, so that r, s are coplanar, contradicting the hypothesis. Hence r, s must be skew.

2. Since $\dim V \geq 3$, there exist three linearly independent vectors in V. Let them be $\underline{u}, \underline{v}, \underline{w}$. Let $P \in A$ and let r be the line $[P, \langle \underline{u} \rangle]$. Next, let $Q = t_{\underline{v}}(P)$ and let s be the line $[Q, \langle \underline{w} \rangle]$. Let us prove that r and s are skew lines. By point 1. we just have to prove that they there is no plane that contains both of them. Suppose by contradiction that there is one, call it $\pi = [P, W]$ with $\dim W = 2$. Since $Q \in \pi$, then $\underline{v} = \overrightarrow{PQ} \in W$. On the other hand, since π contains both r and s we must have $\underline{u}, \underline{w} \in W$. But then $\langle \underline{u}, \underline{v}, \underline{w} \rangle \subseteq W$, that is impossible since $\dim W = 2$.

3. Let $r = [P, \langle \underline{v} \rangle]$ and $s = [Q, \langle \underline{w} \rangle]$ be skew lines. Then $\dim \langle \underline{v}, \underline{w} \rangle = 2$, as otherwise r, s would be parallel. Then the planes $\pi = [P, \langle \underline{v}, \underline{w} \rangle]$ and $\pi' = [Q, \langle \underline{v}, \underline{w} \rangle]$ are clearly parallel and contain r and s, respectively. □

Proposition 6.3.7. Let (A, V, f) be an affine space of dimension 3.

1. A line r and a plane π with empty intersection are parallel.
2. Two planes π, σ with empty intersection are parallel.
3. If two distinct planes π, σ intersect in a point P, then their intersection is a line through P.
4. Every line r is contained in at least two distinct planes.

Proof. 1. Let P be a point of r, so that $r = [P, \langle \underline{u} \rangle]$ for some non-zero $\underline{u} \in V$. Let $\pi = [Q, \langle \underline{v}, \underline{w} \rangle]$ for some linearly independent $\underline{v}, \underline{w} \in V$. Suppose by contradiction that r and π are not parallel. Then $\underline{u} \notin \langle \underline{v}, \underline{w} \rangle$ and hence we have $\dim \langle \underline{u}, \underline{v}, \underline{w} \rangle = 3$. Since $\dim V = 3$ as well, it follows

that $V = \langle \underline{u}, \underline{v}, \underline{w} \rangle$. Therefore $\overrightarrow{PQ} = \alpha\underline{u} + \beta\underline{v} + \gamma\underline{w}$ for some $\alpha, \beta, \gamma \in K$. Let $Q' \in \pi$ be the point such that $\overrightarrow{QQ'} = -\beta\underline{v} - \gamma\underline{w}$. Then

$$\overrightarrow{PQ'} = \overrightarrow{PQ} + \overrightarrow{QQ'} = \alpha\underline{u}.$$

Then $Q' \in r$, but on the other hand by construction $Q' \in \pi$. It follows that $Q' \in r \cap \pi$, contradicting the hypothesis.

2. Let $\pi = [P, W]$ and $\sigma = [Q, W']$ with $\dim W = \dim W' = 2$. Suppose by contradiction that π, σ are not parallel. Then $W \neq W'$, and so there exists a non-zero vector $\underline{v} \in W \setminus W'$. Then $[P, \langle \underline{v} \rangle]$ is a line contained in π that is not parallel to σ. By 1. it follows that r and σ have non-empty intersection, but then also π and σ do, contradicting the hypothesis.

3. Let $\pi = [Q, W]$ and $\sigma = [Q', W']$ with $\dim W = \dim W' = 2$. Let $P \in \pi \cap \sigma$. Since $\pi \neq \sigma$ it must be that $W \neq W'$, as otherwise we could write $\pi = [P, W] = \sigma$. Hence by Grassmann formula it follows that $\dim(W \cap W') = 1$, and by Proposition 6.2.6 we have

$$\pi \cap \sigma = [P, W \cap W'],$$

that is a line through P.

4. Let $r = [P, \langle \underline{u} \rangle]$ for some non-zero $\underline{u} \in V$. Let us complete $(\underline{u})$ to a basis of V, via Theorem 1.4.16: there exist $\underline{v}, \underline{w}$ such that $(\underline{u}, \underline{v}, \underline{w})$ is a basis of V. Then $[P, \langle \underline{u}, \underline{v} \rangle]$ and $[P, \langle \underline{u}, \underline{w} \rangle]$ are two planes both containing r. Moreover, they are distinct because if they were equal then we would have $t_{\underline{w}}(P) \in [P, \langle \underline{u}, \underline{v} \rangle]$ and consequently $\underline{w} \in \langle \underline{u}, \underline{v} \rangle$, that is impossible since $\underline{u}, \underline{v}, \underline{w}$ are linearly independent. □

Definition 6.3.8. Let (A, V, f) be an affine space. Two lines that intersect in a single point, a line and a plane that intersect in a single point or two planes that intersect in a single line are called *incident*.

Thanks to the propositions we have proved, we can give a complete description of the relative position of linear subspaces of affine spaces in dimension 2 and 3.

Theorem 6.3.9. Let (A, V, f) be an affine space of dimension ≥ 2, and let

r, s be two lines. Then:

$$r \cap s = \begin{cases} \emptyset & \begin{cases} \text{skew} \\ \text{coplanar, parallel and distinct} \end{cases} \\ \text{a point} & \text{incident} \\ \text{a line} & r = s \end{cases}.$$

Theorem 6.3.10. Let (A, V, f) be an affine space of dimension 3 and let π, σ be two planes. Then:

$$\pi \cap \sigma = \begin{cases} \emptyset & \text{parallel and distinct} \\ \text{a line} & \text{incident} \\ \text{a plane} & \pi = \sigma \end{cases}.$$

Theorem 6.3.11. Let (A, V, f) be an affine space of dimension 3 and let r be a line and π be a plane. Then:

$$r \cap \pi = \begin{cases} \emptyset & \text{parallel and } r \text{ does not lie on } \pi \\ \text{a point} & \text{incident} \\ \text{a line} & r \subseteq \pi \end{cases}.$$

6.4 Coordinate systems and equations of subspaces

Definition 6.4.1. Let (A, V, f) be an affine space. A *system of coordinates* on (A, V, f) is a pair $(O, \mathcal{B})$ where $O \in A$ is a point called *origin* and $\mathcal{B}$ is a basis of V.

Theorem 6.4.2. Let (A, V, f) be an affine space of dimension n, let $O \in A$ and $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_n)$ be a basis of V.

1. The map
$$\Lambda_{[O,\mathcal{B}]} \colon A \to K^n$$
$$P \mapsto (x_1, \dots, x_n),$$

where $(x_1, \dots, x_n) \in K^n$ is the only n-tuple such that $\overrightarrow{OP} = \sum_{i=1}^n x_i \underline{v}_i$, is a bijection.

2. Let $\Phi_{\mathcal{B}} \colon V \to K^n$ be the bijection defined by

$$\Phi_{\mathcal{B}} \left(\sum_{i=1}^n \alpha_i \underline{v}_i \right) = (\alpha_1, \dots, \alpha_n)$$

(see Corollary 1.4.13). If $P, Q \in A$, are such that $\Lambda_{[O,\mathcal{B}]}(P) = (x_1, \dots, x_n)$ and $\Lambda_{[O,\mathcal{B}]}(Q) = (y_1, \dots, y_n)$, where $\Lambda_{[O,\mathcal{B}]}$ is the bijection given by point 1., then

$$\Phi_{\mathcal{B}}(\overrightarrow{PQ}) = (y_1 - x_1, \dots, y_n - x_n).$$

Proof. 1. First, suppose that $P, Q \in A$ are such that $\Lambda_{[O,\mathcal{B}]}(P) = \Lambda_{[O,\mathcal{B}]}(Q) = (x_1, \dots, x_n)$. This means that $\overrightarrow{OP} = \sum_{i=1}^n x_i \underline{v}_i = \overrightarrow{OQ}$. However, by definition of affine space, given the point $O \in A$ and the vector $\sum_{i=1}^n x_i \underline{v}_i \in V$, there exists a unique point $X \in A$ such that $\overrightarrow{OX} = \sum_{i=1}^n x_i \underline{v}_i$. This means that $P = X = Q$. Therefore $\Lambda_{[O,\mathcal{B}]}$ is injective.

Next, if $(x_1, \dots, x_n) \in K^n$, let $\underline{v} = \sum_{i=1}^n x_i \underline{v}_i \in V$. Once again by definition of affine space, there exists a unique $P \in A$ such that $\overrightarrow{OP} = \underline{v}$. But then $\Lambda_{[O,\mathcal{B}]}(P) = (x_1, \dots, x_n)$. This proves that $\Lambda_{[O,\mathcal{B}]}$ is surjective as well.

2. Since $\Lambda_{[O,\mathcal{B}]}(P) = (x_1, \dots, x_n)$ and $\Lambda_{[O,\mathcal{B}]}(Q) = (y_1, \dots, y_n)$, the vector $\overrightarrow{OP}$ is $\sum_{i=1}^n x_i \underline{v}_i$ while $\overrightarrow{OQ} = \sum_{i=1}^n y_i \underline{v}_i$. It follows that

$$\overrightarrow{PQ} = \overrightarrow{PO} + \overrightarrow{OQ} = -\sum_{i=1}^n x_i \underline{v}_i + \sum_{i=1}^n y_i \underline{v}_i = \sum_{i=1}^n (y_i - x_i) \underline{v}_i,$$

and therefore

$$\Phi_{\mathcal{B}}(\overrightarrow{PQ}) = (y_1 - x_1, \dots, y_n - x_n).$$

□

Theorem 6.4.2 is of the utmost importance. It shows that every affine space of dimension n over a field K, once a coordinate system is chosen, "becomes" the affine space $\mathbb{A}^n(K)$ described in Example 6.1.3. The bijection $\Lambda_{[O,\mathcal{B}]}$, that depends on the choice of a coordinate system, yields a dictionary that allows to translate all properties of an affine space of dimension n over a field K into properties of the very concrete object $\mathbb{A}^n(K)$.

Note:-

Notice that since $\overrightarrow{OO} = \underline{0}$, we have that $\Lambda_{[O,\mathcal{B}]}(O) = (0, \dots, 0)$. Namely, the map $\Lambda_{[O,\mathcal{B}]}$ transforms the origin O of a coordinate system into the point $(0, \dots, 0) \in K^n$.
Moreover, $\Phi_{\mathcal{B}}(\underline{0}) = (0, \dots, 0)$.

From now on, with a slight abuse of notation, we will write $\mathbb{A}^n(K)$ to denote the set of points of the latter affine space, although technically $\mathbb{A}^n(K)$ denotes a triple of objects, according to the definition of affine space.

The next theorem describes how linear subspaces transform under $\Lambda_{[O,\mathcal{B}]}$. First, we prove two preliminary lemmas.

Lemma 6.4.3. Let V be a K-vector space of dimension n and let $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_n)$ be a basis of V.

1. For every $\underline{w}_1, \underline{w}_2 \in V$ and every $\alpha, \beta \in K$ we have
$$\Phi_{\mathcal{B}}(\alpha\underline{w}_1 + \beta\underline{w}_2) = \alpha\Phi_{\mathcal{B}}(\underline{w}_1) + \beta\Phi_{\mathcal{B}}(\underline{w}_2).$$
2. Let $W \subseteq V$ be a subspace of dimension m. Then $\Phi_{\mathcal{B}}(W)$ is a subspace of K^n of dimension m.

Proof. 1. Let $\underline{w}_1 = \sum_{i=1}^n a_i\underline{v}_i$ and $\underline{w}_2 = \sum_{i=1}^n b_i\underline{v}_i$. Then
$$\alpha\underline{w}_1 + \beta\underline{w}_2 = \sum_{i=1}^n (\alpha a_i + \beta b_i)\underline{v}_i,$$
so that
$$\Phi_{\mathcal{B}}(\alpha\underline{w}_1 + \beta\underline{w}_2) = (\alpha a_1 + \beta b_1, \alpha a_2 + \beta b_2, \dots, \alpha a_n + \beta b_n).$$
On the other hand, $\alpha\Phi_{\mathcal{B}}(\underline{w}_1) = \alpha(a_1, \dots, a_n)$ and $\beta\Phi_{\mathcal{B}}(\underline{w}_2) = \beta(b_1, \dots, b_n)$, and the claim follows easily.

2. First, we show that $\Phi_{\mathcal{B}}(W)$ is a subspace of K^n. Let $\underline{w}_1, \underline{w}_2 \in \Phi_{\mathcal{B}}(W)$, so that there exist $\underline{u}_1, \underline{u}_2 \in W$ such that $\Phi_{\mathcal{B}}(\underline{u}_1) = \underline{w}_1$ and $\Phi_{\mathcal{B}}(\underline{u}_2) = \underline{w}_2$. Let $\alpha, \beta \in K$. Then
$$\Phi_{\mathcal{B}}(\alpha\underline{u}_1 + \beta\underline{u}_2) = \alpha\Phi_{\mathcal{B}}(\underline{u}_1) + \beta\Phi_{\mathcal{B}}(\underline{u}_2) = \alpha\underline{w}_1 + \beta\underline{w}_2$$

by point 1. This proves that $\alpha\underline{w}_1 + \beta\underline{w}_2 \in \Phi_{\mathcal{B}}(W)$, and therefore $\Phi_{\mathcal{B}}(W)$ is a vector subspace of V.

To prove that it has dimension m, let $(\underline{u}_1, \dots, \underline{u}_m)$ be a basis of W. If $\underline{w} \in \Phi_{\mathcal{B}}(W)$, then $\underline{w} = \Phi_{\mathcal{B}}(\underline{u})$ for some $\underline{u} \in W$. But $\underline{u} = \sum_{i=1}^m \alpha_i \underline{u}_i$ for some $\alpha_1, \dots, \alpha_m \in K$, since $(\underline{u}_1, \dots, \underline{u}_m)$ is a basis of W. Hence

$$\underline{w} = \Phi_{\mathcal{B}}(\underline{u}) = \Phi_{\mathcal{B}}\left(\sum_{i=1}^m \alpha_i \underline{u}_i\right) = \sum_{i=1}^m \alpha_i \Phi_{\mathcal{B}}(\underline{u}_i)$$

by point 1. This proves that $\Phi_{\mathcal{B}}(\underline{u}_1), \dots, \Phi_{\mathcal{B}}(\underline{u}_m)$ generate $\Phi_{\mathcal{B}}(W)$. To prove that these vectors are linearly independent, suppose first that

$$\sum_{i=1}^m \alpha_i \Phi_{\mathcal{B}}(\underline{u}_i) = \underline{0}$$

for some $\alpha_1, \dots, \alpha_m \in K$. Then once again by point 1. we get

$$\underline{0} = \Phi_{\mathcal{B}}\left(\sum_{i=1}^m \alpha_i \underline{u}_i\right).$$

However $\Phi_{\mathcal{B}}$ is a bijection, and since $\Phi_{\mathcal{B}}(\underline{0}) = \underline{0}$, it follows that $\sum_{i=1}^m \alpha_i \underline{u}_i = \underline{0}$. Since $(\underline{u}_1, \dots, \underline{u}_m)$ is a basis of W, we get that $\alpha_1 = \dots = \alpha_m = 0$. □

Lemma 6.4.4. Let $\bullet$ be the standard scalar product on K^n, i.e. the map

$$K^n \times K^n \to K$$

$$((x_1, \dots, x_n), (y_1, \dots, y_n)) \mapsto \sum_{i=1}^n x_i y_i.$$

Let W be a subspace of K^n.

1. $\dim W^\perp = n - \dim W$.
2. $(W^\perp)^\perp = W$.
3. Let $\dim W = m$, and let $(\underline{u}_1, \dots, \underline{u}_{n-m})$ be a basis of $W^\perp$, where

$$\underline{u}_i = (c_{i1}, c_{i2}, \dots, c_{in}) \in K^n \text{ for every } i.$$

Then the matrix

$$C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ c_{(n-m)1} & c_{(n-m)2} & \dots & c_{(n-m)n} \end{pmatrix} \in M_{(n-m)\times n}(K)$$

has rank $n-m$ and has the property that $\ker C = W$.

Proof. Let $(\underline{w}_1, \dots, \underline{w}_m)$ be a basis of W, so that $\dim W = m$. Write $\underline{w}_i = (a_{i1}, \dots, a_{in}) \in K^n$. Let A be the matrix of size $m \times n$ with coefficients in K whose i-th row is $\begin{pmatrix} a_{i1} & \dots & a_{in} \end{pmatrix}$, for every i. This is nothing else than the transpose of the matrix $A_{\mathcal{B}}$ described in Theorem 2.3.8, with $\mathcal{B}$ being the canonical basis of K^n.

Now let $\bullet$ be the standard scalar product on K^n. We claim that

$$W^\perp = \ker A. \tag{28}$$

In fact, by Proposition 4.1.6 we have that $W^\perp = \{\underline{w}_1, \dots, \underline{w}_m\}^\perp$. Hence $\underline{v} \in W^\perp$ if and only if $\underline{w}_i \bullet \underline{v} = 0$ for every $i = 1, \dots, m$, but on the other hand a moment of reflection shows that

$$(\underline{w}_1 \bullet \underline{v}, \dots, \underline{w}_m \bullet \underline{v}) = A\underline{v},$$

that is, $\underline{v} \in W^\perp$ if and only if $\underline{v} \in \ker A$.

1. Since the rows of A are linearly independent, we have $\mathrm{rk}(A) = m$ by Theorem 2.3.8. By Theorem 3.2.7, we have $\dim \ker A = n - m$, and (28) implies then that

$$\dim W^\perp = n - \dim W.$$

2. By point 1. applied to $W^\perp$ and then to W we have that

$$\dim (W^\perp)^\perp = n - \dim W^\perp = n - (n - \dim W) = \dim W,$$

and since $W \subseteq (W^\perp)^\perp$ by Proposition 4.1.6, it must be $(W^\perp)^\perp = W$.

3. Redoing the construction described at the beginning of the proof to $W^\perp$ we get by (28) that

$$(W^\perp)^\perp = \ker C,$$

and so the claim by 2. □

Theorem 6.4.5. Let (A, V, f) be an affine space of dimension n over a field K. Let $\mathcal{B} = (\underline{v}_1, \dots, \underline{v}_n)$ be a basis of V, let $O \in A$ and let $[P, W]$ be a linear subspace of dimension m.

1. The subset $\Lambda_{[O,\mathcal{B}]}([P, W]) \subseteq \mathbb{A}^n(K)$ is the linear subspace
$$[\Lambda_{[O,\mathcal{B}]}(P), \Phi_{\mathcal{B}}(W)].$$
2. A subset $S \subseteq \mathbb{A}^n(K)$ is a linear subspace of dimension m if and only if there exists a matrix $A \in M_{(n-m)\times n}(K)$ of rank $n-m$ and a matrix $B \in M_{(n-m)\times 1}(K)$ such that S is the set of solutions of the linear system $AX = B$.

Proof. 1. Notice that thanks to Lemma 6.4.3, clearly $[\Lambda_{[O,\mathcal{B}]}(P), \Phi_{\mathcal{B}}(W)]$ is a linear subspace. In order to ease the notation, we will write Λ for $\Lambda_{[O,\mathcal{B}]}$ and Φ for $\Phi_{\mathcal{B}}$. Moreover, we let $\Lambda(P) = (x_1, \dots, x_n)$.

First, let $(y_1, \dots, y_n) \in \Lambda([P, W])$. This means that there is some $Q \in [P, W]$ such that $\Lambda(Q) = (y_1, \dots, y_n)$. Hence $\overrightarrow{OQ} = \sum_{i=1}^n y_i \underline{v}_i$. On the other hand, $\overrightarrow{OP} = \sum_{i=1}^n x_i \underline{v}_i$, and therefore

$$\overrightarrow{PQ} = \overrightarrow{OQ} - \overrightarrow{OP} = \sum_{i=1}^n (y_i - x_i)\underline{v}_i \in W.$$

It follows that

$$\Phi\left(\sum_{i=1}^n (y_i - x_i)\underline{v}_i\right) = (y_1 - x_1, \dots, y_n - x_n) \in \Phi(W),$$

and since $\Lambda(Q) = \Lambda(P) + (y_1 - x_1, \dots, y_n - x_n)$, we get precisely that $\Lambda(Q)$ is a translate of $\Lambda(P)$ via a vector of $\Phi(W)$, i.e. that $\Lambda(Q) \in [\Lambda(P), \Phi(W)]$. We have thus proved that $\Lambda([P, W]) \subseteq [\Lambda(P), \Phi(W)]$.

Conversely, let $(y_1, \dots, y_n) \in [\Lambda(P), \Phi(W)]$. Then

$$(y_1, \dots, y_n) = (x_1, \dots, x_n) + (a_1, \dots, a_n),$$

where $(a_1, \dots, a_n) \in \Phi(W)$. Since the map Λ is a bijection by Theorem 6.4.2, there exists a unique $Q \in A$ such that $\Lambda(Q) = (y_1, \dots, y_n)$, or, in other words, such that $\overrightarrow{OQ} = \sum_{i=1}^n y_i \underline{v}_i$. Since $\overrightarrow{OP} = \sum_{i=1}^n x_i \underline{v}_i$, we get

that

$$\overrightarrow{PQ} = \overrightarrow{OQ} - \overrightarrow{OP} = \sum_{i=1}^{n} a_i \underline{v}_i.$$

Now $\Phi\left(\sum_{i=1}^{n} a_i \underline{v}_i\right) = (a_1, \dots, a_n)$, and since the map Φ is a bijection and $(a_1, \dots, a_n) \in \Phi(W)$ by hypothesis, we must have that $\sum_{i=1}^{n} a_i \underline{v}_i \in W$. Hence $\overrightarrow{PQ} \in W$, that is, Q is a translate of P via a vector of W, i.e. $Q \in [P, W]$. Therefore $\Lambda(Q) = (y_1, \dots, y_n) \in \Lambda([P, W])$. It follows that $[\Lambda(P), \Phi(W)] \subseteq \Lambda([P, W])$.

2. First, suppose that S is a linear subspace. Then $S = [P, W]$, for some $P \in K^n$ and W vector subspace of K^n. By Lemma 6.4.4, there exists an $(n-m) \times n$ matrix A of rank $n-m$ such that $W = \ker A$. Now if $P = (x_1, \dots, x_n)$ then S, as a subset of $\mathbb{A}^n(K) = K^n$, is nothing else that

$$\{(x_1, \dots, x_n) + (z_1, \dots, z_n) \colon (z_1, \dots, z_n) \in \ker A\}.$$

Setting $B \coloneqq A \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}$ and appealing to Proposition 3.2.9, it follows that S is the set of solutions of the linear system $AX = B$.

Conversely, if $AX = B$ is a linear system of $n - m$ equations in n variables and $\operatorname{rk} A = n - m$, then by Theorem 3.2.7 and Proposition 3.2.9, if $(x_1, \dots, x_n) \in K^n$ is a solution of the system then the set S of all solutions is

$$S = \{(x_1, \dots, x_n) + (z_1, \dots, z_n) \colon (z_1, \dots, z_n) \in \ker A\}.$$

In other words, S is the linear subspace $[(x_1, \dots, x_n), \ker A]$. □

Theorem 6.4.5 essentially tells us that we can reduce the study of linear subspaces of affine spaces to the study of solutions of linear systems.

Remark 6.4.6. Theorem 6.4.5 shows that given a linear subspace S of $\mathbb{A}^n(K)$, defined by a linear system of the form $AX = B$ with A an $(n - m) \times n$ matrix of rank $n - m$, the translation space of S is the kernel of A.

