newtheoremtheoremTheorem

Table des Matières

.

Chapitre 1

Polynomials and Rational Fractions

1.1 Polynomials

1.1.1 Properties and definitions

Définition 1 *A polynomial with the form:*

$$\begin{aligned} P(X) &= \sum_{k=0}^{n} a_k X^k, 0 \leq k \leq n \in \mathbb{N}. \\ &= a_0 + a_1 X + a_2 X^2 + ... + a_n X^n, \end{aligned}$$

where X is the variable, the a's are called the coefficients of P, wich are real numbers or complex numbers. Each term of the form $a_k X^k$ is called monomial of P. The associated polynomial function f is then defined by:

$$f(x) = \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n,$$

where the variable x may itself be real or complex.

The set of all polynomials with real coefficients is noted as $\mathbb{R}[X]$ and $\mathbb{C}[X]$ if $a_k \in \mathbb{C}$.

Définition 2 ***(Degree and valuation of a polynomial)***

Let $P(X) = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$, with $P \neq 0$.

(1) The degree of P is the highest power of X noted $\deg P = d^0 P = \max k$ such as $a_k \neq 0, 0 \leq$

$k \leq n$.

(2) The valuation of P is the smallest power of X noted $val(P) = v(P) = \min k$ such as $a_k \neq 0, 0 \leq k \leq n$.

- The term $a_n X^n$ is the leading term $(a_n \neq 0)$ and a_n is the leading coefficient, the polynomial is said to be the n-th degree or degree n.

- If $P = 0$ (the null polynomial) then by convention we have: $\deg P = -\infty$.

Proof: Such that:

$$\deg(P \times Q) = \deg P + \deg Q,$$

in any particular case if $P = 0$ and Q is any, then this equality is true only if $\deg P = \infty$. *in addition*

$$\deg(P + Q) \leq \max(\deg P, \deg Q)$$

which is true if $Q = -P$ which states that $\deg P = -\infty$.

- If $P = 0$ (the null polynomial) then by convention we have: $val(P) = +\infty$.

Concepts and properties

(1) $P(x) = a_0$ with $a_0 \neq 0$ is called the constant polynomial.

(2) A monomial is, roughly speaking, a polynomial which has only one term, that is $P(x) = a_k x^k$ with $a_k \neq 0$.

(3) A monic is a polynomial whose leading coefficient is 1.

(4) If

$$P(X) = \sum_{k=0}^{n} a_k X^k \text{ and } Q(X) = \sum_{k=0}^{n} b_k X^k,$$

then

$$P(X) = Q(X) \Leftrightarrow a_k = b_k, \forall k, 0 \leq k \leq n.$$

1.1.2 Operation on $\mathbb{R}[X]$

Let

$$P(x) = \sum_{k=0}^{n} a_k x^k \text{ and } Q(x) = \sum_{k=0}^{m} b_k x^k,$$

We have the following properties:

(1)
$$P(x) + Q(x) = \sum_{k=0}^{p} c_k x^k,$$
with $c_k = a_k + b_k$ and $p = \max(n, m)$. Moreover if $n > m$, then $b_k = 0$ for all $k, m+1 \leq k \leq n$ and if $m > n$, then $a_k = 0$ for all $k, n+1 \leq k \leq m$.

(2) $\deg(P+Q) \leq \max(\deg P, \deg Q)$.

(3) $\forall \alpha \in \mathbb{R}$,
$$\alpha P(x) = \sum_{k=0}^{n} (\alpha a_k) x^k.$$

(4)
$$P(x) \times Q(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ with } c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

(5) $\deg(P \times Q) = \deg P + \deg Q$.

1.1.3 Types of division between polynomials

Let P and Q two polynomials defined by:

$$P(X) = \sum_{k=0}^{n} a_k X^k \text{ and } Q(X) = \sum_{k=0}^{m} b_k X^k, a_n \neq 0 \text{ and } b_m \neq 0.$$

Euclidean division or division with remainder (division according to decreasing powers)

To make the euclidean division of P on Q it is necessary to order the monomials of the greatest degree to the smallest degree, where we have the following two cases:

1st case: If $n < m$, then:

P	Q
P	0

that is: $P(X) = 0 \times Q(X) + P(X)$.

2nd case: If $n \geq m$, then:

P	Q
R	H

that is: $P(X) = H(X) \times Q(X) + R(X)$ with $\deg R < \deg Q$.

P is called the dividend, Q the divider, H is the quotient and R is the rest of the Euclidean division.

Example 3 *Make the Euclidean division of* $P(X) = -3 + 2X + 4X^2 - 5X^3 + 3X^4$ *on* $Q(X) = 5 + X - X^2$.

$3X^4 - 5X^3 + 4X^2 + 2X + 3$	$-X^2 + X + 5$
$-(3X^4 - 3X^3 - 15X^2)$	$-3X^2 - 8X - 27$
$= 8X^3 + 19X^2 + 2X + 3$	
$-\left(8X^3 - 8X^2 - 40X\right)$	
$= 27X^2 + 42X + 3$	
$-\left(27X^2 - 27X - 135\right)$	
$0 + 69X + 138$	

So,

$$P(X) = \left(-3X^2 - 8X - 27\right) Q(X) + 69X + 138.$$

1.2 The Extended Euclidean Algorithm for Polynomials

The Polynomial Euclidean Algorithm has the same principle of the one who calculates the greatest common divisor (gcd) between natural integers by performing repeated divisions with remainder. We use in each step the property: If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$. The principle is that the dividend is eliminated each time. The algorithm between polynomials is

based for:

$$\begin{aligned} P &= A_1 Q + R_1 \\ Q &= A_2 R_1 + R_2 \\ R_1 &= A_3 R_2 + R_3 \\ R_3 &= A_4 R_2 + R_4 \\ &\vdots \\ R_n &= A_{n+2} R_{n+1} + R_{n+2} \end{aligned}$$

So if $R_{n+2} = 0$ (The null polynomial) then $\gcd(P, Q) = R_{n+1}$ and if $R_{n+2} = a \neq 0$, so $\gcd(P, Q) = 1$. (In this case we say that P and Q are relatively prime).

Example 4 *Find* $\gcd(P, Q)$ *when* $P(X) = X^5 + 1$ *and* $Q(X) = X^3 + 1$

$$\begin{aligned} X^5 + 1 &= X^2\left(X^3 + 1\right) - X^2 + 1 \\ X^3 + 1 &= -X\left(-X^2 + 1\right) + X + 1 \\ -X^2 + 1 &= (X + 1)(-X + 1) + 0. \end{aligned}$$

$$\Rightarrow \gcd\left(X^5 + 1, X^3 + 1\right) = X + 1.$$

Example 5 *(1) Find* $\gcd(P, Q)$ *when* $P(X) = 5X^3 + 2X^2 + 3X - 10$ *and* $Q(X) = X^3 + 2X^2 - 5X + 2$.

$$\begin{aligned} P(X) &= 5 \times Q(X) + \left(-8X^2 + 28X - 20\right) \\ Q(X) &= \left(-\frac{1}{8}X - \frac{11}{16}\right)\left(-8X^2 + 28X - 20\right) + \left(\frac{47}{4}X - \frac{47}{4}\right) \end{aligned}$$

$$\left(-8X^2 + 28X - 20\right) = \frac{4}{47}(-8X + 20)\left(\frac{47}{4}X - \frac{47}{4}\right) + 0$$

$$\Rightarrow \gcd(P, Q) = X - 1. \textit{(Monic polynomial)}$$

(2) Find U *and* V *when*

$$P(X)U + Q(X)V = \gcd(P, Q).$$

$$\frac{47}{4}X - \frac{47}{4} = Q(X) - \left(-\frac{1}{8}X - \frac{11}{16}\right)\left(-8X^2 + 28X - 20\right)$$

$$\begin{aligned}
\Rightarrow \quad & X - 1 = \frac{4}{47}Q(X) + \left(\frac{1}{94}X + \frac{11}{188}\right)\left(-8X^2 + 28X - 20\right) \\
= \quad & \frac{4}{47}Q(X) + \left(\frac{1}{94}X + \frac{11}{188}\right)(P(X) - 5Q(X)) \\
= \quad & \underbrace{\left(\frac{1}{94}X + \frac{11}{188}\right)}_{U}P(X) + \underbrace{\left(-\frac{5}{94}X - \frac{39}{188}\right)}_{V}Q(X).
\end{aligned}$$

Théorème 6 ***(Bézout)*** *Let P and Q two polynomials not both null. If $\gcd(P, Q) = D$ then they exist two polynomials U and V of $\mathbb{k}[X]$ such as:*

$$PU + QV = D.$$

In particular if $D = 1$, then P and Q are relatively prime.

Division by increasing power order

The division by increasing power order has the same principle as the Euclidean division, but the order of the monomial is from the smallest power to the greatest. In the Euclidean division one stops if the degree of the remiender is strictly less than to the degree of the divisor, moreover the degrees of the result (the quotient H) decreased, on the other hand in the division according to the increasing powers the degrees of the result increases for that one has the sentence the division according to the increasing powers to the order k i.e it is necessary to find a polynomial (quotient) of degree $\leq k$.

Example 7 *Make the division according to the increasing powers in order 2 of $P(X) = -3 +$*

$2X + 4X^2 - 5X^3 + 3X^4$ *on* $Q(X) = 5 + X - X^2$.

$-3 + 2X + 4X^2 - 5X^3 + 3X^4$	$5 + X - X^2$
$-\left(-3 - \frac{3}{5}X + \frac{3}{5}X^2\right)$	$-\frac{3}{5} + \frac{13}{25}X + \frac{72}{125}X^2$
$= \frac{13}{5}X + \frac{17}{5}X^2 - 5X^3 + 3X^4$	
$-\left(\frac{13}{5}X + \frac{13}{25}X^2 - \frac{13}{25}X^3\right)$	
$= \frac{72}{25}X^2 - \frac{112}{25}X^3 + 3X^4$	
$-\left(\frac{72}{25}X^2 + \frac{72}{125}X^3 - \frac{72}{125}X^4\right)$	
$-\frac{632}{125}X^3 + \frac{447}{125}X^4$	

Then the result of this division is:

$$P(X) = \left(-\frac{3}{5} + \frac{13}{25}X + \frac{72}{125}X^2\right) Q(X) + X^3\left(-\frac{632}{125} + \frac{447}{125}X\right).$$

Remarque 8 *The two results of the two divisions are completely different despite the fact that the dividend and divisor are the same.*

1.2.1 The root and their order of multiplicity

Définition 9 *Let P be a polynomial defined by:*

$$P(X) = \sum_{k=0}^{n} a_k X^k \text{ such as } a_n \neq 0.$$

It is said that X_0 is a root or a zero of $P(X)$ if and only if:

$$P(X_0) = 0.$$

Définition 10 *If*

$$P(x) = (x - x_0)^m Q(x) \text{ such as } Q(x_0) \neq 0,$$

then m is said to be the order of the multiplicity of the root x_0 of $P(x)$. Moreover we have:

$$P(x_0) = 0, P^{(k)}(x_0) = 0, \forall k \text{ when } 1 \leq k < m \text{ and } P^{(m)}(x_0) \neq 0.$$

On the other hand if:

$$P(x) = (x - x_0) Q(x) \text{ such as } Q(x_0) \neq 0,$$

then x_0 is said to be a simple root of $P(x)$.

Example 11 *Find the order of multiplicity of the root 1 of the polynomial:*

$$P(x) = x^3 + x^2 - 5x + 3.$$

We have:

$$P(1) = 0,$$

and

$$P'(x) = 3x^2 + 2x - 5 \Rightarrow P'(1) = 0,$$

and

$$P''(x) = 6x + 2 \Rightarrow P''(1) \neq 0.$$

Then the multiplicity is 2, wichi mplies that:

$$P(x) = (x - 1)^2 Q(x), \text{ such as } Q(1) \neq 0,$$

in this case we said that 1 a double root of $P(x)$.

