CHAPITRE 22

POLYNÔMES ET FRACTIONS

PARTIE 22.1 : STRUCTURE DES POLYNÔMES

22.1.1 : Définition formelle

Définition 22.1

Soit $\mathbb{K}$ un corps commutatif, on appelle **polynôme à coefficients dans $\mathbb{K}$** une suite $P = (p_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ à support fini. L'ensemble de ces polynômes est donc pour l'instant noté $\mathbb{K}^{(\mathbb{N})}$.
 Pour un tel "polynôme" $P = (p_n)_{n \in \mathbb{N}}$, on définit son **degré**, sa **valuation** ; par convention $\deg(P) = -\infty$ et $\text{val}(P) = +\infty$ si P est nul ; sinon $\deg(P) = \text{Max}(\{k \in \mathbb{N} \mid p_k \neq 0\})$, $\text{val}(P) = \text{Min}(\{k \in \mathbb{N} \mid p_k \neq 0\})$.
 Si P n'est pas le polynôme nul, on définit le **coefficient dominant** de P : $\text{cd}(P) = p_d$ où $d = \deg(P) \in \mathbb{N}$.
 Si $P = 0$, on pose $\text{cd}(P) = 0$. P est appelé un **polynôme unitaire** si $\text{cd}(P) = 1$.
 On dit que P est un **polynôme pair** (resp. **impair**) si $\forall k \in \mathbb{N}$, $p_{2k+1} = 0$ (resp. $\forall k \in \mathbb{N}$, $p_{2k} = 0$).

EXEMPLE 22.1 : $P = (1, 0, 2, 0, 1, 0, \dots) \in \mathbb{R}^{(\mathbb{N})}$ est un polynôme à coefficients réels, pair, unitaire, de valuation 0 et de degré 4.

REMARQUE 22.1 : • L'égalité de polynômes est l'égalité des suites : "identification" des coefficients.

- On a clairement en général $\text{val}(P) \leq \deg(P)$ sauf par convention pour le polynôme nul.
- Les **monômes** sont les polynômes tels que $\text{val}(P) = \deg(P)$: de la forme $(0, \dots, 0, p_d, 0, \dots)$ ($p_d \neq 0$).

22.1.2 : Opérations

Définition 22.2

Avec les notations précédentes, on prend deux polynômes $P = (p_n)_{n \in \mathbb{N}}$ et $Q = (q_n)_{n \in \mathbb{N}}$ à coefficients dans $\mathbb{K}$ et $\lambda \in \mathbb{K}$; on définit les nouveaux polynômes $P + Q$, $\lambda.P$ et $P \times Q$ par :

$$P + Q = (p_n + q_n)_{n \in \mathbb{N}}, \lambda.P = (\lambda p_n)_{n \in \mathbb{N}}, P \times Q = (r_n)_{n \in \mathbb{N}} \text{ où } \forall n \in \mathbb{N}, r_n = \sum_{k=0}^n p_k q_{n-k} = \sum_{i+j=n} p_i q_j.$$

REMARQUE 22.2 : • On vérifie que ceci définit bien trois nouveaux polynômes.

- On vient donc de définir deux lois internes dans $\mathbb{K}^{(\mathbb{N})}$ et une loi externe : tout est en place !

Proposition 22.1

Soit P et Q deux polynômes et $\lambda \in \mathbb{K}$ non nul.

D'abord nous avons $\deg(\lambda.P) = \deg(P)$ et $\text{val}(\lambda.P) = \text{val}(P)$.

Ensuite des inégalités : $\deg(P + Q) \leq \text{Max}(\deg(P), \deg(Q))$ et $\text{val}(P + Q) \geq \text{Min}(\text{val}(P), \text{val}(Q))$.

De plus : $\text{val}(P) \neq \text{val}(Q) \implies \text{val}(P + Q) = \text{Min}(\text{val}(P), \text{val}(Q))$, et

$(\deg(P) \neq \deg(Q) \text{ ou } (\deg(P) = \deg(Q) \text{ et } \text{cd}(P) + \text{cd}(Q) \neq 0)) \implies \deg(P + Q) = \text{Max}(\deg(P), \deg(Q))$.

Enfin : $\deg(P \times Q) = \deg(P) + \deg(Q)$, $\text{val}(P \times Q) = \text{val}(P) + \text{val}(Q)$ et $\text{cd}(P \times Q) = \text{cd}(P) \times \text{cd}(Q)$.

Théorème 22.1

L'ensemble $\mathbb{K}^{(\mathbb{N})}$ des polynômes une $\mathbb{K}$ -algèbre commutative intègre.

REMARQUE 22.3 : • Les polynômes inversibles sont ceux de degrés 0.

- Les polynômes pairs et impairs forment des sous-espaces vectoriels supplémentaires.
- Les polynômes de degré inférieurs ou égaux à $n \in \mathbb{N}$ forment aussi un sev.
- Les polynômes pairs ou les polynômes de degré ≤ 0 forment de plus des sous-algèbres.

22.1.3 : Nouvelle notation des polynômes

REMARQUE 22.4 :

• On identifie $\mathbb{K}$ à une sous-algèbre des polynômes grâce au morphisme injectif $\varphi : \mathbb{K} \rightarrow \mathbb{K}^{(\mathbb{N})}$ d'algèbres défini par : $\forall a \in \mathbb{K}, \varphi(a) = (a, 0, \dots)$; $\text{Im}(\varphi)$ est l'ensemble des polynômes de degré ≤ 0 .

• En notant $X = (0, 1, 0, 0, \dots)$ et on vérifie que $X^n = (\delta_{i,n})_{i \in \mathbb{N}}$. Soit alors un polynôme général

$$P = (p_0, \dots, p_d, 0, \dots), \text{ alors } P = \sum_{k=0}^{+\infty} a_k X^k \text{ ou, en notant } d \text{ son degré, } \sum_{k=0}^d p_k X^k.$$

- On peut noter $\mathbb{K}[X]$ l'ensemble des polynômes, c'est l'algèbre engendrée par le seul polynôme X .
- De même, la sous-algèbre $\mathbb{K}[X^2]$ (engendrée par X^2) est celle des polynômes pairs.
- On note, pour $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieurs ou égaux à n .

22.1.4 : Composition et dérivation

Définition 22.3

Soit $P = \sum_{k=0}^{+\infty} p_k X^k$ un polynôme de $\mathbb{K}[X]$, on définit son **polynôme dérivé**, noté P' , par la relation

$$P' = \sum_{k=1}^{+\infty} k p_k X^{k-1} = \sum_{k=0}^{+\infty} (k+1) p_{k+1} X^k. \text{ Soit } Q \text{ un autre polynôme de } \mathbb{K}[X], \text{ on définit la composée de}$$

$$P \text{ par } Q, \text{ notée } P \circ Q \text{ par } P \circ Q = \sum_{k=0}^{+\infty} p_k Q^k.$$

Proposition 22.2

Pour $(P, Q) \in (\mathbb{K}[X])^2$, on a les formules pour les degrés (sous conditions) :

$$\deg(P') = \deg(P) - 1 \text{ si } \deg(P) \geq 1 \text{ et } \deg(P \circ Q) = \deg(P) \times \deg(Q) \text{ si } \deg(Q) > 0.$$

EXEMPLE 22.2 : Les conditions de la proposition précédente sont indispensables : $P = X^2$ alors $\deg(P') \neq \deg(P) - 1$; si $P = X^2 - 1$ et $Q = 1$, $\deg(P(Q)) \neq \deg(P) \times \deg(Q)$; si $\mathbb{K} = \mathbb{Z}/3\mathbb{Z}$, $(X^3)' = 0$.

