Logique, Ensembles et applications, Polynomes et Fractions rationelles

1 Bases de la logique

- A/ 1) Une proposition (ou assertion) est un énoncé mathématique qui a une et une seule valeur : vrai ou faux.
 - 2) La négation de la proposition P est la proposition qui est vraie si et seulement si P est fausse. Elle est notée nonP.
 - 3) Si P et Q sont deux propositions, P et Q est la proposition qui est vraie si et seulement si P et Q sont toutes les deux vraies.
 - 4) Si P et Q sont deux propositions, P ou Q est la proposition qui est vraie si et seulement si au moins une des deux propositions P ou Q est vraie.
- B/ Les opérateurs non, et, ou, sont reliés par les formules suivantes :

non
$$(P \text{ et } Q)=(\text{non } P) \text{ ou } (\text{non } Q).$$

non $(P \text{ ou } Q)=(\text{non } P) \text{ et } (\text{non } Q).$

- C/ L'implication $P \implies Q$ est la proposition non P ou Q. Pour démontrer $P \implies Q$, on suppose que P est vraie et on démontre que Q est vraie. La négation de la proposition $P \implies Q$ est donc la proposition P et non Q.
- D/ On dit que les proposition P et Q sont équivalentes lorsque l'on a à la fois $P \Longrightarrow Q$ et $Q \Longrightarrow P$ qui sont vraies. On note alors $P \Longleftrightarrow Q$.
- E/ La contraposée de la proposition $P \implies Q$ est la proposition non $Q \implies$ non P. Les deux propositions $P \implies Q$ et non $Q \implies$ non P sont équivalentes. L'une est vraie si et seulement si l'autre est vraie.

F/ Quantificateurs:

- a) Le quantificateur pour tout ou quel que soit est noté \forall . La proposition $\forall x \in E$, P(x) est vraie lorsque, pour tout $x \in E$, la proposition P(x) est vraie.
- b) Le quantificateur il existe (au moins un) est noté \exists . La proposition $\exists x \in E$, P(x) est vraie lorsqu'il existe au moins un $x \in E$ telle que la proposition P(x) soit vraie.
- c) Le quantificateur il existe un unique est noté $\exists !$. La proposition $\exists !x \in E$, P(x) est vraie lorsqu'il existe un unique $x \in E$ telle que la proposition P(x) soit vraie.
- d) La négation de $\forall x \in E$, P(x) est $\exists x \in E$, non P(x).
- e) La négation de $\exists x \in E$, P(x) est $\forall x \in E$, non P(x).
- G/ Conditions nécessaires, conditions suffisantes :

Lorsque $P \implies Q$, on dit que P est une condition suffisante à Q, et que Q est une condition nécessaire à P.

H/ Méthodes de raisonnement

- 1) Par implication : pour prouver que $P \implies Q$, on suppose que P est vraie et on utilise différentes propriétés déjà connues pour établir que Q est vraie.
- 2) Par double implication / par équivalence : Pour démontrer que $P \iff Q$, il y a deux méthodes standard :
 - i) On raisonne par double implication : on suppose d'abord que P est vraie, et on démontre que Q est vraie. Ensuite, on suppose que Q est vraie, et on démontre que P est vraie.
 - ii) On passe de P à Q en utilisant uniquement des équivalences. C'est une méthode souvent déconseillée, car il faut faire très attention à ce que chaque enchaînement logique de la démonstration est bien une équivalence.
- 3) Par contraposée : pour démontrer que $P \implies Q$, il suffit de démontrer la contraposée de cette proposition, c'est-à-dire non $Q \implies$ non P.
- 4) Par l'absurde : pour démontrer que $P \implies Q$, on peut supposer que P et non Q sont toutes les deux vraies, et obtenir une contradiction; pour démontrer que P est vraie, on peut supposer que non P est vraie et obtenir une contradiction.
- 5) Par récurrence : Le raisonnement par récurrence est utilisé pour démontrer des propriétés qui dépendent d'un entier n. Il est basé sur le principe suivant :

Soit P(n) une propriété concernant un entier naturel n. On suppose que P(0) est vraie et que, pour tout entier naturel k, si P(k) est vraie, alors P(k+1) est vraie. Alors la propriété P(n) est vraie pour tout entier naturel n.