1.2.2 Some properties on the roots of a polynomial

Théorème 12 *(Gauss) Let P, Q and R of polynomials such as:*

(1) *P divides the product QR.*

(2) *P and Q are relatively prime.*

Then P divides R.

Preuve: Since P and Q are relatively prime, the theorem of **Bézout** implies that there exist U and V of $\Bbbk[X]$ such as:

$$PU + QV = 1.$$

By multiplying this equality by R, we find:

$$RPU + RQV = R.$$

But P divides QR, then there exists a polynomial S such as:

$$QR = PS \Rightarrow P\left(RU + SV\right) = R,$$

which implies that P divides R. ■

Théorème 13 ***(relative root and rational root)*** *Let:*

$$P\left(x\right) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n,$$

a polynomial function such as $a_0 \neq 0$ *and* $a_n \neq 0$.

(1) If $\alpha \in \mathbb{Z}$ *is a relative root of* P *then* α *divides* a_0.

(2) If $\frac{\alpha}{\beta} \in \mathbb{Q}$ *is a rational root of* P*then* α *divides* a_0 *and* β *divides* a_n.

Preuve: Let $\frac{\alpha}{\beta}$ be a root of P, with α and β are relatively prime. Then,

$$\sum_{k=0}^{n} a_k \left(\frac{\alpha}{\beta}\right)^k = 0,$$

so,

$$a_0 + a_1 \left(\frac{\alpha}{\beta}\right) + a_2 \left(\frac{\alpha}{\beta}\right)^2 + ... + a_n \left(\frac{\alpha}{\beta}\right)^n = 0.$$

By multiplying the members of this equality by β^n, we find:

$$a_0\beta^n + a_1\alpha\beta^{n-1} + ... + a_{n-1}\alpha^{n-1}\beta + a_n\alpha^n = 0, \tag{1.1}$$

which implies that:

$$\alpha\left(a_1\beta^{n-1}+...+a_{n-1}\alpha^{n-2}\beta+a_n\alpha^{n-1}\right)=-a_0\beta^n,$$

so α divides $a_0\beta^n$, but α and β are relatively prime implies that α and β^n are relatively prime; according to the theorem of Guss, α divides a_0. Use another time (1.1) we have:

$$\beta\left(a_0\beta^{n-1}+a_1\alpha\beta^{n-2}+...+a_{n-1}\alpha^{n-1}\right)=-a_n\alpha^n,$$

for the same reasons we get β divides a_n. ■

1.3 Partial fraction decomposition or Partial fraction expansion

Définition 14 *A rational fraction is a function $H(x)=\frac{f(x)}{g(x)}$, where $f(x)$ and $g(x)$ are polynomials with $g(x)\neq 0$. If the degree of $f(x)$ is strictly less than to the degree of $g(x)$, it is said that $H(x)$ is a proper rational fraction, if not, $H(x)$ is said to be improper. In this case we can express $H(x)$ as the sum of a polynomial and a proper rational fraction by the Euclidean division method i.e:*

$$H(x)=L(x)+\frac{R(x)}{g(x)}\ \textit{where}\ \deg R<\deg g.$$

This allows to say that an improper rational fration is the sum of a polynomial and a proper rational fraction.

1.3.1 Partial fraction expansion

A quadratic polynomial $\left(\alpha x^2+\beta x+\lambda\right)$ is reducible if and only if $\triangle=b^2-4ac\geq 0$ and it is irreducible if and only if $\triangle<0$ (In this case the roots are complex). Theoretically any polynomial with real coefficients can be expressed as the product of real linear factors of the form $ax+b$ and other irreducible quadratics of the form $\alpha x^2+\beta x+\lambda$.

The partial fraction expansion is the reverse operation of assembling fractions to a fraction by the method of unification of denominators.

Steps of partial fraction expansion

Step 1: Euclidean division if it exists If the rational fraction $\frac{f(x)}{g(x)}$ is improper then after the Euclidean division we find:

$$\underbrace{\frac{f(x)}{g(x)}}_{\text{Improper}} = \underbrace{P(x)}_{\text{Polynomial}} + \underbrace{\frac{R(x)}{g(x)}}_{\text{Proper}},$$

Knowing that $P(x)$ is a polynomial and $\frac{R(x)}{g(x)}$ is a proper rational fraction.

If no,i.e $\frac{f(x)}{g(x)}$ is a proper then we go directly to the second step.

Step 2: The decomposition of the denominator We take $\frac{R(x)}{g(x)}$ in the case of the euclidean division and $\frac{f(x)}{g(x)}$ if not, that is to say in the second step always one takes the proper rational fraction.

Each polynomial is decomposable as a product of the following four types of factors:

(1) Distinct linear factors: A distinct linear factor is of the form: $ax + b$ (the root of this polynomial is simple for the denominator $g(x)$).

(2) Repeated linear factors: A repeated linear factor is of the form: $(ax + b)^n$ with $n \in \mathbb{N}$ and $n \geq 2$ (the root of this polynomial is of order n for the denominator $g(x)$).

(3) Distinct quadratic factors: It is a factor of form $ax^2 + bx + c$, moreover it is irreducible ($\triangle < 0$).

(4) Repeated quadratic factors: It is a factor of form $\left(ax^2 + bx + c\right)^n$ with $n \in \mathbb{N}$ and $n \geq 2$, moreover $ax^2 + bx + c$ is irreducible.

Step 3: Partial fraction decomposition or Partial fraction expansion It is the writing of a proper rational fraction as the sum of simple elements which are generally of form:

$$\frac{A_1}{a_1x + b_1}, \frac{B_1}{(c_1x + d_1)^n}, \frac{\alpha_1 x + \beta_1}{a_2x^2 + b_2x + c_2} \text{ and } \frac{\alpha_2 x + \beta_2}{(a_3x^2 + b_3x + c_3)^m}.$$

in a way that the denominators of the simple elements are all possible cases for that are common denominator is $g(x)$.

For example if we have in $g(x)$ the factor $(ax+b)^5$then in the decomposition into simple elements the cases of fractions such as are common denominator is $(ax+b)^5$ are:

$$\frac{A_1}{(ax+b)}+\frac{A_2}{(ax+b)^2}+\frac{A_3}{(ax+b)^3}+\frac{A_4}{(ax+b)^4}+\frac{A_5}{(ax+b)^5}.$$

That is to say always it is necessary to start the powers of 1 and to go up to the n (the multiplicity of the factor).

But for numerators there are two rules:

First rule: If the denominator is a linear factor repeated or not repeated then in the numerator it is necessary to ask incongruous constants that we will calculate them in the next step.

2nd rule: If the denominator is a quadratic factor repeated or not repeated then in the numerator it is necessary to put polynomials of degrees 1 with inconus coefficients that we will calculate them in the next step.

Example 15

$$\frac{x}{(x+1)(x-1)^3(x^2+x+1)(x^2+x+3)^2}=\frac{A_1}{x+1}+\frac{A_2}{x-1}+\frac{A_3}{(x-1)^2}+\frac{A_4}{(x-1)^3}+\frac{ax+b}{x^2+x+1}+\frac{cx+d}{x^2+x+3}+\frac{ex+f}{(x^2+x+3)^2}.$$

Remarque 16 *The number of simple elements is the sum of the powers of the denominator factors.*

Step 4: Calculation of coefficients of numerators of simple elements There are methods for calculating numerator coefficients for simple elements for example:

1st method: (Identification) Group the simple elements and by identification of the two numerators of the two members we find the constants, but this method is no longer ifficace especially if the number of inconvenient constants is large enough.

2nd method: (The limits) The principle of this method is based on the following two properties:

$$\begin{aligned}&(1)\text{ If } f(x)=g(x)\text{ then: } \forall x_0\in\mathbb{R}\text{ or }\pm\infty,\ \lim_{x\to x_0} f\ (x)=\lim_{x\to x_0} g(x),\\&(2)\text{ If } f(x)=g(x)\text{ then: } \forall h(x)\text{ we have } h(x)f(x)=h(x)g(x).\end{aligned}$$

To better understand this method, examples are given:

Example 17

$$\begin{aligned}f(x) &= \frac{2x+3}{(x-1)(x+2)^3(x^2+x+2)}\\ f(x) &= \frac{A_1}{x-1}+\frac{A_2}{x+2}+\frac{A_3}{(x+2)^2}+\frac{A_4}{(x+2)^3}+\frac{ax+b}{x^2+x+2},\\ (x+2)^3 f(x) &= A_4+(x+2)^3\left[\frac{A_1}{x-1}+\frac{A_2}{x+2}+\frac{A_3}{(x+2)^2}+\frac{ax+b}{x^2+x+2}\right],\end{aligned}$$

(1) For the non-repeating linear factor: $x-1$, multiplying the two members by $x-1$, we find:

$$\tfrac{2x+3}{(x+2)^3(x^2+x+2)}=A_1+(x-1)\left[\tfrac{A_2}{x+2}+\tfrac{A_3}{(x+2)^2}+\tfrac{A_4}{(x+2)^3}+\tfrac{ax+b}{x^2+x+2}\right],$$

stretching the limit of the two members to 1 (the number that eliminates $x-1$) we find:

$$A_1=\lim_{x\to 1}\frac{2x+3}{(x+2)^3(x^2+x+2)}=\frac{5}{324}.$$

This approach always eliminates the other coefficients.

(2) For the repeated linear factor that is: $x+2$.

(i) The first technique its march for the greatest power is the coefficient A_4 by multiplication of the two members by $(x+2)^3$ we find:

$$\frac{2x+3}{(x-1)(x^2+x+2)}=A_4+(x+2)^3\left[\frac{A_1}{x-1}+\frac{A_2}{x+2}+\frac{A_3}{(x+2)^2}+\frac{ax+b}{x^2+x+2}\right],$$

stretching the limit of the two members to -2 (the number that eliminates $x+2$) we find:

$$A_4=\lim_{x\to -2}\frac{2x+3}{(x-1)(x^2+x+2)}=\frac{1}{12}.$$

(ii) For the smallest power:

$$\begin{aligned}
&f(x) = \tfrac{A_1}{x-1} + \tfrac{A_2}{x+2} + \tfrac{A_3}{(x+2)^2} + \tfrac{A_4}{(x+2)^3} + \tfrac{ax+b}{x^2+x+2} \\
&\Rightarrow \lim_{x\to+\infty} xf(x) = \lim_{x\to+\infty} x\left[\tfrac{A_1}{x-1} + \tfrac{A_2}{x+2} + \tfrac{A_3}{(x+2)^2} + \tfrac{A_4}{(x+2)^3} + \tfrac{ax+b}{x^2+x+2}\right] \\
&\Rightarrow 0 = A_1 + A_2 + a \text{ (is missing } a \text{ to find } A_2).
\end{aligned}$$

(iii) The best method for obtaining all the coefficients of the repeated linear factors is the variable change method, in fact:

Method: (Variable change with division according to increasing powers).

