

Table des Matières

1	Polynomials and Rational Fractions	2
1.1	Polynomials	2
1.1.1	Properties and definitions	2
1.1.2	Operation on $\mathbb{R}[X]$	3
1.1.3	Types of division between polynomials	4
1.2	The Extended Euclidean Algorithm for Polynomials	5
1.2.1	The root and their order of multiplicity	8
1.2.2	Some properties on the roots of a polynomial	9
1.3	Partial fraction decomposition or Partial fraction expansion	11
1.3.1	Partial fraction expansion	11
2	Algebraic structures	19
2.1	Definitions and properties	19
2.1.1	Closure law (Internal composition law or binary operation)	19
2.1.2	Commutative law	19
2.1.3	Associative law	20
2.1.4	Identity law	20
2.1.5	Inverse or symmetric element	21
2.1.6	Regular element	21
2.1.7	Distributive property	21
2.1.8	Stable part	22

2.1.9	External composition law	22
2.2	Structure of a group	22
2.2.1	Definition of a group	22
2.2.2	Group Properties	25
2.2.3	Subgroup	26
2.2.4	Subgroups Properties	27
2.2.5	Homomorphisms	28
2.2.6	The kernel and the image of homomorphism	29
2.3	Structure d'anneau	29
2.3.1	Subrings	29
2.3.2	Homomorphism rings	30
2.4	Fields	30
2.4.1	Inverse element	30
2.4.2	Definition of field	30
2.4.3	Subfield	31

Chapitre 1

Polynomials and Rational Fractions

1.1 Polynomials

1.1.1 Properties and definitions

Définition 1 *A polynomial with the form:*

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

where X is the variable, the a 's are called the coefficients of P , which 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:

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

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 $P(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$, 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 $\text{val}(P) = v(P) = \min k$ 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: $\text{val}(P) = +\infty$.

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:

$$\begin{array}{c|c} P & Q \\ \hline P & 0 \end{array}$$

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

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

$$\begin{array}{c|c} P & Q \\ \hline R & H \end{array}$$

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 $Q(X) = 5 + X - X^2$.

$$\begin{array}{c|c} 3X^4 - 5X^3 + 4X^2 + 2X + 3 & -X^2 + X + 5 \\ \hline -(3X^4 - 3X^3 - 15X^2) & -3X^2 - 8X - 27 \\ = 8X^3 + 19X^2 + 2X + 3 & \\ -(8X^3 - 8X^2 - 40X) & \\ = 27X^2 + 42X + 3 & \\ -(27X^2 - 27X - 135) & \\ 0 + 69X + 138 & \end{array}$$

So,

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

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:

$$\begin{aligned}
P &= A_1Q + R_1 \\
Q &= A_2R_1 + R_2 \\
R_1 &= A_3R_2 + R_3 \\
R_3 &= A_4R_2 + R_4 \\
&\vdots \\
R_n &= A_{n+2}R_{n+1} + R_{n+2}
\end{aligned}$$

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 $Q(X) = X^3 + 1$

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

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

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

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

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

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

(2) Find U and V when

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

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

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

Theorem 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 remainder 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 $\leq k$.

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

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

$$\begin{array}{l|l}
-3 + 2X + 4X^2 - 5X^3 + 3X^4 & 5 + X - X^2 \\
\hline
-(-3 - \frac{3}{5}X + \frac{3}{5}X^2) & -\frac{3}{5} + \frac{13}{25}X + \frac{72}{125}X^2 \\
= \frac{13}{5}X + \frac{17}{5}X^2 - 5X^3 + 3X^4 & \\
-(\frac{13}{5}X + \frac{13}{25}X^2 - \frac{13}{25}X^3) & \\
= \frac{72}{25}X^2 - \frac{112}{25}X^3 + 3X^4 & \\
-(\frac{72}{25}X^2 + \frac{72}{125}X^3 - \frac{72}{125}X^4) & \\
-\frac{632}{125}X^3 + \frac{447}{125}X^4 &
\end{array}$$

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, which implies 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

Theorem 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 $\mathbb{k}[X]$ 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:

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

which implies that P divides R . ■

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

$$P(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n,$$

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,

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

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

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

which implies that:

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

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:

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

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:

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

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

1.3.1 Partial fraction expansion

A quadratic polynomial $(\alpha x^2 + \beta x + \lambda)$ is reducible if and only if $\Delta = b^2 - 4ac \geq 0$ and it is irreducible if and only if $\Delta < 0$ (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 ($\Delta < 0$).
- (4) **Repeated quadratic factors:** It is a factor of form $(ax^2 + bx + c)^n$ 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:

$$\frac{A_1}{a_1x + b_1}, \frac{B_1}{(c_1x + d_1)^n}, \frac{\alpha_1x + \beta_1}{a_2x^2 + b_2x + c_2} \text{ and } \frac{\alpha_2x + \beta_2}{(a_3x^2 + b_3x + c_3)^m}.$$

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.