REMARQUE 22.5 : On définit les **dérivées successives des polynômes**, avec la convention $P^{(0)} = P$, par : $\forall n \in \mathbb{N}^*, \forall P \in \mathbb{K}[X], P^{(n)} = (P^{(n-1)})'$. Au niveau des degrés et des coefficients dominants, on obtient par récurrence des : si $d = \deg(P) \geq n$ alors $\deg(P^{(n)}) = \deg(P) - n$ et $\text{cd}(P^{(n)}) = \frac{d!}{(d-n)!} \text{cd}(P)$.

Proposition 22.3

Soit $(\lambda, \mu) \in \mathbb{K}^2, n \in \mathbb{N}^*$ et $(P, Q) \in (\mathbb{K}[X])^2$, alors on a les formules :

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q', (P \times Q)' = P' \times Q + P \times Q', (P \circ Q)' = Q' \times P' \circ Q \text{ et } (P \times Q)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} \times Q^{(n-k)}.$$

REMARQUE 22.6 : • La dérivation $D : P \mapsto P'$ est linéaire et son noyau est $\mathbb{K}_0[X]$.

- Les dérivées successives sont donc aussi linéaires : $D^n : P \mapsto P^{(n)}$ avec $\text{Ker}(D^n) = \mathbb{K}_{n-1}[X]$.
- X est neutre à gauche et à droite pour la composition, elle est associative, distributive à droite sur $+$ mais elle n'est pas distributive par rapport à la somme à gauche.

PARTIE 22.2 : ARITHMÉTIQUE POLYNOMIALE

22.2.1 : Multiples, diviseurs et polynômes associés

Définition 22.4

Soit $\mathbb{K}$ un corps commutatif, $(A, B) \in \mathbb{K}[X]^2$, on dit que B est un **multiple** de A , ou que A est un **diviseur** de B , ou que A **divise** B , si $\exists C \in \mathbb{K}[X], B = A \times C$: on le note $A|B$.

On note $A \mathbb{K}[X] = \{P \in \mathbb{K}[X] \mid \exists Q \in \mathbb{K}[X], P = A \times Q\} = \{A \times Q \mid Q \in \mathbb{K}[X]\}$: multiples de A .

Quand $A|B$ et $B|A$ simultanément, on dit que A et B sont des **polynômes associés**.

EXEMPLE 22.3 : $X^2 + X + 1$ divise $X^6 - 1$ dans $\mathbb{C}[X]$, et dans $\mathbb{R}[X]$, et dans $\mathbb{Q}[X]$.

REMARQUE 22.7 : • Tout polynôme non nul est associé à un unique polynôme unitaire.

- La relation de divisibilité n'est que réflexive et transitive : ce n'est pas une relation d'ordre.
- Par contre, la relation "être associé à" est une relation d'équivalence".
- Tout diviseur A d'un polynôme non nul B vérifie : $\deg(A) \leq \deg(B)$.
- Comme pour les entiers, $A|B \iff B \mathbb{K}[X] \subset A \mathbb{K}[X]$; de plus $A \mathbb{K}[X] = B \mathbb{K}[X] \iff (A \text{ et } B \text{ associés})$.

Proposition 22.4

Soit $(A, B) \in \mathbb{K}[X]^2$: (A et B sont associés) $\iff (\exists \lambda \in \mathbb{K}^*, A = \lambda B)$.

22.2.2 : Division euclidienne et congruences

REMARQUE 22.8 : Pratique de la **division euclidienne** des polynômes : on prend deux polynômes $B = b_n X^n + \dots + b_0$ de degré $n \geq 0$ et $A = a_m X^m + \dots + a_0$ de degré m et on dispose la division de B par A comme à l'école pour les entiers.

EXEMPLE 22.4 : Division de $B = 2X^4 + 5X^3 - X^2 + 2X + 1$ par $A = 2X^2 - 3X + 1$.

Théorème 22.2

Soit $(A, B) \in \mathbb{K}[X]^2$ avec $A \neq 0$ et $m = \deg(A)$, il existe un unique couple $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}_{m-1}[X]$ tel que $B = AQ + R$ (division euclidienne de B par A).

DÉMONSTRATION : On effectue une récurrence sur le degré du dividende une fois le diviseur fixé.

REMARQUE 22.9 :

- A est le **diviseur**, B est le **dividende**, Q est le **quotient** et R est appelé le **reste**.
- On a encore la notion de **congruence** (qui est encore une relation d'équivalence) sur les polynômes : pour $(A, B, Q) \in (\mathbb{K}[X])^2$ avec $Q \neq 0$, $A \equiv B [Q] \iff Q|(B - A) \iff \exists U \in \mathbb{K}[X], B - A = QU$.
- Comme pour les entiers, si $(A, B, C, D) \in \mathbb{K}[X]^4$, $\lambda \in \mathbb{K}$ et $p \in \mathbb{N}$ on a les compatibilités usuelles :

$$(A \equiv B [Q] \text{ et } C \equiv D [Q]) \implies (A + C \equiv B + D [Q] \text{ et } AC \equiv BD [Q]).$$

$$(A \equiv B [Q] \implies A^p \equiv B^p [Q]) \text{ et } (A \equiv B [Q] \implies \lambda A \equiv \lambda B [Q]).$$
- Si $(A, B, R) \in \mathbb{K}[X]^3$, on a une caractérisation du reste utilisant les congruences :

$$(R \text{ est le reste de la division euclidienne de } B \text{ par } A) \iff (B \equiv R [A] \text{ et } \deg(R) < \deg(A)).$$

EXEMPLE 22.5 : Quel est le reste de la division euclidienne de $X^{58} + 3X^{17} - X^6 - 2$ par $X^3 - 1$.

22.2.3 : Définition du ppcm et du pgcd

Définition 22.5

Soit I une partie de $\mathbb{K}[X]$, on dit que c'est un **idéal** de $\mathbb{K}[X]$ si I est un sous-groupe de $\mathbb{K}[X]$ et que : $\forall P \in I, \forall Q \in \mathbb{K}[X], PQ \in I$. On dit qu'un idéal I est **principal** si $\exists A \in \mathbb{K}[X], I = A \mathbb{K}[X]$.

Proposition 22.5

Les idéaux de $\mathbb{K}[X]$ sont exactement les idéaux principaux.

DÉMONSTRATION : C'est encore une utilisation de la division euclidienne.

REMARQUE 22.10 : Soit I et J deux idéaux, alors $I + J$ et $I \cap J$ sont encore des idéaux de $\mathbb{K}[X]$; plus généralement, pour une famille d'idéaux $(I_1, \dots, I_n)$ avec $n \geq 2$, alors $\sum_{k=1}^n I_k$ et $\bigcap_{k=1}^n I_k$ sont des idéaux.

Définition 22.6

Soit $n \in \mathbb{N}^*$ et $(A_1, \dots, A_n) \in \mathbb{K}[X]^n$, on définit le **plus grand commun diviseur** (en abrégé **pgcd**) D de cette famille, c'est le polynôme unitaire tel que $D \mathbb{K}[X] = \sum_{k=1}^n A_k \mathbb{K}[X]$. De même, avec ces notations, on définit le **plus petit commun multiple** (en abrégé **ppcm**) M de cette famille, c'est le polynôme unitaire tel que $M \mathbb{K}[X] = \bigcap_{k=1}^n A_k \mathbb{K}[X]$. On note $D = A_1 \wedge \dots \wedge A_n$ et $M = A_1 \vee \dots \vee A_n$.