This method is valid for the repeated linear factors of type $(ax+b)^n$ *i.e., whether:*

$$f(x) = \frac{p(x)}{(ax+b)^n k(x)}, \tag{1.2}$$

then we put:

$$y = ax + b \Rightarrow x = \frac{y-b}{a},$$

replacing then in (1.2) according to y *and making the division according to the increasing power of* $p\left(\frac{y-b}{a}\right)$ *over* $k\left(\frac{y-b}{a}\right)$ *in order* $n-1$ *without the use of the term* $(y)^n$*, whose result is of the form:*

$$a_0 + a_1 y + ... + a_{n-1} y^{n-1},$$

which gives after division on y^n *(not used in the division) that:*

$$\begin{aligned}
&a_{n-1} = A_1 \text{ (numerator of } y = ax+b), \\
&a_{n-2} = A_2 \text{ (numerator of } y^2 = (ax+b)^2), \\
&\qquad\qquad \vdots \\
&a_0 = A_n \text{ (numerator of } y^n = (ax+b)^n).
\end{aligned}$$

To better understand we will apply this in the example:

$$\begin{aligned}
f(x) &= \frac{2x+3}{(x-1)(x+2)^3(x^2+x+2)} \\
&= \frac{A_1}{x-1} + \frac{A_2}{x+2} + \frac{A_3}{(x+2)^2} + \frac{A_4}{(x+2)^3} + \frac{ax+b}{x^2+x+2}.
\end{aligned}$$

We put:

$$y = x + 2 \Rightarrow x = y - 2.$$

We will replace according to the new variable and make the division according to the increasing powers in order 2 *because the multiplicity order of the root is* 3 *(We take that the powers less than or equal to* 2*).*

$$\begin{aligned}
\frac{2x+3}{(x-1)(x^2+x+2)} &= \frac{2(y-2)+3}{(y-2-1)\left((y-2)^2+y-2+2\right)} \\
&= \frac{-1+2y}{(y-3)(y^2-3y+4)} \\
&= \frac{-1+2y}{-12+13y-6y^2} \\
&= \frac{1}{12} - \frac{11}{144}y - \frac{215}{1728}y^2
\end{aligned}$$

because:

$$\begin{array}{ll}
-1+2Y & -12+13Y-6Y^2 \\
-\left(-1+\frac{13}{12}Y-\frac{1}{2}Y^2\right) & \frac{1}{12}-\frac{11}{144}Y-\frac{215}{1728}Y^2 \\
\frac{11}{12}Y+\frac{1}{2}Y^2 & \\
-\left(\frac{11}{12}Y-\frac{143}{144}Y^2\right) & \\
\frac{215}{144}Y^2 &
\end{array}$$

We divided by y^3 *we find:*

$$A_4 = \frac{1}{12}, A_3 = -\frac{11}{144} \text{ and } A_2 = -\frac{215}{1728}.$$

(3) For the non-repeated quadratic factor that is: $x^2 + x + 2$ *which admits two complex roots:*

$$z_1 = \frac{-1+i\sqrt{7}}{2} \text{ and } z_2 = \frac{-1-i\sqrt{7}}{2}.$$

Multiplying the two members by x^2+x+2 *we find:*

$$\frac{2x+3}{(x-1)(x+2)^3} = ax+b+\left(x^2+x+2\right)\left[\frac{A_1}{x-1}+\frac{A_2}{x+2}+\frac{A_3}{(x+2)^2}+\frac{A_4}{(x+2)^3}\right]$$
$$x^2+x+2=0 \Rightarrow \triangle = -7 = i^2 7 \Rightarrow z_1 = \frac{-1-i\sqrt{7}}{2} \text{ and } z_1 = \frac{-1+i\sqrt{7}}{2}$$
$$\Rightarrow \lim_{x\to z_1} \frac{2x+3}{(x-1)(x+2)^3} = \lim_{x\to z_1} ax+b+\left(x^2+x+2\right)\left[\frac{A_1}{x-1}+\frac{A_2}{x+2}+\frac{A_3}{(x+2)^2}+\frac{A_4}{(x+2)^3}\right]$$
$$\Rightarrow \frac{2z_1+3}{(z_1-1)(z_1+2)^3} = az_1+b,$$
$$\Rightarrow \frac{-23+5i\sqrt{7}}{128} = a\left(\frac{-1+i\sqrt{7}}{2}\right)+b$$
$$\Rightarrow \begin{cases} \frac{a\sqrt{7}}{2} = \frac{5\sqrt{7}}{128} \\ -\frac{a}{2}+b = -\frac{23}{128} \end{cases} \Rightarrow a = \frac{5}{56} \text{ et } b = -\frac{9}{64}.$$

In the last example we use the parity of the function which is useful to eliminate some coefficients to better understand we give you the following example.

Example 18

$$f(x) = \frac{1}{x^6\left(x^2+1\right)} = \frac{a_1}{x}+\frac{a_2}{x^2}+\frac{a_3}{x^3}+\frac{a_4}{x^4}+\frac{a_5}{x^5}+\frac{a_6}{x^6}+\frac{a_7x+a_8}{x^2+1}.$$

$$f(-x) = f(x) \text{ (even),}$$

$\Rightarrow$

$$a_1 = a_3 = a_5 = a_7 = 0.$$

$\Rightarrow$

$$\frac{1}{x^6\left(x^2+1\right)} = \frac{a_2}{x^2}+\frac{a_4}{x^4}+\frac{a_6}{x^6}+\frac{a_8}{x^2+1}$$

$$\begin{aligned} a_8 &= \lim_{x\to i}\frac{1}{x^6} = -1. \\ a_6 &= \lim_{x\to 0}\frac{1}{\left(x^2+1\right)} = 1. \\ a_2+a_8 &= 0 \text{ (multiplying by } x^2 \text{and making tender } x\to+\infty) \\ &\Rightarrow a_2 = 1 \\ \text{For } x &= 1 \Rightarrow \frac{1}{2} = a_2+a_4+a_6+\frac{a_8}{2} \Rightarrow a_4 = -1. \end{aligned}$$

Another method for calculating coefficients of repeated linear factors: (The use of successive derivatives)

Example 19

$$\begin{aligned} G(x) &= \frac{1}{(x-1)^5 (x^2+1)} \\ &= \frac{a_1}{x-1} + \frac{a_2}{(x-1)^2} + \frac{a_3}{(x-1)^3} + \frac{a_4}{(x-1)^4} + \frac{a_5}{(x-1)^5} + \frac{a_6 x + a_7}{x^2+1} \end{aligned}$$

$\Rightarrow$

$h(x) = \frac{1}{(x^2+1)} = a_1 (x-1)^4 + a_2 (x-1)^3 + a_3 (x-1)^2 + a_4 (x-1) + a_5 + (x-1)^5 \left[\frac{a_6 x + a_7}{x^2+1}\right]$

$a_5 = \lim_{x \to 1} \frac{1}{(x^2+1)} = \frac{1}{2}$,

$a_4 = h'(1) = \left(\frac{-2x}{(x^2+1)^2}\right)(1) = -\frac{1}{2}$,

$2a_3 = h''(1) = \left(\frac{2x^2-2}{(x^2+1)^3}\right)(1) = 0$,

$6a_2 = h^{(3)}(1) = \left(\frac{-8x^3+4x}{(x^2+1)^4}\right)(1) = \frac{-1}{4}$,

and $24a_1 = h^{(4)}(1) = \left(\frac{40x^4-52x^2+4}{(x^2+1)^5}\right)(1) = -\frac{1}{4}$.

On the other hand:

$\lim_{x \to i} a_6 x + a_7 = \lim_{x \to i} \frac{1}{(x-1)^5}$ *(i is a root of* x^2+1*)*

$\Rightarrow i a_6 + a_7 = \frac{1}{8}(i+1)$

$\Rightarrow a_6 = \frac{1}{8}$ *and* $a_6 = \frac{1}{8}$.

Remarque 20 *Partial fraction decomposition or Partial fraction expansion is very useful in the course of integrals. aim calls*

Chapitre 2

Algebraic structures

The following concepts are of interest in terms of terminology and structure before approaching the study of vector spaces.

2.1 Definitions and properties

2.1.1 Closure law (Internal composition law or binary operation)

Let E and F be two non-empty sets and f an application of $E \times E$ in F. If $f(E \times E)$ is included in E, then f is a closure law on E. Let it be noted for each couple $(u, v) \in E \times E$ by:

$$u * v,\ u \triangle v \text{ or } u \perp v...$$

it is said that $*$ is a bianary operation on E.

$$\forall u, v \in E, u * v \in E.$$

Exemple 2.1 *Addition and multiplication are a closure laws in* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *and* $\mathbb{C}$ *but the subtraction is n't a closure law in* $\mathbb{N}$.

2.1.2 Commutative law

Let $*$ be a closure law in E, $*$ is called commutative in E if and only if:

$$\forall u, v \in E, u * v = v * u.$$

Example 21 *Intersection and union are commutative closure laws on all parts of a set.*

2.1.3 Associative law

Let $*$ be a closure law in E, $*$ is called associative in E if and only if:

$$\forall u, v, w \in E, u * (v * w) = (u * v) * w.$$

Example 22 *The composition of applications is an associative law.*

Example 23 *Let $*$ be a closure law in $\mathbb{Q}$ defined by:*

$$\forall x, y \in \mathbb{Q}; x * y = \frac{x + y}{2}.$$

Let $x, y, z \in \mathbb{Q}$,

$$x * (y * z) = x * \left(\frac{y + z}{2}\right) = \frac{x + \left(\frac{y+z}{2}\right)}{2} = \frac{x}{2} + \frac{y}{4} + \frac{z}{4},$$

and

$$(x * y) * z = \left(\frac{x + y}{2}\right) * z = \frac{\left(\frac{x+y}{2}\right) + z}{2} = \frac{x}{4} + \frac{y}{4} + \frac{z}{2},$$

so we have:

$$x * (y * z) \neq (x * y) * z,$$

wich implies that $*$ is n't associative in $\mathbb{Q}$.

2.1.4 Identity element (élément neutre)

Let $*$ be a closure law in E, e is called the identity element of E if and only if:

$$\forall u \in E, u * e = e * u = u.$$

In other words, the identity element is the element that does n't affect the law right and left.

In addition, the law is commutative, it suffices to show that:

$$\forall u \in E, u * e = u \text{ either } e * u = u.$$

Example 24 1 *is an identity element of multiplication in* $\mathbb{R}$.

2.1.5 Inverse or symmetric element

Let $*$ be a closure law in E and admitting an identity element e. It's said that u is the inverse of v for the law $*$ if and only if:

$$u * v = v * u = e.$$

It's noted v by u^{-1} or $(-u)$ knowing that power and minus are just symbols.

If, in addition, the law $*$ is commutative, all we need is:

$$u * u^{-1} = e \text{ either } u^{-1} * u = e.$$

Example 25 *The inverse of* x *in the addition is:* $(-x)$.

2.1.6 Regular element

It is said that $\blacksquare$ is a regular element for a closure law in E if it checks:

$$\forall u \in E, u * \alpha = v * \alpha \Rightarrow u = v.$$

Example 26 *For the addition in* $\mathbb{C}$*, all elements are regular.*

2.1.7 Distributive property

Let $*$ and $\triangle$ be two closure laws in E. Then $*$ is distributive to $\triangle$ if and only if:

$$\forall u, v, w \in E, u * (v \triangle w) = (u * v) \triangle (u * w)$$

and

$$(v \triangle w) * u = (v * u) \triangle (w * u).$$

If, besides, the law $*$ is commutative, it is enough to show one of the two equalities.

Example 27 *The multiplication is distributive by the addition in* $\mathbb{C}$.

2.1.8 Stable part

Let $*$ be a closure law in E. A part A is said to be stable of E for the law $*$, if:

$$\forall u, v \in A, u * v \in A \ (* \text{ is a closure law in } A).$$

Example 28 *The set of even natural integers is stable for addition, but the set of odd integers is not stable for addition because:*

$$3 + 5 = 8 \text{ is even.}$$

2.1.9 External composition law

Let be E, F, Ω three non-empty sets, and f an application of $\Omega \times E$ in F.

f is an external composition law on E to operators in Ω, if and only if:

$$\forall \alpha \in \Omega, u \in E \Rightarrow f(\alpha, u) \in E.$$

$f(\alpha, u)$ est souvent notée: $\alpha \cdot u$.