6.5 Equations for lines, planes and hyperplanes

Recall that a *line* in $\mathbb{A}^n(K)$ is a linear subspace of dimension 1. Given Theorem 6.4.5, a line corresponds to the set of solutions of a linear system $AX = B$, with $A \in M_{(n-1)\times n}(K)$ a matrix of rank $n-1$. This means that a line $\ell \subseteq \mathbb{A}^n(K)$ can be described by a system of equations of the form:

$$\ell\colon \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots \\ a_{(n-1)1}x_1 + \ldots + a_{(n-1)n}x_n = b_{n-1} \end{cases}, \tag{29}$$

where the matrix associated to the system has rank $n-1$.

Definition 6.5.1. A system of the form (29) that describes a line in $\mathbb{A}^n(K)$ is called a system of *cartesian equations* for a line.

Example 6.5.2. In $\mathbb{A}^2(K)$, a system as (29) becomes

$$a_{11}x_1 + a_{12}x_2 = b_1,$$

where the rank condition simply means that $(a_{11}, a_{12}) \neq (0,0)$.

In $\mathbb{A}^3(K)$, a system of cartesian equations for a line has the form:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2 \end{cases},$$

with the condition that

$$\operatorname{rk}\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} = 2$$

or, in other words, that the two vectors (a_{11}, a_{12}, a_{13}) and (a_{21}, a_{22}, a_{23}) are linearly independent.

The description of a line ℓ via a system of the form (29) is implicit, namely, we don't have a parametrization for the points of the line. To do this, it is enough to solve the system. Notice that since $\operatorname{rk}(A) = n-1$, Theorem 3.2.7 implies that $\ker A$ is a 1-dimensional vector subspace of K^n, that is therefore

generated by a non-zero vector $(a_1, \dots, a_n) \in K^n$. Proposition 3.2.9 implies that the solutions of system (29) all have the form

$$(p_1, \dots, p_n) + t(a_1, \dots, a_n)$$

with $t \in K$ and $(p_1, \dots, p_n) \in K^n$. In other words, the same line defined by (29) can be described by the following set of equations:

$$\ell\colon \begin{cases} x_1 = p_1 + ta_1 \\ x_2 = p_2 + ta_2 \\ \dots \\ x_n = p_n + ta_n \end{cases} . \tag{30}$$

We stress the fact that $(p_1, \dots, p_n)$ and $(a_1, \dots, a_n)$ are two elements of K^n, the second one being non-zero, while t is a parameter. The point $(p_1, \dots, p_n)$ is a point lying on the line, corresponding to $t = 0$. All other points can be found by letting t vary in K.

Definition 6.5.3. A system in the form of (30) is called *parametric equation* for a line.

In order to pass from a cartesian equation to a parametric one, it is enough to solve the linear system. However it is also possible to pass from a parametric equation to a cartesian one. In fact, equations (30) can be read in the following way: for all points $(\overline{x}_1, \dots, \overline{x}_n) \in \ell$, the vectors $(\overline{x}_1 - p_1, \dots, \overline{x}_n - p_n)$ and $(a_1, \dots, a_n)$ are linearly dependent, as they are proportional. This means that the matrix

$$\begin{pmatrix} \overline{x}_1 - p_1 & \overline{x}_2 - p_2 & \dots & \overline{x}_n - p_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

has rank 1. In other words, points of ℓ satisfy the system of equations determined by imposing

$$\operatorname{rk} \begin{pmatrix} x_1 - p_1 & x_2 - p_2 & \dots & x_n - p_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = 1.$$

Since the above matrix has 2 lines and n columns, and the bottom row is non-zero, asking that it has rank 1 is equivalent to asking that every 2×2 submatrix has determinant 0. Again, since the bottom row is non-zero there exists some $i \in \{1, \dots, n\}$ such that $a_i \neq 0$. Then by Theorem 2.3.20 the condition on

the rank is satisfied if and only if every 2×2 submatrix containing the i-th column has determinant 0. Assuming that $a_1 \neq 0$, we get:

$$\det \begin{pmatrix} x_1 - p_1 & x_i - p_i \\ a_1 & a_i \end{pmatrix} = 0 \text{ for every } i = 2, \dots, n,$$

that amounts to the system of cartesian equations for ℓ:

$$\ell\colon \begin{cases} a_2 x_1 - a_1 x_2 = a_2 p_1 - a_1 p_2 \\ a_3 x_1 - a_1 x_3 = a_3 p_1 - a_1 p_3 \\ \dots \\ a_n x_1 - a_1 x_n = a_n p_1 - a_1 p_n \end{cases}.$$

Notice that the matrix corresponding to the above system is:

$$\begin{pmatrix} a_2 & -a_1 & 0 & 0 & \dots & 0 \\ a_3 & 0 & -a_1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_n & 0 & 0 & \dots & 0 & -a_1 \end{pmatrix},$$

that clearly has rank $n-1$ because if we erase the first column the resulting square matrix has determinant $(-a_1)^{n-1} \neq 0$, since we assumed that $a_1 \neq 0$.

Example 6.5.4. Consider the line $\ell \subseteq \mathbb{A}^3(\mathbb{R})$ given by the system of equations:

$$\ell\colon \begin{cases} 2x + 3y + z = 1 \\ x + z = 3 \end{cases}.$$

In order to find a system of parametric equations for ℓ, all we have to do is to solve the system. Letting

$$A = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

be the matrix associated with the system, we see that it has rank 2, and

hence the system has ∞^1 solutions. Rewriting it as:

$$\begin{cases} 2x + 3y = 1 - z \\ x = 3 - z \end{cases}$$

and setting $z = t$, we see immediately that the set of solutions is:

$$S = \{(3 - t, -5/3 + 1/3t, t) \colon t \in \mathbb{R}\}$$

and therefore a system of parametric equations for ℓ is:

$$\begin{cases} x = 3 - t \\ y = -5/3 + 1/3t \\ z = t \end{cases}.$$

Notice that the line ℓ passes through the point $(3, -5/3, 0)$.

Example 6.5.5. Consider the line $\ell \subseteq \mathbb{A}^3(\mathbb{R})$ given by the system of parametric equations:

$$\begin{cases} x = 1 + t \\ y = -t \\ z = 1 + 2t \end{cases}.$$

In order to find a system of cartesian equations, all we have to do is to consider the matrix

$$\begin{pmatrix} x - 1 & y & z - 1 \\ 1 & -1 & 2 \end{pmatrix}$$

and to impose that the 2×2 submatrices all have determinant 0. As explained, it is enough to fix a column whose bottom entry is non-zero and to look at the two 2×2 submatrices containing it. In this case, we can fix the first column and get:

$$\det \begin{pmatrix} x - 1 & y \\ 1 & -1 \end{pmatrix} = \det \begin{pmatrix} x - 1 & z - 1 \\ 1 & 2 \end{pmatrix} = 0,$$

getting the system

$$\ell\colon \begin{cases} x+y=1 \\ 2x-z=1 \end{cases}.$$

By Theorem 6.4.5, in general a linear subspace of $\mathbb{A}^n(K)$ of dimension m is simply the set of solutions of a system of the form:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots \\ a_{(n-m)1}x_1 + \ldots + a_{(n-m)n}x_n = b_{n-m} \end{cases},$$

where the matrix associated to the system has rank $n-m$. Therefore we immediately get the following proposition.

Proposition 6.5.6. A linear subspace $\pi \subseteq \mathbb{A}^n(K)$ is a hyperplane if and only if it is described by an equation of the form:

$$\pi\colon a_1x_1 + a_2x_2 + \ldots + a_nx_n = b,$$

where $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$.

Notice that a hyperplane in $\mathbb{A}^2(K)$ is simply a line, and a hyperplane in $\mathbb{A}^3(K)$ is simply a plane.

In general a plane in $\mathbb{A}^n(K)$ is a linear subspace of dimension 2. Thanks to Proposition 6.5.6, we see that in $\mathbb{A}^3(K)$ a plane is described by an equation of the form:

$$a_1x_1 + a_2x_2 + a_3x_3 = b,$$

with $(a_1, a_2, a_3) \neq (0, 0, 0)$. It becomes then immediately clear that a system of cartesian equations for a line in $\mathbb{A}^3(K)$ represents, geometrically, the intersection of two incident planes.

6.6 Relative position of subspaces via equations

Let $S, S' \subseteq \mathbb{A}^n(K)$ be two linear subspaces of dimension m and m', respectively. These are defined by two linear systems $AX = B$ and $A'X = B'$, respectively, where $A \in M_{(n-m)\times n}(K)$, $A' \in M_{(n-m')\times n}(K)$ are matrices of rank $n-m$ and $n-m'$, respectively. As noticed in Remark 6.4.6, the translation spaces of S and S' are nothing else than $\ker A$ and $\ker A'$. Hence we have

that

$$S \text{ is parallel to } S' \iff \ker A \subseteq \ker A' \text{ or } \ker A' \subseteq \ker A. \tag{31}$$

Lemma 6.6.1. Let m, p, n be positive integers with $m \leq p \leq n$. Let $A \in M_{m\times n}(K)$ and $B \in M_{p\times n}(K)$ and assume that $\mathrm{rk}(A) = m$ and $\mathrm{rk}(B) = p$. Then we have that $\ker(B) \subseteq \ker(A)$ if and only if

$$\mathrm{rk}\begin{pmatrix} A \\ B \end{pmatrix} = \mathrm{rk}(B)$$

where $\begin{pmatrix} A \\ B \end{pmatrix}$ is the $(m+p)\times n$ matrix obtained by adjoining the rows of B below those of A.

Proof. We denote by $\bullet$ the standard scalar product on K^n. With respect to this scalar product, the rows of A are orthogonal to vectors in $\ker A$, and those of B are orthogonal to vectors of $\ker B$. This means that

$$\mathcal{R}(A) \subseteq \ker(A)^\perp \text{ and } \mathcal{R}(B) \subseteq \ker(B)^\perp, \tag{32}$$

where $\mathcal{R}$ denotes the space generated by the rows.

Now by Lemma 6.4.4 we have that

$$\dim(\ker(A)^\perp) = n - \dim(\ker(A)) \text{ and } \dim(\ker(B)^\perp) = n - \dim(\ker(B)),$$

and since $\mathrm{rk}(A) = m$ and $\mathrm{rk}(B) = p$, by Theorem 3.2.7 we have that

$$\dim \ker(A)^\perp = m \text{ and } \dim \ker(B)^\perp = p. \tag{33}$$

On the other hand, by Theorem 2.3.18 we have that $\dim \mathcal{R}(A) = m$ and $\dim \mathcal{R}(B) = p$, so by (32) and (33) we get that

$$\mathcal{R}(A) = \ker(A)^\perp \text{ and } \mathcal{R}(B) = \ker(B)^\perp. \tag{34}$$

It follows that the rows of A are a basis of $(\ker A)^\perp$ and those of B are a basis of $(\ker B)^\perp$.

If $\ker B \subseteq \ker A$, then $(\ker A)^\perp \subseteq (\ker B)^\perp$, so $\mathcal{R}(A) \subseteq \mathcal{R}(B)$. But then it follows immediately that $\operatorname{rk}\begin{pmatrix} A \\ B \end{pmatrix} = \operatorname{rk}(B)$.

Conversely, if $\operatorname{rk}\begin{pmatrix} A \\ B \end{pmatrix} = \operatorname{rk}(B)$ then it means that each row of A is linearly dependent from the rows of B and hence if R is a row of A then $R \in \mathcal{R}(B)$. Hence $\mathcal{R}(A) \subseteq \mathcal{R}(B)$, and therefore by (34) we have that $(\ker A)^\perp \subseteq (\ker B)^\perp$. It follows that

$$((\ker B)^\perp)^\perp \subseteq ((\ker A)^\perp)^\perp,$$

and by Lemma 6.4.4 we have that $\ker B \subseteq \ker A$. □

We can now proceed to describe relative positions of lines and planes in $\mathbb{A}^2(K)$ and $\mathbb{A}^3(K)$ (as we did in Theorems 6.3.9,6.3.10 and 6.3.11) but using their equations.

Theorem 6.6.2. Let $\ell\colon ax + by = c$ and $\ell'\colon a'x + b'y = c'$ be two lines in $\mathbb{A}^2(K)$.

1. $\ell \parallel \ell'$ if and only if
$$\operatorname{rk}\begin{pmatrix} a & b \\ a' & b' \end{pmatrix} = 1.$$
If $\ell \parallel \ell'$, then $\ell = \ell'$ if and only if
$$\operatorname{rk}\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 1.$$
2. ℓ and ℓ' are incident if and only if
$$\operatorname{rk}\begin{pmatrix} a & b \\ a' & b' \end{pmatrix} = 2.$$

Proof. By Remark 6.4.6, lines ℓ and ℓ' are associated with the linear

systems $AX = B$ and $A'X = B'$, respectively, where

$$A = \begin{pmatrix} a & b \end{pmatrix}, \quad B = \begin{pmatrix} c \end{pmatrix} \quad A' = \begin{pmatrix} a' & b' \end{pmatrix}, \quad B = \begin{pmatrix} c' \end{pmatrix}$$

and their translation spaces are $\ker A$ and $\ker A'$, respectively. Since $\operatorname{rk}(A) = \operatorname{rk}(A') = 1$, by (31) and Lemma 6.6.1, we have that $\ell \parallel \ell'$ if and only if

$$\operatorname{rk} \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} = 1,$$

and consequently ℓ and ℓ' are incident if and only if

$$\operatorname{rk} \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} = 2.$$

If $\ell \parallel \ell'$, by Proposition 6.2.8 we have $\ell = \ell'$ if and only if $\ell \cap \ell' \neq \emptyset$, that is, if and only if the system

$$\begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases}$$

is compatible. Since $\operatorname{rk} \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} = 1$, by Theorem 3.1.4 this happens if and only if $\operatorname{rk} \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 1$. □

Theorem 6.6.3. Let $\pi\colon ax + by + cz = d$ and $\pi'\colon a'x + b'y + c'z = d'$ two planes in $\mathbb{A}^3(K)$.

1. $\pi \parallel \pi'$ if and only if

$$\operatorname{rk} \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 1.$$

If $\pi \parallel \pi'$ then $\pi = \pi'$ if and only if

$$\operatorname{rk}\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} = 1.$$

2. π and π' are incident if and only if

$$\operatorname{rk}\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 2.$$

Proof. The translation spaces of the planes π, π' are $\ker A$, $\ker A'$, respectively, where

$$A = \begin{pmatrix} a & b & c \end{pmatrix} \text{ and } A' = \begin{pmatrix} a' & b' & c' \end{pmatrix}.$$

Since $\operatorname{rk}(A) = \operatorname{rk}(A') = 1$, by (31) and Lemma 6.6.1, it follows that $\pi \parallel \pi'$ if and only if $\operatorname{rk}\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 1$.

In this case, by Proposition 6.2.8 we have $\pi = \pi'$ if and only if $\pi \cap \pi' \neq \emptyset$, that is, if and only if the system

$$\begin{cases} ax + by + cz = d \\ a'x + b'y + c'z = d' \end{cases}$$

is compatible, and since $\operatorname{rk}\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 1$, this happens precisely when $\operatorname{rk}\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} = 1$. □

Theorem 6.6.4. Let

$$\ell\colon \begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \end{cases} \quad \text{and} \quad \pi\colon a_3x + b_3y + c_3z = d_3$$

be a line and a plane in $\mathbb{A}^3(\mathbb{R})$, respectively.

1. $\ell \parallel \pi$ if and only if
$$\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} = 2.$$
If ℓ and π are parallel, then $\ell \subseteq \pi$ if and only if
$$\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix} = 2.$$

2. ℓ and π are incident if and only if
$$\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} = 3.$$

Proof. The translation spaces of ℓ, π are $\ker A$ and $\ker A'$, respectively, where
$$A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix} \text{ and } A' = \begin{pmatrix} a_3 & b_3 & c_3 \end{pmatrix}.$$
Of course since $\dim\ker A = 1$ and $\dim\ker A' = 2$ we have that $\ell \parallel \pi$ if and only if $\ker A \subseteq \ker A'$, and since $\operatorname{rk}(A) = 2$ and $\operatorname{rk}(A') = 1$, by Lemma 6.6.1 this happens precisely when $\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} = 2$.

By Proposition 6.2.8, we have that $\ell \subseteq \pi$ if and only if $\ell \cap \pi \neq \emptyset$, namely if and only if the system
$$\begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \end{cases}$$

is compatible, and since $\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} = 2$ this happens precisely when $\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \end{pmatrix} = 2$. □

Theorem 6.6.5. Let

$$\ell\colon \begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \end{cases} \quad \text{and} \quad \ell'\colon \begin{cases} a_3x + b_3y + c_3z = d_3 \\ a_4x + b_4y + c_4z = d_4 \end{cases}$$

be two lines in $\mathbb{A}^3(K)$.

1. We have that $\ell \parallel \ell'$ if and only if

$$\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \\ a_4 & b_4 & c_4 \end{pmatrix} = 2.$$

   If this is the case, then $\ell = \ell'$ if and only if

$$\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix} = 2.$$

2. ℓ and ℓ' are skew if and only if

$$\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \\ a_4 & b_4 & c_4 \end{pmatrix} = 3 \text{ and } \operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix} = 4.$$

3. ℓ and ℓ' are incident if and only if

$$\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \\ a_4 & b_4 & c_4 \end{pmatrix} = \operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix} = 3.$$

Proof. The translation spaces of ℓ, ℓ' are $\ker A$ and $\ker A'$, respectively, where

$$A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix} \text{ and } A' = \begin{pmatrix} a_3 & b_3 & c_3 \\ a_4 & b_4 & c_4 \end{pmatrix}.$$

Since $\operatorname{rk}(A) = \operatorname{rk}(A') = 2$, we have $\ell \parallel \ell'$ if and only if $\ker A = \ker A'$. By Lemma 6.6.1, $\ker A = \ker A'$ if and only if $\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \\ a_4 & b_4 & c_4 \end{pmatrix} = 2$. If this is the case, then by Proposition 6.2.8 we have that $\ell = \ell'$ if and only if $\ell \cap \ell' \neq \emptyset$, that is, if and only if the system

$$\begin{cases} a_1x + b_1y + c_1z = d_1 \\ a_2x + b_2y + c_2z = d_2 \\ a_3x + b_3y + c_3z = d_3 \\ a_4x + b_4y + c_4z = d_4 \end{cases} \tag{35}$$

is compatible, and since $\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \\ a_4 & b_4 & c_4 \end{pmatrix} = 2$ this happens precisely when $\operatorname{rk}\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix} = 2$. If ℓ and ℓ' are not parallel, then either they are skew or they are incident. This depends on $\ell \cap \ell'$, that is empty in the first case and has one point in the second. This is governed by system (35): the system has no solution when the lines are skew and has precisely one solution when they are incident. Theorem 3.1.4 allows then to conclude. □

6.7 Pencils and bundles of lines and planes

Definition 6.7.1. A *pencil of lines* in $\mathbb{A}^2(K)$ is the set of all lines that pass through a given point.

An *improper pencil of lines* in $\mathbb{A}^2(K)$ is the set of all lines that are parallel to a given one.

The next proposition explains how to write down equations for pencils of lines in $\mathbb{A}^2(K)$.

Proposition 6.7.2.

1. Let $P = (x_P, y_P) \in \mathbb{A}^2(K)$. Let $r\colon ax+by+c=0$ and $s\colon a'x+b'y+c'=0$ be any two distinct lines of $\mathbb{A}^2(K)$ passing through P. Let $\ell\colon a''x+b''y+c''=0$ be a line. Then ℓ belongs to the pencil of lines through P if and only if there exist $\lambda, \mu \in K$ with $(\lambda, \mu) \neq (0,0)$ such that:
$$a''x + b''y + c'' = \lambda(ax + by + c) + \mu(a'x + b'y + c').$$
2. Let $r\colon ax + by + c = 0$ be a line. A line $\ell \subseteq \mathbb{A}^2(K)$ belongs to the

improper pencil of lines parallel to r if and only if there exists $k \in K$ such that an equation for ℓ is:

$$ax + by + k = 0.$$

Proof. 1. First, assume that the line ℓ passes through P. Then $a''x_P + b''y_P + c'' = 0$. This means that the vectors (a'', b'', c'') and $(x_P, y_P, 1)$ are orthogonal with respect to the standard scalar product on K^3. Hence, $(a'', b'', c'') \in \langle (x_P, y_P, 1) \rangle^\perp$. Now since r and s both pass through P, the same reasoning holds true, so that

$$(a, b, c), (a', b', c') \in \langle (x_P, y_P, 1) \rangle^\perp.$$

On the one hand the space $\langle (x_P, y_P, 1) \rangle^\perp$ has dimension 2 by Lemma 6.4.4. Since by hypothesis the lines r and s are distinct, the vectors (a, b, c) and (a', b', c') are linearly independent in K^3. It follows that these two vector form a basis of $\langle (x_P, y_P, 1) \rangle^\perp$, and therefore there exist $\lambda, \mu \in K$ such that

$$(a'', b'', c'') = \lambda(a, b, c) + \mu(a', b', c'),$$

as required.

Conversely, if the equation of ℓ is $\lambda(ax + by + c) + \mu(a'x + b'y + c') = 0$ then ℓ passes through P since $ax_P + by_P + c = a'x_P + b'y_P + c = 0$ by hypothesis, and therefore

$$\lambda(ax_P + by_P + c) + \mu(a'x_P + b'y_P + c) = 0.$$

2. This follows immediately from Theorem 6.6.2. □

Remark 6.7.3. Let $P = (x_P, y_P) \in \mathbb{A}^2(\mathbb{R})$. In order to find the pencil of lines through P we first need to find two distinct lines through such point. For example, we can pick $x - x_P = 0$ and $y - y_P = 0$. Next, the equation of the pencil is simply:

$$\lambda(x - x_P) + \mu(y - y_P) = 0.$$

One might think that the pencil of lines through a point (x_P, y_P) is $y - y_P = m(x - x_P)$, where $m \in K$. However, this equation misses one of the lines of the pencil, namely the line $x = x_P$. In fact this equation comes from the following simplification: given the correct equation of the

pencil of lines through P, namely $\lambda r + \mu s = 0$ for some lines r, s through P, we can divide everything by μ, since proportional equations give rise to the same line. This way we obtain an equation that depends only on one parameter, namely λ/μ, but we miss the equation of the line of the pencil that corresponds to $\mu = 0$.

Definition 6.7.4. A *pencil of planes* in $\mathbb{A}^3(K)$ is the set of all planes that contain a given line.

An *improper pencil of planes* in $\mathbb{A}^3(K)$ is the set of all planes that are parallel to a given one.

Proposition 6.7.5.

1. Let $\ell \subseteq \mathbb{A}^3(K)$ be a line. Let $\pi\colon ax + by + cz + d = 0$ and $\sigma\colon a'x + b'y + c'z + d' = 0$ be two distinct planes that contain ℓ. Then a plane $\vartheta\colon a''x + b''y + c''z + d'' = 0$ belongs to the pencil of planes through ℓ if and only if there exist $\lambda, \mu \in K$ with $(\lambda, \mu) \neq (0, 0)$ such that:

$$a''x + b''y + c''z + d'' = \lambda(ax + by + cz + d) + \mu(a'x + b'y + c'z + d).$$

2. Let $\pi\colon ax + by + cz + d = 0$ be a plane in $\mathbb{A}^3(K)$. Then a plane $\sigma \subseteq \mathbb{A}^3(K)$ belongs to the improper pencil of planes parallel to π if and only if there exists $k \in K$ such that an equation for σ is:

$$ax + by + cz + k = 0.$$

Proof. 1. Let $\ell\colon \begin{cases} x = x_0 + v_1 t \\ y = y_0 + v_2 t \\ z = z_0 + v_3 t \end{cases}$ be a parametric equation for ℓ, with $(v_1, v_2, v_3) \neq (0, 0, 0)$.