Théorème 22.3

Avec ces notations et si $P \in \mathbb{K}[X]$, on a les équivalences pratiques :

$$(\forall k \in [1; n], P|A_k) \iff (P|D = A_1 \wedge \dots \wedge A_n) \text{ et } (\forall k \in [1; n], A_k|P) \iff (A_1 \vee \dots \vee A_n = M|P).$$

REMARQUE 22.11 :

- Par conséquent, les noms de ces deux polynômes D et M sont justifiés car D est bien le plus grand (au sens de $\deg$ mais à constante près tout de même) parmi tous les diviseurs communs de $A_1, \dots, A_n$ (et même au sens de $|$) ; de même M est bien le plus petit (au sens de $\deg$...) parmi les multiples communs des entiers $A_1, \dots, A_n$.
- Il y a un seul cas pour lequel la définition algébrique ne correspond pas exactement avec le sens de "plus grand commun diviseur", et c'est quand $A_1 = \dots = A_n = 0$ car alors $D = 0$ alors qu'il n'existe pas de plus grand commun diviseur au sens usuel.

Proposition 22.6

Nous disposons des équivalences suivantes, pour $(A, B) \in \mathbb{K}[X]^2$ en notant le polynôme normalisé $P^* = \text{cd}(P)^{-1}P$ si $P \neq 0$: $A \wedge B = A^* \iff A|B$ et $A \vee B = B^* \iff A|B$. De plus, si $(A, B, C) \in \mathbb{K}[X]^3$, on a : $(AC) \wedge (BC) = C^*(A \wedge B)$ et $(AC) \vee (BC) = C^*(A \vee B)$.

REMARQUE 22.12 : Comme dans $\mathbb{Z}$, on a associativité et commutativité de $\wedge$ et $\vee$ dans $\mathbb{K}[X]$.

REMARQUE 22.13 : **Algorithme d'EUCLIDE** pour la recherche du pgcd de deux polynômes :

- Tout d'abord, si $(A, B) \in \mathbb{K}[X]^2$ et si on a $B = AQ + R$ alors $B \wedge A = A \wedge R$.
- L'algorithme consiste donc, à partir d'un couple $(A, B) \in \mathbb{K}[X]^2$ tel que $\deg(B) \geq \deg(A) \geq 0$, à poser $A_0 = B$ et $A_1 = A$ et à effectuer successivement les divisions euclidiennes : $A_0 = A_1 Q_0 + A_2$, $A_1 = A_2 Q_1 + A_3$, etc... Il est clair que l'on a $\deg(A_0) > \deg(A_1) > \deg(A_2) > \dots$ de sorte que, puisque l'on a affaire à des entiers naturels, il existe un indice r tel que $A_r = 0$. Ensuite, il suffit d'écrire $A \wedge B = A_0 \wedge A_1 = \dots = A_{r-1} \wedge A_r = A_{r-1}$ donc le pgcd de A et B est le dernier reste non nul dans l'algorithme d'EUCLIDE.

EXEMPLE 22.6 : Trouver le pgcd de $X^{20} - 1$ et $X^{12} - 1$.

REMARQUE 22.14 : Supposons toujours que $n = \deg(B) \geq \deg(A)$, avec l'algorithme précédent, le nombre d'étapes est majoré par n : donc la complexité de cet algorithme est $O(n^2)$.

22.2.4 : Polynômes premiers entre eux**Définition 22.7**

On dit que deux polynômes A et B sont **premiers entre eux** si $A \wedge B = 1$.

Proposition 22.7

Soit $(A, B) \in \mathbb{K}[X]^2$, et $D \in \mathbb{K}[X]$ unitaire, alors on a l'équivalence :

$$D = A \wedge B \iff (\exists (A_1, B_1) \in \mathbb{K}[X]^2, A = DA_1, B = DB_1 \text{ et } A_1 \wedge B_1 = 1).$$

Proposition 22.8

Soit A, B et C trois polynômes : $(A \wedge B = 1 \text{ et } C|B) \implies A \wedge C = 1$.

REMARQUE 22.15 : Bien sûr comme pour les entiers, on a les **théorèmes de BÉZOUT et de GAUSS** :

Théorème 22.4

Soit $(A, B) \in \mathbb{K}[X]^2$, alors : $A \wedge B = 1 \iff \exists (U, V) \in \mathbb{K}[X]^2, AU + BV = 1$ (BÉZOUT).

REMARQUE 22.16 : Soit $(A, B) \in \mathbb{K}[X]^2$ et $D \in \mathbb{K}[X]$ unitaire, alors on a en général juste une implication qui ressemble au théorème de BÉZOUT : $A \wedge B = D \implies \exists (U, V) \in \mathbb{K}[X]^2, AU + BV = D$.

REMARQUE 22.17 : En pratique on utilise l'algorithme d'EUCLIDE en remontant les calculs pour trouver des polynômes de BÉZOUT (U et V) mais il y a un algorithme général (EUCLIDE étendu).

EXEMPLE 22.7 : Trouver U et V tels que $(1 - X)^4 \cdot U + X^3 \cdot V = 1$

REMARQUE 22.18 : Bien sûr, comme pour les entiers, on dit que des polynômes $A_1, \dots, A_r$ sont **premiers entre eux dans leur ensemble** si $A_1 \wedge \dots \wedge A_r = 1$, il existe alors une famille de polynômes $(U_1, \dots, U_r) \in \mathbb{K}[X]^r$ telle que : $A_1 U_1 + \dots + A_r U_r = 1$.

Théorème 22.5

Soit $(A, B, C) \in \mathbb{K}[X]^3$, on a : $(A|BC \text{ et } A \wedge B = 1) \implies A|C$ (GAUSS).

Proposition 22.9

Soit A et B deux polynômes premiers entre eux et non constants, alors :

$$\exists (U, V) \in \mathbb{K}[X]^2, AU + BV = 1 \text{ et } \deg(U) < \deg(B) \text{ et } \deg(V) < \deg(A).$$

REMARQUE 22.19 : C'est ce couple (U, V) qu'on a par l'algorithme d'EUCLIDE (voir exemple 22.7).

REMARQUE 22.20 : Soit $(A, B, C) \in \mathbb{K}[X]^3$ et $(E) : AP + BQ = C$. Posons $D = A \wedge B$:

- Si $D \nmid C$ alors (E) n'admet aucune solution.
- Si $D|C$ alors en posant $A = DA_1, B = DB_1$ et $C = DC_1$, on a $A_1 \wedge B_1 = 1$ et $(E) : A_1 P + B_1 Q = C_1$, donc on peut ramener la résolution de (E) au cas où A et B sont premiers entre eux.

On suppose donc maintenant que $A \wedge B = 1$ de sorte qu'il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$. On montre alors que les solutions de (E) sont les couples $(RB + UC, -RA + VC)$ où R parcourt $\mathbb{K}[X]$.

Proposition 22.10

Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$ et $(A_1, \dots, A_n)$ une famille de polynômes, alors on a l'équivalence suivante : $(\forall k \in [1; n], P \wedge A_k = 1) \iff P \wedge \left(\prod_{k=1}^n A_k \right) = 1$.

Proposition 22.11

Soit $(A, B) \in \mathbb{K}[X]^2$ et $(n, m) \in (\mathbb{N}^*)^2$, alors : $A \wedge B = 1 \iff A^n \wedge B^m = 1$.

Proposition 22.12

Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$ et $(A_1, \dots, A_n)$ une famille de polynômes premiers entre eux deux à deux, alors on a l'équivalence : $(\forall k \in \llbracket 1; n \rrbracket, A_k | P) \iff \prod_{k=1}^n A_k | P$.

REMARQUE 22.21 : Cette proposition est intéressante car, par exemple, un polynôme est un multiple de $(X^2 - 1)$ si et seulement si c'est un multiple de $X - 1$ et de $X + 1$.