Example 29 *In the set of vectors the multiplication by a scalar is an external law.*

2.2 Structure of a group

2.2.1 Definition of a group

Définition 30 *A set* $(E, *)$ *is a group if one has the following properties:*

(1) $*$ *is a closure law in* E.

(2) $*$ *is associative in* E.

(3) E admits an identity element corresponds to $*$.

(4) Each element of E has an inverse to $*$.

If more $*$ is commutative then the group is said to be a commutative group or an abelian group.

Example 31 *$(\mathbb{Z}, +)$ is an abelian group.*

Example 32 *In $E =]-1; 1[$, we define $*$ by:*

$$\forall (a, b) \in E^2, a * b = \frac{a + b}{1 + ab}.$$

Show that $(E, *)$ is an abelian group.

(1) The commutativity:

$$\forall a, b \in E : a * b = \frac{a + b}{1 + ab} = \frac{b + a}{1 + ba} = b * a.$$

That is $*$ is commutative.

(2) Let's check that $*$ is a closure law in E.

Show that:

$$\forall a, b \in E, a * b \in E \Rightarrow \frac{a + b}{1 + ab} \in E =]-1; 1[$$

that is:

$$\forall (a, b) \in E^2, -1 < \frac{a + b}{1 + ab} < 1?$$

Let's calculate:

(a)

$$\begin{aligned} \frac{a + b}{1 + ab} - 1 &= \frac{a + b - 1 - ab}{1 + ab} \\ &= \frac{(1 - b)(a - 1)}{1 + ab} < 0 \text{ car: } b < 1 \text{ et } a < 1 \\ &\Rightarrow \frac{a + b}{1 + ab} < 1. \end{aligned}$$

(b) Same:

$$\begin{aligned}\frac{a+b}{1+ab}+1 &= \frac{a+b+1+ab}{1+ab}=\frac{(1+b)(1+a)}{1+ab}>0 \text{ car: } b>-1 \text{ et } a>-1\\ &\Rightarrow \frac{a+b}{1+ab}>-1.\end{aligned}$$

So,

$$\forall (a,b)\in E^2, a*b\in E,$$

which implies that $*$ is a closure law in E.

(3) Show that $*$ is an associative law?

$$\forall a,b,c\in E; (a*b)*c=a*(b*c)?$$

Let $a,b,c\in E$:

$$(a*b)*c=\frac{a+b}{1+ab}*c=\frac{\frac{a+b}{1+ab}+c}{1+\frac{a+b}{1+ab}.c}=\frac{a+b+c+abc}{1+ab+ac+bc},$$

and

$$a*(b*c)=a*\frac{b+c}{1+bc}=\frac{a+\frac{b+c}{1+bc}}{1+a.\frac{b+c}{1+bc}}=\frac{a+b+c+abc}{1+ab+ac+bc},$$

which implies that:

$$(a*b)*c=a*(b*c),$$

so $*$ is associative.

(4) The existence of the identity element? Show that:

$$\forall a\in E, a*e=a?$$

$$\begin{aligned}a*e &= a\Rightarrow \frac{a+e}{1+ae}=a\Rightarrow e=ea^2\\ &\Rightarrow e\left(1-a^2\right)=0, \forall a\in E\Rightarrow e=0.\end{aligned}$$

(5) The existence of the inverse element for each element $a\in E$?

a admits a symmetric element a^{-1} *if:*

$$\begin{aligned} a * a^{-1} &= e = 0 \Rightarrow \frac{a + a^{-1}}{1 + aa^{-1}} = 0 \\ &\Rightarrow a + a^{-1} = 0 \\ &\Rightarrow a^{-1} = -a \in E \text{ if } a \in E. \end{aligned}$$

Conclusion: $(E, *)$ *is an abelian group.*

2.2.2 Group Properties

The above definitions are derived from the following properties:

(1) (Uniqueness of identity element) The identity element of a group is unique.

Preuve: By absurdity supposing that they exist two identity elements e_1 and e_2 with $e_1 \neq e_2$,then:

$$e_1 * e_2 = e_1 \text{ because } e_2 \text{ is an identity element,}$$

and

$$e_1 * e_2 = e_2 \text{ because } e_1 \text{ is an identity element,}$$

then $e_1 = e_2$ (contradiction). ■

(2) (Uniqueness of inverse element) The symmetric of an element x is unique noted x^{-1}. With $x_1^{-1} \neq x_2^{-1}$.

Preuve: By absurdity supposing that they exist x_1^{-1} and x_2^{-1} two symmetrical elements of $x \in E$.

$$\begin{aligned} x * x_1^{-1} &= e \Rightarrow x_2^{-1} * \left(x * x_1^{-1}\right) = x_2^{-1} * e \\ &\Rightarrow \underbrace{\left(x_2^{-1} * x\right)}_{e} * x_1^{-1} = x_2^{-1} * e \text{ because } * \text{ is associative.} \\ &\Rightarrow e * x_1^{-1} = x_2^{-1} \Rightarrow x_1^{-1} = x_2^{-1} \text{(contradiction).} \end{aligned}$$

■

(3)

$$\begin{aligned}(a)e^{-1} &= e.\\ (b)\forall x &\in G; \left(x^{-1}\right)^{-1} = x.\\ (c)\forall x &\in G, \forall y \in G; (x*y)^{-1} = y^{-1}*x^{-1}.\end{aligned}$$

Preuve: We use the propritie:

$$\alpha * B = B * \alpha = e \Leftrightarrow \alpha = \beta^{-1} \text{ and } \beta = \alpha^{-1}.$$

(a)

$$e * e = e \Rightarrow e^{-1} = e. (\alpha = e, \beta = e)$$

(b)

$$\begin{aligned}\forall x &\in G, x * x^{-1} = x^{-1} * x = e\\ &\Rightarrow \left(x^{-1}\right)^{-1} = x. \left(\alpha = x, \beta = x^{-1}\right)\end{aligned}$$

(c)

$$\alpha = y^{-1} * x^{-1} \text{ and } \beta = x * y.$$

$$\begin{aligned}\forall x, y &\in G, (x*y) * \left(y^{-1} * x^{-1}\right) = x * \left(y * y^{-1}\right) * x^{-1}\\ &= x * e * x^{-1} = x * x^{-1} = e,\end{aligned}$$

and

$$\begin{aligned}\left(y^{-1} * x^{-1}\right) * (x*y) &= y^{-1} * \left(x^{-1} * x\right) * y\\ &= y^{-1} * e * y = y^{-1} * y = e.\end{aligned}$$

Then

$$(x*y)^{-1} = y^{-1} * x^{-1}.$$

■

2.2.3 Subgroup

Let $(G, *)$ be a group. A part H not empty of G provided with the law $*$ is called a subgroup if and only if:

(1) $e \in H$ (H contains the identity element).

(2) $\forall x, y \in H;\ x * y \in H$.(Closure law in H)

(3) $\forall x \in H, x^{-1} \in H$.

The last two properties can be written in one:

$$\forall x, y \in H; x * y^{-1} \in H.$$

Example 33 *The center of a group G is called the set defined by:*

$$C = \{x \in G \text{ such as: } \forall y \in G, x * y = y * x\}.$$

Elements that switch with all elements of G.

Show that $(C, *)$ is a subgroup of G.

(1) We have:

$$e \in G, \forall y \in G; y * e = e * y = y \Rightarrow e \in C.$$

(2) $\forall x_1, x_2 \in C, \forall y \in G$:

$$x_1 * x_2 \in G \text{ because } G \text{ is a group}$$

$$\begin{aligned}
(x_1 * x_2) * y &= x_1 * (x_2 * y) \ \textit{(associativity)}, \\
&= x_1 * (y * x_2) \ (x_2 \in C), \\
&= (x_1 * y) * x_2 \ \textit{(associativity)}, \\
&= (y * x_1) * x_2 \ (x_1 \in C), \\
&= y * (x_1 * x_2) \ \textit{(associativity)}, \\
&\Rightarrow x_1 * x_2 \in C.
\end{aligned}$$

(3) $\forall x \in C, x^{-1} \in C$.

$$\begin{aligned}
\forall x &\in C, \forall y \in G, x^{-1} * y = \left(y^{-1} * x\right)^{-1} \\
&= \left(x * y^{-1}\right)^{-1} \left(\textit{because } x \in C, y^{-1} \in G\right) \\
&= y * x^{-1} \Rightarrow x^{-1} \in C.
\end{aligned}$$

Conclusion: $(C, *)$ *is a subgroup of* G.

2.2.4 Subgroups Properties

(1) The intersection of subgroups is a subgroup.

(2) The union is not a subgroup.

2.2.5 Homomorphisms

Définition 34 *Let* $(G, *)$ *and* $(G', \triangle)$ *be groups, a homomorphism* f *from* $(G, *)$ *to* $(G', \triangle)$ *is an application:*

$$\begin{aligned}
f &: G \to G' \\
x &\mapsto f(x) = x',
\end{aligned}$$

such as:

$$\forall x, y \in G, f(x * y) = f(x) \triangle f(y).$$

Example 35

$$\begin{aligned} f &: \left(\mathbb{R}_+^*, \times\right) \to (\mathbb{R}, +) \\ x &\mapsto f(x) = \ln x, \end{aligned}$$

is a homomorphism.

Lemme 1 *If f is a homomorphism from $(G, *)$ to $(G', \triangle)$ so:*

$$f(e_G) = e_{G'}.$$

On the other hand:

$$\forall x \in G; [f(x)]^{-1} = f(x^{-1}).$$

Preuve:

$$\forall x \in G, f(x) \triangle f(e_G) = f(x * e_G) = f(x) \Rightarrow f(e_G) = e_{G'}.$$

And,

$$f(x) \triangle f(x^{-1}) = f\left(x * x^{-1}\right) = f(e_G) = e_{G'} \Rightarrow f(x^{-1}) = [f(x)]^{-1}.$$

■

Définition 36 *If f is a homomorphism of groups and bijective, it is called an isomorphism. In this case we use the notation: $f : G \xrightarrow{\sim} G'$ or $G \cong G'$.*

Définition 37 *If f is a isomomorphism of groups from G to G', it is called an automorphism.*

2.2.6 The kernel and the image of homomorphism

(1) We call the kernel of homomorphism $f : G \to H$ the subset of G defined by:

$$\ker f = f^{-1}(e_H) = \{x \in G / f(x) = e_H\}.$$

(2) We call the kernel of homomorphism $f : G \to H$ the subset of H defined by:

$$\mathrm{Im}(f) = f(G) = \{f(x) / x \in G\}.$$

Proposition 38 *A homomorphism $f : G \to H$ is:*

(1) Injective if and only if $\ker f = \{e_G\}$.

(2) Surjective if and only if $\mathrm{Im}(f) = H$.

2.3 Rings structures

Let A be a set with two laws of internal compositions $*$ and $\triangle$and then $(A, *, \triangle)$ is a ring if and only if:

(1) $(A, *)$ is an abelian group, where the identity element is noted 0_A.

(2) $\triangle$ has a identity element noted 1_A.

(3) $\triangle$ is associative.

(4) The law $\triangle$ is distributive right and left on the law $*$.

If the law $\triangle$ is commutative, the ring is commutative.

2.3.1 Subrings

Définition 39 *Part B of the ring $(A, *, \triangle)$ is called a subring of A if and only if:*

(1) $1_A \in B$.

(2) $\forall a, b \in B, a * b^{-1} \in B$.

(3) $\forall a, b \in B, a \triangle b \in B$.

2.3.2 Homomorphism rings

Définition 40 *Let A, B be two rings. An application $f : (A, *, \triangle) \to (B, *, \triangle)$ is homomorphism rings if the following conditions are met:*

(1) $f(1_A) = 1_B$.