First, assume that ϑ contains ℓ. Then we must have:

$$a''(x_0 + v_1 t) + b''(y_0 + v_2 t) + c''(z_0 + v_3 t) + d'' = 0,$$

and this is equivalent to the pair of conditions:

$$\begin{cases} a''x_0 + b''y_0 + c''z_0 + d'' = 0 \\ a''v_1 + b''v_2 + c''v_3 = 0 \end{cases}.$$

In turn, these two conditions are equivalent to asking that the vector (a'', b'', c'', d'') is orthogonal, via the standard scalar product on K^4, to both $(x_0, y_0, z_0, 1)$ and $(v_1, v_2, v_3, 0)$. In other words, if we let $W := \langle (x_0, y_0, z_0, 1), (v_1, v_2, v_3, 0) \rangle$, we have:

$$(a'', b'', c'', d'') \in W^\perp.$$

Now, since $(v_1, v_2, v_3, 0) \neq \underline{0}$, the vectors $(x_0, y_0, z_0, 1)$ and $(v_1, v_2, v_3, 0)$ are linearly independent, since the last coordinate of the former is 1 and that of the latter is 0. It follows that $\dim W = 2$ and hence $\dim W^\perp = 2$ by Lemma 6.4.4. Now since both π and σ contain ℓ, the same argument we used above proves that (a, b, c, d) and (a', b', c', d') both belong to $W^\perp$. On the other hand these vectors must be linearly independent, since $\pi \neq \sigma$. Hence they form a basis of $W^\perp$, and it follows that there exist $\lambda, \mu \in K$ such that:

$$(a'', b'', c'', d'') = \lambda(a, b, c, d) + \mu(a', b', c', d').$$

Conversely, if the equation of ϑ is of the form $\lambda\pi + \mu\sigma$, then necessarily $\ell \subseteq \vartheta$, since it is contained in both π and σ.

2. This follows immediately from Theorem 6.6.3. □

Remark 6.7.6. Let $\ell\colon \begin{cases} ax + by + cz = d \\ a'x + b'y + c'z + d' = 0 \end{cases}$ be a line in $\mathbb{A}^3(K)$. Since the two equations defining it represent two distinct planes through ℓ, an equation for the pencil of planes through ℓ is:

$$\lambda(ax + by + cz + d) + \mu(a'x + b'y + c'z + d') = 0.$$

Definition 6.7.7. A *bundle of lines* in $\mathbb{A}^3(K)$ is the set of all lines that pass through a given point.

An *improper bundle of lines* in $\mathbb{A}^3(K)$ is the set of all lines that are parallel to a given one.

A *bundle of planes* in $\mathbb{A}^3(K)$ is the set of all planes that pass through

a given point.

An *improper bundle of planes* in $\mathbb{A}^3(K)$ is the set of all planes that are parallel to a given line.

Given a point $P = (x_P, y_P, z_P) \in \mathbb{A}^3(K)$, the parametric equation for the bundle of lines through P is:

$$\begin{cases} x = x_P + \lambda t \\ y = y_P + \mu t \\ z = z_P + \nu t \end{cases},$$

where $(\lambda, \mu, \nu) \in K^3 \setminus \{(0,0,0)\}$. Notice that two non-zero triples $(\lambda_0, \mu_0, \nu_0)$ and $(\lambda_0', \mu_0', \nu_0')$ in K^3 determine the same line in the bundle if and only if they are proportional. Equivalently, one can write down a cartesian equation for the bundle of lines through P, that is the following:

$$\begin{cases} \mu(x - x_P) - \lambda(y - y_P) = 0 \\ \nu(x - x_P) - \lambda(z - z_P) = 0 \end{cases}.$$

Given a line $\ell \subseteq \mathbb{A}^3(K)$ with translation space generated by a non-zero vector $(v_1, v_2, v_3) \in K^3$, the parametric equation for the bundle of lines parallel to ℓ is:

$$\begin{cases} x = \lambda + v_1 t \\ y = \mu + v_2 t \\ z = \nu + v_3 t \end{cases},$$

where $(\lambda, \mu, \nu) \in K^3$. Two triples $(\lambda_0, \mu_0, \nu_0)$ and $(\lambda_0', \mu_0', \nu_0')$ in K^3 determine the same line in the bundle if and only if the line through the points $(\lambda_0, \mu_0, \nu_0)$ and $(\lambda_0', \mu_0', \nu_0')$ of $\mathbb{A}^3(K)$ has direction (v_1, v_2, v_3). This happens precisely when

$$\operatorname{rk} \begin{pmatrix} \lambda_0 - \lambda_0' & \mu_0 - \mu_0' & \nu_0 - \nu_0' \\ v_1 & v_2 & v_3 \end{pmatrix} = 1.$$

The proof of the following proposition is completely analogous to that of Proposition 6.7.2, so we omit it. We invite the interested readers to try to write it down themselves.

Proposition 6.7.8.

1. Let $P \in \mathbb{A}^3(K)$ and let $\pi_1, \pi_2, \pi_3 \subseteq \mathbb{A}^3(K)$ be three planes through P such that $\pi_1 \cap \pi_2 \cap \pi_3 = \{P\}$. Then a plane σ belongs to the

bundle of planes through P if and only if there exist $\lambda, \mu, \nu \in K$ not all zero such that

$$\sigma = \lambda\pi_1 + \mu\pi_2 + \nu\pi_3.$$

2. Let $\ell \subseteq \mathbb{A}^3(K)$ be a line. Let $\pi_1, \pi_2, \pi_3 \subseteq \mathbb{A}^3(K)$ be three planes parallel to ℓ such that $\pi_1 \cap \pi_2 \cap \pi_3 = \emptyset$ and π_1, π_2, π_3 are not all parallel to each other. Then a plane σ belongs to the bundle of planes parallel to ℓ if and only if there exist $\lambda, \mu, \nu \in K$ not all zero such that

$$\sigma = \lambda\pi_1 + \mu\pi_2 + \nu\pi_3.$$

Remark 6.7.9. Similarly to what happens for pencils of lines, the bundle of planes through a given point $P = (x_P, y_P, z_P) \in \mathbb{A}^3(K)$ has equation:

$$\lambda(x - x_P) + \mu(y - y_P) + \nu(z - z_P) = 0.$$

Note:-

A pencil is, roughly speaking, an family that is determined by a pair of parameters, while a bundle is determined by a triple of parameters. However, since proportional parameters define the same object in the pencil/bundle, in a pencil there is just 1 "degree of freedom", while in a bundle there are 2. When $K = \mathbb{R}$, we sometimes say that a pencil contains ∞^1 objects, while a bundle contains ∞^2 objects.

We will see later on that projective geometry yields a framework where there is no real distinction between proper and improper pencils and bundles.

Chapter 7: Euclidean geometry

7.1 Euclidean spaces

Definition 7.1.1. A *euclidean space* of dimension n is a 4-tuple $(E, V, f, \bullet)$, where V is an $\mathbb{R}$-vector space of dimension n, the triple (E, V, f) is an affine space of dimension n over the field $\mathbb{R}$ and $\bullet$ is a positive definite scalar product on V.

Example 7.1.2. The affine space $\mathbb{A}^n(\mathbb{R})$ can be seen as an euclidean space of dimension n when the underlying vector space $\mathbb{R}^n$ is endowed with the standard scalar product. This euclidean space is denoted by $\mathbb{E}^n(\mathbb{R})$.

Definition 7.1.3. Let $(E, V, f, \bullet)$ be a euclidean space of dimension n. Two linear subspaces $[O, W]$ and $[O', W']$ are *orthogonal* if $W^\perp \subseteq W'$ or $W \subseteq W'^\perp$.

We write $[O, W] \perp [O', W']$ to denote orthogonality.

Note:-

In this chapter we will appeal several times to the following facts, without citing them every time. Let V be an $\mathbb{R}$-vector space of dimension n with a positive definite scalar product $\bullet$ and $W \subseteq V$ be a vector subspace. Then:

- $W \oplus W^\perp = V$;
- $\dim W^\perp = n - \dim W$;
- $(W^\perp)^\perp = W$.

These facts are the content of Theorem 4.2.13 and Corollary 4.2.14.

Remark 7.1.4. Let $(E, V, f, \bullet)$ be a euclidean space of dimension n. Two linear subspaces $[O, W]$ and $[O', W']$ such that $1 \leq \dim W, \dim W' \leq n-1$ cannot be parallel and orthogonal at the same time. In fact, if $W \parallel W'$ then suppose without loss of generality that $W \subseteq W'$. If it was $W^\perp \subseteq W'$ then it would also be $W + W^\perp \subseteq W'$. But $W + W^\perp = V$, and therefore $W' = V$, contradicting the fact that $\dim W' < n$. If on the other hand

it was $W \subseteq W'^{\perp}$, then it would be $W' \subseteq W^{\perp}$ by taking orthogonal complements, and hence $W \subseteq W^{\perp}$, that is impossible because $\dim W > 0$.

Proposition 7.1.5. Let $(E, V, f, \bullet)$ be a euclidean space of dimension n. Let ℓ be a line, H be a hyperplane and P be a point.

1. There exists a unique hyperplane through P that is orthogonal to ℓ.
2. There exists a unique line through P that is orthogonal to H.

Proof. 1. Let W be the translation space of ℓ. Then $\dim W^{\perp} = n - 1$, so if W' is the translation space of a hyperplane that is orthogonal to ℓ, we must necessarily have $W' = W^{\perp}$. Hence $[P, W^{\perp}]$ is the unique hyperplane orthogonal to ℓ passing through P.

2. Let U be the translation space of H. This has dimension $n - 1$, and so $\dim U^{\perp} = 1$. Hence if U' is the translation space of a line that is orthogonal to H, we must necessarily have $U' = U^{\perp}$. Hence $[P, U^{\perp}]$ is the unique line through P that is orthogonal to H. □

Proposition 7.1.6. Let $(E, V, f, \bullet)$ be a euclidean space of dimension 3. Let $\ell, \pi \subseteq E$ be a line and a plane, respectively.

1. If $\ell \perp \pi$, then ℓ is orthogonal to every line $\ell' \subseteq \pi$.
2. If ℓ is not orthogonal to π, then there exists a unique plane π' that is orthogonal to π and such that $\ell \subseteq \pi'$.

Proof. 1. Let W be the translation space of ℓ and let U be the translation space of π. Since $\dim W^{\perp} = 2$ and $\ell \perp \pi$, it must be that $W^{\perp} = U$. If $\ell' \subseteq \pi$, then the translation space U' of ℓ' is contained in U, and therefore $U' \subseteq W^{\perp}$. But then $\ell \perp \ell'$, by definition.

2. Let W be the translation space of π. If σ is another plane with translation space U, then in order for π and σ to be orthogonal it must be that $W^{\perp} \subseteq U$, since by dimension counting it cannot happen that $W \subseteq U^{\perp}$.

Now let W' be the translation space of ℓ. The space $W^{\perp}$ is a 1-dimensional subspace of V, and since ℓ is not orthogonal to π, we cannot have that $W^{\perp} = W'$. Since $W', W^{\perp}$ are both 1-dimensional, this means that $\dim(W' + W^{\perp}) = 2$. On the other hand, any plane containing ℓ

must have a translation space that contains W'. Hence the plane $\pi' = [P, W' + W^\perp]$, where P is any point of ℓ, is the unique plane containing ℓ that is orthogonal to π. □

Proposition 7.1.7. Let $(E, V, f, \bullet)$ be a euclidean space of dimension 3 and let $\ell, \ell' \subseteq (E, V, f, \bullet)$ be two skew lines. Then there exists a unique line that is orthogonal and incident to both ℓ and ℓ'.

Proof. Let W, W' be the translation spaces of ℓ, ℓ', respectively. Since the two lines are skew, we have $W \neq W'$. Therefore it cannot be $W^\perp = W'^\perp$, as otherwise taking orthogonal complements we would get that $W = W'$. Hence $W^\perp$ and $W'^\perp$ are two distinct 2-dimensional subspaces of V, and necessarily we must have $W^\perp + W'^\perp = V$. By the Grassmann formula it follows that

$$\dim(W^\perp \cap W'^\perp) = 1,$$

namely, there exists a unique 1-dimensional subspace of V that is orthogonal to W and W' at the same time. Let $U := W^\perp \cap W'^\perp$ be such subspace. Now let $P \in \ell$ and consider the plane $\pi = [P, U + W]$ (notice that $\dim(U + W) = 2$ since $U \subseteq W^\perp$). Clearly, any line that is orthogonal and incident to both ℓ and ℓ' must be contained in π. Now we claim that π is not parallel to ℓ'. In fact, suppose by contradiction that it is. Then we necessarily have $W' \subseteq U + W$. Let $\underline{w}' \in W'$ be a non-zero vector. Then there exists $\underline{w} \in W$ such that $\underline{w}' - \underline{w} \in U$. But $U = W^\perp \cap W'^\perp$, and hence $\underline{w}' - \underline{w}$ is orthogonal to both $\underline{w}$ and $\underline{w}'$, i.e.

$$\underline{w} \bullet (\underline{w}' - \underline{w}) = \underline{w}' \bullet (\underline{w}' - \underline{w}) = 0,$$

and subtracting the two equations term by term and using the properties of the scalar product we would get

$$\|\underline{w}' - \underline{w}\|^2 = 0,$$

that implies $\underline{w}' = \underline{w}$ since $\bullet$ is positive definite. Hence $\underline{w} \in W \cap W'$, but since $W \neq W'$ we have $W \cap W' = \{\underline{0}\}$, so that $\underline{w} = \underline{0}$, which contradicts the hypothesis.

Hence π and ℓ' are not parallel, and the only other possibility is that they are incident. Let $Q = \pi \cap \ell'$ be the incidence point. The line $[Q, U]$ is the only line that can be orthogonal and incident to both ℓ and ℓ'. We already know that it is orthogonal to both ℓ and ℓ', since its direction is U,

and it is incident to ℓ', by construction. On the other hand it is contained in π, that is a 2-dimensional affine space that contains ℓ, and it is not parallel to ℓ, and therefore it must be incident to ℓ as well. □

Definition 7.1.8. Let $(E, V, f, \bullet)$ be a euclidean space of dimension n and let $P, Q \in E$ be two points.

1. The *distance* between P and Q is defined as $d(P,Q) = \|\overrightarrow{PQ}\|$.
2. The *segment* with endpoints P and Q is defined as
$$\overline{PQ} = \{t_{\lambda\overrightarrow{PQ}}(P) \colon \lambda \in [0,1]\},$$
namely it is the set of all translates of P by a vector of the form $\lambda\overrightarrow{PQ}$, where λ is a real number between 0 and 1.
3. The *midpoint* of the segment of endpoints P and Q is $t_{\frac{1}{2}\overrightarrow{PQ}}(P)$.
4. The *axis* of the segment $\overline{PQ}$ is the unique hyperplane through the midpoint of $\overline{PQ}$ that is orthogonal to the line through P and Q (this exists unique thanks to Proposition 7.1.5).
5. Let H be a hyperplane. The *orthogonal projection* of P onto H is the unique intersection between H and the line through P that is orthogonal to H.

7.2 Coordinate systems, orthogonality and distance

Definition 7.2.1. Let $(E, V, f, \bullet)$ be a euclidean space of dimension n. A *coordinate system* is a pair $(O, \mathcal{B})$ where $O \in E$ is a point called *origin* and $\mathcal{B}$ is an orthonormal basis of V.

Of course since a euclidean space is, in particular, an affine space, once a coordinate system is chosen then Theorems 6.4.2 and 6.4.5 can be applied, and E can be "transformed" into the well-known affine space $\mathbb{A}^n(\mathbb{R})$. However, this time we have an additional piece of structure, that is a positive definite scalar product. Hence it is natural to ask what happens to the scalar product on V, once we apply the map $\Lambda_{[O,\mathcal{B}]}$.

Theorem 7.2.2. Let $(E, V, f, \bullet)$ be euclidean space of dimension n and let $\mathcal{B} = \{\underline{v}_1, \dots, \underline{v}_n\}$ be an orthonormal basis of V. Let

$$\Phi_{\mathcal{B}} \colon V \to \mathbb{R}^n$$

$$\underline{v} \mapsto (\alpha_1, \dots, \alpha_n)$$

where $\underline{v} = \sum_{i=1}^n \alpha_i \underline{v}_i$ be the bijection of Theorem 6.4.2. Then for every $\underline{v}, \underline{w} \in V$ we have:

$$\underline{v} \bullet \underline{w} = \Phi_{\mathcal{B}}(\underline{v}) \cdot \Phi_{\mathcal{B}}(\underline{w}),$$

where the scalar product on the right hand side is the standard scalar product on $\mathbb{R}^n$.

Proof. Let $\underline{v} = \sum_{i=1}^n \alpha_i \underline{v}_i$ and $\underline{w} = \sum_{i=1}^n \beta_i \underline{v}_i$, where $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbb{R}$. Then $\Phi_{\mathcal{B}}(\underline{v}) = (\alpha_1, \dots, \alpha_n)$ and $\Phi_{\mathcal{B}}(\underline{w}) = (\beta_1, \dots, \beta_n)$, so that

$$\Phi_{\mathcal{B}}(\underline{v}) \cdot \Phi_{\mathcal{B}}(\underline{w}) = \sum_{i=1}^n \alpha_i \beta_i.$$

On the other hand,

$$\underline{v} \bullet \underline{w} = \left(\sum_{i=1}^n \alpha_i \underline{v}_i \right) \bullet \left(\sum_{i=1}^n \beta_i \underline{w}_i \right) = \sum_{i=1}^n \sum_{j=1}^n (\alpha_i \beta_j) \underline{v}_i \bullet \underline{w}_j = \sum_{i=1}^n \alpha_i \beta_i,$$

where in the second equality we just used the properties of scalar products and in the third equality we used the fact that $\mathcal{B}$ is an orthonormal basis. □

Theorem 7.2.2 essentially says that once we choose a coordinate system, a euclidean space of dimension n "becomes" the euclidean space $\mathbb{E}^n(\mathbb{R})$. Therefore we can now focus on the latter, and see how orthogonality relations are detectable from equations of linear subspaces.

Proposition 7.2.3. Let $\ell \colon ax + by = c$ and $\ell' \colon a'x + b'y = c'$ be two lines in $\mathbb{E}^2(\mathbb{R})$. Then $\ell \perp \ell'$ if and only if $aa' + bb' = 0$.

Proof. The translation spaces of ℓ, ℓ' are $\ker A$ and $\ker A'$, respectively, where $A = \begin{pmatrix} a & b \end{pmatrix}$ and $A' = \begin{pmatrix} a' & b' \end{pmatrix}$. It is immediate to see that $\ker A = \langle (-b, a) \rangle$ and $\ker A' = \langle (-b', a') \rangle$. Since $\dim(\ker A)^\perp = 1 = \dim \ker A'$,

we have that $\ell \perp \ell'$ if and only if $(\ker A)^\perp = \ker A'$. Clearly $(\ker A)^\perp = \langle (a,b) \rangle$, and this coincides with $\ker A'$ if and only if the vectors (a,b) and $(-b',a')$ are linearly dependent, namely if and only if $\det \begin{pmatrix} a & b \\ -b' & a' \end{pmatrix} = 0$, that is precisely the condition $aa' + bb' = 0$. □

Proposition 7.2.4.

1. Let $\pi\colon ax+by+cz+d=0$ be a plane in $\mathbb{E}^3(\mathbb{R})$ and let $W \subseteq \mathbb{R}^3$ be its translation space. Then $W^\perp = \langle (a,b,c) \rangle$.
2. Let $\pi\colon ax+by+cz+d=0$ and $\pi'\colon a'x+b'y+c'z+d'=0$ be two planes in $\mathbb{E}^3(\mathbb{R})$. Then $\pi \perp \pi'$ if and only if $aa'+bb'+cc'=0$.
3. Let $\pi\colon ax+by+cz+d=0$ be a plane in $\mathbb{E}^3(\mathbb{R})$ and let $\ell \subseteq \mathbb{E}^3(\mathbb{R})$ be a line with translation space generated by a vector $(a',b',c') \in \mathbb{R}^3$. Then $\pi \perp \ell$ if and only if $\operatorname{rk} \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} = 1$.

Proof. 1. The translation space of π is $\ker A$, where $A = \begin{pmatrix} a & b & c \end{pmatrix}$. Since for every $\underline{v} \in \ker A$ we have that $A\underline{v} = \underline{0}$, and clearly $A\underline{v}$ is the scalar product of the vectors (a,b,c) and $\underline{v}$, it follows that $(a,b,c) \in (\ker A)^\perp$. But $\dim \ker A = 2$, so $\dim(\ker A)^\perp = 1$ and therefore $(\ker A)^\perp$ is generated by (a,b,c).

2. The translation spaces of π and π' are, respectively, $\ker A$ and $\ker A'$ where $A = \begin{pmatrix} a & b & c \end{pmatrix}$ and $A' = \begin{pmatrix} a' & b' & c' \end{pmatrix}$. Since they both have dimension 2, their orthogonal complements both have dimension 1. Hence $\pi \perp \pi'$ if and only if $(\ker A)^\perp \subseteq \ker A'$. By point 1., $(\ker A)^\perp = \langle (a,b,c) \rangle$. Hence $(\ker A)^\perp$ is contained in $\ker A'$ if and only if $A' \cdot (a,b,c) = 0$, namely if and only if $aa'+bb'+cc'=0$.

3. By 1., the orthogonal complement to the translation space of π is generated by (a,b,c). Since the translation space of ℓ is also 1-dimensional, we have that $\ell \perp \pi$ if and only if (a,b,c) and (a',b',c') generate the same space, i.e. if and only if they are linearly dependent. □

Remark 7.2.5. In general, if $H\colon a_1x_1 + a_2x_2 + \ldots + a_nx_n + a_0 = 0$ is a hyperplane in $\mathbb{E}^n(\mathbb{R})$, the orthogonal complement of its translation space is generated by the vector $(a_1, \ldots, a_n)$.

Definition 7.2.6. Given a point $P \in \mathbb{E}^n(\mathbb{R})$ and a hyperplane $H \subseteq \mathbb{E}^n(\mathbb{R})$, the *distance* between P and H is the distance of P from the orthogonal projection of P onto H.

Theorem 7.2.7. Let $H\colon a_1x_1 + \ldots + a_nx_n + a_0 = 0$ be a hyperplane in $\mathbb{E}^n(\mathbb{R})$ and let $P = (x_1^P, x_2^P, \ldots, x_n^P) \in \mathbb{E}^n(\mathbb{R})$. Then the distance between P and H is given by the formula:

$$\frac{|a_1x_1^P + a_2x_2^P + \ldots + a_nx_n^P + a_0|}{\sqrt{\sum_{i=1}^n a_i^2}}.$$

Proof. We have to compute the orthogonal projection of P onto H. The direction orthogonal to H is, thanks to Remark 7.2.5, $(a_1, \ldots, a_n)$. Hence the unique line through P that is orthogonal to H is

$$\ell\colon \begin{cases} x_1 = x_1^P + a_1t \\ x_2 = x_2^P + a_2t \\ \ldots \\ x_n = x_n^P + a_nt \end{cases}.$$

To find its intersection with H, we susbstitute the parametric equation into the equation of H, obtaining

$$a_1(x_1^P + a_1t) + \ldots + a_n(x_n^P + a_nt) + a_0 = 0,$$

namely $t = -\frac{H(P)}{\sum_{i=1}^n a_i^2}$, where we set $H(P) = a_1x_1^P + a_2x_2^P + \ldots + a_nx_n^P + a_0$. This means that the orthogonal projection Q of P onto H has coordinates

$$\left(x_1^P - a_1\frac{H(P)}{\sum_{i=1}^n a_i^2}, x_2^p - a_2\frac{H(P)}{\sum_{i=1}^n a_i^2}, \ldots, x_n^P - a_n\frac{H(P)}{\sum_{i=1}^n a_i^2}\right).$$

Hence the vector $\overrightarrow{PQ}$ is just

$$\overrightarrow{PQ} = -\left(a_1\frac{H(P)}{\sum_{i=1}^n a_i^2}, a_2\frac{H(P)}{\sum_{i=1}^n a_i^2}, \dots, a_n\frac{H(P)}{\sum_{i=1}^n a_i^2}\right)$$

and its norm, which is the distance between P and H, is

$$\sqrt{\sum_{i=1}^n \frac{a_i^2 H(P)^2}{\left(\sum_{i=1}^n a_i^2\right)^2}} = \frac{|H(P)|}{\sum_{i=1}^n a_i^2}.$$

□

Definition 7.2.8.