Proposition 22.13

Soit $A_1, \dots, A_n$ premiers entre eux 2 à 2 : $A_1 \vee \dots \vee A_n = \left(\prod_{k=1}^n A_k \right)^*$.

Proposition 22.14

Soit $(A, B) \in \mathbb{K}[X]^2$ alors : $(A \wedge B) \times (A \vee B) = (AB)^*$.

22.2.5 : Polynômes irréductibles**Définition 22.8**

Soit $P \in \mathbb{K}[X]$ non constant, on dit que le polynôme P est **irréductible** dans $\mathbb{K}[X]$ s'il vérifie :
 $\forall (U, V) \in \mathbb{K}[X]^2, P = UV \implies (\deg(U) = 0 \text{ ou } \deg(V) = 0)$.

EXEMPLE 22.8 : $P = X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

REMARQUE 22.22 : • On note $I_{\mathbb{K}}$ l'ensemble de tous les polynômes irréductibles unitaires dans $\mathbb{K}[X]$.

- Quel que soit $\mathbb{K} : \forall \alpha \in \mathbb{K}, X - \alpha$ est irréductible dans $\mathbb{K}[X]$.
- Les polynômes réels $X^2 + aX + b$ de degré 2 sont irréductibles si $a^2 - 4b < 0$.
- Soit deux corps $\mathbb{K} \subset \mathbb{L}$ et $P \in \mathbb{K}[X] : (P \text{ irréductible dans } \mathbb{L}[X]) \implies (P \text{ irréductible dans } \mathbb{K}[X])$.
- Bien sûr la réciproque est fautive comme le montre l'exemple précédent.

Proposition 22.15

Soit $P \in \mathbb{K}[X]$ irréductible et $A \in \mathbb{K}[X]$, alors $(P|A \text{ ou } P \wedge A = 1)$.

Proposition 22.16

Soit $P \in \mathbb{K}[X]$ irréductible, $n \in \mathbb{N}^*$ et $(A_1, \dots, A_n) \in \mathbb{K}[X]^n$ une famille de polynômes, alors on a la nouvelle équivalence : $P | \prod_{k=1}^n A_k \iff (\exists k \in \llbracket 1; n \rrbracket, P | A_k)$

Théorème 22.6

Soit $A \in \mathbb{K}[X]$ un polynôme non constant, alors il existe une unique décomposition (à l'ordre près) de A en produit de polynômes irréductibles unitaires :

$$\exists! r \in \mathbb{N}^*, \exists! (P_1, \dots, P_r) \in I_{\mathbb{K}}^r \text{ (distincts deux à deux), } \exists! (\alpha_1, \dots, \alpha_r) \in (\mathbb{N}^*)^r, A = \text{cd}(A) \prod_{k=1}^r P_k^{\alpha_k}.$$

EXEMPLE 22.9 : Décomposer $X^{12} + 1$ dans $\mathbb{R}[X]$.

REMARQUE 22.23 :

- On peut définir l'équivalent de la valuation p-adique pour les entiers, si $P \in \mathbb{I}_{\mathbb{K}}$ et $A \in \mathbb{K}[X]$, on note $v_P(A) = \alpha_k$ si $P|A$ et $P = P_k$ (voit théorème 22.22) et $v_P(A) = 0$ sinon.
- Alors on peut écrire : $\forall A \in \mathbb{K}[X]$ non constant : $A = \text{cd}(A) \prod_{P \in \mathbb{I}_{\mathbb{K}}} P^{v_P(A)}$.
- On a encore : $\forall P \in \mathbb{I}_{\mathbb{K}}, \forall (A, B) \in \mathbb{K}[X]^2$ (non constants), $v_P(AB) = v_P(A) + v_P(B)$.
- On a toujours : $\forall P \in \mathbb{I}_{\mathbb{K}}, \forall (A, B) \in \mathbb{K}[X]^2$ (non constants), $v_P(A + B) \geq \text{Min}(v_P(A), v_P(B))$.
- On a de nouveau : $\forall (A, B) \in \mathbb{K}[X]^2$ (non constants) : $A|B \iff (\forall P \in \mathbb{I}_{\mathbb{K}}, v_P(A) \leq v_P(B))$.
- On a aussi : $\forall (A, B) \in \mathbb{K}[X]^2, (A \wedge B)^* = \prod_{P \in \mathbb{I}_{\mathbb{K}}} P^{\text{Min}(v_P(A), v_P(B))}$ et $(A \vee B)^* = \prod_{P \in \mathbb{I}_{\mathbb{K}}} P^{\text{Max}(v_P(A), v_P(B))}$.
- Ces formules de calcul du pgcd ou du ppcm se généralisent à plusieurs polynômes.
- On en déduit comme pour les entiers distributivité du ppcm par rapport au pgcd et vice-versa : $\forall (A, B, C) \in \mathbb{K}[X]^3, A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ et $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$ car ce sont des polynômes unitaires et Min et Max sont distributifs l'un par rapport à l'autre.

PARTIE 22.3 : RACINES DES POLYNÔMES

22.3.1 : Fonctions polynomiales

Définition 22.9

Soit $\mathbb{K}$ un corps commutatif, une **fonction polynomiale** est une application $f : \mathbb{K} \rightarrow \mathbb{K}$ pour laquelle il existe $P = \sum_{k=0}^d p_k X^k \in \mathbb{K}[X]$ tel que : $\forall x \in \mathbb{K}, f(x) = \sum_{k=0}^d p_k x^k$. On note cette application $f = \tilde{P}$. L'ensemble de toutes les fonctions polynomiales est noté $\text{Pol}(\mathbb{K})$.

REMARQUE 22.24 : L'application $\phi : \mathbb{K}[X] \rightarrow \text{Pol}(\mathbb{K})$ définie par : $\forall P \in \mathbb{K}[X], \phi(P) = \tilde{P}$ est un morphisme surjectif d'algèbres. De plus, il est clair que si $(P, Q) \in \mathbb{K}[X]^2$, on a $\widetilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$; de plus, si $\mathbb{K} = \mathbb{R}, \tilde{P}' = \tilde{P}'$. Par contre, ϕ n'est pas injectif en général comme le montre l'exemple suivant.

EXEMPLE 22.10 : Déterminer $\widetilde{X^7 - X}$ si $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$.

REMARQUE 22.25 : Soit $P = a_d X^d + \dots + a_0, x \in \mathbb{K}$, voici le **schéma de HORNER** (calcul de $\tilde{P}(x)$) :

- On initialise $y = a_n$.
- Pour chaque $k \in \llbracket 0; n - 1 \rrbracket$, on pose $y = a_k + xy$.
- Le dernier y est alors $\tilde{P}(x)$.

22.3.2 : Zéros ou racines

Définition 22.10

Soit $P \in \mathbb{K}[X], \mathbb{K} \subset \mathbb{L}$ (avec $\mathbb{K} \subset \mathbb{L}$ 2 corps), $\alpha \in \mathbb{L}, \alpha$ est une **racine** (ou **zéro**) de P si $\tilde{P}(\alpha) = 0$.

REMARQUE 22.26 : Soit $P = a_d X^d + \dots + a_0$ à coefficients entiers (avec $a_d \neq 0$). On montre avec le théorème de GAUSS (dans $\mathbb{Z}$) que si $\frac{p}{q} \in \mathbb{Q}$ est une racine de P (avec $p \wedge q = 1$), alors $q|a_d$ et $p|a_0$.

Ceci nous fournit un nombre fini de rationnels parmi lesquels chercher des solutions rationnelles de (E).