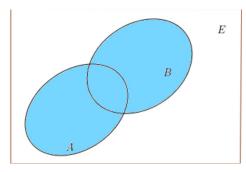
Pour bien rédiger une démonstration par récurrence, il est nécessaire de faire apparaître clairement les 4 étapes : définir précisément quelle est la propriété P(n) que l'on souhaite démontrer, écrire la phase d'initialisation, la phase d'hérédité, puis la conclusion. Il existe deux erreurs fréquentes de rédaction de la phase d'hérédité.

- i) commencer cette phase par la phrase : "supposons que, pour tout $n \in \mathbb{N}$, P(n) est vraie et prouvons P(n+1)". Si P(n) est vraie pour tout entier n, il n'y a plus rien à prouver!
- ii) Commencer cette phase par la phrase : supposons qu'il existe un $n \in \mathbb{N}$ tel que P(n) est vraie et prouvons P(n+1). L'erreur est plus subtile. Le principe de récurrence s'écrit formellement $\left(P(0) \text{ vraie } ET \ (\forall n \in \mathbb{N} \ P(n) \implies P(n+1)\right) \implies \forall n \in \mathbb{N}, P(n) \text{ vraie. La}$ dernière rédaction serait correcte si le principe de récurrence s'écrivait $\left(P(0) \text{ vraie } ET \ (\exists n \in \mathbb{N} \ P(n) \implies P(n+1)\right) \implies \forall n \in \mathbb{N}, P(n) \text{ vraie. ce qui est faux}$

2 Ensembles, applications, relations

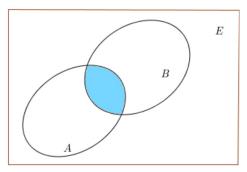
- A/ On appelle élément d'un ensemble E tout objet qui appartient à E.
- B/ Si E et F sont deux ensembles, on dit que E est une partie de F, que E est un sous-ensemble de F, ou encore que E est inclus dans F si tout élément de E est aussi élément de F. On note $E \subset F$.
- C/ Il existe un unique ensemble qui ne contient aucun élément, l'ensemble vide. Il est noté ∅.
- D/ Un ensemble peut être écrit en extension, c'est-à-dire que l'on donne la liste de tous ses éléments, ou en compréhension, c'est-à-dire que l'on définit cet ensemble par une propriété. Par exemple, $E = \{a,b,c,d\}$ est défini en extension, et $F = \{n \in \mathbb{N}; 2 \le n < 6\}$ est défini en compréhension.

- E/ L'ensemble des parties de E est lui-même un autre ensemble, appelé ensemble des parties et noté $\mathcal{P}(E)$.
- F/ Étant donné un ensemble E et deux parties A et B de E, on peut définir
 - i) La réunion de A et B, noté $A \cup B$. $A \cup B$ est l'ensemble des éléments qui appartiennent à A ou à B



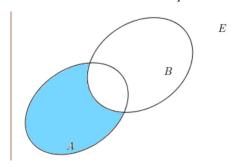
On a toujours $A \subset A \cup B$ et $B \subset A \cup B$.

ii) L'intersection de A et B, noté $A \cap B$. $A \cap B$ est l'ensemble des éléments qui appartiennent à A et à B.

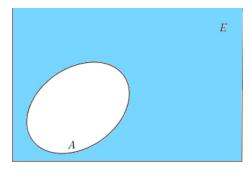


On a toujours $A \cap B \subset A$ et $A \cap B \subset B$.

iii) La différence $A \setminus B : A \setminus B$ est l'ensemble des éléments qui sont dans A, mais pas dans B.



iv) Le complémentaire de A dans E, noté \bar{A} , ou C_EA , ou $E \setminus A$, l'ensemble des éléments de E qui ne sont pas dans A.



v) Si E et F sont deux ensembles, le produit cartésien de E et F, noté $E \times F$, est l'ensemble constitué de tous les couples (x, y), où x est un élément de E et y est un élément de F.