1. Let $\pi, \pi' \subseteq \mathbb{E}^3(\mathbb{R})$ be two parallel planes. Their *distance* is defined as the distance of any point of π from π'.
2. Let $\ell, \pi \subseteq \mathbb{E}^3(\mathbb{R})$ be a line and a plane, respectively, that are parallel. Their *distance* is defined as the distance of any point of ℓ from π.

Remark 7.2.9. The distance between two parallel planes is well-defined, that is, it does not depend on the choice of a point on π. In fact, suppose π and π' are parallel planes. Then by Theorem 6.6.3, they have cartesian equations of the form $\pi\colon ax+by+cz+d=0$ and $\pi'\colon ax+by+cz+d'=0$. Let $P=(x_P, y_P, z_P) \in \pi$. By Theorem 7.2.7 we have that

$$d(P,\pi') = \frac{|ax_P + by_P + cz_P + d'|}{\sqrt{a^2+b^2+c^2}} = \frac{|d'-d|}{\sqrt{a^2+b^2+c^2}},$$

that is a formula that does not depend on the coordinates of P. Moreover, it is symmetric in π and π', that is, the distance between π and π' can also be computed as the distance from π of any point of π'.

If ℓ and π are a line and a plane that are parallel, then there is a unique plane π' containing ℓ that is parallel to π, so the distance between ℓ and π is the same as the distance between π and π'.

Definition 7.2.10. Let $\ell, \ell' \subseteq \mathbb{E}^3(\mathbb{R})$ be two skew lines. Let r be the unique line that is orthogonal and incident to both ℓ and ℓ', whose exis-

tence is granted by Proposition 7.1.7. Let P, Q be the incidence points. Then the distance of ℓ and ℓ' is defined as the distance of P and Q.

Proposition 7.2.11. Let $\ell, \ell' \subseteq \mathbb{E}^3(\mathbb{R})$ be two skew lines. Let $\pi, \pi' \subseteq \mathbb{E}^3(\mathbb{R})$ be two parallel planes such that $\ell \subseteq \pi$ and $\ell' \subseteq \pi'$. Then

$$d(\ell, \ell') = d(\pi, \pi').$$

Proof. Since $\pi \parallel \pi'$, the two planes have the same translation space W. Since $\ell \subseteq \pi$ and $\ell' \subseteq \pi'$, if U is the translation space of ℓ and U' is the translation space of ℓ' then necessarily $U + U' \subseteq W$. On the other hand since ℓ and ℓ' are not parallel then $U \neq U'$ and hence $U \oplus U' = W$. In particular, if $(\underline{u})$ is a basis of U and $(\underline{u}')$ is a basis of U', then $(\underline{u}, \underline{u}')$ is a basis of W.

Let r be the unique line that is incident and orthogonal to both ℓ and ℓ', and let $U_r = \langle \underline{u}_r \rangle$ be its translation space. Since $r \perp \ell$ and $r \perp \ell'$, we have that $\underline{u}_r \bullet \underline{u} = 0$ and $\underline{u}_r \bullet \underline{u}' = 0$; it follows that $\underline{u}_r \in W^\perp$. Namely, $r \perp \pi$. Let $P = \ell \cap r$ and $Q = \ell' \cap r$. Then Q is the orthogonal projection of P on π', because it is the intersection of the unique line orthogonal to π' and passing through P, that is r. Hence $d(P, Q)$ is both the distance from ℓ to ℓ' and that of π from π'. □

Example 7.2.12. Let us compute the distance between the two lines

$$\ell\colon \begin{cases} x + y = 0 \\ x - z = 1 \end{cases} \quad \text{and} \quad \ell'\colon \begin{cases} x - y = 0 \\ 2x + z = 0 \end{cases}.$$

By solving the two systems one sees that the translation space W of ℓ is generated by $(1, -1, 1)$ while the translation space W' of ℓ' is generated by $(1, 1, -2)$. Hence

$$W^\perp = \langle (1, 1, 0), (1, 0, -1) \rangle \text{ and } W'^\perp = \langle (1, -1, 0), (2, 0, 1) \rangle.$$

To find $W^\perp \cap W'^\perp$, we need to solve the linear system

$$a(1, 1, 0) + b(1, 0, -1) = c(1, -1, 0) + d(2, 0, 1),$$

and we see easily that

$$W^\perp \cap W'^\perp = \langle (1,3,2) \rangle.$$

Any line that is orthogonal and incident to ℓ must be contained in the plane through ℓ that has translation space $\langle (1,-1,1), (1,3,2) \rangle$. This has equation:

$$\pi \colon 5x + y - 4z - 4 = 0,$$

and its intersection with ℓ' is the point $Q = (2/7, 2/7, -4/7)$. The line r with direction $(1,3,2)$ passing through Q has equation

$$r \colon \begin{cases} x = 2/7 + t \\ y = 2/7 + 3t \\ z = -4/7 + 2t \end{cases},$$

and its intersection with ℓ is the point $P = (1/7, -1/7, -6/7)$. Hence we have

$$d(\ell, \ell') = d(P, Q) = \sqrt{(2/7 - 1/7)^2 + (2/7 + 1/7)^2 + (-4/7 + 6/7)^2} =$$

$$= \frac{\sqrt{14}}{7} = \frac{\sqrt{2}}{\sqrt{7}}.$$

Now let us try to compute $d(\ell, \ell')$ using Proposition 7.2.11. First, we need to find two parallel planes π, π' such that $\ell \subseteq \pi$ and $\ell' \subseteq \pi'$. To do this, notice that the pencil of planes through ℓ has equation:

$$\lambda(x + y) + \mu(x - z - 1) = 0,$$

while the pencil of planes through ℓ' has equation:

$$\lambda'(x - y) + \mu'(2x + z) = 0.$$

Rewrite these equations as:

$$(\lambda + \mu)x + \lambda y - \mu z - \mu = 0 \text{ and } (\lambda' + 2\mu')x - \lambda' y + \mu' z = 0.$$

Now impose parallelism, namely:

$$\begin{cases} \lambda + \mu = \lambda' + 2\mu' \\ \lambda = -\lambda' \\ -\mu = \mu' \end{cases}.$$

This system yields:

$$\begin{cases} \mu = -2/3\lambda \\ \lambda' = -\lambda \\ \mu' = 2/3\lambda \end{cases}$$

so that the parameters $\lambda = 3$, $\mu = -2$, $\lambda' = -3$, $\mu' = 2$ yield the two parallel planes

$$\pi\colon x + 3y + 2z + 2 = 0 \text{ and } \pi'\colon x + 3y + 2z = 0.$$

Now pick a point on π', such as $(0, 0, 0)$, and use Theorem 7.2.7. We get:

$$d(\pi, \pi') = \frac{2}{\sqrt{1 + 9 + 4}} = \frac{2}{\sqrt{14}} = \frac{\sqrt{2}}{\sqrt{7}}.$$

Chapter 8: Projective geometry

8.1 Equivalence relations

Definition 8.1.1. Let S be a set. A *relation* on S is a subset $\mathcal{R}$ of $S \times S$. A relation $\mathcal{R} \subseteq S \times S$ is said to be:

1. *reflexive* if for every $s \in \mathcal{R}$ we have that $(s, s) \in \mathcal{R}$;
2. *symmetric* if $(s, t) \in \mathcal{R}$ if and only if $(t, s) \in \mathcal{R}$;
3. *transitive* if $(s, t) \in \mathcal{R}$ and $(t, u) \in \mathcal{R}$ implies that $(s, u) \in \mathcal{R}$.

A relation that is reflexive, symmetric and transitive is called an *equivalence relation.*

Example 8.1.2.

- Let S be a set. The relation $\mathcal{R} = S \times S$ is an equivalence relation.
- Let S be a set. The relation $\mathcal{R} = \{(s, s) \colon s \in S\}$ is an equivalence relation.
- Let $S = \mathbb{N}$. The relation $\mathcal{R} = \{(s, t) \in \mathbb{N} \times \mathbb{N} \colon s - t \geq 0\}$ is reflexive, since $s - s = 0$ for every $s \in \mathbb{N}$, it is transitive because if $s - t \geq 0$ and $t - u \geq 0$ then adding up the two inequalities it follows that $s - u \geq 0$, so that $(s, u) \in \mathcal{R}$, but it is not symmetric, since for example $(2, 1) \in \mathcal{R}$ but $(1, 2) \notin \mathcal{R}$.
- Let $S = \mathbb{Z}$. The relation $\mathcal{R} = \{(s, t) \in \mathbb{Z} \times \mathbb{Z} \colon s \cdot t \leq 0\}$ is clearly symmetric, since $s \cdot t = t \cdot s$ but it is not reflexive, since for example $(2, 2) \notin \mathcal{R}$, and it is not transitive since for example $(1, -2) \in \mathcal{R}$, $(-2, 3) \in \mathcal{R}$ but $(1, 3) \notin \mathcal{R}$.
- Let $S = \mathbb{Z}$. The relation $\mathcal{R} = \{(s, t) \in \mathbb{Z} \times \mathbb{Z} \colon s + t \text{ is even}\}$ is an equivalence relation: $(s, s) \in \mathcal{R}$ for every $s \in \mathbb{Z}$ since $2s$ is always even, if $s + t$ then so is $s + t$ and if $s + t$ is even and $t + u$ is even, then $(s + t) + (t + u)$ is also even. Since the latter sum is $s + u + 2t$, then $s + u$ needs to be even as well.

Definition 8.1.3. Let S be a set and $\mathcal{R}$ be an equivalence relation. If $(s,t) \in \mathcal{R}$ we write $s \sim_{\mathcal{R}} t$, or just $s \sim t$ when there is no risk of ambiguity. We say that s *is in relation with* t.

Given $s \in S$, the set

$$[s] \coloneqq \{t \in S \colon s \sim t\}$$

is called the *equivalence class* of s.

If $[s]$ is an equivalence class, an element of $[s]$ is called a *representative* of $[s]$.

Remark 8.1.4. Equivalence classes are never empty because equivalence relations are reflexive, and hence $s \in [s]$ for every $s \in S$.

Proposition 8.1.5. Let S be a set and $\mathcal{R}$ be an equivalence relation on S. Let $s, t \in S$. Then either $[s] = [t]$ or $[s] \cap [t] = \emptyset$.

Proof. Suppose that $[s] \cap [t] \neq \emptyset$, so that there exists $u \in [s] \cap [t]$. Now let $v \in [s]$. Then by definition $v \sim s$. On the other hand $u \in [s]$ as well, so that $u \sim s$. Since the relation $\mathcal{R}$ is symmetric and transitive, it follows that $v \sim u$. On the other hand $u \in [t]$, and hence $u \sim t$. Since the relation $\mathcal{R}$ is transitive, it follows that $v \sim t$, and hence $v \in [t]$. This shows that $[s] \subseteq [t]$. A completely symmetric argument shows that $[t] \subseteq [s]$, and hence $[s] = [t]$. □

Proposition 8.1.5 shows that an equivalence relation on S defines a *partition* on S. That is, we can "slice" S into equivalence classes that have empty intersection, and are such that every element of S belongs to exactly one equivalence class.

Definition 8.1.6. Let S be a set and $\mathcal{R}$ an equivalence relation on S. The set $S/\sim$ of equivalence classes with respect to $\mathcal{R}$ is called *quotient set*.

Example 8.1.7.

- Let S be a set and $\mathcal{R} = S \times S$. Then every element of S is in relation with every other element. Hence there is a single equivalence class,

i.e. $S/\sim$ is a set with just one element.

- Let S be a set and $\mathcal{R} = \{(s,s)\colon s \in S\}$. Then the equivalence class of an element s contains only s. Hence the set $S/\sim$ is in bijection with S, since equivalence classes are in bijection with elements.
- Let $S = \mathbb{Z}$ and $\mathcal{R} = \{(s,t) \in \mathbb{Z}\times\mathbb{Z}\colon s+t \text{ is even}\}$. Then if $s \in \mathbb{Z}$ is even, it is in relation with every other even number, and it is not in relation with any odd number. On the other hand if s is odd then it is in relation with every other odd number but it is not in relation with any even number. Hence there are just two equivalence classes: that of even numbers and that of odd numbers. That is $S/\sim$ is a set with two elements (that we conventionally identify with 0 and 1). This quotient set is conventionally denoted by $\mathbb{F}_2$ (cf. Example 1.1.14).

8.2 Projective spaces

Let K be a field and let $n \geq 0$ be a natural number. Consider the following equivalence relation on the set $S = K^{n+1} \setminus \{\underline{0}\}$. We let

$$\mathcal{R} = \{(\underline{v},\underline{w}) \in S\times S\colon \exists\, \lambda \in K\setminus\{0\} \text{ s.t. } \lambda\underline{v} = \underline{w}\}.$$

In other words, we consider two non-zero vectors of K^{n+1} to be equivalent if they are proportional. Let us check that this is an equivalence relation.

- If $(x_1,\dots,x_{n+1}) \in S$ then
$$(x_1,\dots,x_{n+1}) = 1\cdot(x_1,\dots,x_{n+1}),$$
so the relation is reflexive.
- If $\lambda(x_1,\dots,x_{n+1}) = (y_1,\dots,y_{n+1})$ then since both vectors are non-zero it must be $\lambda \neq 0$, and therefore
$$\lambda^{-1}(y_1,\dots,y_{n+1}) = (x_1,\dots,x_{n+1}),$$
so the relation is symmetric.
- If
$$\lambda(x_1,\dots,x_{n+1}) = (y_1,\dots,y_{n+1}) \text{ and } \mu(y_1,\dots,y_{n+1}) = (z_1,\dots,z_{n+1})$$
then
$$\lambda\mu(x_1,\dots,x_{n+1}) = (z_1,\dots,z_{n+1}),$$
and so the relation is transitive.

Definition 8.2.1. The quotient space $K^{n+1} \setminus \{\underline{0}\}/\sim$ is called *projective space of dimension* n, and it is denoted by $\mathbb{P}^n(K)$.

Let us try to understand in detail elements of the projective space. The key observation is the following: suppose that $(x_1, \dots, x_{n+1}) \in K^{n+1} \setminus \{\underline{0}\}$ is such that $x_{n+1} \neq 0$. Then

$$(x_1, \dots, x_{n+1}) \sim x_{n+1}^{-1}(x_1, \dots, x_{n+1}) = (x_{n+1}^{-1}x_1, \dots, x_{n+1}^{-1}x_n, 1).$$

That is, whenever the last entry of $(x_1, \dots, x_{n+1})$ is non-zero, the equivalence class of $(x_1, \dots, x_{n+1})$ contains an element whose last coordinate is 1. On the other hand, suppose that $(x_1, \dots, x_n, 1), (y_1, \dots, y_n, 1) \in K^{n+1} \setminus \{\underline{0}\}$. Then these two elements are either equal or they are not in relation with each other. In fact, if they were then there would be some non-zero $\lambda \in K$ such that

$$\lambda(x_1, \dots, x_n, 1) = (y_1, \dots, y_n, 1),$$

but $\lambda(x_1, \dots, x_n, 1) = (\lambda x_1, \dots, \lambda x_n, \lambda)$, and if this equals $(y_1, \dots, y_n, 1)$ then necessarily $\lambda = 1$. But then $(x_1, \dots, x_n, 1) = (y_1, \dots, y_n, 1)$.

Hence we can easily prove the following proposition.

Proposition 8.2.2. There exists a bijection between K^n and the set of equivalence classes of elements $(x_1, \dots, x_{n+1}) \in K^{n+1} \setminus \{\underline{0}\}$ with $x_{n+1} \neq 0$.

Proof. Consider the function

$$\phi \colon K^n \to \mathbb{P}^n(K)$$

$$(x_1, \dots, x_n) \mapsto [(x_1, \dots, x_n, 1)].$$

As we have seen above, this map is injective. On the other hand, if $[X] \in \mathbb{P}^n(K)$ is the equivalence class of an element $(x_1, \dots, x_{n+1})$ with $x_{n+1} \neq 0$ then

$$\phi((x_{n+1}^{-1}x_1, \dots, x_{n+1}^{-1}x_n)) = [(x_{n+1}^{-1}x_1, \dots, x_{n+1}^{-1}x_n, 1)] = [X],$$

so every such equivalence class $[X]$ is in the image of ϕ. □

Definition 8.2.3. Equivalence classes $[(x_1, \dots, x_{n+1})] \in \mathbb{P}^n(K)$ with $x_{n+1} \neq 0$ are called *proper points* of $\mathbb{P}^n(K)$.

Now let us focus our attention on equivalence classes of elements of $K^{n+1} \setminus \{\underline{0}\}$ of the form $(x_1, \dots, x_n, 0)$. Notice that the subset of all such elements in bijection with $K^n \setminus \{0\}$, because since the last coordinate is 0 then it must be $(x_1, \dots, x_n) \neq (0, \dots, 0)$. Now if $(x_1, \dots, x_n, 0), (y_1, \dots, y_n, 0) \in K^{n+1} \setminus \{\underline{0}\}$, these are in relation with each other exactly when $(x_1, \dots, x_n)$ and $(y_1, \dots, y_n)$ are in relation with each other as elements of $K^n \setminus \{\underline{0}\}$, because

$$\lambda(x_1, \dots, x_n, 0) = (y_1, \dots, y_n, 0) \iff \lambda(x_1, \dots, x_n) = (y_1, \dots, y_n).$$

But equivalence classes of $K^n \setminus \{\underline{0}\}$ are, by definition, elements of $\mathbb{P}^{n-1}(K)$. We have therefore proved the following proposition.

Proposition 8.2.4. There exists a bijection between $\mathbb{P}^{n-1}(K)$ and the set of equivalence classes of elements $(x_1, \dots, x_{n+1}) \in K^{n+1} \setminus \{\underline{0}\}$ with $x_{n+1} = 0$.

Definition 8.2.5. Equivalence classes $[(x_1, \dots, x_{n+1})] \in \mathbb{P}^n(K)$ with $x_{n+1} = 0$ are called *improper points* of $\mathbb{P}^n(K)$.

From now on, we will denote equivalence classes of the form $[(x_1, \dots, x_{n+1})]$ by $(x_1 : x_2 : \dots : x_{n+1})$.

We have seen that the space $\mathbb{P}^n(K)$ decomposes into two parts: the proper points and the improper points. Let us now understand them more in detail in the cases $n = 1, 2, 3$.

For $n = 1$, the proper points are in bijection with K, and they are in bijection with points of the form $(x : 1)$, where x is an element of K. What are improper points? They are points of the form $(x : 0)$, where x is a non-zero element of K. But of course any two elements $(x, 0), (y, 0) \in K^2 \setminus \{\underline{0}\}$ are in relation with each other, since $x^{-1}y(x, 0) = (y, 0)$. Therefore there is a unique improper point, that is $(1 : 0)$. Hence $\mathbb{P}^1(K)$ is the union of K and an improper point. This should be thought as a "point at infinity", and it is sometimes denoted by ∞. Hence we have, as sets, $\mathbb{P}^1(K) = K \cup \{\infty\}$.

On the other hand, K can be thought as the set of points of the affine space $\mathbb{A}^1(K)$, and hence we can write

$$\mathbb{P}^1(K) = \mathbb{A}^1(K) \cup \{\infty\}.$$

In other words, the projective space of dimension 1, that is called *projective line*, is the union of the affine line and an extra point "at infinity".

Remark 8.2.6. Another way we can think about points in $\mathbb{P}^1(K)$, without distinguishing between proper and improper points, is as 1-dimensional vector subspaces of K^2. In fact, every non-zero $(x, y) \in K^2$ generates a 1-dimensional subspace, that coincides with the subspace generated by $\lambda(x, y)$, for every $\lambda \in K \setminus 0$. Conversely, every 1-dimensional subspace is generated by a non-zero vector of K^2. Therefore there is a bijection

$$\mathbb{P}^1(K) \to \{\text{1-dimensional vector subspaces of } K^2\}.$$

The projective space $\mathbb{P}^2(K)$ is called *projective plane*. Its proper points are in bijection with K^2, and in turn they are in bijection with points of the form $(x : y : 1)$, where $(x, y) \in K^2$. Since K^2 is the set of points of $\mathbb{A}^2(K)$, we can say that proper points are in bijection with $\mathbb{A}^2(K)$. Improper points are points of the form $(x : y : 0)$, and they are in bijection with $\mathbb{P}^1(K)$. Thanks to Remark 8.2.6, we can think of these as 1-dimensional subspaces of K^2. Now every line in $\mathbb{A}^2(K)$ has a translation space, that is simply a 1-dimensional subspace of K^2. Hence improper points of $\mathbb{P}^2(K)$ can be thought as translation spaces of the lines in $\mathbb{A}^2(K)$. In other words there is a bijection

$$\mathbb{P}^2(K) \to \mathbb{A}^2(K) \cup \{\text{translation spaces of lines in } \mathbb{A}^2(K)\}.$$

Hence the projective plane should be thought as the affine plane $\mathbb{A}^2(K)$ together with some "extra points" that represent directions of the lines in $\mathbb{A}^2(K)$.

This view extends to higher dimensions as well, since $K^n \setminus \{\underline{0}\}/\sim$ can always be thought as the set of 1-dimensional subspaces of K^n. Hence for example there is a bijection

$$\mathbb{P}^3(K) \to \mathbb{A}^3(K) \cup \{\text{translation spaces of lines in } \mathbb{A}^3(K)\}.$$

8.3 Linear subspaces

Definition 8.3.1. A *linear subspace* of dimension m in $\mathbb{P}^n(K)$ is a subset of the form

$$S = \{(x_1 : \ldots : x_{n+1}) \in \mathbb{P}^n(K) \colon (x_1, \ldots, x_{n+1}) \in \ker A\},$$

where $A \in M_{(n-m)\times(n+1)}(K)$ is a matrix of rank $n - m$.

In other words, a linear subspace of dimension m is the set of equivalence classes of vectors in the kernel of an $(n - m) \times (n + 1)$ matrix of rank $n - m$,

with $\underline{0}$ removed. Similarly to what we do for affine spaces, we call a *line* a linear subspace of dimension 1, *plane* a linear subspace of dimension 2 and *hyperplane* a linear subspace of dimension $n-1$.

Example 8.3.2.

- A line in $\mathbb{P}^2(K)$ is a subset of the form
$$\ell = \{(x : y : z) \in \mathbb{P}^2(K) \colon ax + by + cz = 0\},$$
where $a, b, c \in K$ are not all 0.
- A plane in $\mathbb{P}^3(K)$ is a subset of the form
$$\pi = \{(x : y : z : t) \in \mathbb{P}^3(K) \colon ax + by + cz + dt = 0\},$$
where $a, b, c, d \in K$ are not all 0.
- A line in $\mathbb{P}^3(K)$ is a subset of the form
$$\ell = \{(x : y : z : t) \in \mathbb{P}^3(K) \colon ax+by+cz+dt = a'x+b'y+c'z+d't = 0\},$$
where $a, b, c, d, a', b', c', d' \in K$ and $\operatorname{rk} \begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} = 2$.

Geometrically, one can define a surjective map

$$\psi \colon K^{n+1} \setminus \{\underline{0}\} \to \mathbb{P}^n(K)$$
$$(x_1, \dots, x_{n+1}) \mapsto (x_1 : \dots : x_{n+1}).$$

Namely, each non-zero vector in K^{n+1} is mapped to its equivalence class in the quotient set.