Proposition 22.17

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{L}$, on a : $(\alpha \text{ racine de } P) \iff (X - \alpha)|P$.

Théorème 22.7

Soit $P \in \mathbb{K}[X]$ de degré $d \in \mathbb{N}^*$, $n \in \mathbb{N}^*$ et $(\alpha_1, \dots, \alpha_n) \in \mathbb{L}^n$ des racines distinctes 2 à 2 de P :

- on a $\prod_{k=1}^n (X - \alpha_k) \mid P$ donc $n \leq d$,
- si $n = d$ on a plus précisément $P = cd(P) \prod_{k=1}^d (X - \alpha_k)$.

EXEMPLE 22.11 : Factoriser, pour $n \in \mathbb{N}^*$, le polynôme $X^n - 1$.

REMARQUE 22.27 : Soit $P = a_d X^d + \dots + a_0$ un polynôme réciproque $\forall k \in \llbracket 0; d \rrbracket$, $a_{d-k} = a_k$, alors pour $x \in \mathbb{K}^*$, on a $P\left(\frac{1}{x}\right) = \frac{1}{x^d} P(x)$ donc pour $\alpha \in \mathbb{L}^*$, $P(\alpha) = 0 \iff P\left(\frac{1}{\alpha}\right) = 0$. De plus, si d est impair, -1 est une racine évidente et si d pair il faut poser $u = x + \frac{1}{x}$ pour réduire le degré.

EXEMPLE 22.12 : Résoudre $x^7 - 5x^6 + 8x^5 - 4x^4 - 4x^3 + 8x^2 - 5x + 1 = 0$ dans $\mathbb{C}$.

Théorème 22.8

Soit $P \in \mathbb{K}_d[X]$ et $n > d$ tel qu'il existe $(\alpha_1, \dots, \alpha_n) \in \mathbb{L}^n$ des racines distinctes deux à deux de P , alors $P = 0$. A fortiori, tout polynôme qui admet une infinité de racines distinctes deux à deux est le polynôme nul.

REMARQUE 22.28 : Si $\mathbb{K}$ est infini, alors le morphisme d'algèbres ϕ de la remarque 22.24 est un isomorphisme ; on pourra donc dorénavant (pour $\mathbb{K}$ infini) confondre polynômes et fonctions polynomiales.

Proposition 22.18

Soit $n \in \mathbb{N}^*$ et $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$ distincts entre eux deux, et $(\beta_1, \dots, \beta_n) \in \mathbb{K}^n$, alors il existe un unique polynôme $L \in \mathbb{K}_{n-1}[X]$ tel que : $\forall k \in \llbracket 1; n \rrbracket$, $L(\alpha_k) = \beta_k$ et c'est le polynôme dont l'expression est : $L = \sum_{k=1}^n \beta_k \prod_{\substack{j=1 \\ j \neq k}}^n \frac{X - \alpha_j}{\alpha_k - \alpha_j}$ (L pour LAGRANGE).

EXEMPLE 22.13 : Trouver le polynôme d'interpolation de LAGRANGE (donc de degré inférieur ou égal à 2) qui vérifie les conditions : $L(0) = 1$, $L(1) = 3$ et $L(2) = 7$.

Proposition 22.19

Soit $(P, Q) \in \mathbb{K}_d[X]^2$, s'il existe $(\alpha_1, \dots, \alpha_n) \in \mathbb{L}^n$ distincts deux à deux tels que l'on ait les égalités $\forall k \in \llbracket 1; d \rrbracket$, $P(\alpha_k) = Q(\alpha_k)$ (P et Q coïncident en n valeurs distinctes) alors on $P = Q$. A fortiori, si $(P, Q) \in \mathbb{K}[X]^2$ et si P et Q coïncident en une infinité de valeurs alors $P = Q$.

22.3.3 : Formules de TAYLOR et ordre de multiplicité des racines**Proposition 22.20**

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ alors on a les trois formes de la formule de TAYLOR :

$$P = \sum_{n=0}^{+\infty} \frac{P^{(n)}(0)}{n!} X^n ; P(X + \alpha) = \sum_{n=0}^{+\infty} \frac{P^{(n)}(\alpha)}{n!} X^n \text{ et } P = \sum_{n=0}^{+\infty} \frac{P^{(n)}(\alpha)}{n!} (X - \alpha)^n.$$

Définition 22.11

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{L}$, on définit l'ordre de multiplicité de α dans le polynôme P , noté $\omega_\alpha(P)$, et c'est l'exposant de $(X - \alpha)$ dans la décomposition de P en produit de polynômes irréductibles dans $\mathbb{L}[X]$ ou encore $\omega_\alpha(P) = \text{Max}(\{p \in \mathbb{N} \mid (X - \alpha)^p \mid P\}) = \nu_{X-\alpha}(P)$.

REMARQUE 22.29 : Avec ces notations, on a : $\omega_\alpha(P) > 0 \iff \alpha$ racine de P . Si $\omega_\alpha(P) = 1$ on dit que α est une **racine simple** de P , si $\omega_\alpha(P) = 2$ on dit que α est une **racine double** de P , etc...

Théorème 22.9

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{L}$ et $m \in \mathbb{N}$, nous avons l'équivalence entre :

- $m = \omega_\alpha(P)$.
- $\exists R \in \mathbb{L}[X]$, $P = (X - \alpha)^m R$ avec $R(\alpha) \neq 0$.
- $P(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

Théorème 22.10

Soit $P \in \mathbb{K}[X]$ de degré $d \in \mathbb{N}^*$ et $(\alpha_1, \dots, \alpha_n) \in \mathbb{L}^n$ distincts deux à deux tels que $\forall k \in [1; n]$, α_k est une racine d'ordre $m_k \geq 1$ de P , alors :

- on a $\prod_{k=1}^n (X - \alpha_k)^{m_k} \mid P$ donc $\sum_{k=1}^n m_k \leq d$,
- si $\sum_{k=1}^n m_k = d$ on a plus précisément $P = cd(P) \prod_{k=1}^n (X - \alpha_k)^{m_k}$.

DÉMONSTRATION : On constate que les $((X - \alpha_k)_k^m)_{1 \leq k \leq n}$ sont premiers entiers eux deux à deux.

REMARQUE 22.30 : Quand $P \in \mathbb{K}[X]$ peut s'écrire sous la forme précédente : $P = cd(P) \prod_{k=1}^d (X - \alpha_k)^{m_k}$ (que la somme des ordres de multiplicité de ses racines est égal à son degré), on dit que P est **scindé**.

Proposition 22.21

Soit $d \in \mathbb{N}^*$ et $P \in \mathbb{K}_d[X]$, si $(\alpha_1, \dots, \alpha_n) \in \mathbb{L}^n$ sont des racines de P avec ordres respectifs supérieurs ou égaux à $m_1, \dots, m_n$ avec $m_1 + \dots + m_n > d$, alors $P = 0$ (on dit que P possède au moins $d + 1$ racines comptées avec leur ordre de multiplicité).

22.3.4 : Polynômes irréductibles dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$

Théorème 22.11

Tout polynôme $P \in \mathbb{C}[X]$ non constant possède au moins une racine complexe : c'est le théorème de d'ALEMBERT-GAUSS.

DÉMONSTRATION : Par l'absurde, si P non constant ne s'annule pas, on admet qu'il existe alors $z_0 \in \mathbb{C}$ tel que $|P(z_0)| = \text{Min}_{z \in \mathbb{C}} |P(z)| > 0$, alors d'après TAYLOR : $P(z_0 + h) - P(z_0) = \sum_{k=1}^{+\infty} \frac{P^{(k)}(z_0)}{k!} h^k$ et en notant v la valuation de $\sum_{k=1}^{+\infty} \frac{P^{(k)}(z_0)}{k!} X^k$ on a : $P(z_0 + h) - P(z_0) \sim_0 \frac{P^{(v)}(z_0)}{v!} h^v$ qui fournit une contradiction.