(2) $\forall a, b \in B, f(a * b) = f(a) * f(b)$.

(3) $\forall a, b \in B, f(a \triangle b) = f(a) \triangle f(b)$.

If moreover f is bijective, it is said to be an isomorphism rings.

Définition 41 *A ring* $(A, *, \triangle)$ *is an integer ring if the equation* $a \triangle b = 0_A$ *results* $a = 0_A$ *or* $b = 0_A$.

2.4 Fields

2.4.1 Symmetric element

Définition 42 *An element* $x \in K$ *has a symmetric with respect to the law* $\triangle$ *if there is an element* $y \in K$ *such that:*

$$x \triangle y = y \triangle x = e_2 \, , (e_2 \text{ is the identity element of } \triangle) \, .$$

Remarque 43 *The definition of the invertible element is the same as the symmetric element except the first is for the 2nd law noted* $(-x)$*, and the symmetric is for the 1st law noted* $\left(x^{-1}\right)$.

2.4.2 Definition of field

Définition 44 *It is said that* $(\mathbb{k}, *, \triangle)$ *is a field if and onlu if:*
(1) $(\mathbb{k}, *, \triangle)$ *is a ring.*
(2) Any element other than e_1 *(the identity element for the operation* $*$*) has a symmetric for the law* $\triangle$*. If* $\triangle$ *is commutative then* $\mathbb{k}$ *is a commutative field.*

Example 45 $(\mathbb{R}, +, \times)$ *is a commutative field but* $(\mathbb{Z}, +, \times)$ *is n't a field.*

2.4.3 Subfield

Définition 46 *A part* L *of a field* $\mathbb{k}$ *is a subfield of* $\mathbb{k}$ *if* L *is a subring of* $\mathbb{k}$.

Chapitre 3

Vector spaces

3.1 Introduction

On the vectors, in the sense of elementary geometry, that is to say as they are encountered in elementary physics, we could define two types of operation that give as a result a vector: addition and multiplication by a scalar. In this chapter, we will generalize these notions by giving them a more abstract scope, therefore broader.

3.2 Definition of a vector space

Définition 47 *A vector space E over a commutative field $\mathbb{k}$ (especially note $\mathbb{R}$ or $\mathbb{C}$) is a nonempty set on which two binary operations can be defined on the elements of E (called vectors) that check the following properties:*

I- ***A binary operation, the addition (noted $+$)*** *which verifies:*

$(E, +)$ *is an abelian group.*

II- An external composition law, the multiplication of a vector by a scalar of $\mathbb{k}$*:*

This external law (product noted .) has the following properties:

$\forall \alpha,\ \beta \in \Bbbk,\ \forall u, v \in E$:

$(1)\alpha.\left(u+v\right)=\left(\alpha.u\right)+\left(\alpha.v\right)$ *(distributivity of a scalar on E).*

$(2)\left(\alpha+\beta\right).u=\left(\alpha.u\right)+\left(\beta.u\right)$ *(distributivity of a vector on* $\Bbbk$*).*

$(3)\alpha.\left(\beta.u\right)=\left(\alpha\times\beta\right).u.$

$(4)1_{\Bbbk}.u=u$ *(*$1_{\Bbbk}$ *is the identity element of* $\Bbbk$*).*

Remarque 48 *We note in the passage of the property* (3) *that in the first member the two multiplications are external that is to say between a scalar and a vector against in the second member the first is between two scalars (noted:* $\times$*) and the second and between a scalar and a vector (noted: .).*

Example 49 *The following sets have vector space structures on* $\mathbb{R}$ *(optionally on* $\mathbb{C}$*).*

(1) The set $\mathbb{R}^n, n \geq 1(\mathbb{R}, \mathbb{R}^2, \mathbb{R}^3, ...)$.

(2) The set of the real or complex sequences.

(3) The set of continuous functions over an interval I*.*

(4) The set of polynomials with one variable, of degree less than or equal to n*.*

(5) The set of polynomials to one variable, of degree equal to $n \in \mathbb{N}^*$*, is n't a vector space because the null polynomial (the identity element) is n't of degree* n*.*

3.3 Immediate properties of operations in a vector space

Note that in vector spaces we can write αu instead of $\alpha.u$, to simplify the notions.

Properties 1 *From the axioms of the definition of a vector space, the following properties result:*

(1) $\forall u \in E,\ 0.u = 0_E$. *(*$0_E$ *is the identity element of* E *which is the zero vector).*

(2) $\forall \alpha \in \Bbbk, \alpha.0_E = 0_E$.

(3) $\forall \alpha \in \Bbbk, \forall u \in E, \alpha u = 0_E \Longrightarrow \alpha = 0$ *or* $u = 0_E$.

(4) $\forall u \in E, (-1)\, u = -u$.

(5) $\forall\left(\alpha,\beta\right) \in \Bbbk^2, \forall u \in E - \{0_E\} : \alpha u = \beta u \Rightarrow \alpha = \beta$.

(6) $\forall \alpha \in \Bbbk^*, \forall\left(u,v\right) \in E^2 : \alpha u = \alpha v \Rightarrow u = v$.

3.4 Subspaces

Définition 50 *Vector subspace (abbreviated notation: s.e.v) of a vector space E, on a field $\mathbb{k}$, is any part of E that has the vector space structure on $\mathbb{k}$. Otherwise a non-empty part F of a vector space E is a subspace of E, it is necessary and sufficient that any combination of two vectors of F be a vector of F, ie:*

$$\begin{aligned} &(1) F \neq \varnothing, \\ &(2) \forall u, v \in F, u + v \in F, \\ &(3) \forall \alpha \in \mathbb{k}, \forall u \in F, \alpha u \in F. \end{aligned} \tag{3.1}$$

Or,

$$\begin{aligned} &(1) F \neq \varnothing, \\ &(2) \forall \alpha, B \in \mathbb{k}; \forall u, v \in F, \alpha u + \beta v \in F. \end{aligned}$$

Proposition 51 *If F is a subspace of E then it contains the identity element of E.*

Preuve: *F is a subspace of E, then:*

$$\begin{aligned} F \neq \emptyset &\Rightarrow \exists u \in F \\ &\Rightarrow \text{ if } \alpha = 0 \text{ for } (3) \text{ of (3.1) } 0.u = 0_E \in F. \end{aligned}$$

■

Remarque 52 *So according to the proposition 51 to show that $F \neq \emptyset$ is more convenient to see the identity element because if $O_E \notin F$ then F is n't a subspace of E.*

Some useful examples of identity elements are given:

(1) 0 is the identity element of $\mathbb{R}$.

(2) $(0,0)$ is the identity element of $\mathbb{R}^2$.

(3) $(0,0,0)$ is the identity element of $\mathbb{R}^3$.

(4) The null polynomial is the identity element of the set of polynomials.

(5) The null sequence is the identity element of the set of sequences.

(6) The null function is the identity element of the set of functions.

Examples 53 *(1)The set of convergent sequences is a subspace of all real or complex sequences. Because:*

a) The null sequence converge to zero.

b) The sum of two two converging sequences is a converge sequence.

c) The multiplication of a scalar and a converge sequence is a converge sequence.

(2) The set of divergent sequences is n't a subspace of all real or complex sequences because, the null sequence hwo is the identity element of the set of sequences is n't divergent sequence.

(3) $A=\left\{(x,y,z)\in\mathbb{R}^3;x=y=z\right\}$ *is a subspace of* $\mathbb{R}^3$*, because:*

$$A=\left\{(x,x,x)\in\mathbb{R}^3;x\in\mathbb{R}\right\}.$$

$$a)\ \ (0,0,0)\in A\Rightarrow A\neq\varnothing.$$

$$b)\ \forall u_1\left(x_1,x_1,x_1\right),u_2\left(x_2,x_2,x_2\right)\in A,$$

$$u_1+u_2=_1\left(\underbrace{x_1+x_2}_{X},\underbrace{x_1+x_2}_{X},\underbrace{x_1+x_2}_{X}\right)\in A.$$

$$c)\ \forall\alpha\in\mathbb{R},\forall u\left(x;x;x\right)\in A,$$

$$\alpha u=_1\left(\underbrace{\alpha x}_{X},\underbrace{\alpha x}_{X},\underbrace{\alpha x}_{X}\right)\in A.$$

(4) $B=\left\{(x,y,1)\in\mathbb{R}^3\right\}$ *is n't a subspace of* $\mathbb{R}^3$*, because:*

$$(x,y,1)\in B\ \textit{but}\ 3\left(x,y,1\right)=(3x,3y,3)\notin B.$$

Or say:

$$\textit{The identity elemnt of}\ \mathbb{R}^3,(0,0,0)\notin B,$$

implies that B *is n't a subspace of* $\mathbb{R}^3$.

3.5 Intersection and union of two vector subspaces

proposition 3.1 *The intersection of two vector subspaces (and therefore a finite number) of E is a subspace of E.*

Preuve: Let F and G be two vector subspaces of E then:

$$(1)0_E \in F \text{ and } 0_E \in G,$$

we use the uniqueness of the identity elemnt of E.So,

$$0_E \in F \cap G \Rightarrow F \cap G \neq \varnothing.$$

$$(2)\forall u, v \in F \cap G \Rightarrow u, v \in F \text{ and } u, v \in G,$$

then:

$$u + v \in F \text{ and } u + v \in G$$

because F and G are subspaces of E, wich implies that:

$$u + v \in F \cap G.$$

$$\begin{aligned} (3)\forall \alpha \quad &\in \quad \Bbbk, \forall u \in F \cap G \Rightarrow u \in F \text{ and } u \in G \\ &\Rightarrow \quad \alpha u \in F \text{ and } \alpha u \in G \\ &\Rightarrow \quad \alpha u \in F \cap G. \end{aligned}$$

Conclusion: $F \cap G$ is a subspace of E.

■

proposition 3.2 *The union of two vector subspaces of E is not necessarily a subspace of E.*

Example 54 *Let $A = \{(x, 0), x \in \mathbb{R}\}$ and $B = \{(0, y), y \in \mathbb{R}\}$ be two subspaces of $\mathbb{R}^2$ bacause we have for A :*

(1) $(0,0) \in A \Rightarrow A \neq \emptyset$.

(2) $\forall u, v \in A$:

$$u = (a,0) \ \ and \ v = (b,0) \Rightarrow u + v = (a+b,0) \in A.$$

(3) $\forall \alpha \in \mathbb{R}, \forall u \in A$:

$$u = (a,0) \Rightarrow \alpha u = (\alpha a, 0) \in A.$$

Conclusion: A is a subspace $\mathbb{R}^2$.

for B :

(1) $(0,0) \in B \Rightarrow B \neq \emptyset$.

(2) $\forall u, v \in B$:

$$u = (0,a) \ \ and \ v = (0,b) \Rightarrow u + v = (0,a+b) \in B.$$

(3) $\forall \alpha \in \mathbb{R}, \forall u \in B$:

$$u = (0,a) \Rightarrow \alpha u = (0, \alpha a) \in B.$$

Conclusion: B is a subspace $\mathbb{R}^2$.

So,

$$u = (1,0) \in A \subset A \cup B \ \ and \ v = (0,1) \in B \subset A \cup B,$$

but,

$$u + v = (1,1) \notin A \cup B,$$

then: $A \cup B$ is n't a subspace of $\mathbb{R}^2$.

3.6 Basis and dimension

3.6.1 Linear dependence - Linear independence

The following definitions are of major importance of the theory.