Now if we think of K^{n+1} as of the set of points of the affine space $\mathbb{A}^{n+1}(K)$, then a linear subspace of $\mathbb{P}^n(K)$ of dimension m is simply the image, via ψ, of a linear subspace of $\mathbb{A}^{n+1}(K)$ of dimension $m+1$ passing through $(0, 0, \dots, 0)$, with $(0, 0, \dots, 0)$ removed.

Let now $\ell \colon ax + by + cz = 0$ be a line in $\mathbb{P}^2(K)$. We have seen that

$$\mathbb{P}^2(K) = \mathbb{A}^2(K) \cup \{\text{directions of lines in } \mathbb{A}^2(K)\}.$$

Hence we can ask what are the sets

$$\ell \cap \mathbb{A}^2(K) \text{ and } \ell \cap \{\text{directions of lines in } \mathbb{A}^2(K)\}$$

or, in other words, what are the proper points of ℓ and what are the improper points. Let us start by assuming that $(a, b) \neq (0, 0)$. To find proper points, we just have to find which points $(x_0 : y_0 : 1)$ of $\mathbb{P}^2(K)$ satisfy $ax_0 + bx_0 + c = 0$. These are clearly in bijection with points on the affine line $ax + by + c = 0$. On the other hand, improper points of ℓ are points of the form $(x_0 : y_0 : 0)$ that satisfy

$$ax_0 + by_0 = 0$$

It is immediate to see that there is just one such point, and it is $(-b : a : 0)$. Moreover, the space $\langle(-b, a)\rangle$ is precisely the translation space of the line $ax + by + c = 0$. All in all, we have proven that the line $ax + by + cz$ has two types of points: its proper points are essentially points of the affine line $ax + by + c = 0$, its unique improper point is $(-b : a : 0)$, and it represents the direction of the line $ax + by + c = 0$ in $\mathbb{A}^2(K)$.

When $(a, b) = (0, 0)$ the line ℓ becomes $z = 0$.

Definition 8.3.3. The line $z = 0$ in $\mathbb{P}^2(K)$ is called *improper line*.

The improper line contains no proper points but it contains all improper points of $\mathbb{P}^2(K)$.

An analogous reasoning can be applied to planes in $\mathbb{P}^3(K)$. If $\pi\colon ax + by + cz + dt = 0$ is a plane with $(a, b, c) \neq (0, 0, 0)$, its proper points are essentially the points on the affine plane $ax + by + cz + d = 0$, while its improper points are the points of the form $(x_0 : y_0 : z_0 : 0)$ that satisfy $ax_0 + bx_0 + cz_0 = 0$. Of course vectors $(x_0, y_0, z_0) \in K^3$ that satisfy such relation constitute the kernel of the matrix $\begin{pmatrix} a & b & c \end{pmatrix}$, and this is the translation space of the plane $ax + by + cz = 0$ in $\mathbb{A}^3(K)$. Therefore improper points of π correspond to directions of the lines that are contained in the plane $ax + by + cz = 0$.

When $(a, b, c) = (0, 0, 0)$, the plane π becomes $t = 0$.

Definition 8.3.4. The plane $t = 0$ in $\mathbb{P}^3(K)$ is called *improper plane*.

The improper plane contains no proper points but it contains all improper points of $\mathbb{P}^3(K)$.

The above discussion can also be reversed. Namely, given a linear subspace S of $\mathbb{A}^n(K)$, we can find a linear subspace S' of $\mathbb{P}^n(K)$ such that $S' \cap \mathbb{A}^n(K) = S$. This is very easy to do: all we need to do is to *homogeneize* the equation of the subspace. A subspace of $\mathbb{A}^n(K)$ is given by a system of linear equations, in which all variables $x_1, \dots, x_n$ appear to the first degree. If we think of these

as of the proper points of a linear subspace of $\mathbb{P}^n(K)$, this means that each variable x_i has to be thought as x_i/x_{n+1}. For instance, if $ax + by + c = 0$ is the equation of a line in $\mathbb{A}^2(K)$, then all we need to do is to replace x with x/z and y with y/z. The equation then becomes $ax/z + by/z + c = 0$, and multiplying by z we get $ax + by + cz = 0$, that is the equation of a line in $\mathbb{P}^2(K)$.

8.4 Equations of linear subspaces

As it happens for affine spaces, projective lines and planes have parametric equations, too. Given two distinct points $P = (x_P : y_P : z_P), Q = (x_Q : y_Q : z_Q) \in \mathbb{P}^2(K)$, a *parametric equation* of the line through P and Q is:

$$\ell\colon \begin{cases} x = \lambda x_P + \mu x_Q \\ y = \lambda y_P + \mu y_Q \\ z = \lambda z_P + \mu z_Q \end{cases};$$

here one should think of λ and μ as varying parameters that cannot be both zero. In order to obtain a cartesian equation for ℓ one just has to impose that

$$\det \begin{pmatrix} x & y & z \\ z_P & y_P & z_P \\ x_Q & y_Q & z_Q \end{pmatrix} = 0.$$

Conversely, given a line $ax+by+cz = 0$, in order to find a parametric equation we just solve the linear system. Assuming without loss of generality that $a \neq 0$ we get that $x = -(b/a)y - (c/a)z$, so that the resulting parametric equation is:

$$\begin{cases} x = \lambda \cdot (-b/a) + \mu \cdot (-c/a) \\ y = \lambda \\ z = \mu \end{cases}.$$

Given two distinct points $P = (x_P : y_P : z_P : t_P), Q = (x_Q : y_Q : z_Q : t_Q) \in \mathbb{P}^3(K)$, the parametric equation of the line through them is:

$$\begin{cases} x = \lambda x_P + \mu x_Q \\ y = \lambda y_P + \mu y_Q \\ z = \lambda z_P + \mu z_Q \\ t = \lambda t_P + \mu t_Q \end{cases};$$

to recover a cartesian equation we have to impose that

$$\operatorname{rk}\begin{pmatrix} x & y & z & t \\ z_P & y_P & z_P & t_P \\ x_Q & y_Q & z_Q & t_Q \end{pmatrix} = 2.$$

Conversely, given a cartesian equation of the form $ax + by + cz + dt = 0 = a'x + b'y + c'z + d't$ for a line in $\mathbb{P}^3(K)$, to find a parametric equation we just need to solve the system.

Example 8.4.1.

- Let $x+y-2z = 0$ be a line in $\mathbb{P}^2(\mathbb{R})$. To find a parametric equation, simply notice that $x = -y + 2z$, so we get

$$\begin{cases} x = -\lambda + 2\mu \\ y = \lambda \\ z = \mu \end{cases}.$$

- Let

$$\begin{cases} x = \lambda - \mu \\ y = 2\lambda \\ z = -\lambda + 2\mu \end{cases}$$

be a parametric equation for a line in $\mathbb{P}^2(\mathbb{R})$. To find a cartesian equation, we let

$$\det\begin{pmatrix} x & y & z \\ 1 & 2 & -1 \\ -1 & 0 & 2 \end{pmatrix} = 4x - y + 2z = 0.$$

- Let

$$\begin{cases} x = 2\lambda + \mu \\ y = 2\lambda - \mu \\ z = \mu \\ t = \lambda \end{cases}$$

be a parametric equation for a line in $\mathbb{P}^3(\mathbb{R})$. To find a cartesian equation, we have to impose

$$\operatorname{rk}\begin{pmatrix} x & y & z & t \\ 2 & 2 & 0 & 1 \\ 1 & -1 & 1 & 0 \end{pmatrix} = 2.$$

To do this, we can for example select the 2×2 submatrix given by the third and fourth row and column and use Theorem 2.3.20. This way we get:

$$\det\begin{pmatrix} x & z & t \\ 2 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \det\begin{pmatrix} y & z & t \\ 2 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} = 0,$$

which in turn yields the cartesian equation:

$$\begin{cases} x - z - 2t = 0 \\ y + z - 2t = 0 \end{cases}.$$

Analogously to the case of lines, given three distinct points $P = (x_P : y_P : z_P : t_P)$, $Q = (x_Q : y_Q : z_Q : t_Q)$ and $R = (x_R : y_R : z_R : t_R)$ in $\mathbb{P}^3(K)$ that do not lie on the same line, a *parametric equation* of the plane that contains them is:

$$\begin{cases} x = \lambda x_P + \mu x_Q + \nu x_R \\ y = \lambda y_P + \mu y_Q + \nu y_R \\ z = \lambda z_P + \mu z_Q + \nu z_R \end{cases}.$$

To obtain a cartesian equation, just impose

$$\det\begin{pmatrix} x & y & z & t \\ x_P & y_P & z_P & t_P \\ x_Q & y_Q & z_Q & t_Q \\ x_R & y_R & z_R & t_R \end{pmatrix} = 0.$$

Conversely, given a cartesian equation such as $ax+by+cz+dt = 0$, to obtain a parametric one we just have to solve the linear system. If $a \neq 0$, for example,

we get $x = -(b/a)y - (c/a)z - (d/a)t$, so that

$$\begin{cases} x = \lambda \cdot (-b/a) + \mu \cdot (-c/a) + \nu \cdot (-d/a) \\ y = \lambda \\ z = \mu \\ t = \nu \end{cases}.$$

8.5 Relative position of linear subspaces

Lemma 8.5.1. Two lines in $\mathbb{P}^2(K)$ always have non-empty intersection. The same holds true for a plane and a line in $\mathbb{P}^3(K)$ and for two planes in $\mathbb{P}^3(K)$.

Proof. Let $\ell\colon ax + by + cz = 0$ and $\ell'\colon a'x + b'y + c'z = 0$ be two lines in $\mathbb{P}^2(K)$. Their intersection is given by the system

$$\begin{cases} ax + by + cz = 0 \\ a'x + b'y + c'z = 0 \end{cases}.$$

This is a homogeneous system of 2 equations in 3 variables, and therefore the set of its solutions is a vector subspace of dimension at least 1. It follows that it always contains least one non-zero solution (x_0, y_0, z_0). This gives rise to a point $(x_0 : y_0 : z_0) \in \mathbb{P}^2(K)$ that lies on the intersection of the two lines.

If $\pi\colon ax + by + cz + dt = 0$ and $\pi'\colon a'x + b'y + c'z + d't = 0$ are two planes in $\mathbb{P}^3(K)$, their intersection is given by the system

$$\begin{cases} ax + by + cz + dt = 0 \\ a'x + b'y + c'z + d't = 0 \end{cases}.$$

This is a homogeneous system of 2 equations in 4 variables, and hence the set of its solutions is a vector subspace of dimension at least 2. Therefore it always contains a non-zero solution.

Similarly, if $\ell\colon \begin{cases} ax + by + cz + dt = 0 \\ a'x + b'y + c'z + d't = 0 \end{cases}$ is a line and $\pi\colon a''x + b''y + c''z + d''t = 0$ is a plane, the system that determines $\ell \cap \pi$ is a homogeneous system of 3 equation in 4 variables, and therefore its set of solutions is a vector space of dimension at least 1. □

Example 8.5.2.

- Let $\ell\colon x+2y+z=0$ and $\ell'\colon x-y-z=0$ be two lines in $\mathbb{P}^2(\mathbb{R})$, and let us determine their intersection. To do this, we need to solve the linear system
$$\begin{cases} x+2y+z=0 \\ x-y-z=0 \end{cases}.$$
The set of solutions of such system is:
$$\{(s,-2s,3s)\colon s\in\mathbb{R}\}$$
or, in other words, it is the vector subspace of $\mathbb{R}^3$ generated by $(1,-2,3)$. Notice that since this is 1-dimensional, all non-zero vectors in this subspace belong to the same equivalence class, that is that of $(1,-2,3)$. This simply means that $\ell\cap\ell'=\{(1:-2:3)\}$: the two lines intersect in a proper point.

- Let $\pi\colon x+y+t=0$ and $\pi'\colon x-y+t=0$ be two planes in $\mathbb{P}^3(\mathbb{R})$. To find their intersection, we need to solve the linear system
$$\begin{cases} x+y+t=0 \\ x-y+t=0 \end{cases}.$$
The matrix representing this linear system, namely $\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & -1 & 0 & 1 \end{pmatrix}$ has rank 2. Therefore, this system of two equations represents a line in $\mathbb{P}^3(\mathbb{R})$, that is exactly the intersection of π and π'.

  Of course one can also find the solutions to the system. The set of solutions is a 2-dimensional subspace of $\mathbb{R}^4$ and a basis is, for example, $((1,0,0,-1),(0,0,1,0))$. It follows that a parametric equation for $\pi\cap\pi'$ is:
$$\begin{cases} x=\lambda \\ y=0 \\ z=\mu \\ t=-\lambda \end{cases}.$$

- Let $\ell\colon x+y+t=x-y+t=0$ be the line of the previous point and let $\pi\colon x+3y+t=0$ be a plane. In order to find $\ell\cap\pi$, we need to solve the system:

$$\begin{cases} x+y+t=0 \\ x-y+t=0 \\ x+3y+t=0 \end{cases},$$

whose set of solutions is a 1-dimensional vector subspace of $\mathbb{R}^4$ generated by the vector $(0,0,1,0)$. This means that $\ell\cap\pi$ is the point $(0:0:1:0)$. Notice that since its last coordinate is 0, this is an improper point. In fact, the affine part of ℓ is the line $\ell'\colon x+y+1=x-y+1=0$, while the affine part of π is $\pi'\colon x+3y+1=0$. In $\mathbb{A}^3(\mathbb{R})$, ℓ' and π' are parallel and ℓ' does not lie on π', and hence they have no intersection. In the projective space instead, these two subspaces have an improper intersection point, that represents the direction of the line ℓ'.

If we start with two parallel linear subspaces in $\mathbb{A}^2(K)$ or $\mathbb{A}^3(K)$ that have empty intersection and we extend them to the projective space $\mathbb{P}^2(K)$ or $\mathbb{P}^3(K)$, Lemma 8.5.1 tells us that these have non-empty intersection. Hence their intersection points must belong to the improper line of $\mathbb{P}^2(K)$ or the improper plane in $\mathbb{P}^3(K)$. In fact, if for example $ax+by+c=0$ and $ax+by+c'=0$ are two parallel lines with empty intersection in $\mathbb{A}^2(K)$, once we homogeneize their equations we obtain the projective lines $ax+by+cz=0$ and $ax+by+c'z=0$. Their intersection is the improper point $(-b:a:0)$. That is, two parallel line in $\mathbb{A}^2(K)$ meet in $\mathbb{P}^2(K)$ in the improper point that represents their direction.

Similarly, two distinct parallel planes in $\mathbb{A}^3(K)$ given by $\pi\colon ax+by+cz+dt=0$ and $\pi'\colon ax+by+cz+d't=0$ meet in the line given by the equation $\begin{cases} ax+by+cz=0 \\ t=0 \end{cases}$. This is a line contained in the improper plane whose points represent the directions of the lines contained in π (or π', that is the same since they are parallel).

Finally, a line and a plane in $\mathbb{A}^3(K)$ that are parallel and distinct meet in $\mathbb{P}^3(K)$ in the improper point that represents the direction of the line.

8.6 Projective pencils and bundles

The concepts of pencils and bundles of lines and planes that we encountered in Chapter 6 can be revisited in the projective setting.

Definition 8.6.1.

1. A *pencil of lines* in $\mathbb{P}^2(K)$ is the set of all lines through a given point of $\mathbb{P}^2(K)$.
2. A *pencil of planes* in $\mathbb{P}^3(K)$ is the set of all planes that contain a given line.
3. A *bundle of lines* in $\mathbb{P}^3(K)$ is the set of all lines through a given point of $\mathbb{P}^3(K)$.
4. A *bundle of planes* in $\mathbb{P}^3(K)$ is the set of all planes through a given point of $\mathbb{P}^3(K)$.

Proposition 8.6.2.

1. Let $P \in \mathbb{P}^2(K)$ and let $r\colon ax+by+cz=0$ and $s\colon a'x+b'y+c'z=0$ be two distinct lines through P. Then the pencil of lines through $P \in \mathbb{P}^2(K)$ is given by the equation
$$\lambda(ax+by+cz)+\mu(a'x+b'y+c'z)=0.$$
2. Let $\ell \subseteq \mathbb{P}^3(K)$ be a line and let $r\colon ax+by+cz+dt=0$ and $s\colon a'x+b'y+c'z+d't=0$ be two distinct planes containing ℓ. Then the pencil of planes in $\mathbb{P}^3(K)$ containing ℓ is given by the equation
$$\lambda(ax+by+cz+dt)+\mu(a'x+b'y+c'z+d't)=0.$$

In the projective space there is no distinction between proper and improper pencil, since the concept of parallelism does not make sense anymore. On the other hand once we have a pencil of lines/planes in the affine space, we can homogeneize the equation of the pencil, obtaining a set of lines in $\mathbb{P}^2(K)$ or $\mathbb{P}^3(K)$. If we start with a proper pencil, we end up with a pencil in the projective space.

Example 8.6.3.

- Consider the pencil of lines through the point $(1,1) \in \mathbb{A}^2(K)$. This is given by the equation:

$$\lambda(x-1)+\mu(y-1)=0,$$

and homogeneizing this we get:

$$\lambda(x-z)+\mu(y-z)=0. \tag{36}$$

Since $x-z=0$ and $y-z=0$ are two lines in $\mathbb{P}^2(K)$ through $(1:1:1)$, by Proposition 8.6.2, equation (36) is that of the pencil of lines through $(1:1:1)$.

- Consider the pencil of planes through the line $x-y-1=z-2=$ in $\mathbb{A}^3(K)$. This is given by the equation:

$$\lambda(x-y-1)+\mu(z-2)=0.$$

Homogeneizing, we get

$$\lambda(x-y-t)+\mu(z-2t)=0,$$

that is the pencil of planes through the line $x-y-t=z-2t=0$ in $\mathbb{P}^3(K)$.

What happens if, on the other hand, we start with an improper pencil of lines/planes? Suppose first we have an improper pencil of lines in $\mathbb{A}^2(K)$, that is given by the equation:

$$ax+by+\mu=0,$$

where $(a,b) \in K^2 \setminus \{(0,0)\}$ are given coefficients and $\mu \in K$ is a varying parameter. Homogeneizing this, we get:

$$ax+by+\mu z=0. \tag{37}$$

Now this closely recalls the equation of a pencil of lines in $\mathbb{P}^2(K)$, except for the fact that we have only one parameter μ. However, consider the equation

$$\lambda(ax+by)+\mu z=0, \tag{38}$$

where $\lambda,\mu \in K$ are not both zero. This is precisely the equation of a pencil of lines in $\mathbb{P}^2(K)$. The lines $z=0$ and $ax+by=0$ intersect in the point

$(-b : a : 0)$, so (38) is an equation for the pencil of lines through $(-b : a : 0)$. Notice that this is the improper point corresponding to the direction of the affine line $ax + by + \mu = 0$!

How different is this from (37)? Not much: if $\lambda \neq 0$, we can divide (38) by λ, obtaining a line that belongs to the family (37). If $\lambda = 0$, on the other hand, we obtain the line $z = 0$, that does not appear in (37) for any value of μ. Hence (38) only differs from (37) by the improper line. We have therefore understood what improper pencils represent in the projective space: they are simply pencils of lines through an improper point, and thus the name.

Similarly, consider an improper pencil of planes in $\mathbb{A}^3(K)$ given by

$$ax + by + cz + \mu = 0,$$

where $(a, b, c) \in K^3$ is not the zero vector and μ is a varying parameter. Mimicking the above argument, we can consider the pencil of projective planes:

$$\lambda(ax + by + cz) + \mu t = 0.$$

This is the pencil defined by the planes $ax+by+cz = 0$ and $t = 0$, that intersect (as already explained in this chapter) in the line $ax + by + cz = t = 0$, that lies on the improper plane and contains all points corresponding to directions of lines lying on $ax + by + cz = 0$. This explains what an improper pencil of planes becomes in the projective space: it simply becomes the pencil of planes that contain the line $ax + by + cz = t = 0$, plus the improper plane itself.

This is why in the projective space there is no distinction between proper and improper pencils: they are defined exactly in the same way, but the latter's support is contained in the improper line/plane.

Proposition 8.6.4. Let $P = (x_P : y_P : z_P : t_P) \in \mathbb{P}^3(K)$.

1. The bundle of lines through P has equation:

$$\begin{cases} x = \lambda x_P + \mu v_1 \\ y = \lambda y_P + \mu v_2 \\ z = \lambda z_P + \mu v_3 \\ t = \lambda t_P + \mu v_4 \end{cases},$$

   where $(v_1, v_2, v_3, v_4) \neq (0, 0, 0, 0)$.

2. Let π_1, π_2, π_3 be pairwise distinct planes passing through P. Then

the bundle of planes through P is given by

$$\lambda\pi_1 + \mu\pi_2 + \nu\pi_3 = 0,$$

where $(\lambda, \mu, \nu) \neq (0, 0, 0)$.

Of course, the same argument we used for pencils applies to bundles as well: in the projective space there is no distinction between proper and improper bundles because an improper bundle of lines/planes is simply a bundle of lines/planes passing through an improper point.

8.7 Real and imaginary points

In this section, we focus on the case $K = \mathbb{C}$.

Definition 8.7.1. A point $P = (x_1 : \ldots : x_{n+1}) \in \mathbb{P}^{n+1}(\mathbb{C})$ is called *real* if there exists $\lambda \in \mathbb{C}$ such that $\lambda x_i \in \mathbb{R}$ for every $i = 1, \ldots, n+1$. If P is not real, then it is *imaginary*.

The *conjugate* of P is the point $\overline{P} = (\overline{x}_1 : \ldots : \overline{x}_{n+1})$.

Example 8.7.2. The point $(i : i : i) \in \mathbb{P}^2(\mathbb{C})$ is real, since multiplying its entries by $-i$ we obtain $(1 : 1 : 1) \in \mathbb{P}^2(\mathbb{R})$. The point $(i : 1) \in \mathbb{P}^1(\mathbb{C})$ is imaginary, since if there was $\lambda \in \mathbb{C}$ such that $\lambda i, \lambda \in \mathbb{R}$, then in particular $\lambda \in \mathbb{R}$ and therefore $\lambda i \notin \mathbb{R}$.

Note:-

The notion of conjugate is well-defined, that is, it does not depend on the representative of the equivalence class of P. In fact suppose $P = (x_1 : \ldots : x_{n+1}) \in \mathbb{P}^{n+1}(\mathbb{C})$ and let $\lambda \in \mathbb{C} \setminus \{0\}$, so that $P = (\lambda x_1 : \ldots : \lambda x_{n+1})$. Then

$$\overline{\lambda P} = (\overline{\lambda x_1} : \ldots : \overline{\lambda x_{n+1}}) = \overline{\lambda}(\overline{x}_1 : \ldots : \overline{x}_{n+1}) = \overline{P}.$$

Lemma 8.7.3. A point $P = (x_1 : \ldots : x_{n+1}) \in \mathbb{P}^{n+1}(\mathbb{C})$ is real if and only if $P = \overline{P}$.