REMARQUE 22.31 : Les polynômes irréductibles unitaires de $\mathbb{C}[X]$ sont de la forme $X - \alpha$ ($\alpha \in \mathbb{C}$).

Théorème 22.12

Soit $P \in \mathbb{C}[X]$ non nul, alors il existe une unique écriture (à l'ordre près) de P sous la forme $P = cd(P) \prod_{k=1}^r (X - \alpha_k)^{m_k}$ où $r \in \mathbb{N}$, $\alpha_1, \dots, \alpha_r$ sont les racines complexes distinctes deux à deux de P et $m_1, \dots, m_r$ sont les ordres de multiplicité associés.

REMARQUE 22.32 :

- Tous les polynômes complexes sont donc scindés : un polynôme de degré n admet donc n racines "comptées avec leurs ordres de multiplicité".
- On résume tout ceci en disant que $\mathbb{C}$ est un corps algébriquement clos.

Proposition 22.22

Soit $(P, Q) \in \mathbb{C}[X]$ non nuls, on a : $P|Q \iff (\forall \alpha \in \mathbb{C}, \omega_\alpha(P) \leq \omega_\alpha(Q))$.

REMARQUE 22.33 : • Soit $P = \sum_{k=0}^{+\infty} p_k X^k \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}$, il est clair que $P(\bar{\alpha}) = \overline{P(\alpha)}$.

- Plus généralement, pour $n \in \mathbb{N}^*$, $P^{(n)}(\bar{\alpha}) = \overline{P^{(n)}(\alpha)}$.
- On en déduit que l'ordre de α est le même que celui de α dans le polynôme P réel.

Proposition 22.23

Soit $P \in \mathbb{R}[X]$, il existe une unique décomposition (à l'ordre près) de P sous la forme $P = \text{cd}(P) \prod_{k=1}^r (X - \alpha_k)^{m_k} \prod_{j=1}^s (X^2 + a_j X + b_j)^{p_j}$ où $r \in \mathbb{N}$, $s \in \mathbb{N}$, $\alpha_1, \dots, \alpha_r$ sont les racines réelles de P d'ordres $m_1, \dots, m_r$ et $a_1, b_1, \dots, a_s, b_s$ des réels tels que $\forall j \in \llbracket 1; s \rrbracket$, $a_j^2 - 4b_j < 0$ et $p_1, \dots, p_s$ sont les valuations correspondantes.

REMARQUE 22.34 : Les polynômes irréductibles unitaires de $\mathbb{R}[X]$ sont de degré 1 ($X - \alpha$ avec $\alpha \in \mathbb{R}$) ou de degré 2 avec un discriminant strictement négatif ($X^2 + aX + b$ avec $(a, b) \in \mathbb{R}^2$ et $a^2 - 4b < 0$).

EXEMPLE 22.14 : Soit $P = X^3 + X + 1$, alors P est irréductible dans $\mathbb{Q}[X]$.

22.3.5 : Relations entre coefficients et racines**Définition 22.12**

Soit, pour $n \in \mathbb{N}^*$, les n fonctions symétriques élémentaires "des racines", notées $\sigma_1, \dots, \sigma_n$ et définies par : $\forall k \in \llbracket 1; n \rrbracket$, $\sigma_k : \mathbb{C}^n \rightarrow \mathbb{C}$ et $\forall (\alpha_1, \dots, \alpha_n)$, $\sigma_k(\alpha_1, \dots, \alpha_n) = \sum_{\substack{I \subset \llbracket 1; n \rrbracket \\ \text{card}(I)=k}} \left(\prod_{i \in I} \alpha_i \right)$.

EXEMPLE 22.15 : Si $n = 3$, $k = 1$: $\sigma_1(\alpha_1, \alpha_2, \alpha_3) = \alpha_1 + \alpha_2 + \alpha_3 = \sigma_1$ (abus de notation).

Théorème 22.13

Soit $P = \sum_{k=0}^d p_k X^k \in \mathbb{C}[X]$ de degré d (donc $p_d \neq 0$) ; alors en notant $\alpha_1, \dots, \alpha_d$ ses d racines (pas forcément distinctes), on a les relations entre coefficients et racines du polynôme P :

$$\forall k \in \llbracket 0; d-1 \rrbracket, \sigma_{d-k} = (-1)^{d-k} \frac{p_k}{p_d} \text{ ou } \forall k \in \llbracket 1; d \rrbracket, \sigma_k = (-1)^k \frac{p_{d-k}}{p_d}.$$

EXEMPLE 22.16 : Comme les racines de $X^n - 1$ sont les n racines n -ièmes de l'unité, si $n \geq 2$, on en déduit que leur somme est nulle, et que leur produit vaut $(-1)^{n+1}$.

REMARQUE 22.35 : Ce théorème possède une réciproque (déjà vue pour $n = 2$ au chapitre 3) :

Proposition 22.24

Soit $(\alpha_1, \dots, \alpha_n) \in \mathbb{C}^n$ (pas forcément distincts deux à deux), et aussi $(s_1, \dots, s_n) \in \mathbb{C}^n$, alors : $(\alpha_1, \dots, \alpha_n \text{ est la liste des racines de } P = X^n - \sum_{k=1}^n s_k X^{n-k}) \iff (\forall k \in \llbracket 1; n \rrbracket, s_k = \sigma_k(\alpha_1, \dots, \alpha_n))$.

REMARQUE 22.36 : Pour $n \in \mathbb{N}^*$, $(\alpha_1, \dots, \alpha_n) \in \mathbb{C}^n$ et $p \in \mathbb{N}^*$, notons $S_p = \sum_{k=1}^n \alpha_k^p$. Ce sont des fonctions symétriques : $\sigma \in \mathcal{S}_n \implies S_k(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) = S_k(\alpha_1, \dots, \alpha_n)$. On peut montrer que les fonctions $\sigma_1, \dots, \sigma_n$ sont "élémentaires" en ce sens qu'elles engendrent toutes les fonctions symétriques.

EXEMPLE 22.17 : Par exemple : $S_1 = \sigma_1$, $S_2 = \sigma_1^2 - 2\sigma_2$, $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. Et S_4 ?

PARTIE 22.4 : FRACTIONS RATIONNELLES

22.4.1 : Structure des fractions rationnelles

Définition 22.13

Soit $\mathbb{K}$ un corps commutatif, on appelle **fraction rationnelle à coefficients dans $\mathbb{K}$** un élément de la forme $F = \frac{P}{Q}$ avec $(P, Q) \in \mathbb{K}[X]^2$ avec $Q \neq 0$ avec la condition d'égalité : $\frac{P_1}{Q_1} = \frac{P_2}{Q_2} \iff P_1 Q_2 = P_2 Q_1$ (dans $\mathbb{K}[X]$). On note $\mathbb{K}(X)$ l'ensemble de toutes les fractions rationnelles.

REMARQUE 22.37 : • Il y a comme un air d'analogie avec la construction des rationnels ($\mathbb{Q}$).

- On définit dans $\mathbb{K}(X)$ les deux lois internes $+$ et $\times$ par les relations :

$$\forall (P_1, P_2, Q_1, Q_2) \in \mathbb{K}[X]^4 \text{ avec } Q_1 Q_2 \neq 0, \quad \frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{P_1 Q_2 + P_2 Q_1}{Q_1 Q_2} \text{ et } \frac{P_1}{Q_1} \times \frac{P_2}{Q_2} = \frac{P_1 P_2}{Q_1 Q_2}.$$

- On définit aussi la loi externe : $\forall (P, Q) \in \mathbb{K}[X]^2$ avec $Q \neq 0$ et $\lambda \in \mathbb{K}$, $\lambda \cdot \frac{P}{Q} = \frac{\lambda P}{Q}$.
- On vérifie comme d'habitude que ceci ne dépend pas de l'écriture des fractions.