Exemple 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 efficace 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:

- (1) If $f(x) = g(x)$ then: $\forall x_0 \in \mathbb{R}$ or $\pm\infty$, $\lim_{x \rightarrow x_0} f(x) = \lim_{x \rightarrow x_0} g(x)$,
- (2) If $f(x) = g(x)$ then: $\forall h(x)$ we have $h(x)f(x) = h(x)g(x)$.

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:

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

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

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

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:

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

(ii) For the smallest power:

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

(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:

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

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:

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

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

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

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:

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

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:

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

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.

Exemple 18

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

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

\Rightarrow

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

\Rightarrow

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

$$a_8 = \lim_{x \rightarrow i} \frac{1}{x^6} = -1.$$

$$a_6 = \lim_{x \rightarrow 0} \frac{1}{(x^2+1)} = 1.$$

$$a_2 + a_8 = 0 \text{ (multiplying by } x^2 \text{ and making tender } x \rightarrow +\infty)$$

$$\Rightarrow a_2 = 1$$

$$\text{For } x = 1 \Rightarrow \frac{1}{2} = a_2 + a_4 + a_6 + \frac{a_8}{2} \Rightarrow a_4 = -1.$$

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

Exemple 19

$$\begin{aligned} G(x) &= \frac{1}{(x-1)^5(x^2+1)} \\ &= \frac{a_1}{x-1} + \frac{a_2}{(x-1)^2} + \frac{a_3}{(x-1)^3} + \frac{a_4}{(x-1)^4} + \frac{a_5}{(x-1)^5} + \frac{a_6x+a_7}{x^2+1} \end{aligned}$$

\Rightarrow

$$h(x) = \frac{1}{(x^2+1)} = a_1(x-1)^4 + a_2(x-1)^3 + a_3(x-1)^2 + a_4(x-1) + a_5 + (x-1)^5 \left[\frac{a_6x+a_7}{x^2+1} \right]$$

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

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

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

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

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

On the other hand:

$$\lim_{x \rightarrow i} a_6x + a_7 = \lim_{x \rightarrow i} \frac{1}{(x-1)^5} (i \text{ is a root of } x^2+1)$$

$$\Rightarrow ia_6 + a_7 = \frac{1}{8} (i+1)$$

$$\Rightarrow a_6 = \frac{1}{8} \text{ and } a_7 = \frac{1}{8}.$$

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

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:

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

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

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

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

which implies that $*$ is not associative in \mathbb{Q} .

2.1.4 Identity law

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 not 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 α is a regular element for a closure law in E if it checks:

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

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:

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

Exemple 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: $\alpha \cdot u$.

Exemple 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 with an internal composition law is a group if one has the following three properties:*

- (1) *$*$ is associative in E .*
- (2) *E admits an identity element corresponds to $*$.*
- (3) *Each element of E has a symmetric to $*$.*

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

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

Show that:

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

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 .

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

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

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

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

and

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

which implies that

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

so $*$ is associative.

$*$ is also commutative because $\forall (a, b) \in E^2$:

$$a * b = \frac{a + b}{1 + ab} = \frac{b + a}{1 + ba} = b * a.$$

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

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

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

(4) The existence of the symmetrical 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 neutral elements e_1 and 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 symmetric element) The symmetric of an element x is unique noted x^{-1} .

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

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

■

(3)

$$\forall x \in G, \forall y \in G; (x^{-1})^{-1} = x \text{ and } (x * y)^{-1} = y^{-1} * x^{-1}.$$

Preuve: (a) $\forall x \in G, x * x^{-1} = x^{-1} * x = e$, then x is the symmetric of x^{-1} , which implies that:

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

(b) We use:

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

Indeed,

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

and

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

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) $\forall x \in H, \forall y \in H; x * y \in H$.

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

The last two properties can be written in one:

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

Exemple 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:*

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

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

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

(3)

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

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:

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

such as:

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

Exemple 35

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

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,

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

■

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 isomorphism 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 $f : G \rightarrow H$ the subset of G defined by:

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

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

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

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

- (1) *Injective if and only if $\ker f = \{e_G\}$.*
- (2) *Surjective if and only if $\text{Im}(f) = H$.*

2.3 Structure d'anneau

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 $f : (A, *, \triangle) \rightarrow (B, *, \triangle)$ 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 Inverse element

Définition 42 An element $x \in K$ is inversible 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 (x^{-1}) ..

2.4.2 Definition of field

Définition 44 It is said that $(K, *, \triangle)$ is a field if and only if:

(1) $(K, *, \triangle)$ is a ring.

(2) Any element other than e_1 (the identity element for the operation $*$) has an inverse for the law \triangle . If \triangle is commutative then K is a commutative field.

Exemple 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 K is a subfield of K if L is a subring of K .

END OF THE COURSE