Proof. If P is real, then by definition we can write $P = (y_1 : \ldots : y_{n+1})$

with $y_i \in \mathbb{R}$ for every i, and therefore

$$\overline{P} = (\overline{y}_1 : \ldots : \overline{y}_{n+1}) = (y_1 : \ldots : y_{n+1}) = P.$$

Conversely, suppose that $P = \overline{P}$. Let $i \in \{1, \ldots, n+1\}$ be such that $x_i \neq 0$. Then

$$P = (x_i^{-1}x_1 : x_i^{-1}x_2 : \ldots : x_i^{-1}x_{i-1} : 1 : x_i^{-1}x_{i+1} : \ldots : x_i^{-1}x_{n+1})$$

and

$$\overline{P} = (\overline{x}_i^{-1}\overline{x}_1 : \overline{x}_i^{-1}\overline{x}_2 : \ldots : \overline{x}_i^{-1}\overline{x}_{i-1} : 1 : \overline{x}_i^{-1}\overline{x}_{i+1} : \ldots : \overline{x}_i^{-1}\overline{x}_{n+1}).$$

Since these points are equal, by definition there exists $\lambda \in \mathbb{C}$ such that

$$\lambda(x_i^{-1}x_1, x_i^{-1}x_2, \ldots, x_i^{-1}x_{i-1}, 1, x_i^{-1}x_{i+1}, \ldots, x_i^{-1}x_{n+1}) = \overline{P} =$$

$$= (\overline{x}_i^{-1}\overline{x}_1, \overline{x}_i^{-1}\overline{x}_2, \ldots, \overline{x}_i^{-1}\overline{x}_{i-1}, 1, \overline{x}_i^{-1}\overline{x}_{i+1}, \ldots, \overline{x}_i^{-1}\overline{x}_{n+1}).$$

The i-th entry of the left hand side is λ, while the i-th entry of the right hand side is 1. Therefore $\lambda = 1$, and $x_i^{-1}x_j = \overline{x_i}^{-1}\overline{x}_j$ for every j. This means that $x_i^{-1}x_j \in \mathbb{R}$ for every $j \in \{1, \ldots, n\}$, and hence P is real. □

Definition 8.7.4. Let $L \subseteq \mathbb{P}^n(\mathbb{C})$ be a linear subspace of dimension m, defined by the kernel of an $(n-m) \times (n+1)$ matrix A of rank $n-m$. We say that L is *real* if

$$\ker A = \ker \overline{A},$$

where $\overline{A}$ is the matrix whose entries are the conjugates of the entries of A. If L is not real, then we say that it is *imaginary*.

The *conjugate* of L is the linear subspace defined by $\ker \overline{A}$.

Equivalently, real subspaces can be characterized by the property explained by the following lemma.

Lemma 8.7.5. Let $L \subseteq \mathbb{P}^n(K)$ be defined by a matrix A. Then L is real if and only if for every $P \in \mathbb{P}^n(K)$ we have

$$P \in L \iff \overline{P} \in L.$$

Proof. First suppose that L is real and let $P = (x_1 : \ldots : x_{n+1}) \in$

$\mathbb{P}^n(K)$. Then $P \in L$ if and only if $A \begin{pmatrix} x_1 \\ \dots \\ x_{n+1} \end{pmatrix} = \underline{0}$, i.e. if and only if $(x_1, \dots, x_{n+1}) \in \ker A$. Since L is real then $\ker A = \ker \overline{A}$, so this last condition is equivalent to $(x_1, \dots, x_{n+1}) \in \ker \overline{A}$. Taking conjugates, this becomes equivalent to $\overline{P} \in L$.

Conversely, suppose that $P \in L$ if and only if $\overline{P} \in L$. Suppose that $(x_1, \dots, x_{n+1}) \in \ker A$. Then $(x_1 : \dots : x_{n+1}) \in L$, and hence $(\overline{x}_1 : \dots : \overline{x}_{n+1}) \in L$. This implies that $(\overline{x}_1, \dots, \overline{x}_{n+1}) \in \ker A$, and taking conjugates $(\overline{x}_1 : \dots : \overline{x}_{n+1}) \in \ker \overline{A}$. Therefore $\ker A \subseteq \ker \overline{A}$. The symmetric argument shows that $\ker \overline{A} \subseteq \ker A$. □

Proposition 8.7.6. In $\mathbb{P}^2(\mathbb{C})$, the following hold true.

1. A line $\ell\colon ax + by + cz = 0$ is real if and only if $(a : b : c)$ is a real point of $\mathbb{P}^2(\mathbb{C})$.
2. A line through two imaginary conjugate points is real.
3. If P is imaginary, there exists a unique real line ℓ with $P \in \ell$.
4. If ℓ is an imaginary line, then $\ell \cap \overline{\ell}$ is a single real point.
5. If ℓ is an imaginary line, then ℓ contains precisely one real point.

Proof. 1. ℓ is defined by $\ker A$, with $A = \begin{pmatrix} a & b & c \end{pmatrix}$.

If $(a : b : c)$ is a real point of $\mathbb{P}^2(\mathbb{C})$, then $\lambda a, \lambda b, \lambda c \in \mathbb{R}$ for some non-zero $\lambda \in \mathbb{C}$. Clearly $\ker A = \ker(\lambda A)$, where $\lambda A = \begin{pmatrix} \lambda a & \lambda b & \lambda c \end{pmatrix}$. Taking conjugates, $\ker \overline{A} = \ker(\overline{\lambda A})$, but λA is a real matrix, and hence the latter is $\ker \lambda A$. It follows that $\ker A = \ker \overline{A}$, so that ℓ is real.

Conversely, suppose that $\ker A = \ker \overline{A}$. Without loss of generality, suppose that $a \neq 0$, so that another equation for ℓ is $x + b'y + c'z = 0$. Assume by contradiction that $(a : b : c)$ is an imaginary point: then at least one between b' and c' is not real. Suppose it is b'. Then $(-b', 1, 0) \in \ker A$, and since $\ker A = \ker \overline{A}$ we must have $(-b', 1, 0) \in \ker \overline{A}$. But

$\overline{A} = \begin{pmatrix} 1 & \overline{b'} & \overline{c'} \end{pmatrix}$ and hence

$$\overline{A} \begin{pmatrix} -b' \\ 1 \\ 0 \end{pmatrix} = -b' + \overline{b'},$$

which is not 0 since b' is not real. This contradicts the fact that $\ker A = \ker \overline{A}$, and hence $(a : b : c)$ must be real.

2. Let $P = (x_1 : x_2 : x_3) \in \mathbb{P}^2(\mathbb{C})$ be an imaginary point, and let $\overline{P}$ be its conjugate. Let $\ell \colon ax + by + cz = 0$ be a line through P and $\overline{P}$. Then

$$\begin{cases} ax_1 + bx_2 + cx_3 = 0 \\ a\overline{x}_1 + b\overline{x}_2 + c\overline{x}_3 = 0 \end{cases}.$$

Taking conjugates we get that

$$\begin{cases} \overline{a}x_1 + \overline{b}x_2 + \overline{c}x_3 = 0 \\ \overline{a}\overline{x}_1 + \overline{b}\overline{x}_2 + \overline{c}\overline{x}_3 = 0 \end{cases}$$

and therefore $\overline{\ell}$ also passes through P and $\overline{P}$. However since P is imaginary P and $\overline{P}$ are two distinct points, and there exists a unique line that passes through them. Hence $\ell = \overline{\ell}$.

3. Let ℓ be the line through P and $\overline{P}$. By point 2., ℓ is real, so there exists at least one real line that passes through P. On the other hand, if $\ell' \colon ax+by+cz = 0$ is a real line (with $a, b, c \in \mathbb{R}$) containing the imaginary point $P = (x_1 : x_2 : x_3)$, then $ax_1 + bx_2 + cx_3 = 0$ and taking conjugates we get $a\overline{x}_1 + b\overline{x}_2 + c\overline{x}_3 = 0$. This means that ℓ' passes through $\overline{P}$ as well, and hence it must coincide with ℓ.

4. Let $\ell \colon ax + by + cz$ be an imaginary line, so that $\ell \neq \overline{\ell}$. If $P = (x_1 : x_2 : x_3) \in \mathbb{P}^2(\mathbb{C})$ belongs to $\ell \cap \overline{\ell}$ then

$$\begin{cases} ax_1 + bx_2 + cx_3 = 0 \\ \overline{a}x_1 + \overline{b}x_2 + \overline{c}x_3 = 0 \end{cases}$$

and taking conjugates we get

$$\begin{cases} \overline{a}\overline{x}_1 + \overline{b}\overline{x}_2 + \overline{c}\overline{x}_3 = 0 \\ a\overline{x}_1 + b\overline{x}_2 + c\overline{x}_3 = 0 \end{cases},$$

showing that $\overline{P} \in \ell \cap \overline{\ell}$. But since $\ell \neq \overline{\ell}$ the intersection point is unique, and so $P = \overline{P}$.

5. If $P \in \ell$ is real, then $P \in \overline{\ell}$, but $\ell \cap \overline{\ell}$ contains a unique real point by 3. □

The proof of the next proposition is very similar to that of Proposition 8.7.6. We omit it, but encourage the interested reader in writing it down themselves.

Proposition 8.7.7. In $\mathbb{P}^3(\mathbb{C})$, the following hold true.

1. A plane $ax + by + cz + dt = 0$ is real if and only if $(a : b : c : d)$ is a real point of $\mathbb{P}^3(\mathbb{C})$.
2. If $P \in \mathbb{P}^3(\mathbb{C})$ is imaginary, the line through P and $\overline{P}$ is real.
3. If $P \in \mathbb{P}^3(\mathbb{C})$ is imaginary, there exists a unique real line through P.
4. If a real line or a real plane contain an imaginary point, then they contain the conjugate as well.
5. Two imaginary conjugate planes intersect in a real line.
6. An imaginary plane contains a unique real line.
7. An imaginary line contains at most one real point and there exists at most one real plane containing it.

Chapter 9: Conics

9.1 Algebraic curves, intersection multiplicities and tangents

We denote by $\mathbb{C}[x,y,z]$ the set of polynomials in 3 variables over the complex field. That is, elements of $\mathbb{C}[x,y,z]$ are expressions of the form

$$\sum_{i,j,k=1}^{n} a_{ijk}x^i y^j z^k.$$

The *degree* of a term $a_{ijk}x^i y^j z^k$ is $i+j+k$.

Definition 9.1.1. A polynomial $f \in \mathbb{C}[x,y,z]$ is called *homogeneous of degree d* if there exists a non-negative integer d such that every term of f has degree d. That is, f is homogeneous of degree d if it has the form

$$\sum_{i+j+k=d} a_{ijk}x^i y^j z^k.$$

Example 9.1.2.

- Homogeneous polynomials of degree 0 are constant polynomials.
- The polynomial $x^2 + 3xz - iz^2$ is homogeneous of degree 2.
- The polynomial $x^4 + zy^3 + z^2 + y^4$ is not homogeneous.
- The polynomial $2x^5 + x^3yz - 4y^4z + 6z^4x + iz^3y^2$ is homogeneous of degree 5.

Definition 9.1.3. An *algebraic plane curve of degree d* is a set of the form

$$\{(x:y:z) \in \mathbb{P}^2(\mathbb{C}) \colon f(x,y,z) = 0\},$$

where $f \in \mathbb{C}[x,y,z]$ is a non-zero homogeneous polynomial of degree d.

Since all of our curves will be contained in $\mathbb{P}^2(\mathbb{C})$, we will drop the adjective "plane".

Note:-

The definition of algebraic curve makes sense only because f is homogeneous. In fact, if $(x_1 : x_2 : x_3)$ is such that $f(x_1, x_2, x_3) = 0$, with f homogeneous of the form $\sum_{i+j+k=d} a_{ijk} x^i y^j z^k$, then for every $\lambda \in \mathbb{C}$ we have

$$f(\lambda x_1, \lambda x_2, \lambda x_3) = \sum_{i+j+k=d} a_{ijk} (\lambda x_1)^i (\lambda x_2)^j (\lambda x_3)^k =$$

$$= \sum_{i+j+k=d} \lambda^{i+j+k} a_{ijk} x_1^i x_2^j x_3^k = \lambda^d \sum_{i+j+k=d} a_{ijk} x_1^i x_2^j x_3^k = \lambda^d f(x_1, x_2, x_3) = 0.$$

Example 9.1.4. A line in $\mathbb{P}^2(\mathbb{C})$ is defined by an equation of the form $ax + by + cz = 0$. Therefore, a line is an algebraic curve of degree 1.

Definition 9.1.5. An algebraic curve $\mathcal{C}\colon f(x, y, z) = 0$ of degree d is *reducible* if there exist homogeneous polynomials $g, h \in \mathbb{C}[x, y, z]$, each of degree > 0, such that $f = gh$. If $\mathcal{C}$ is not reducible, then it is called *irreducible*.

Example 9.1.6.

- If f, g are homogeneous polynomials, of degree d, e, respectively, then gh is a homogeneous polynomial of degree $d + e$. Hence since lines have degree 1, they are also irreducible.
- The curve $x^2 + xy + xz + yz = 0$ is reducible, because
$$x^2 + xy + xz + yz = (x + y)(x + z).$$
- The curve $x^2 + y^2 = 0$ is reducible, since $x^2 + y^2 = (x + iy)(x - iy)$.
- The curve $x^2 + y^2 + z^2 = 0$ is irreducible.

Let $\mathcal{C}\colon f(x, y, z) = 0$ be an algebraic curve of degree d, and write $f = \sum_{i+j+k=d} a_{ijk} x^i y^j z^k$. Let $P = (x_0 : y_0 : z_0) \in \mathbb{P}^2(\mathbb{C})$ be a point of $\mathcal{C}$, so that $f(x_0, y_0, z_0) = 0$ and let $\ell\colon ax + by + cz = 0$ be a line through P. Since $(a, b, c) \neq (0, 0, 0)$ we can assume without loss of generality that $c \neq 0$, and rewrite ℓ as $z = \alpha x + \beta y$, where $\alpha = -a/c$ and $\beta = -b/c$, so that $z_0 = \alpha x_0 + \beta y_0$.

The equation

$$f(x, y, \alpha x + \beta y) = 0$$

certainly has a solution, because $f(x_0, y_0, \alpha x_0 + \beta y_0) = f(x_0, y_0, z_0) = 0$. On the other hand, we have that

$$f(x, y, \alpha x + \beta y) = \sum_{i+j+k=0} a_{ijk} x^i y^j (\alpha x + \beta y)^k.$$

Notice that $(\alpha x + \beta y)^k = \sum_{h=0}^{k} \binom{k}{h} \alpha^h \beta^{k-h} x^h y^{k-h}$ is a homogeneous polynomial of degree k. Hence every term $a_{ijk} x^i y^j (\alpha x + \beta y)^k$ of $f(x, y, \alpha x + \beta y)$ is homogeneous of degree d, and in turn the polynomial $f(x, y, \alpha x + \beta y)$ is homogeneous of degree d as well. Hence we can write

$$f(x, y, \alpha x + \beta y) = \sum_{h=0}^{d} a_h x^h y^{d-h} \tag{39}$$

for some coefficients $a_0, \dots, a_d \in \mathbb{C}$.

Now we need to make an important assumption: the fact that $f(x, y, \alpha x + \beta y)$ is <u>not</u> the zero polynomial.

Remark 9.1.7. The fact that $f(x, y, \alpha x + \beta y) = 0$ is equivalent to saying that every point of ℓ solves the equation $f(x, y, z) = 0$, that is in turn equivalent to saying that $\ell \subseteq \mathcal{C}$. Conversely, if $\ell \subseteq \mathcal{C}$ then of course $f(x, y, \alpha x + \beta y)$ must be the zero polynomial. If one thinks of $f(x, y, z)$ as a polynomial in one variable z with coefficients in the ring $\mathbb{C}[x, y]$ (the concept of ring has not been treated in these notes, but you can think of a ring just as a field where not every element has a multiplicative inverse), the fact that $f(x, y, \alpha x + \beta y) = 0$ implies that the polynomial $z - (\alpha x + \beta y)$ divides $f(x, y, z)$, so that there exists a homogeneous polynomial $h \in \mathbb{C}[x, y, z]$ such that $f(x, y, z) = h(x, y, z)(ax + by + cz)$.

Next, notice that we cannot have $x_0 = y_0 = 0$, as otherwise $z_0 = 0$. Suppose without loss of generality that $y_0 \neq 0$. Since (x_0, y_0) solves the equation $f(x, y, \alpha x + \beta y) = 0$, also $(y_0^{-1} x_0, 1)$ does. Hence we can set $y = 1$ in (39) (that is equivalent to dividing everything by y and then replacing x/y by x), and look at the equation

$$\sum_{h=0}^{d} a_h x^h = 0, \tag{40}$$

of which $y_0^{-1} x_0$ is a solution.

Definition 9.1.8. The multiplicity of $y_0^{-1}x_0$ as a root of (40) is called *intersection multiplicity* of ℓ and $\mathcal{C}$ in P and it is denoted by $m_P(\mathcal{C}, \ell)$.

Note:-

Since Equation (40) has degree d, the intersection multiplicity is at most d. Moreover, it is also at least 1.

The definitoin of intersection multiplicity looks intricate at first, but in fact computing it is rather easy. Let us see some examples.

Example 9.1.9.

- Let $f = x^2+y^2+z^2$ and let $\mathcal{C}\colon f = 0$ be the corresponding algebraic curve. Let $P = (1 : 0 : i) \in \mathcal{C}$ and let $\ell\colon ix + y - z = 0$ be a line through P. First, we rewrite the equation of ℓ as $z = ix + y$. Next, we substitute this into f and we equate to 0, getting

$$f(x, y, ix + y) = x^2 + y^2 + (ix + y)^2 = 2ixy + 2y^2 = 0. \tag{41}$$

  Now we look at which coordinate of P, between the x-coordinate and the y-coordinate, is 0. It is the first one, and therefore we can set $x = 1$ in (41), getting

$$iy + y^2 = 0.$$

  Now this equation has, as a solution, $x_0^{-1}y_0$, where $x_0 = 1$ is the x-coordinate of P and y_0 is the y-coordinate. Notice that $x_0^{-1}y_0 = 0$, so we have to look at 0 as a root of the equation. This clearly has multiplicity 1, and hence $m_P(\mathcal{C}, \ell) = 1$.

- Let $f = x^2+y^2+z^2$ and let $\mathcal{C}\colon f = 0$ be the corresponding algebraic curve. Let $P = (1 : 0 : i) \in \mathcal{C}$ and let $\ell\colon ix - z = 0$ be a line through P. Let us compute the intersection multiplicity of ℓ and $\mathcal{C}$ in P. First, we rewrite the equation of ℓ as $z = ix$. Next, we substitute in the equation of $\mathcal{C}$, getting

$$x^2 + y^2 - x^2 = y^2 = 0. \tag{42}$$

Now we look at which coordinate of P is non-zero. It is clearly the x-coordinate, so we need to look at the root $y = x_0^{-1}y_0 = 0$ of (42). This has multiplicity 2, and hence $m_P(\mathcal{C}, \ell) = 2$.

- Let $f = x^3 - x^2z - y^2z$ and $\mathcal{C}\colon f = 0$ be the corresponding curve. Let $P = (1 : 0 : 1) \in \mathcal{C}$ and let $x - z = 0$ be a line through P. We write ℓ as $z = x$ and substitute, getting:

$$y^2x = 0.$$

The non-zero coordinate of P, between x and y, is the x coordinate, so we set $x = 1$ and look at 0 as a root of $y^2 = 0$. This has multiplicity 2, so $m_P(\mathcal{C}, \ell) = 2$.

Definition 9.1.10. Let $\mathcal{C}$ be an algebraic curve, let $P \in \mathcal{C}$ be a point and ℓ be a line that passes through P. We say that ℓ is a *tangent* in P if $m_P(\mathcal{C}, \ell) \geq 2$.

Referring to 9.1.9, in the first example the line is not tangent, while in the other two it is.

Definition 9.1.11. Let $\mathcal{C}$ be an algebraic curve. A point $P \in \mathcal{C}$ is called *smooth* or *non-singular* if there exists a unique tangent in P. If P is not smooth, then it is *singular*.

Example 9.1.12.

- Consider the curve $x^3 - x^2z - y^2z = 0$ and the point $P = (0 : 0 : 1)$. Let $m \in \mathbb{C}$ and consider the line $y = mx$ through P. Substituting in the equation of the curve, we get

$$x^3 - x^2z - m^2x^2z = 0.$$

The non-zero coordinate of P is the third one, so to understand $m_P(\mathcal{C}, \ell)$ we need to look at $x = 0$ as a solution of

$$x^3 - x^2 - m^2x^2 = x^3 - (1 + m^2)x^2 = 0.$$

This has multiplicity at least 2 for every m, so every line through P of the form $y = mx$ is a tangent. Hence P is singular.

- Consider the curve $x^3 - xz^2 - y^2z = 0$ and the point $P = (0 : 0 : 1)$. Let $m \in \mathbb{C}$ and consider a line $y = mx$ through P. We get

$$x^3 - xz^2 - m^2x^2z = 0,$$

and since the z-coordinate of P is non-zero, we need to look at 0 as a root of

$$x^3 - m^2x^2 - x = 0.$$

This has multiplicity 1 for every m, so no line of the form $y = mx$ is a tangent in P.

The only other line through P is $x = 0$. Substituting, we get

$$y^2z = 0,$$

and we get to look at the multiplicity of $y = 0$ as a root of $y^2 = 0$. This has multiplicity 2, and hence $x = 0$ is a tangent in P.

Theorem 9.1.13. Let $\mathcal{C}\colon f(x, y, z) = 0$ be an algebraic curve and let $P = (x_0 : y_0 : z_0) \in \mathcal{C}$. Then P is singular if and only if the following relations hold true:

$$\begin{cases} f(x_0, y_0, z_0) = 0 \\ \frac{\partial f}{\partial x}(x_0, y_0, z_0) = 0 \\ \frac{\partial f}{\partial y}(x_0, y_0, z_0) = 0 \\ \frac{\partial f}{\partial z}(x_0, y_0, z_0) = 0 \end{cases}.$$

As a corollary of Theorem 9.1.13, one gets the following fundamental fact.

Corollary 9.1.14. Let $\mathcal{C}\colon f(x, y, z) = 0$ be an algebraic curve and let $P = (x_0 : y_0 : z_0) \in \mathcal{C}$ be a singular point. Then for every line ℓ through P we have $m_P(\mathcal{C}, \ell) \geq 2$.

Theorem 9.1.15. Let $\mathcal{C}\colon f(x, y, z) = 0$ be an algebraic curve and let $P = (x_0 : y_0 : z_0) \in \mathcal{C}$. If P is smooth, then the tangent line in P is given by

the equation

$$\frac{\partial f}{\partial x}(x_0, y_0, z_0)x + \frac{\partial f}{\partial y}(x_0, y_0, z_0)y + \frac{\partial f}{\partial z}(x_0, y_0, z_0)z = 0.$$

We close the section with a theorem that explains, in a precise sense, "how many" intersections does an algebraic curve of degree d have with a line.

Theorem 9.1.16. Let $\mathcal{C}\colon f(x, y, z) = 0$ be an algebraic curve of degree d and $\ell\colon ax + by + cz = 0$ be a line. Assume that $\ell \not\subseteq \mathcal{C}$. Then:

$$\sum_{P \in \mathcal{C} \cap \ell} m_P(\mathcal{C}, \ell) = d.$$

Proof. Write $f(x, y, z) = \sum_{i+j+k=d} a_{ijk} x^i y^j z^k$. Intersecting $\mathcal{C}$ and ℓ means studying the system

$$\begin{cases} \sum_{i+j+k=d} a_{ijk} x^i y^j z^k = 0 \\ ax + by + cz = 0 \end{cases}. \tag{43}$$

Since $(a, b, c) \neq (0, 0, 0)$ we can assume without loss of generality that $c \neq 0$, and rewrite ℓ as $z = \alpha x + \beta y$, where $\alpha = -a/c$ and $\beta = -b/c$. Substituting in (43), we get

$$f(x, y, \alpha x + \beta y) = 0.$$

The polynomial $f(x, y, \alpha x + \beta y)$ cannot be the 0 polynomial, as otherwise we would have $\ell \subseteq \mathcal{C}$, violating the hypotheses. Then, as we have already noted in (39), the polynomial $f(x, y, \alpha x + \beta y)$ is homogeneous of degree d, and hence we can write

$$f(x, y, \alpha x + \beta y) = \sum_{h=0}^{d} a_h x^h y^{d-h}$$

for some coefficients $a_0, \ldots, a_d \in \mathbb{C}$.

We know that in order to find the multiplicity of intersection at a point $(x_0 : y_0 : z_0) \in \mathcal{C} \cap \ell$, we need to compute the multiplicity of (x_0, y_0) as a root of

$$\sum_{h=0}^{d} a_h x^h y^{d-h} = 0. \tag{44}$$

Therefore the theorem is proved if we can show that equation (44) has exactly d solutions, when counted with multiplicity.