Définition 55 *A family $(v_i)_{1 \leq i \leq n}$ of vectors of a vector $\mathbb{k}$-space $(E, +, .)$ is said to be linearly*

dependent if they exist $\lambda_1, \lambda_2, ..., \lambda_n \in \mathbb{k}$ *not all null such as:*

$$\boxed{\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n = 0_E.}$$

In the contrary if:

$$\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n = 0_E,$$

implies that:

$$\lambda_1 = \lambda_2 = ... = \lambda_n = 0, \textit{(The unique solution)}$$

so the family $(v_i)_{1 \leq i \leq n}$ *is called linearly independent.*

Example 56 *In* $E = \mathbb{R}_2[x]$*, (the vector space of polynomial functions of degree less than or equal to* 2 *and with real coefficients) , the vectors* f_1, f_2, f_3 *defined for all* $x \in \mathbb{R}$ *by:*

$$f_1(x) = x^2 + 1, f_2(x) = x^2 - 1 \text{ and } f_3(x) = x^2 \text{ are dependent,}$$

because if $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ *such as:*

$$\begin{aligned}
&\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 = 0 \Rightarrow \lambda_1 \left(x^2 + 1\right) + \lambda_2 \left(x^2 - 1\right) + \lambda_3 x^2 = 0, \\
&\Rightarrow (\lambda_1 + \lambda_2 + \lambda_3) x^2 + (\lambda_1 - \lambda_2) = 0, \forall x \in \mathbb{R}, \\
&\Rightarrow \begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ \lambda_1 - \lambda_2 = 0 \end{cases} \Rightarrow \lambda_1 = \lambda_2 = -\tfrac{\lambda_3}{2},
\end{aligned}$$

which gives an infinity of solutions $\left(-\frac{\lambda_3}{2}, -\frac{\lambda_3}{2}, \lambda_3\right)$*, with* λ_3 *an arbitrary real.*

Example 57 *In* $\mathbb{R}^3$*, the vectors* $u_1 = (0, 1, 3), u_2 = (2, 0, -1)$ *and* $u_3 = (2, 0, 1)$ *are indepen-*

dent because:

$$\begin{aligned}
&\lambda_1 u_1 + \lambda_2 u_2 + \lambda_3 u_3 = (0,0,0) \\
&\Rightarrow \lambda_1 (0,1,3) + \lambda_2 (2,0,-1) + \lambda_3 (2,0,1) = (0,0,0) \\
&\Rightarrow (0 + 2\lambda_2 + 2\lambda_3, \lambda_1 + 0 + 0, 3\lambda_1 - \lambda_2 + \lambda_3) = (0,0,0) \\
&\Rightarrow \begin{cases} 2\lambda_2 + 2\lambda_3 = 0 \\ \lambda_1 = 0 \\ 3\lambda_1 - \lambda_2 + \lambda_3 = 0 \end{cases} \\
&\Rightarrow \begin{cases} \lambda_2 + \lambda_3 = 0 \\ -\lambda_2 + \lambda_3 = 0 \end{cases} \Rightarrow \begin{cases} \lambda_2 = -\lambda_3 \\ \lambda_2 = \lambda_3 \end{cases} \\
&\Rightarrow \lambda_3 = 0 \\
&\Rightarrow \lambda_1 = \lambda_2 = \lambda_3 = 0,
\end{aligned}$$

3.6.2 Linear combinations

Définition 58 *A vector v is called a linear combination of the vectors $v_1, v_2, ..., v_n$ if it can be expressed in the form*

$$v = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n,$$

where $\alpha_i, 1 \leq i \leq n$ are scalars.

Example 59 *Let v_1, v_2, v_3 be a vectors of $\mathbb{R}^3$ defined by $v_1 = (0,1,3), v_2 = (2,0,-1)$ and $v_3 = (2,0,1)$, so for example if we calculate:*

$$2v_1 - 3v_2 + 4v_3 = 2(0,1,3) - 3(2,0,-1) + 4(2,0,1) = (2,2,13),$$

then the vector $v = (2,2,13)$ is a linear combination of the vectors v_1, v_2 and v_3.

3.6.3 Spanning (generating)

Définition 60 *Let the vector family $\{v_1, v_2, ..., v_n\}$ of a $\mathbb{k}$-vector space $(E, +, .)$. Then the subset noted*

$$\langle v_1, v_2, ..., v_n \rangle = \{\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n / \alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{k}\},$$

is said the subspace of E spanned by $\{v_1, v_2, ..., v_n\}$ and we write

$$E = span\{v_1, v_2, ..., v_n\} = \langle v_1, v_2, ..., v_n \rangle.$$

This writing means

$$\forall v \in E, \exists \alpha_1, \alpha_2, ..., \alpha_n \in \Bbbk \text{ such as: } v = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n.$$

Example 61 *$\mathbb{R}^2$ is it spanned by $u = (2, 3)$ and $v = (-1, 5)$?*

$$\mathbb{R}^2 = span\{u, v\} = \langle u, v \rangle ?$$

$$\begin{aligned} \forall w \quad &\in \quad \mathbb{R}^2, \exists \alpha_1, \alpha_2 \in \mathbb{R} \text{ such as: } w = (x, y) = \alpha_1 u + \alpha_2 v ? \\ &\Rightarrow \quad (x, y) = \alpha_1 (2, 3) + \alpha_2 (-1, 5) = (2\alpha_1 - \alpha_2, 3\alpha_1 + 5\alpha_2) \\ &\Rightarrow \quad \begin{cases} 2\alpha_1 - \alpha_2 = x ...(1) \\ 3\alpha_1 + 5\alpha_2 = y ...(2) \end{cases} \Rightarrow \begin{cases} 5 \times (1) + (2) \Rightarrow \alpha_1 = \frac{5x+y}{13} \\ -3 \times (1) + 2 \times (2) \Rightarrow \alpha_2 = \frac{-3x+2y}{13} \end{cases} , \end{aligned}$$

so (α_1, α_2) exists for all $(x, y) \in \mathbb{R}^2$. Finally

$$\mathbb{R}^2 = span\{u, v\}.$$

Théorème 62 *Let $F = \{v_1, v_2, ..., v_n\}$ and $G = \{w_1, w_2, ..., w_m\}$ be two sets od vectors in a vector space E. Then*

$$span(F) = span(G)$$

if and only if each vector in F is a linear combination of those in G and conversely each vector in G is a linear combination of those in F.

3.6.4 Basis

Définition 63 *A subset $B = \{v_1, v_2, ..., v_n\}$ of a $\Bbbk$-vector space $(E, +, .)$ is called a basis of E if B is lineary independent and every element of E is a linear combination of elements of B*

$(E = span(B))$.

Example 64 *It is easy to check that* $B = \{u, v, w\}$ *with* $u = (2, 3, 0)$, $v = (1, -1, 1)$ *and* $w = (-1, 3, 5)$ *is a basis of* $\mathbb{R}^3$.

1) $\{u, v, w\}$ *are linearly independent.or*

2) $\mathbb{R}^3 = span\{u, v, w\}$.

Remarque 65 *In vector spaces there is what is called the canonical or standard basis of space, for example:*

(1) $\{(1, 0), (0, 1)\}$ *is the canonical basis of* $\mathbb{R}^2$.

(2) $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ *is the canonical basis of* $\mathbb{R}^3$.

(3) $\left\{1, X, X^2, ..., X^n\right\}$ *is the canonical basis of* $\mathbb{R}_n[X]$ *: set of polynomials of degree less than or equal to n.*

Invariance of Basis Size

Théorème 66 *If* $\{v_1, v_2, ..., v_n\}$ *and* $\{w_1, w_2, ..., w_m\}$ *are two basis of a vector space K over a field* $\mathbb{k}$*, then* $n = m$.

Preuve: By absurdity we suppose that $n < m$. Consider the set $\{w_1, v_1, v_2, ..., v_n\}$. w_1 is a linear combination of the v's because the v's span E. The fact that

$$w_1 = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n \text{ with } \alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{k},$$

such as not all α's are 0. Then $\{w_1, v_2, ..., v_n\}$ spans E. By the same technique if we add w_2 we find $\{w_1, w_2, v_3, ..., v_n\}$ spans E. Continuing in this way, we see that $\{w_1, w_2, ..., w_n\}$ spans E, so w_{n+1} is a linear combination of $w_1, w_2, ..., w_n$, wich implies that $\{w_1, w_2, ..., w_m\}$ is not linearly independent. Contradiction. ■

3.6.5 Dimension of a vector space

Définition 67 *The dimension of a vector space E is the number of vectors that form the basis of E; in this case E is called finite-dimentional. In other words the finite dimension n of a vector space E, is the maximum number of vectors that can contain a independent system*

extracted from E, and note $\dim E = n$.

If the number of elements of a free system of E is not limited, it is said that E is of infinite-dimensional for example the vector space of functions defined in $(-\infty, \infty)$.

We take by convention: $\dim(\{0_E\}) = 0$.

Example 68

$\dim \mathbb{R}^n = n.$
$\dim \mathbb{R}_n[x] = n+1,$

such as: $\mathbb{R}_n[x]$ is the set of polynomials of less than or equal to n.

Proposition 69 *To show that the vector family $F = \{v_1, v_2, ..., v_n\}$ of a $\mathbb{k}$-vector space $(E, +, .)$ is a base of E, knowing that* $\dim E = n = cardF$*(number of vectors), then it is enough to show that$\{v_1, v_2, ..., v_n\}$ is either linearly independent or spans E.*

Example 70 *In $\mathbb{R}^3$, the vectors $u = (1,3,1)$, $v = (4,2,1)$ and $w = (0,0,5)$ are a basis of $\mathbb{R}^3$, just show that $\{u, v, w\}$ are independent because* $\dim \mathbb{R}^3 = 3$ *and we have three vectors:*

$$\lambda_1 u + \lambda_2 v + \lambda_3 v = (0,0,0) \Rightarrow \lambda_1(1,3,1) + \lambda_2(4,2,1) + \lambda_3(0,0,5) = (0,0,0)$$
$$\Rightarrow (\lambda_1 + 4\lambda_2, 3\lambda_1 + 2\lambda_2, 5\lambda_3) = (0,0,0)$$
$$\Rightarrow \begin{cases} \lambda_1 + 4\lambda_2 = 0 ...(1) \\ 3\lambda_1 + 2\lambda_2 = 0 ...(2) \\ \lambda_3 = 0, \end{cases}$$
$$[3 \times (1)] - (2) \Rightarrow 10\lambda_2 = 0 \Rightarrow \lambda_1 = \lambda_2 = \lambda_3 = 0,$$

then $\{u, v, w\}$ are independent, so a basis of $\mathbb{R}^3$.

Théorème 71 *If E is a vector space with a basis $\{v_1, v_2, ..., v_n\}$, then:*

(1) Every set with more than n vectors is linearly dependent.

(2) No set with fewer than n vectors spans E.

Exemple 3.1 *Are the following sets bases?*

(1) $A = \{(2,1), (3,-1), (4,5)\}$.

A is n't basis of $\mathbb{R}^2$ *because:*

$$cardA = 3 > 2 = \dim \mathbb{R}^2 \textit{(A is dependent).}$$

(2) $B = \{(2,1,0),(3,-1,4)\}$.
B n'est plus une base de $\mathbb{R}^3$ *car:*

$$cardB = 2 < 3 = \dim \mathbb{R}^3 \textit{(A is n't spans } \mathbb{R}^3\textit{).}$$

Proposition 72 *If E is a vector space with a basis* $\{v_1, v_2, ..., v_n\}$*, and F is a subspace of E then:*

$$\boxed{F \subset E \Rightarrow \dim F \leq \dim E.}$$

Moreover, if

$$\dim F \leq \dim E \Rightarrow F = E.$$

3.6.6 Rank of a vector system

Définition 73 *The rank, or dimension, of a vector system* $F = \{u_1, u_2, ..., u_p\}$ *in E, such as* $\dim E = n$*, is equal the maximal number of linearly independent vectors in this system, noted* $rankF$ *or* rkF*, such as* $rankF \leq n$.