Proposition 22.25

$(\mathbb{K}(X), +, \times)$ est un corps commutatif et $(\mathbb{K}(X), +, \times, \cdot)$ une $\mathbb{K}$ -algèbre.

REMARQUE 22.38 :

- On dit que $\mathbb{K}(X)$ est le **corps des fractions** de l'anneau commutatif intègre $\mathbb{K}[X]$.
- On peut dire que $\mathbb{K}[X]$ est "inclus" dans $\mathbb{K}(X)$ en considérant le morphisme injectif d'algèbres suivant : $\phi : \mathbb{K}[X] \rightarrow \mathbb{K}(X)$ défini par : $\forall P \in \mathbb{K}[X], \phi(P) = \frac{P}{1}$.
- On dit que $F = \frac{P}{Q}$ est **mis sous forme irréductible** si $P \wedge Q = 1$.

Définition 22.14

Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$ mis sous forme irréductible et $G \in \mathbb{K}(X)$, on définit :

- le **degré** de F , noté $\deg(F)$ par la relation : $\deg(F) = \deg(P) - \deg(Q) \in \mathbb{Z} \cup \{-\infty\}$.
- le **coefficient dominant** de F , noté $\text{cd}(F)$, par la relation : $\text{cd}(F) = \text{cd}(P)\text{cd}(Q)^{-1}$.
- les **racines** de F sont les racines de P , leurs multiplicités étant celles en tant que racines de P .
- les **pôles** de F sont les racines de Q , leurs multiplicités étant celles en tant que racines de Q .
- la **dérivée** de F , notée F' , par la relation : $F' = \frac{P'Q - PQ'}{Q^2}$.
- les **dérivées successives** de F par : $F^{(0)} = F$ et $\forall n \in \mathbb{N}, F^{(n+1)} = (F^{(n)})'$.
- la **composée** de F par G (si elle existe) par la relation $F(G) = F \circ G = \frac{P(G)}{Q(G)}$ (et on simplifie).

REMARQUE 22.39 : • La notion de racine et de composée prolonge celle vue sur les polynômes.

- Les notions de dérivée (même successives) et de coefficient dominant prolongent aussi celles de $\mathbb{K}[X]$.
- Si $F = \frac{P}{Q} \in \mathbb{K}(X)$, alors on a $\deg(F) = \deg(P) - \deg(Q)$ et aussi $\text{cd}(F) = \text{cd}(P)\text{cd}(Q)^{-1}$ et ceci même si F n'est pas mis sous forme irréductible.

Proposition 22.26

Soit $(F, G) \in \mathbb{K}(X)^2$ et $\lambda \in \mathbb{K}$, on a les relations inégalités suivantes :

- $\deg(FG) = \deg(F) + \deg(G)$, $\text{cd}(FG) = \text{cd}(F)\text{cd}(G)$, $\deg(\lambda F) = \deg(F)$ si $\lambda \neq 0$.
- $\deg(F + G) \leq \text{Max}(\deg(F), \deg(G))$ avec égalité si $\deg(F) \neq \deg(G)$.
- $(F + G)' = F' + G'$, $(\lambda F)' = \lambda F'$ et $(FG)' = F'G + FG'$; en particulier la dérivée est linéaire.
- $\left(\frac{F}{G}\right)' = \frac{F'G - FG'}{G^2}$ et $(F \circ G)' = G' \times (F' \circ G)$; les formules habituelles.
- $(FG)^{(n)} = \sum_{k=0}^n \binom{n}{k} F^{(k)} G^{(n-k)}$; pourquoi pas la formule de LEIBNIZ.

REMARQUE 22.40 : Il n'y a pas de formule simple pour le degré de la dérivée ou de la composée.

Proposition 22.27

Soit $F \in \mathbb{K}(X)$ avec F non constant, alors il existe une unique écriture (à l'ordre près) de F comme produit et rapport de polynômes irréductibles unitaires :

$$\exists! r \in \mathbb{N}^*, \exists!(P_1, \dots, P_r) \in I_{\mathbb{K}}^r \text{ (distincts deux à deux)}, \exists!(\alpha_1, \dots, \alpha_r) \in (\mathbb{Z}^*)^r, F = \text{cd}(F) \prod_{k=1}^r P_k^{\alpha_k}.$$

REMARQUE 22.41 : Pour $P \in I_{\mathbb{K}}$, on vient de prolonger la valuation ν_P ; $\nu_P : \mathbb{K}(X)^* \rightarrow \mathbb{Z}$ définie par : $\forall (A, B) \in (\mathbb{K}[X]^*)^2$, $\nu_P\left(\frac{A}{B}\right) = \nu_P(A) - \nu_P(B)$. Cette application est bien définie et est (comme pour les rationnels) un morphisme de groupes. On peut même écrire : $\forall F \in \mathbb{K}(X)^*$, $F = \text{cd}(F) \prod_{P \in I_{\mathbb{K}}} P^{\nu_P(F)}$.

EXEMPLE 22.18 : Renseignements sur $F = \frac{X^6 + 2X^4 + 2X^2 + 1}{X^6 - X^5 + X^4 - X^2 + X - 1}$?

Définition 22.15

Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$, on note $\mathcal{P}(F)$ l'ensemble des pôles de F , alors on peut définir la fonction rationnelle associée à F , c'est $\tilde{F} : \mathbb{K} \setminus \mathcal{P}(F) \rightarrow \mathbb{K}$ définie par : $\forall x \notin \mathcal{P}(F)$, $\tilde{F}(x) = \frac{\tilde{P}(x)}{\tilde{Q}(x)}$.

Proposition 22.28

Soit $(F, G) \in \mathbb{K}(X)^2$, si $\tilde{F}$ et $\tilde{G}$ coïncident en une infinité de valeurs, alors : $F = G$.

REMARQUE 22.42 : On fait donc comme pour les polynômes, comme on travaille la plupart du temps sur les corps $\mathbb{R}$ ou $\mathbb{C}$, on se débarrasse du $\sim$ pour parler de fonctions rationnelles.

22.4.2 : Décomposition en éléments simples : théorie

Proposition 22.29

Soit $F = \frac{A}{B} \in \mathbb{K}(X)$, il existe une unique écriture de la forme $F = Q + G$ avec $Q \in \mathbb{K}[X]$, $G \in \mathbb{K}(X)$ et $\deg(G) < 0$. Q est en fait le quotient de la division euclidienne de A par B et $G = \frac{R}{B}$ où R est le reste de cette même division euclidienne.

Définition 22.16

Cet unique polynôme Q est la **partie entière** de F , notée $E(F)$.

Théorème 22.14

Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$ sous forme irréductible et $Q = \prod_{i=1}^r P_i^{\alpha_i}$ unitaire où $r \in \mathbb{N}$, $(P_1, \dots, P_r) \in I_{\mathbb{K}}^r$ (distincts 2 à 2) et $(\alpha_1, \dots, \alpha_r) \in (\mathbb{N}^*)^r$, il existe une unique écriture de F sous la forme : $F = E(F) + \sum_{i=1}^r \left(\sum_{j=1}^{\alpha_i} \frac{R_{i,j}}{P_i^j} \right)$ avec $\forall i \in [1; r], \forall j \in [1; \alpha_i], R_{i,j} \in \mathbb{K}[X]$ et $\deg(R_{i,j}) < \deg(P_i)$.