Suppose that (x_0, y_0) is a solution of (44). We can assume that $(x_0, y_0) \neq (0,0)$ because if $x_0 = 0 = y_0$ then $z = \alpha x_0 + \beta y_0 = 0$, which does not define a point of $\mathbb{P}^2(\mathbb{C})$. Now suppose that $y_0 \neq 0$. Then $(x_0 y_0^{-1}, 1)$ is also a solution of (44). On the other hand, if $(x_0, 0)$ is a solution than also $(1,0)$ is. Since proportional pairs (x_0, y_0) and $(\lambda x_0, \lambda y_0)$ give rise to the same point $P = (x_0 : y_0 : \alpha x_0 + \beta y_0)$, we can just count solution of (44) of the form $(x_0, 1)$ or $(1,0)$. Now, if $\sum_{h=0}^{d} a_h x^h y^{d-h} = a_d y^d$ then we are done, since $(1,0)$ is the unique root and it has multiplicity d. Otherwise, there is a unique $e \geq 0$ such that

$$\sum_{h=0}^{d} a_h x^h y^{d-h} = y^e \left(\sum_{h=0}^{d} a_h x^h y^{d-h-e} \right)$$

with $a_{d-e} \neq 0$. Then $(1,0)$ is a root with multiplicity e, and the equation

$$\sum_{h=0}^{d} a_h x^h y^{d-h-e} = 0$$

has precisely $d-e$ roots of the form $(x_0, 1)$, when counted with multiplicity. All in all, we have $e + d - e = d$ roots. □

9.2 Conics

Definition 9.2.1. A *conic* is a plane algebraic curve of degree 2.

Equivalently, a conic is a plane algebraic curve given by an equation of the form

$$\mathcal{C}\colon a_{11}x^2 + 2a_{12}xy + 2a_{13}xz + a_{22}y^2 + 2a_{23}yz + a_{33}z^2 = 0,$$

where $a_{ij} \in \mathbb{C}$ are not all zero.

There is a convenient way to rewrite the above equation. Namely, a conic is the set of points $(x_0 : y_0 : z_0) \in \mathbb{P}^2(\mathbb{C})$ that satisfy

$$\begin{pmatrix} x_0 & y_0 & z_0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = 0.$$

The matrix $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}$ is the matrix *associated to the conic* $\mathcal{C}$.

Setting $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ we can write the equation of $\mathcal{C}$ as:

$$^tXAX = 0.$$

Definition 9.2.2. Let $\mathcal{C}$ be a conic. We say that $\mathcal{C}$ is:

1. *generic* if it has no singular points;
2. *simply degenerate* if it has exactly one singular point;
3. *doubly degenerate* if all of its points are singular.

Theorem 9.2.3. Let $\mathcal{C}\colon {}^tAX = 0$ be a conic. Then $\mathcal{C}$ is:

1. *generic* if $\det A \neq 0$ or, equivalently, if $\mathrm{rk}(A) = 3$;
2. *simply degenerate* if $\mathrm{rk}(A) = 2$;
3. *doubly degenerate* if $\mathrm{rk}(A) = 1$.

Proof. Let

$$f = a_{11}x^2 + 2a_{12}xy + 2a_{13}xz + a_{22}y^2 + 2a_{23}yz + a_{33}z^2$$

be the equation of $\mathcal{C}$. By Theorem 9.1.13, a point $(x_0 : y_0 : z_0) \in \mathcal{C}$ is

singular if and only if:

$$\begin{cases} \frac{\partial f}{\partial x}(x_0, y_0, z_0) = 0 \\ \frac{\partial f}{\partial y}(x_0, y_0, z_0) = 0 \\ \frac{\partial f}{\partial z}(x_0, y_0, z_0) = 0 \end{cases}.$$

Now notice that:

$$\begin{cases} \frac{\partial f}{\partial x} = 2a_{11}x + 2a_{12}y + 2a_{13}z \\ \frac{\partial f}{\partial y} = 2a_{12}x + 2a_{22}y + 2a_{23}z \\ \frac{\partial f}{\partial z} = 2a_{13}x + 2a_{23}y + 2a_{33}z \end{cases}$$

So that $(x_0 : y_0 : z_0) \in \mathcal{C}$ is singular if and only if

$$A \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = 0.$$

Namely, in order to find singular points we need to solve the homogenous linear system

$$AX = 0. \tag{45}$$

Notice that any non-zero solution of (45) automatically yields a point of the conic, since if $AX = 0$ then clearly ${}^tXAX = 0$.

If $\det A \neq 0$, then by Theorem 3.1.5, system (45) only has the trivial solution $X = \underline{0}$. But this does not define a point of $\mathbb{P}^2(\mathbb{C})$, and therefore $\mathcal{C}$ has no singular points.

If $\mathrm{rk}(A) = 2$, the solutions of system (45) form a 1-dimensional $\mathbb{C}$-vector space, generated by a non-zero vector $(x_0, y_0, z_0) \in \mathbb{C}^3$. This means that $(x_0 : y_0 : z_0)$ is the unique singular point of the conic, and hence $\mathcal{C}$ is simply degenerate.

If $\mathrm{rk}(A) = 1$, the solutions of system (45) form a 2-dimensional $\mathbb{C}$-vector space. This gives rise, in $\mathbb{P}^2(\mathbb{C})$, to a line ℓ made entirely of singular points. The line ℓ is entirely contained in $\mathcal{C}$. We claim that the converse is also true, namely, every point of $\mathcal{C}$ belongs to ℓ. In fact, if this was not true then let $P \in \mathcal{C} \setminus \ell$ and let $Q \in \ell$. Now consider the line r through P and Q: its intersection multiplicity with $\mathcal{C}$ at Q is ≥ 2, since Q is singular.

Its intersection multiplicity with $\mathcal{C}$ at P is at least 1. But then

$$\sum_{R \in \mathcal{C} \cap \ell} m_R(\mathcal{C}, r) \geq 2 + 1 = 3,$$

contradicting Theorem 9.1.16. Since every point of $\mathcal{C}$ is a point of ℓ, and points of ℓ are all singular, $\mathcal{C}$ is doubly degenerate. □

Next, we see what it means geometrically to be generic, simply degenerate and doubly degenerate.

Lemma 9.2.4. Let $\mathcal{C}\colon f(x, y, z) = 0$ be a conic.

1. $\mathcal{C}$ is generic if and only if it is irreducible.
2. $\mathcal{C}$ is simply degenerate if and only if there exist two distinct lines $\ell\colon ax + by + cz = 0$, $\ell'\colon a'x + b'y + c'z = 0$ such that
$$f(x, y, z) = (ax + by + cz)(a'x + b'y + c'z).$$
3. $\mathcal{C}$ is doubly degenerate if and only if there exists a line $\ell\colon ax + by + cz = 0$ such that $f(x, y, z) = (ax + by + cz)^2$.

Proof. 1. First, let $\mathcal{C}$ be irreducible. By contradiction, assume that it is not generic. Then it has (at least) a singular point $P \in \mathcal{C}$. Now let Q be another point of $\mathcal{C}$. Let $\ell\colon ax + by + cz = 0$ be the line through P and Q. If $\ell \not\subseteq \mathcal{C}$, then by Theorem 9.1.16 we have

$$\sum_{R \in \ell \cap \mathcal{C}} m_R(\mathcal{C}, \ell) = 2, \tag{46}$$

but $m_P(\mathcal{C}, \ell) \geq 2$ since P is singular and $m_Q(\mathcal{C}, \ell) \geq 1$, and this contradicts (46). Therefore we must have $\ell \subseteq \mathcal{C}$, and by Remark 9.1.7 this implies that $f(x, y, z) = (ax + by + cz)h(x, y, z)$, so that $\mathcal{C}$ is reducible, contradicting our assumption. Hence $\mathcal{C}$ is generic.

Conversely, let $\mathcal{C}$ be generic. By contradiction, assume that it is reducible. Then there are lines $\ell\colon ax+by+cz = 0$ and $\ell'\colon a'x+b'y+c'z = 0$ such that

$$f(x, y, z) = (ax + by + cz)(a'x + b'y + c'z). \tag{47}$$

Now let $P = (x_0 : y_0 : z_0) \in \ell \cap \ell'$. Assume without loss of generality that

$x_0 \neq 0$ and consider the line $r\colon z_0x - x_0z = 0$ through P. We claim that $m_P(\mathcal{C}, r) \geq 2$. To compute the multiplicity, write r as $z = \frac{z_0}{x_0}x$, substitute in (47) and equate to 0, getting:

$$((ax_0 + cz_0)x + bx_0y)((a'x_0 + c'z_0)x + b'x_0y) = 0.$$

Since $x_0 \neq 0$, in order to find the intersection multiplicity we have to solve

$$((ax_0 + cz_0) + bx_0y)((a'x_0 + c'z_0) + b'x_0y) = 0.$$

But both factors have $x_0^{-1}y_0$ as a root, and hence $m_P(\mathcal{C}, r) \geq 2$. On the other hand, one can repeat the same argument with the line $r'\colon x_0y - y_0x = 0$, finding that $m_P(\mathcal{C}, r') \geq 2$. Hence there are at least two tangent lines in P; in other words, P is singular. This contradicts the fact that $\mathcal{C}$ is generic.

2. We have proved in 1. that if $\mathcal{C}$ decomposes as the product of two lines, the intersection point is singular. Hence if $f(x, y, z) = (ax + by + cz)(a'x + b'y + c'z)$ with $ax + by + cz = 0$ and $a'x + b'y + c'z = 0$ distinct lines, their unique intersection point P is singular. On the other hand, no other point Q can be singular, as otherwise if ℓ is the line through P, Q then $m_p(\mathcal{C}, \ell) + m_Q(\mathcal{C}, \ell) \geq 3$, contradicting Theorem 9.1.16. Conversely, suppose that $\mathcal{C}$ is simply degenerate. Then by 1. it must be reducible, and since $\deg f = 2$, we can only have $f(x, y, z) = g(x, y, z)h(x, y, z)$ with g, h homogeneous polynomials of degree 1. If $g = 0$ and $h = 0$ define the same line, then any point on such line is singular, but then every point of $\mathcal{C}$ would be singular. Hence $g = 0$ and $h = 0$ must define distinct lines.

3. If $f = (ax + by + cz)^2$, then every point of $\mathcal{C}$ is singular, and so $\mathcal{C}$ is doubly degenerate. Conversely, if $\mathcal{C}$ is doubly degenerate then it is reducible, and we showed in 2. that if it decomposes as the product of two distinct lines then there is a unique singular point. Then it must decompose as the square of a line. □

The next lemma shows how to compute tangent lines in smooth points of conics.

Lemma 9.2.5. Let $\mathcal{C}\colon {}^tXAX = 0$ be a conic, where $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \in$

$M_3(\mathbb{C})$. Let $P = (x_P : y_P : z_P) \in \mathcal{C}$ be a smooth point. Then the unique tangent in P is the line

$$\begin{pmatrix} x_P & y_P & z_P \end{pmatrix} A \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0.$$

Proof. By Theorem 9.1.15, the tangent line in P is given by the equation

$$\frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial y}(P)y + \frac{\partial f}{\partial z}(P)z = 0,$$

where $f(x, y, z) = a_{11}x^2 + 2a_{12}xy + 2a_{13}xz + a_{22}y^2 + 2a_{23}yz + a_{33}z^2$. Hence we just need to verify that this expression coincides with that of the claim. We compute:

$$\frac{\partial f}{\partial x}(P) = 2a_{11}x_P + 2a_{12}y_P + 2a_{13}z_P$$
$$\frac{\partial f}{\partial y}(P) = 2a_{22}y_P + 2a_{12}x_P + 2a_{23}z_P$$
$$\frac{\partial f}{\partial z}(P) = 2a_{33}z_P + 2a_{13}x_P + 2a_{23}y_P$$

so that the equation of the tangent line in P is given by:

$$(a_{11}x_P+a_{12}y_P+a_{13}z_P)x+(a_{22}y_P+a_{12}x_P+a_{23}z_P)y+(a_{33}z_P+a_{13}x_P+a_{23}y_P)z = 0.$$

On the other hand,

$$\begin{pmatrix} x_P & y_P & z_P \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11}x_P + a_{12}y_P + a_{13} & a_{22}y_P + a_{12}x_P + a_{23}z_P & a_{33}z_P + a_{13}x_P + a_{23}y_P \end{pmatrix}$$

so that when we multiply the above matrix by $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ and we equate to 0 we obtain precisely the equation of the tangent line. □

Definition 9.2.6. Let $\mathcal{C}\colon f(x,y,z)=0$ be a conic. The *improper points* of $\mathcal{C}$ are the intersections of $\mathcal{C}$ with the line $z=0$.

If $\mathcal{C}$ is general, an *asymptote* of $\mathcal{C}$ is a proper tangent in an improper point of $\mathcal{C}$.

Remark 9.2.7. To find the improper points of $\mathcal{C}$ one simply needs to solve the equation $f(x,y,0)=0$. By Theorem 9.1.16, a conic either has two distinct improper points or it has a unique improper point with multiplicity 2; in the latter case, the line $z=0$ is tangent in such point.

If $\mathcal{C}$ is general and it has 2 improper points, then these are smooth and $z=0$ is not tangent in either of them, since otherwise we would contradict Theorem 9.1.16. Hence the tangents in the improper points must be proper, and the conic has two asymptotes.

If $\mathcal{C}$ is general and it has only one improper point, then this is smooth and $z=0$ is tangent in such point; it follows that the conic has no asymptotes.

Example 9.2.8.

- Let $\mathcal{C}\colon x^2+2y^2+z^2=0$. To find the improper points, we need to solve $x^2+2y^2=0$. It follows that the two improper points are: $P=(i\sqrt{2}:1:0)$ and $\overline{P}=(-i\sqrt{2}:1:0)$. Since $\mathcal{C}$ is a general conic, there is a unique tangent line in both P and $\overline{P}$. To compute these tangents, we use Lemma 9.2.5. The tangent in P is given by:

$$\begin{pmatrix} i\sqrt{2} & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0,$$

that is,

$$i\sqrt{2}x + 2y = 0.$$

Similarly, the line

$$-i\sqrt{2}x + 2y = 0$$

is the tangent in $\overline{P}$. Since these lines are proper, they are the asymptotes of $\mathcal{C}$.

- Let $\mathcal{C}\colon x^2+4xy+4y^2-2xz+z^2 = 0$. To find the improper points, we need to solve $x^2+4xy+4y^2 = 0$. This is equivalent to $(x+2y)^2 = 0$, so this conic has a unique improper point that is $P = (2 : -1 : 0)$. Its tangent line has equation:

$$\begin{pmatrix} 2 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & -1 \\ 2 & 4 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0,$$

that is just $z = 0$. This means that the tangent line in P is improper, and hence it is not an asymptote.

9.3 Real conics

Definition 9.3.1. A *real conic* is a conic $\mathcal{C}$ which has a defining equation $f(x, y, z) = 0$ with $f(x, y, z) \in \mathbb{R}[x, y, z]$.

The conic $\mathcal{C}$ is called:

1. An *ellipse* if it has two imaginary conjugate improper points;
2. A *hyperbola* if it has two real distinct improper points;
3. A *parabola* if it has one real improper point with multiplicity 2.

By Remark 9.2.7, ellipses and hyperbolas have two asymptotes, while parabolas have no asymptotes.

Theorem 9.3.2. Let $\mathcal{C}\colon {}^tXAX = 0$ be a real general conic, where

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \in M_3(\mathbb{R}).$$

Let

$$\widetilde{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}.$$

Then $\mathcal{C}$ is:

1. an ellipse if $\det \widetilde{A} > 0$;
2. a hyperbola if $\det \widetilde{A} < 0$;
3. a parabola if $\det \widetilde{A} = 0$.

Proof. In order to find improper points of $\mathcal{C}$ we need to solve

$$\begin{pmatrix} x & y & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \begin{pmatrix} x \\ y \\ 0 \end{pmatrix} = 0,$$

that is,

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 = 0. \tag{48}$$

Now we need to consider three cases. First, if $a_{11} = a_{22} = 0$ then it must be $a_{12} \neq 0$, because if it was also $a_{12} = 0$ then the first two rows of A would be linearly dependent, so that $\mathrm{rk}(A) < 3$ and A would not be general. Then the equation becomes $xy = 0$, so the conic has two improper points $(1 : 0 : 0)$ and $(0 : 1 : 0)$, hence it is a hyperbola and $\det \widetilde{A} = -a_{12}^2 < 0$, as required.

Next, if $a_{11} \neq 0$ then $y = 0$ does not yield a solution of (48). Hence we can assume that $y = 1$ and look at the equation

$$a_{11}x^2 + 2a_{12}x + a_{22} = 0,$$

that has two real solutions precisely when $\Delta = a_{12}^2 - a_{11}a_{22} > 0$, it has one solution with multiplicity two when $a_{12}^2 - a_{11}a_{22} = 0$ and has two imaginary conjugate solutions when $a_{12}^2 - a_{11}a_{22} < 0$. Since $a_{12}^2 - a_{11}a_{22} = -\det \widetilde{A}$, we are done.

Finally, if $a_{22} \neq 0$ then $x = 0$ does not yield any solution of (48), so we can just set $x = 1$ and reason like in the previous case. □

Definition 9.3.3. Let $\mathcal{C} \colon {}^tXAX = 0$ be a real general conic, where

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \in M_3(\mathbb{R}).$$

Let $P = (x_P : y_P : z_P) \in \mathbb{P}^2(\mathbb{C})$ be any point. A point $Q = (x_Q : y_Q : z_Q) \in \mathbb{P}^2(\mathbb{C})$ is said to be *conjugate* to P with respect to $\mathcal{C}$ if

$$\begin{pmatrix} x_P & y_P & z_P \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \begin{pmatrix} x_Q \\ y_Q \\ z_Q \end{pmatrix} = 0.$$

We write the above equation as ${}^tPAQ = 0$, with a slight abuse of notation.

Remark 9.3.4. Notice that P is conjugate to Q with respect to $\mathcal{C}$ if and only if Q is conjugate to P with respect to P. In fact,

$${}^tPAQ = 0 \iff {}^t({}^tPAQ) = 0 \iff {}^tQ{}^tAP = 0 \iff {}^tQAP = 0,$$

using the fact that ${}^tA = A$.

Definition 9.3.5. Let $\mathcal{C}$ be a real general conic and let $P \in \mathbb{P}^2(\mathbb{C})$. The set of points of $\mathbb{P}^2(\mathbb{C})$ that are conjugate to P with respect to $\mathcal{C}$ is called the *polar* of P with respect to $\mathcal{C}$.

Proposition 9.3.6. Let $\mathcal{C}\colon {}^tXAX = 0$ be a real general conic.

1. Let $P \in \mathbb{P}^2(\mathbb{C})$. Then the polar of P with respect to $\mathcal{C}$ is a line.
2. Let $P, Q \in \mathbb{P}^2(\mathbb{C})$ be such that $P \neq Q$, and let ℓ_P, ℓ_Q be the polar of P, Q with respect to $\mathcal{C}$, respectively. Then $\ell_P \neq \ell_Q$.

Proof. 1. The polar is the set of points that solve the equation

$$\begin{pmatrix} x_P & y_P & z_P \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0,$$

where $P = (x_P : y_P : z_P)$. This clearly defines a line unless

$$\begin{pmatrix} x_P & y_P & z_P \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} = 0,$$

namely unless ${}^tPA = 0$. Transposing and using the fact that A is symmetric, the latter condition is equivalent to $AP = 0$. Since the vector of the coordinates of P cannot be the zero vector because $(0 : 0 : 0)$ is not a point of the projective plane, in order for this to happen we need $\ker A$ to be non-zero, but this happens precisely when $\det A = 0$, namely when A is not general.

2. Let $P = (x_P : y_P : z_P)$ and $Q = (x_Q : y_Q : z_Q)$. Since $P \neq Q$ as points of $\mathbb{P}^2(\mathbb{C})$, the vectors (x_P, y_P, z_P) and (x_Q, y_Q, z_Q) are not linearly dependent in $\mathbb{C}^3$. Suppose by contradiction that $\ell_P = \ell_Q$. Then AP and AQ are proportional vectors, i.e. there exists $\lambda \in \mathbb{C}$ such that $AP = \lambda AQ$ and hence $AP = A(\lambda Q)$, that implies

$$A(P - \lambda Q) = 0.$$

In other words, $P - \lambda Q \in \ker A$. But $\ker A = \{\underline{0}\}$ since $\mathcal{C}$ is general, and hence $P = \lambda Q$, contradicting the hypothesis. □

Definition 9.3.7. Let $\mathcal{C}$ be a real general conic and let $\ell \subseteq \mathbb{P}^2(\mathbb{C})$ be a line. We say that a point $P \in \mathbb{P}^2(\mathbb{C})$ is a *pole* of ℓ if the polar of P with respect to $\mathcal{C}$ is ℓ.

Proposition 9.3.8. Let $\mathcal{C}$ be a real general conic and let $\ell \subseteq \mathbb{P}^2(\mathbb{C})$ be a line. Then ℓ has a unique pole.

Proof. Let $\ell\colon ax+by+cz=0$ and let $A = \begin{pmatrix} x_P & y_P & z_P \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}$ be the matrix associated to $\mathcal{C}$. Then a point $P = (x_P : y_P : z_P) \in \mathbb{P}^2(\mathbb{C})$ is a pole of ℓ if and only if $\begin{pmatrix} x_P & y_P & z_P \end{pmatrix} A$ is proportional to $\begin{pmatrix} a & b & c \end{pmatrix}$ or, equivalently (transposing), if $A \begin{pmatrix} x_P \\ y_P \\ z_P \end{pmatrix}$ is proportional to $B = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$. Now the linear system $AX = B$ has exactly one solution by Theorem 3.1.5, because being $\mathcal{C}$ general the matrix A has non-zero determinant. It follows that ℓ has a pole P. Such pole is unique because of Proposition 9.3.6: if Q was another pole for ℓ then P and Q would be distinct points with the same polar. □

Therefore we have proven that given a general real conic $\mathcal{C}$, the polar of every point $P \in \mathbb{P}^2(\mathbb{C})$ with respect to $\mathcal{C}$ is a line and every line has a unique pole in $\mathbb{P}^2(\mathbb{C})$.

Theorem 9.3.9 (Reciprocity principle)**.** Let $\mathcal{C}$ be a general real conic, let $P \in \mathbb{P}^2(\mathbb{C})$ and let p be the polar of P with respect to $\mathcal{C}$.

1. If $Q \in p$, the polar of Q with respect to $\mathcal{C}$ passes through P.
2. If ℓ is a line containing P, its pole belongs to p.

Proof. Let $\mathcal{C}$ have equation ${}^tXAX = 0$.

1. Since p is the set of points that are conjugate to P with respect to $\mathcal{C}$, if $Q \in p$ then we have ${}^tPAQ = 0$. Transposing and using the fact

that A is symmetric, we get ${}^tQAP = 0$, so that P is conjugate to Q with respect to $\mathcal{C}$. But this means precisely that P belongs to the polar of Q with respect to $\mathcal{C}$.

2. Let Q be the pole of ℓ. This means that ℓ is the set of points of $\mathbb{P}^2(\mathbb{C})$ that are conjugate to Q with respect to $\mathcal{C}$. Since $P \in \ell$, then P is conjugate to Q with respect to $\mathcal{C}$, i.e. ${}^tQAP = 0$. Transposing, we get that ${}^tPAQ = 0$, namely, Q is conjugate to P with respect to $\mathcal{C}$. But then by definition Q belongs to the polar of P, that is p. □

Proposition 9.3.10. Let $\mathcal{C}$ be a general real conic, let $P \in \mathbb{P}^2(\mathbb{C})$ and let p be the polar of P with respect to $\mathcal{C}$.