Example 74 $F = \{u_1, u_2, u_3\}$ *with* $u_1 = (1,2), u_2 = (2,3), u_3 = (6,7)$. *Since the vectors are in* $\mathbb{R}^2$*, then:*

$$1 \leq rangF \leq 2.$$

The vector u_3 *is depending with* u_1 *and* u_2 *because:*

$$cardF = 3 > 2 = \dim \mathbb{R}^2,$$

so,

$$\lambda_1 u_1 + \lambda_2 u_2 = (0,0) \Rightarrow \lambda_1 (1,2) + \lambda_2 (2,3) = (0,0)$$
$$\Rightarrow (\lambda_1 + 2\lambda_2, 2\lambda_1 + 3\lambda_2) = (0,0)$$
$$\Rightarrow \begin{cases} \lambda_1 + 2\lambda_2 = 0 ... (1) \\ 2\lambda_1 + 3\lambda_2 = 0 ... (2) \end{cases}$$
$$[2 \times (1)] - (2) \Rightarrow \lambda_2 = 0 \Rightarrow \lambda_1 = 0,$$

then $\{u_1, u_2\}$ *is independent, wich implies that* $rangF = 2$.

3.7 Sum of vector subspaces - Direct sums

3.7.1 Sum of vector subspaces

Définition 75 *Let* F *and* G *be two subspaces of* E*, the sum of* F *and* G *is defined by:*

$$\boxed{F + G = \{v \in E \text{ such as: } v = u + w \text{ with } u \in F \text{ and } w \in G\}.}$$

E *is said to be the sum of* F *and* G *if each vector* v *of* E *has at least on expression*

$$v = u + w, u \in F \text{ and } w \in G.$$

In this case we write: $E = F + G$.

Example 76 *Let* $A = \{(x, 0), x \in \mathbb{R}\}$ *and* $B = \{(0, y), y \in \mathbb{R}\}$*, then:*

$$\mathbb{R}^2 = A + B.$$

3.7.2 Direct sums (supplementary subspaces)

Définition 77 *Two subspaces* F *and* G *of a vector space* E *are supplementary subspaces, or supplement of each other, if they are independent and generate* E *. In this case it is also said that:* E *is the direct sum of* F *and* G *, written*

$$\boxed{E = F \oplus G,}$$

if every vector $v \in E$ has the unique expression

$$v = u + w, u \in F \text{ and } w \in G.$$

Lemme 2 *Let E be a vector space, $F, G \subseteq E$ subspaces. Then $E = F \oplus G$ if and only if*
(i) $E = F + G$
(ii) $F \cap G = \{0_E\}$.

Preuve: " $\Rightarrow$ "(i) Since $v \in E$, so $v = u + w, u \in F$ and $w \in G$ (uniquely) and we have

$$F \subseteq E \text{ and } G \subseteq E \Rightarrow F + G \subseteq E.$$

(ii) $\{0_E\} \subset F \cap G$ and if

$$\begin{aligned} v &\in F \cap G \Rightarrow v \in F \text{ and } v \in G \\ &\Rightarrow v = v + 0_E \text{ (where } v \in F, 0_E \in G) \text{ and } v = 0_E + v \text{(where } 0_E \in F, v \in G) \end{aligned}$$

But the expression $v = u + w$ is unique, hence $v = 0_E$.
" $\Leftarrow$ " Since $v = u + w$, we must only check uniqueness. So suppose by absurdity that:

$$\begin{aligned} v &= u_1 + w_1 \text{ and } v = u_2 + w_2 \text{ with } u_1, u_2 \in F \text{ and } w_1, w_2 \in G \\ &\Rightarrow u_1 + w_1 = u_2 + w_2 \\ &\Rightarrow \underbrace{u_1 - u_2}_{\in F} = \underbrace{w_2 - w_1}_{\in G} \\ &\Rightarrow u_1 - u_2 = w_2 - w_1 = 0_E \text{ because } F \cap G = \{0_E\}. \\ &\Rightarrow u_1 = u_2 \text{ and } w_2 = w_1 \\ &\Rightarrow v \text{ has a unique expression.} \end{aligned}$$

■

Exemple 3.2 *In* $\mathbb{R}$:

$$F = \{(x, y, z) ; x = y = z\} \text{ and } G = \{(x, y, 0) ; x, y \in \mathbb{R}\},$$

are supplementary subspaces ($\mathbb{R}^3 = F \oplus G$). *Indeed:*

(1) We have $\mathbb{R}^3 = F + G$ *because:*

a) $F \subset \mathbb{R}^3$ *and* $G \subset \mathbb{R}^3 \Rightarrow F + G \subset \mathbb{R}^3$.

b) $\forall u \in \mathbb{R}^3$,

$$\begin{aligned} u &= (x, y, z) = (z, z, z) + (x - z, y - z, 0) \in F + G \\ &\Rightarrow \mathbb{R}^3 \subset F + G. \end{aligned}$$

(2) $F \cap G = \{0_E\}$ *because:*

a)

$$\begin{aligned} 0_E &\in F \text{ and } 0_E \in G \text{ because } F \text{ and } G \text{ are subspaces of } E \\ &\Rightarrow 0_E \in F \cap G \Rightarrow \{0_E\} \subset F \cap G. \end{aligned}$$

b)

$$\begin{aligned} \text{If } u &\in F \cap G \Rightarrow u \in F \text{ and } u \in G \\ &\Rightarrow u = (x, x, x) \text{ and } u = (\alpha, \beta, 0) \\ &\Rightarrow \alpha = \beta = x = y = 0 \\ &\Rightarrow u = (0, 0, 0) \Rightarrow F \cap G \subset \{0_E\}. \end{aligned}$$

Conclusion: $\mathbb{R}^3 = F \oplus G$.

3.7.3 Relationship between dimension and direct sums

proposition 3.3 *In spaces of finite dimensions the formula is:*

$$\boxed{\dim(F + G) = \dim F + \dim G - \dim(F \cap G).}$$

In the case of the direct sum: $F \cap G = \{0_E\}$, *hence:*

$$\boxed{\dim(F \oplus G) = \dim F + \dim G.}$$

Finally, to show that vector subspaces of finite dimensions are supplementary subspaces in E, we have:

$$\boxed{E = F \oplus G \Leftrightarrow \begin{cases} \dim E = \dim F + \dim G \\ \text{and} \\ F \cap G = \{0_E\}. \end{cases}}$$

Example 78 *In $\mathbb{R}^3$the two subspaces :*

$$F = \{(x, y, z) ; x = y = z\} \text{ and } G = \{(x, y, 0) ; x, y \in \mathbb{R}\}, \text{ are supplementary.}$$

Indeed:

$$\begin{aligned} &\text{(1) } \forall u \in F, u = (x, x, x) = x(1, 1, 1) \\ &\Rightarrow \{(1, 1, 1)\} \text{ is a basis of } F \Rightarrow \dim F = 1. \\ &\text{(2) } \forall v \in G, v = (x, y, 0) = x(1, 0, 0) + y(0, 1, 0) \\ &\Rightarrow \{(1, 0, 0), (0, 1, 0)\} \text{ spans } G\text{,more:} \\ &\alpha(1, 0, 0) + \beta(0, 1, 0) = 0 \Rightarrow \alpha = \beta = 0 \\ &\Rightarrow \{(1, 0, 0), (0, 1, 0)\} \text{ is independent so a basis of } G, \\ &\Rightarrow \dim G = 2 \\ &\Rightarrow \dim \mathbb{R}^3 = \dim F + \dim G = 3. \end{aligned}$$

The rest of the proof is already done.

3.7.4 Another definition of direct sum

Lemme 3 *Let E be a vector space, $F, G \subseteq E$ subspaces. If B_F is a basis of F and B_G is a basis of G Then $E = F \oplus G$ if and only if the set of vectors formed by the combination of B_F and B_G vectors is a basis of E.*

Example 79 *In $\mathbb{R}^3$the two subspaces :*

$$F = \{(x, y, z) ; x = y = z\} \text{ and } G = \{(x, y, 0) ; x, y \in \mathbb{R}\}, \text{ are supplementary in } \mathbb{R}^3.$$

$$B_1 = \{(1, 1, 1)\} \text{ is a basis of } F \text{ and } B_2 = \{(1, 0, 0), (0, 1, 0)\},$$

so for,

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

since $cardB = 3 = \dim \mathbb{R}^3$,*it is sufficient toshow that* $\{u,v,w\}$ *are independent.*

$$a(1,0,0) + b(0,1,0) + c(1,1,1) = (0,0,0)$$

$$\Rightarrow a + c = 0, b + c = 0 \text{ and } c = 0 \Rightarrow a = b = c = 0.$$

Then B *is independent, so a basis of* $\mathbb{R}^3$.

3.8 Subspace spanning by a set or family of vectors

Définition 80 *Let* A *be a part of a vector space* E. *The vector subspace spanning by a set* A *is the smallest vector subspace containing the set* A, *and it is noted by:* $span(A)$ *or* $\langle A \rangle$.

Example 81 *(1) If* A *is a subspace of* E *then:* $span(A) = A$.

Exemple 3.3 *(2)* $span(\emptyset) = \{0_E\}$.

Définition 82 *It is said that a vector space* E *is spanning by a vector family* $\{u_1, u_2, ..., u_n\}$ *if and only if:*

$$\forall u \in E, \exists \alpha_i \in \mathbb{R}, 1 \leq i \leq n \text{ such as: } u = \alpha_1 u_1 + \alpha_2 u_2 + ... + \alpha_n u_n,$$

and we write:

$$E = span\{u_1, u_2, ..., u_n\}.$$

Example 83

$$\mathbb{R}^3 = span\{u_1, u_2, u_3\} \text{ with: } u_1(1,0,0), u_2(0,1,0) \text{ and } u_3(0,0,1),$$

because

$$\forall u \in \mathbb{R}^3, \exists \alpha_i \in \mathbb{R}, 1 \leq i \leq 3 \text{ such as: } u(x,y,z) = \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_n,$$
$$\text{with:} \alpha_1 = x, \alpha_2 = y \text{ and } \alpha_3 = z.$$

Chapitre 4

Linear applications (Linear maps-linear transformations)

4.1 Linear application

Définition 84 *Let E, F be two $\mathbb{k}$-vector spaces and f an application of E in F. Then f is linear, if the following properties are satisfied:*

$$(1)\, \forall u, v \in E;\ f(u+v) = f(u) + f(v).$$
$$(2)\, \forall u \in E, \forall \alpha \in \mathbb{k};\ f(\alpha u) = \alpha f(u).$$

Or

$$\boxed{\forall u, v \in E, \forall \alpha, \beta \in \mathbb{k}; f\ \ (\alpha u + \beta v) = \alpha f(u) + \beta f(v).}$$

Remarque 85 *The notations of the E elements of the most used cases are given in the fol-*

lowing table:

E	***Notation of*** u ***and*** v
$\mathbb{R}$	x *and* y
$\mathbb{R}^2$	(x_1, y_1) *and* (x_2, y_2)
$\mathbb{R}^3$	(x_1, y_1, z_1) *and* (x_2, y_2, z_2)
of functions	f_1 *and* f_2
of polynomials	P_1 *and* P_2
of sequences	U_n *and* V_n