DÉMONSTRATION : Exceptionnellement, on admet la **décomposition en éléments simples**.

Définition 22.17

Si $P_i = X - \alpha_i$ ci-dessus, on dit que $\sum_{j=1}^{\alpha_i} \frac{R_{i,j}}{P_i^j}$ est la **partie polaire** relative au pôle α_i .

REMARQUE 22.13 :

- Comme tout polynôme de $\mathbb{C}[X]$ est scindé, si $F = \frac{P}{Q} \in \mathbb{C}(X)$ est sous forme irréductible et si on a $Q = \prod_{k=1}^r (X - \alpha_k)^{m_k}$ alors $F = E(F) + \sum_{k=1}^r \sum_{j=1}^{m_k} \frac{\beta_{k,j}}{(X - \alpha_k)^j}$ où les $\beta_{k,j}$ sont des complexes.
- Si $F = \frac{P}{Q} \in \mathbb{R}(X)$ est sous forme irréductible et si $Q = \prod_{k=1}^r (X - \alpha_k)^{m_k} \prod_{j=1}^s (X^2 + a_j X + b_j)^{p_j}$ alors : $F = E(F) + \sum_{k=1}^r \sum_{i=1}^{m_k} \frac{\beta_{k,i}}{(X - \alpha_k)^i} + \sum_{j=1}^s \sum_{i=1}^{p_j} \frac{\gamma_{j,i} X + \delta_{j,i}}{(X^2 + a_j X + b_j)^i}$ où les $\beta_{k,i}$, les $\gamma_{j,i}$ et les $\delta_{j,i}$ sont des réels.

Proposition 22.30

Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$ sous forme irréductible de pôle simple α , d'où $Q = (X - \alpha)R$ avec $R(\alpha) \neq 0$, alors la **partie polaire** relative à α est $\frac{\beta}{X - \alpha}$ avec $\beta = \frac{P(\alpha)}{R(\alpha)} = \frac{P(\alpha)}{Q'(\alpha)}$.

REMARQUE 22.14 : Soit $P \in \mathbb{C}[X]$ de degré $n \geq 1$, alors $P = \text{cd}(P) \prod_{k=1}^r (X - \alpha_k)^{m_k}$ où $\alpha_1, \dots, \alpha_r$ sont les racines distinctes de P et $m_1, \dots, m_r$ leurs ordres respectifs. Alors, on a : $\frac{P'}{P} = \sum_{k=1}^r \frac{m_k}{X - \alpha_k}$.

22.4.3 : Décomposition en éléments simples : pratique

⊙ On vous donne une fraction $F = \frac{P}{Q} \in \mathbb{K}[X]$ en vous demandant de la décomposer dans $\mathbb{K}(X)$.

REMARQUE 22.45 : Algorithme :

- **Étape 1** : on met F sous forme irréductible.
- **Étape 2** : on calcule la partie entière de F .
- **Étape 3** : on écrit la décomposition a priori de F en éléments simples dans $\mathbb{K}(X)$ (le nombre de paramètres de cette décomposition doit être égal au degré du dénominateur).
- **Étape 4** : on détermine ces paramètres avec les techniques déjà vues ou ci-dessous.

⊙ On suppose dans toute la suite que $F = \frac{P}{Q}$ est mis sous forme irréductible et vérifie $\deg(F) < 0$.

REMARQUE 22.46 : Techniques :

- **Technique 1** : on réduit au même dénominateur et on procède par identification (à éviter).
- **Technique 2** : si α est un pôle simple, d'après la proposition 22.30, le terme β_1 tel que $\frac{\beta_1}{(X - \alpha)}$ est la partie polaire relative à α vérifie $\beta_1 = \frac{P(\alpha)}{R(\alpha)} = \frac{P(\alpha)}{Q'(\alpha)}$; codé par $\times(X - \alpha)$ et $X \leftarrow \alpha$.
- **Technique 3** : si α est un pôle d'ordre n alors $Q = (X - \alpha)^n R$ avec $R(\alpha) \neq 0$, on généralise la technique précédente : le terme β_n tel que $\frac{\beta_n}{(X - \alpha)^n}$ fait partie de la partie polaire relative à α vérifie la relation $\beta_n = \frac{P(\alpha)}{R(\alpha)} = \frac{n!P(\alpha)}{Q^{(n)}(\alpha)}$; codé par $\times(X - \alpha)^n$ et $X \leftarrow \alpha$.
- **Technique 4** : on fait tendre x vers $+\infty$ dans la fonction rationnelle associée à $XF(x)$, ce qui donne : $\lim_{x \rightarrow +\infty} xF(x) = \sum_{k=1}^r \beta_{k,1}$ si $F \in \mathbb{C}(X)$ avec l'expression de la remarque 22.43 ; codé par $\times X$ et $X \leftarrow +\infty$.
- **Technique 5** : on prend une valeur particulière dans la fonction rationnelle F (hors de ses pôles), pour obtenir une relation supplémentaire entre les paramètres de la décomposition ; codé par $X \leftarrow \alpha$.
- **Technique 6** : on utilise la parité ou l'imparité éventuelle de F et l'unicité de la décomposition en éléments simples pour réduire le nombre de paramètres.
- **Technique 7** : on passe par les complexes pour décomposer une fraction $F \in \mathbb{R}(X)$: là encore on réduit de moitié le nombre de paramètres complexes ; on recompose la décomposition réelle ensuite.
- **Technique 8** : si $F \in \mathbb{R}(X)$ et que $(X^2 + aX + b)$ (avec a, b réels, $a^2 - 4b < 0$ et $\alpha \in \mathbb{C} \setminus \mathbb{R}$ racine de $X^2 + aX + b$) apparaît en facteur dans Q avec un exposant 1, alors on trouve simultanément β_1 et γ_1 réels tels que $\frac{\beta_1 X + \gamma_1}{X^2 + aX + b}$ soit dans la décomposition en remplaçant X par α dans $(X^2 + aX + b)F$ et en identifiant partie réelle et partie imaginaire ; codé par $\times(X^2 + aX + b)$ et $X \leftarrow \alpha$.
- **Technique 9** : si $F \in \mathbb{R}(X)$ et que $(X^2 + aX + b)$ (avec a, b réels, $a^2 - 4b < 0$ et $\alpha \in \mathbb{C} \setminus \mathbb{R}$ racine de $X^2 + aX + b$) apparaît en facteur dans Q avec un exposant m , alors on trouve simultanément β_m et γ_m réels tels que $\frac{\beta_m X + \gamma_m}{(X^2 + aX + b)^m}$ soit dans la décomposition en remplaçant X par α dans $(X^2 + aX + b)^m F$ et en identifiant partie réelle et partie imaginaire ; codé par $\times(X^2 + aX + b)^m$ et $X \leftarrow \alpha$.

EXEMPLE 22.19 : Voici quelques fractions à décomposer avec les différentes techniques :

- $\frac{X^4 - 2}{X^3 - 3X^2 + 2X}$ dans $\mathbb{R}(X)$: partie entière et technique 2.1 seulement.
- $\frac{1}{X^n - 1}$ dans $\mathbb{C}(X)$: technique 2.2 uniquement..
- $\frac{1}{X^4 + X^2}$ dans $\mathbb{R}(X)$: techniques 3, 4 (adaptée) et 6 ou plus simplement technique 2.
- $\frac{1}{(X^4 + X^2 + 1)(X^2 + 1)^2 X(X^2 - 1)}$ dans $\mathbb{R}(X)$: techniques 2.1, 4, 5, 6, 7, 8, 9.