1. $P \in p$ if and only if $P \in \mathcal{C}$, and in such case the polar of P is the tangent line in P.
2. If $P \notin \mathcal{C}$, there exist exactly two lines ℓ_1 and ℓ_2 through P that are tangent to $\mathcal{C}$, and p is the line through the two points $\ell_1 \cap \mathcal{C}$ and $\ell_2 \cap \mathcal{C}$.

Proof. 1. $P \in p$ if and only if P is conjugate to itself with respect to $\mathcal{C}$, namely if and only if ${}^tPAP = 0$. But this is equivalent to saying that $P \in \mathcal{C}$. Lemma 9.2.5 shows that in this case the equation of the polar is precisely the equation of the tangent line.

2. Consider $p \cap \mathcal{C}$. By theorem 9.1.16, this consists either of two distinct points or of a single point with multiplicity 2. Suppose that the latter holds, and let $Q = p \cap \mathcal{C}$. Since the intersection multiplicity of p and $\mathcal{C}$ in Q is 2, p is tangent to $\mathcal{C}$ in Q, and hence by 1. the line p is the polar of Q. But a line has a unique pole by Proposition 9.3.8, and hence $P = Q$. But then $P \in \mathcal{C}$, contradicting the hypothesis. Hence $p \cap \mathcal{C}$ consists of two distinct points P_1, P_2. Now let ℓ_i be the tangent in P_i, for $i = 1, 2$. Since $P_i \in \mathcal{C}$, by Theorem 9.3.9 we have that $P \in \ell_i$, for $i = 1, 2$.

So we proved that there exist two lines ℓ_1, ℓ_2 through P that are tangent to $\mathcal{C}$, and p is the line through $\ell_1 \cap \mathcal{C}$ and $\ell_2 \cap \mathcal{C}$. It remains to show that there are no other lines through P that are tangent to $\mathcal{C}$. Let ℓ_3 be another line with such property and let $P_3 = \ell_3 \cap \mathcal{C}$. Then ℓ_3 is the polar of P_3, and since $P \in \ell_3$, by Theorem 9.3.9 we have that $P_3 \in p$. But then $\{P_1, P_2, P_3\} \subseteq p \cap \mathcal{C}$, contradicting Theorem 9.1.16 since the three points are all distinct. □

Definition 9.3.11. Let $\mathcal{C}$ be a general real conic. The *center* of $\mathcal{C}$ is the pole of the improper line $z = 0$. The *diameters* of $\mathcal{C}$ are the polars of the improper points of $\mathbb{P}^2(\mathbb{C})$.

Remark 9.3.12. Let $\mathcal{C}$ be a general real conic. Then every diameter of $\mathcal{C}$ passes through the center of $\mathcal{C}$. In fact, if P is the center of $\mathcal{C}$ then by definition the polar of P is $z = 0$. Hence by Theorem 9.3.9, the polars of the points lying on $z = 0$, that are the diameters, pass through P.

Proposition 9.3.13. Let $\mathcal{C}$ be a general real conic with defining matrix $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}$.

1. The center of $\mathcal{C}$ is the unique point $(x_P : y_P : z_P) \in \mathbb{P}^2(\mathbb{C})$ such that:
$$\begin{cases} a_{11}x_P + a_{12}y_P + a_{13}z_P = 0 \\ a_{12}x_P + a_{22}y_P + a_{23}z_P = 0 \end{cases}.$$
2. The center of $\mathcal{C}$ is improper if and only if $\mathcal{C}$ is a parabola, and in this case its center is the unique improper point of $\mathcal{C}$.
3. If $\mathcal{C}$ is not a parabola, the asymptotes of $\mathcal{C}$ are the lines through the center and the improper points of $\mathcal{C}$.

Proof. 1. By Remark 9.3.12, in order to compute the center we can compute the polars of the points $(1 : 0 : 0)$ and $(0 : 1 : 0)$ and intersect them. These polars are, respectively,
$$a_{11}x + a_{12}y + a_{13}z = 0 \text{ and } a_{12}x + a_{22}y + a_{23}z = 0.$$
Hence the center is given by the unique solution of the system
$$\begin{cases} a_{11}x + a_{12}y + a_{13}z = 0 \\ a_{12}x + a_{22}y + a_{23}z = 0 \end{cases} \tag{49}$$

(notice that the solution is unique because since $\mathcal{C}$ is general, the rows of A are linearly independent, hence all solutions of (49) are proportional to each other).

2. System (49) has a solution of the form $(x_P : y_P : 0)$ if and only if (x_P, y_P) solves the system

$$\begin{cases} a_{11}x + a_{12}y = 0 \\ a_{12}x + a_{22}y = 0 \end{cases} . \tag{50}$$

But this is a homogeneous system of two equations in two indeterminates, and therefore by Theorem 3.1.5 it has a non-zero solution if and only if $\det \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix} = 0$, namely if and only if $\mathcal{C}$ is a parabola by Theorem 9.3.2.

Suppose then that $\mathcal{C}$ is a parabola. Its center then is $(x_P : y_P : 0)$ where (x_P, y_P) solves (51). Since $\mathcal{C}$ is a parabola, $a_{11}a_{22} - a_{12}^2 = 0$, so the two equations are linearly dependent. Now if $(a_{11}, a_{12}) \neq (0, 0)$ then the solution is $(-a_{12} : a_{11} : 0)$. Otherwise we must have $a_{22} \neq 0$, since $\mathcal{C}$ is general, and the center is $(1 : 0 : 0)$.

On the other hand, to find the improper points of $\mathcal{C}$ we need to solve

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 = 0 \tag{51}$$

If $(a_{11}, a_{12}) \neq (0, 0)$ then plugging in $x = -a_{12}$ and $y = a_{11}$ in the above expression we get $-a_{11}a_{12}^2 + a_{22}a_{11}^2 = a_{11}(-a_{12}^2 + a_{11}a_{22})$, that is 0 since $\mathcal{C}$ is a parabola. If $(a_{11}, a_{12}) = (0, 0)$ then as we have seen the center is $(1 : 0 : 0)$ and (51) becomes $a_{22}y^2 = 0$, that is satisfied by $(1 : 0 : 0)$. In any case, the center coincides with the unique improper point.

3. Since $\mathcal{C}$ is not a parabola, it has two distinct improper points P_1 and P_2. The polar p_i of P_i is the tangent line in P_i for $i = 1, 2$ by Proposition 9.3.10, and hence p_1 and p_2 are the asymptotes of $\mathcal{C}$. By Remark 9.3.12, they pass through the center, and hence they must be the lines through the center and the improper points. □

Remark 9.3.14. The center of a real general conic $\mathcal{C}$ is a point of $\mathcal{C}$ if and only if $\mathcal{C}$ is a parabola. In fact, if $\mathcal{C}$ is a parabola then by Proposition 9.3.13 its center lies on it. If $\mathcal{C}$ is not a parabola, by Proposition 9.3.13 the center P is proper. Hence if it was a point of $\mathcal{C}$, by Proposition 9.3.10

its polar would be the tangent in P, that is a proper line. But this is impossible since the polar of the center is the improper line by definition.

Example 9.3.15. Let $\mathcal{C}\colon x^2 - 2xy + 2y^2 + 4xz - 2z^2 = 0$. By Proposition 9.3.13, the center is found by solving the system

$$\begin{cases} x - y + 2z = 0 \\ -x + 2y = 0 \end{cases},$$

that yields the point $(-4 : -2 : 1)$.

Of course one can also compute the center by using its very definition, namely that of being the pole of the improper line. So $P = (x_P : y_P : z_P)$ is the center of $\mathcal{C}$ if and only if its polar is $z = 0$, namely if and only if

$$\begin{pmatrix} x_P & y_P & z_P \end{pmatrix} \begin{pmatrix} 1 & -1 & 2 \\ -1 & 2 & 0 \\ 2 & 0 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

is the improper line. The above line has equation

$$(x_P - y_P + 2z_P)x + (-x_P + 2y_P)y + (2x_P - 2z_P)z = 0,$$

which is the equation of the improper line if and only if

$$\begin{cases} x_P - y_P + 2z_P = 0 \\ -x_P + 2y_P = 0 \end{cases},$$

that is the very same system we already solved.

Proposition 9.3.16. Let $\mathcal{C}$ be a general real conic. The diameters of $\mathcal{C}$ constitute the pencil of lines through the center of $\mathcal{C}$.

Proof. Every diameter passes through the center, by Remark 9.3.12. Conversely, let ℓ be a line through the center P of $\mathcal{C}$. By Theorem 9.3.9, the pole of ℓ must lie on the polar of P. But this is the improper line, by definition of center. Hence ℓ is the polar of an improper point. □

Remark 9.3.17. When looking at the affine part of a general real conic $\mathcal{C}$, if $\mathcal{C}$ is not a parabola then its center is proper, and therefore the diameters will be the pencil of affine lines through such proper point. If $\mathcal{C}$ is a parabola, since the center is improper the affine part of the diameters will constitute a pencil of parallel lines, all with direction $(-a_{12} : a_{11} : 0)$ by Proposition 9.3.13.

9.4 Conics in $\mathbb{E}^2(\mathbb{R})$

Definition 9.4.1. A conic in $\mathbb{E}^2(\mathbb{R})$ is the set of solutions of an equation of the form:

$$\mathcal{C}\colon a_{11}x^2 + 2a_{12}xy + 2a_{13}x + a_{22}y^2 + 2a_{23}y + a_{33} = 0,$$

where $a_{ij} \in \mathbb{R}$ for every i, j and a_{11}, a_{12}, a_{22} are not all 0.

Of course by homogeneizing the equation of a conic in $\mathbb{E}^2(\mathbb{R})$ one obtains the equation of a real conic $\widetilde{\mathcal{C}}$ in $\mathbb{P}^2(\mathbb{C})$. However, we maintain the concepts distinct, in a formal way, in order to be able to talk about orthogonality, that is a notion that makes no sense in $\mathbb{P}^2$.

Every notion we have seen in the previous sections for conics in $\mathbb{P}^2(\mathbb{C})$ carries over to conics in $\mathbb{E}^2(\mathbb{R})$; to make sense of such notions we'll think of them as associated to the conic $\widetilde{\mathcal{C}}$. For example, if $x^2 + y^2 + 1$ is a conic in $\mathbb{E}^2(\mathbb{R})$, we can talk of its improper points: these will be the improper points in $\mathbb{P}^2(\mathbb{C})$ of the conic $x^2 + y^2 + z^2 = 0$.

In the Euclidean setting we distinguish (for reasons that will not be treated in these notes) circles from ellipses, although the former are a special case of the latter.

Definition 9.4.2. A *circle* in $\mathbb{E}^2(\mathbb{R})$ is a conic with equation

$$\mathcal{C}\colon a_{11}x^2 + a_{11}y^2 + 2a_{13}x + 2a_{23}y + a_{33} = 0,$$

with $a_{11} \neq 0$.

Therefore, in the Euclidean setting we will use the word "ellipse" to denote an ellipse that is <u>not</u> a circle.

Definition 9.4.3. The *cyclic points* in $\mathbb{P}^2(\mathbb{C})$ are $(1 : i : 0)$ and $(1 : -i : 0)$.

Lemma 9.4.4. A general conic $\mathbb{C} \subseteq \mathbb{E}^2(\mathbb{R})$ is a circle if and only $\widetilde{\mathcal{C}}$ passes through the cyclic points.

Proof. Simply impose to the general equation of a conic the passage through the cyclic points. This yields:

$$a_{11} \pm 2ia_{12} - a_{22} = 0,$$

so that we must have $a_{11} = a_{22}$ and $a_{12} = 0$. □

Definition 9.4.5. Let $\mathcal{C} \subseteq \mathbb{E}^2(\mathbb{R})$ be a hyperbola. We say that $\mathcal{C}$ is *equilateral* if its asymptotes are orthogonal.

Proposition 9.4.6. Let

$$\mathcal{C} \colon a_{11}x^2 + 2a_{12}xy + 2a_{13}x + a_{22}y^2 + 2a_{23}y + a_{33} = 0$$

be a hyperbola in $\mathbb{E}^2(\mathbb{R})$. Then $\mathcal{C}$ is equilateral if and only if $a_{11} + a_{22} = 0$.

Proof. To find the improper points of $\mathcal{C}$ we need to solve the equation

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 = 0. \tag{52}$$

Since $\mathcal{C}$ is a hyperbola, we know that this equation will yield two real distinct improper points: $(x_0 : y_0 : 0)$ and $(x_0' : y_0' : 0)$. Let P be the center of $\mathcal{C}$, that is proper by Proposition 9.3.13. Since the asymptotes are the lines through P and the improper points, again by Proposition 9.3.13, their directions are (x_0, y_0) and (x_0', y_0'). Hence they are orthogonal if and only if

$$x_0x_0' + y_0y_0' = 0. \tag{53}$$

If, without loss of generality, we assume that $a_{22} \neq 0$, then $x_0 \neq 0$ as otherwise to solve (52) we would also need $y_0 = 0$. For the same reason,

$x_0' \neq 0$. Hence (53) can be rewritten as:

$$\frac{y_0}{x_0} \cdot \frac{y_0'}{x_0'} = -1.$$

Now since $\frac{y_0}{x_0}$ and $\frac{y_0'}{x_0'}$ are the roots of the equation

$$a_{22}t^2 + 2a_{12}t + a_{11} = 0,$$

their product is -1 if and only if $\frac{a_{11}}{a_{22}} = -1$, that is if and only if $a_{11} + a_{22} = 0$. □

Definition 9.4.7. Let $\mathcal{C} \subseteq \mathbb{E}^2(\mathbb{R})$ be a general conic. An *axis* of $\mathcal{C}$ is a proper diameter whose direction is orthogonal to that of its own pole. If ℓ is an axis of $\mathcal{C}$ and $P \in \ell \cap \mathcal{C}$ is proper, then it is called a *vertex* of $\mathcal{C}$.

Proposition 9.4.8. Let $\mathcal{C} \subseteq \mathbb{E}^2(\mathbb{R})$ be a general conic.

1. If $\mathcal{C}$ is a circle, all diameters are axes and all proper points of $\mathcal{C}$ are vertices.
2. If $\mathcal{C}$ is a hyperbola or an ellipse, then its has 2 axes and 4 vertices.
3. If $\mathcal{C}$ is a parabola, there is a unique axis and a unique vertex and the tangent in the vertex is orthogonal to the axis.

Proof. Let $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}$ be the matrix of the associated projective conic $\widetilde{\mathcal{C}}$. Let $(x_P : y_P : 0)$ be an improper point. Its polar is given by the equation:

$$(x_P a_{11} + y_P a_{12})x + (x_P a_{12} + y_P a_{22})y + (x_P a_{13} + y_P a_{23})z = 0.$$

The direction of such polar is $(x_P a_{12} + y_P a_{22}, -x_P a_{11} - y_P a_{12})$, while that of the pole is (x_P, y_P). Hence in order for them to be orthogonal we need $(x_P a_{12} + y_P a_{22})x_P - (x_P a_{11} + y_P a_{12})y_P = 0$ or, in other words,

$$a_{12}x_P^2 + (a_{22} - a_{11})x_P y_P - a_{12}y_P^2 = 0. \tag{54}$$

1. If $\mathcal{C}$ is a circle, then $a_{11} = a_{22}$ and $a_{12} = 0$, so that (54) is satisfied by every pair (x_P, y_P). This is equivalent to saying that every diameter is an axis.

If Q is the center of $\mathcal{C}$ and R is a point of $\mathcal{C}$, by Theorem 9.3.9 the pole of the line ℓ through Q and R is improper. Therefore ℓ is a diameter, and it is an axis by what we said above. Hence R is a vertex.

2. If $a_{12} = 0$, then the two solutions of (54) yield the points $P_1 = (1 : 0 : 0)$ and $P_2 = (0 : 1 : 0)$. If $a_{12} \neq 0$, then the solutions to (54) yield two points $P_1 = (x_P : y_P : 0)$ and $P_2 = (-y_P : x_P : 0)$. These points coincide if and only if $y_P = ix_P$, and if this happens then it must be $x_P \neq 0$. Then (54) becomes:

$$x_P^2(2a_{12} + (a_{22} - a_{11})i) = 0,$$

and since the a_{ij}'s are all real and $x_P \neq 0$ it must be $a_{11} = a_{22}$ and $a_{12} = 0$, contradicting the hypothesis that $\mathcal{C}$ is a hyperbola or an ellipse. Therefore $P_1 \neq P_2$.

Now we need to prove that the polars of P_1, P_2 are proper. Let ℓ_i be the polar of P_i, for $i = 1, 2$. If ℓ_i was the improper line, then $P_i \in \ell_i$, which implies that $P_i \in \mathcal{C}$ by Proposition 9.3.10. But the polar of a point of $\mathcal{C}$ is its tangent, by the same proposition, so that the improper line would be tangent in an improper point of $\mathcal{C}$. This would imply that $\mathcal{C}$ is a parabola by Remark 9.2.7, contradicting the hypothesis. Therefore, ℓ_1 and ℓ_2 are proper, and hence they are the axes of $\mathcal{C}$. They are distinct by Proposition 9.3.6, because they are polars of two distinct points.

Next, we need to prove that $\ell_i \cap \mathcal{C}$ consists of two distinct proper points. Let $i \in \{1, 2\}$. If ℓ_i was tangent to $\mathcal{C}$ in a point Q, then ℓ_i would be the polar of Q by Proposition 9.3.10. But since the pole of ℓ_i is improper, then Q would be improper and its direction would be the same as that of ℓ_i, which is impossible. Hence $\ell_i \cap \mathcal{C}$ consists of two distinct points for $i = 1, 2$. If $\ell_1 \cap \mathcal{C}$ contains an improper point P', then by Theorem 9.3.9 the polar of P' would pass by P_2. But the polar of P' is the tangent line in P', and since P' and P_2 are both improper, this means that the improper line $z = 0$ is tangent to $\mathcal{C}$. Hence $\mathcal{C}$ should a parabola, contradicting the hypothesis. This shows that $\ell_1 \cap \mathcal{C}$ consists of two distinct proper points, and with a simmetric argument also $\ell_2 \cap \mathcal{C}$ does.

Let then $\ell_1 \cap \mathcal{C} = \{Q_1, Q_2\}$ and $\ell_2 \cap \mathcal{C} = \{R_1, R_2\}$ with Q_1, Q_2, R_1, R_2 proper points with $Q_1 \neq Q_2$ and $R_1 \neq R_2$. If it was $Q_1 = R_1$, then

Q_1 would be the center of the conic, since all diameters pass through the center. But $Q_1 \in \mathcal{C}$, and this contradicts Remark 9.3.14. Hence $\{Q_1, Q_2\} \cap \{R_1, R_2\} = \emptyset$, proving that $\mathcal{C}$ has 4 vertices.

3. By Theorem 9.3.13, diameters of a parabola are exactly the lines that pass through its unique improper point. If $a_{11} \neq 0$ or $a_{12} \neq 0$, the improper point is $(a_{12} : -a_{11} : 0)$. Otherwise, we must have $a_{22} \neq 0$ as otherwise $\widetilde{\mathcal{C}}$ would be degenerate, and the improper point is $(1 : 0 : 0)$. Let us assume that we are in the first case, the other case can be treated similarly. Then all diameters have equation

$$a_{11}x + a_{12}y + kz = 0,$$

for some $k \in \mathbb{C}$. Therefore the unique improper point whose direction is orthogonal to that of its own diameter is $(a_{11} : a_{12} : 0)$. Since one between a_{11} and a_{12} is non-zero, the corresponding diameter is proper, and it is therefore the unique axis. One intersection with $\widetilde{\mathcal{C}}$ is $(a_{12} : -a_{11} : 0)$, and hence the second intersection must be proper, as otherwise the whole axis would be improper. Hence there is a unique vertex. By Theorem 9.3.9, the polar of the vertex, that is tangent to $\mathcal{C}$ therein, passes through the pole of the axis, that is $(a_{11} : a_{12} : 0)$, and hence its direction is orthogonal to that of the axis. □

Example 9.4.9.

- Let $\mathcal{C}\colon x^2 + 2y^2 - 2x - 2y + 3 = 0$. This is an ellipse, so it has two axes and four vertices. Let us compute them. To find axes, we first need to solve equation (54), that in this case is:

  $$xy = 0.$$

  Hence the points $P_1 = (1 : 0 : 0)$ and $P_2 = (0 : 1 : 0)$ are such that their polars are the axes of $\mathcal{C}$. Since the matrix of $\widetilde{\mathcal{C}}$ is $\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 3 \end{pmatrix}$, the axes have equation

  $$x - z = 0 \text{ and } 2y - z = 0$$

or, in affine coordinates,

$$x - 1 = 0 \text{ and } 2y - 1 = 0.$$

In order to find the vertices, we simply need to intersect the axes with $\mathcal{C}$. Hence we have to solve

$$\begin{cases} 1 + 2y^2 - 2 - 2y + 3 = 0 \\ x = 1 \end{cases} \quad \text{and} \quad \begin{cases} x^2 + 1/2 - 2x - 1 + 3 = 0 \\ y = 1/2 \end{cases},$$

which yield the points $(1 : (1 \pm i\sqrt{3})/2 : 1)$ and $(1 \pm i\sqrt{3/2} : 1/2 : 1)$. These are the four vertices of $\mathcal{C}$. Notice that they are all imaginary points! One can prove easily that $\widetilde{\mathcal{C}}$ has no real point.

- Let $\mathcal{C}\colon x^2 - y^2 - 2xy + 3 = 0$. This is a hyperbola, so it has two axes and four vertices. The matrix of $\widetilde{\mathcal{C}}$ reads as: $\begin{pmatrix} 1 & -1 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$, and equation (54) becomes:

$$-x^2 - 2xy + y^2 = 0,$$

which yields the two points $(1 : 1 \pm \sqrt{2} : 0)$. Now the axes of $\mathcal{C}$ are the polars of these points, namely the lines:

$$\sqrt{2}x + (2 + \sqrt{2})y = 0 \text{ and } \sqrt{2}x - (2 - \sqrt{2})y = 0.$$

To find the vertices, we need to solve:

$$\begin{cases} ((\sqrt{2} + 1)y)^2 - y^2 + 2y(\sqrt{2} + 1)y + 3 = 0 \\ x = -(\sqrt{2} + 1)y \end{cases}$$

and

$$\begin{cases} ((\sqrt{2} - 1)y)^2 - y^2 + 2y(\sqrt{2} - 1)y + 3 = 0 \\ x = (\sqrt{2} - 1)y \end{cases},$$

finding the four points

$$\left((\sqrt{2}+1)\sqrt{3-3\sqrt{2}} : -\sqrt{3-3\sqrt{2}} : 2\right),$$

$$\left(-(\sqrt{2}+1)\sqrt{3-3\sqrt{2}} : \sqrt{3-3\sqrt{2}} : 2\right),$$

$$\left((\sqrt{2}-1)\sqrt{3+3\sqrt{2}} : \sqrt{3+3\sqrt{2}} : 2\right),$$

$$\left((\sqrt{2}-1)\sqrt{3+3\sqrt{2}} : \sqrt{3+3\sqrt{2}} : -2\right).$$

These are the four vertices of $\mathcal{C}$; notice that the first two are imaginary, since $3-3\sqrt{2}<0$ while the other two are real.

- Let $\mathcal{C}\colon x^2+2xy+y^2+2y+3=0$. This is a parabola, and therefore it has one axis and one vertex. The matrix of $\widetilde{\mathcal{C}}$ is $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 3 \end{pmatrix}$ and the axes equation (54) is:

$$x^2-y^2=0,$$

yielding the points $(1:1:0)$ and $(1:-1:0)$. Their polars are:

$$x+y=0 \text{ and } z=0,$$

so the only axis is $x+y=0$. Intersecting it with $\mathcal{C}$ we find

$$\begin{cases} -2x+3=0 \\ y=-x \end{cases},$$

and hence the unique vertex is $(3:-3:2)$.

Notes