Example 86 *Let* f *the application defined to* $\mathbb{R}^3$ *in* $\mathbb{R}^2$ *by:*

$$f(x, y, z) = (x - y, y + 2z),$$

is linear because:$\forall u(x_1, y_1, z_1), v(x_2, y_2, z_2) \in \mathbb{R}^3, \forall \alpha, \beta \in \mathbb{R}$;

$$\begin{aligned} f\ (\alpha u + \beta v) &= f(\alpha(x_1, y_1, z_1) + \beta(x_2, y_2, z_2)) \\ &= f(\alpha x_1 + \beta x_2, \alpha y_1 + \beta y_2, \alpha z_1 + \beta z_2) \\ &= ((\alpha x_1 + \beta x_2) - (\alpha y_1 + \beta y_2), (\alpha y_1 + \beta y_2) + 2(\alpha z_1 + \beta z_2)) \\ &= \alpha(x_1 - y_1, y_1 + 2z_1) + \beta(x_2 - y_2, y_2 + 2z_2) \\ &= \alpha f((x_1, y_1, z_1)) + \beta f((x_2, y_2, z_2)) \\ &= \alpha f(u) + \beta f(v). \end{aligned}$$

4.2 The kernel of linear application

Définition 87 *Let* E, F *be two* $\Bbbk$*-vector-spaces and* f *a linear application of* E *in* F*. Then the kernel, also known as the null space or nullspace of a linear application noted by* $\ker f$ *is given by:*

$$\boxed{\ker f = \{x \in E, f(x) = 0_F\},}$$

which is a vector subspace of E*.*

Example 88 *From the linear application defined of* $\mathbb{R}^3$ *in* $\mathbb{R}^2$ *by:*

$$f(x,y,z) = (x-y, y+2z),$$

the kernel is given by:

$$\ker f = \left\{ u(x,y,z) \in \mathbb{R}^3, f(u) = 0_{\mathbb{R}^2} \right\}.$$

$$\begin{aligned} u \quad &\in \quad \ker f \Leftrightarrow f(u) = (0,0) \Leftrightarrow (x-y, y+2z) = (0,0) \\ &\Leftrightarrow \begin{cases} x-y=0 \\ \quad and \\ y+2z=0 \end{cases} \Longleftrightarrow \begin{cases} x=y \\ z=-\frac{y}{2} \end{cases} \Longleftrightarrow u = y\left(1,1,-\frac{1}{2}\right), \end{aligned}$$

so $\ker f$ *is the subspace spanning bu the vector* $v\left(1,1,-\frac{1}{2}\right)$ *noted by:*

$$\ker f = span\left\{ \left(1,1,-\frac{1}{2}\right) \right\}.$$

Remarque 89 *The identity element* $0_E \in \ker f$ *because:*

$$f(0_E) = f(0 \times 0_E) = 0 \times f(0_E) = 0_F.$$

4.3 Injectivity of linear application

Définition 90 *Let be* E, F *two* $\Bbbk$*-vector spaces and* f *a linear application of* E *in* F*. Note that* f *is injective (one-to-one) if and only if:* $\forall u_1, u_2 \in E$;

$$u_1 \neq u_2 \Rightarrow f(u_1) \neq f(u_2).$$

Or,

$$f(u_1) = f(u_2) \Rightarrow u_1 = u_2.$$

But for linear application:

$$f \text{ is injective} \Leftrightarrow \ker f = \{0_E\} \text{ (The zero vector space)},$$

with $\dim\{0_E\} = 0$.

Preuve: " $\Rightarrow$ "By absurdity

$$\begin{aligned}
&\ker f \neq \{0_E\} \Rightarrow \exists u \neq 0_E \text{ such as: } f(u) = 0_F \\
&\Rightarrow u \neq 0_E \text{ and } \ f(u) = f(0_E) = 0_F \\
&\Rightarrow f \text{ is n't injective.}
\end{aligned}$$

" $\Leftarrow$ "By absurdity

$$\begin{aligned}
&f \text{ is n't injective} \Rightarrow \exists u_1 \neq u_2 \text{ and } f(u_1) = f(u_2), \\
&\Rightarrow u_1 - u_2 \neq 0_E \text{ and } f(u_1) - f(u_2) = 0_F, \\
&\Rightarrow u_1 - u_2 \neq 0_E \text{ and } f(u_1 - u_2) = 0_F, \\
&\Rightarrow u_1 - u_2 \in \ker f, \\
&\Rightarrow \ker f \neq \{0_E\}.
\end{aligned}$$

■

Example 91 *Let f be a linear application defined of $\mathbb{R}^2$ in $\mathbb{R}^2$ by:*

$$f(x, y) = (x - y, y + x).$$

We have:

$$\begin{aligned}
u &= (x, y) \in \ker f \Leftrightarrow f(u) = 0_{\mathbb{R}^2} \\
&\Leftrightarrow (x - y, y + x) = (0, 0) \\
&\Leftrightarrow \begin{cases} x - y = 0 \\ y + x = 0 \end{cases} \Leftrightarrow x = y \text{ and } x = -y \Leftrightarrow x = y = 0, \\
&\Leftrightarrow u = (0, 0) \\
&\Rightarrow \ker f = \{(0, 0)\},
\end{aligned}$$

then f is injective.

4.4 Image of linear application

Définition 92 *Let E, F be two $\mathbb{k}$-vector spaces and f a linear application of E in F. The image of f is the set of all the images of the elements of E by f Thus:*

$$\operatorname{Im} f = \{f(u), u \in E\}.$$

Also if $\{e_1, e_2, ..., e_n\}$ is a basis of E, then:

$$\operatorname{Im} f = span\{f(e_1), f(e_2), ..., f(e_n)\},$$

i.e. the subspace spanning by $\{f(e_1), f(e_2), ..., f(e_n)\}$.

Example 93 *Let $B = \left(\vec{i}, \vec{j}, \vec{k}\right)$ be the canonical (standard) basis of $\mathbb{R}^3$ and f a linear application of $\mathbb{R}^3$ in $\mathbb{R}^3$ defined by:*

$$f\left(\vec{i}\right) = -\vec{i} + \vec{k}, f\left(\vec{j}\right) = \vec{j} + \vec{k} \text{ and } f\left(\vec{k}\right) = \vec{i} + \vec{j}.$$

Then the image of f is defined as follows:

$$\begin{aligned} \operatorname{Im} f &= Vect\left\{f\left(\vec{i}\right), f\left(\vec{j}\right), f\left(\vec{k}\right)\right\} \text{ but: } f\left(\vec{k}\right) = f\left(\vec{j}\right) - f\left(\vec{i}\right) \\ &\Rightarrow \operatorname{Im} f = Vect\left\{f\left(\vec{i}\right), f\left(\vec{j}\right)\right\} = \left\{x\left(-\vec{i} + \vec{k}\right) + y\left(\vec{j} + \vec{k}\right), x, y \in \mathbb{R}\right\} \\ &= \{(-x, y, x + y), x, y \in \mathbb{R}\}. \end{aligned}$$

Théorème 94 *Let E, F be two $\mathbb{k}$-vector spaces and f a linear application of E in F. $\operatorname{Im} f$ is a subspace of F.*

4.5 Rank of linear application

Définition 95 *Let E, F be two $\mathbb{k}$-vector spaces and f a linear application of E in F. The rank of a linear application is the dimension of the image of this application noted $rankf$ that is to say:*

$$rankf = \dim(\operatorname{Im} f).$$

Moreover, if E and F are finite dimensions, we have the following rank theorem:

$$\dim E = rank\ f + \dim(\ker f).$$

Example 96 *Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be a linear application defined by:*

$$f(x, y) = (4x - 2y, 6x - 3y).$$

Then

$$\begin{aligned} \operatorname{Im} f &= \{f(x, y); x, y \in \mathbb{R}\} = \{(4x - 2y, 6x - 3y); x, y \in \mathbb{R}\} \\ &= \{(2x - y)(2, 3); x, y \in \mathbb{R}\} = \{\alpha(2, 3); \alpha \in \mathbb{R}\} \\ &= Vect\{(2, 3)\}, \end{aligned}$$

The vector $v(2, 3)$ is a basis of $\operatorname{Im} f$*, wich implies that $rank\ f = 1$.*

Définition 97 *Let E, F be two $\mathbb{k}$-vector spaces and f a linear application of E in F.*

$$f \text{ is surjective (onto) if and only if } \operatorname{Im} f = F.$$

4.6 Endomorphism, Isomorphism, Automorphism

Définition 98 *Let E, F be two $\mathbb{k}$-vector spaces and f a linear application of E in F, then:*
(1) if f is bijective, so f is called an isomorphism.
(2) an endomorphism of E is a linear application defined of E in E.
(3) an automorphism is an isomorphism of E in E.

Example 99 *Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be a linear application defined by:*

$$f(x, y) = (x - y, x + y).$$

f is an automorphism because:

$$\ker f = \left\{(x,y) \in \mathbb{R}^2 / f(x,y) = (0,0)\right\},$$

$$\begin{aligned} f(x,y) &= (0,0) \Rightarrow (x-y, x+y) = (0,0) \\ &\Rightarrow \begin{cases} x - y = 0 \\ \quad and \qquad \Rightarrow (x,y) = (0,0) \\ x + y = 0 \end{cases} \\ &\Rightarrow \ker f = \{(0,0)\} \Rightarrow \dim \ker f = 0 \\ &\Rightarrow f \text{ is injective,} \end{aligned}$$

but

$$\begin{aligned} \dim \mathbb{R}^2 &= rank\ f + \dim(\ker f) \\ &\Rightarrow rank\ f = 2, \text{ with } f\left(\mathbb{R}^2\right) \subset \mathbb{R}^2 \Rightarrow \operatorname{Im} f = \mathbb{R}^2, \\ &\Rightarrow f \text{ is surjective.} \\ &\Rightarrow f \text{ is bijective.} \end{aligned}$$

4.7 Projection

Définition 100 *Let f be an endomorphism of $\mathbb{k}$-vector space E. f is called a projection if:*

$$f \circ f = f,$$

or

$$\operatorname{Im} f \text{ and } \ker f \text{ are supplementary in } E: \ \forall x \in \operatorname{Im} f, \ f(x) = x.$$

We will say that f is the projection on $\operatorname{Im} f$ parallel to $\ker f$.

Example 101 *Let $f : \mathbb{R}^2 \to \mathbb{R}^2$ be a linear application defined by:*

$$f(x,y) = (4x - 2y, 6x - 3y),$$

then:

$$\begin{aligned}(f\circ f)(u) &= f(f(u)) = f(f(x,y)) = f(4x-2y,6x-3y)\\ &= (4x-2y,6x-3y) = f(u),\end{aligned}$$

and as a result f is a projection.

4.8 Symmetric

Définition 102 *Let f be an endomorphism of $\mathbb{k}$-vector space E. f is called symmetric if:*

$$f\circ f = Id_E \text{ (the identity application),}$$

or

$$\ker(f - Id_E) \text{ and } \ker(f + Id_E) \text{ are supplementary in } E.$$

We will say that f is the symmetric on $\ker(f - Id_E)$ parallel to $\ker(f + Id_E)$.

Example 103 *Let $f:\mathbb{R}^2\to\mathbb{R}^2$ be a linear application defined by:*

$$f(x,y) = (y,x),$$

then f is symmetric.

Chapitre 5

Matrices

The purpose of this chapter is to find a tool to solve a system of n equations to m unknown, it is the notion of matrices.

In the general case an M matrix is represented by:

$$\boxed{M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix} \in M_{n,m},}$$

that it can be simplified by:

$$\boxed{M = \begin{pmatrix} & \vdots & \\ \dots & a_{ij} & \dots \\ & \vdots & \end{pmatrix} \in M_{n,m} \Rightarrow 1 \leq i \leq n \text{ and } 1 \leq j \leq m,}$$

where $M_{n,m}$ is the set of matrices that contains n rows and m columns,in additioa_{ij} represents the coefficient of the matrix M that is in the i^{th} row and the j^{th} column.

5.1 Properties and notions on matrices