3 Applications

- A/ Soient E et F deux ensembles. Une application de E dans F associe à tout élément de E un unique élément de F. L'ensemble des applications de E dans F est noté $\mathcal{F}(E,F)$, ou F^E .
- B/ On appelle graphe de l'application $f: E \to F$ la partie Γ de $E \times F$ définie par

$$\Gamma = \{(x, f(x)) \mid x \in E\}.$$

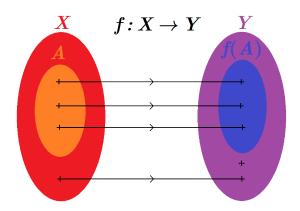
C/ Si A est une partie de E, l'application indicatrice de A, notée $\mathbf{1}_A$, est la fonction définie par

$$\mathbf{1}_{A}(x) = \begin{cases} 1 & si \ x \in A \\ 0 & sinon. \end{cases}$$

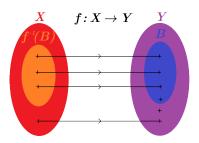
- D/ Si E est un ensemble, l'application identité de E est la fonction Id_E , définie de E dans E par $Id_E(x) = x$.
- E/ Si f est une fonction de E dans F, on appelle restriction de f à A, et on note $f_{|A}$ la fonction définie sur A par

$$f_{|A}(x) = f(x).$$

F/ Si f est une application de E dans F et si A est une partie de E, on appelle image directe de A par f l'ensemble $f(A) := \{f(x); x \in A\}$. Ainsi, $y \in f(A) \iff \exists x \in A, y = f(x)$.



G/ Si f est une application de E dans F et si B est une partie de F, on appelle image réciproque de B par f l'ensemble $f^{-1}(B) = \{x \in E; f(x) \in B\}$. Ainsi, $x \in f^{-1}(B) \iff f(x) \in B$.



H/ Si E, F et G sont trois ensembles et si $f: E \to F$ et $g: F \to G$ sont deux applications, on appelle application composée de f et g l'application notée $g \circ f: E \to G$ définie par la formule

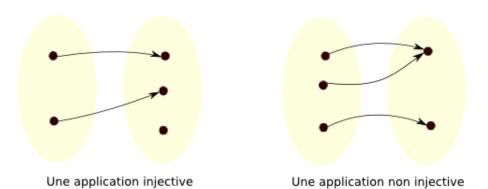
4

$$g \circ f(x) := g(f(x)).$$

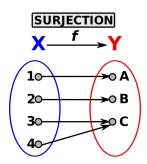
4 Injection, surjection, bijection

Soit $f: E \to F$ une application. On dit que f est

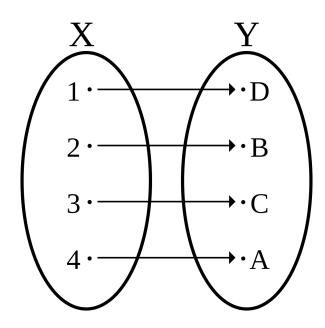
1) injective pour tout couple $(x, x') \in E^2$, si f(x) = f(x'), alors x = x'.



2) surjective si, pour tout $y \in F$, l'équation y = f(x) admet au moins une solution $x \in E$.



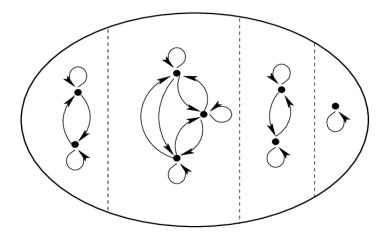
3) bijective si, pour tout $y \in F$, l'équation y = f(x) admet exactement une solution $x \in E$.



5 Relations binaires

On appelle relation binaire sur un ensemble E la donnée d'une partie Γ de $E \times E$. On dit que x est en relation avec y et on écrit $x\mathcal{R}y$ lorsque $(x,y) \in \Gamma$. On dit que la relation \mathcal{R} est

- *i)* réflexive si, pour tout $x \in E$, xRx.
- ii) symétrique si, pour tous $x, y \in E$, si xRy, alors yRx.
- iii) anti-symétrique si, pour tous $x, y \in E$, si xRy et yRx, alors x = y.
- iv) transitive si, pour tous $x, y, z \in E$, si xRy et yRz, alors xRz.
- 1) Une relation d'équivalence est une relation réflexive, symétrique, transitive. Si R est une relation d'équivalence et x est un élément de E, on appelle classe d'équivalence de x l'ensemble des éléments y de E tels que xRy. Soit E un ensemble muni d'une relation d'équivalence R. Alors les classes d'équivalence pour R forment une partition de E.



- 2) Une relation d'ordre est une relation réflexive, anti-symétrique, transitive. $Si \prec est$ une relation d'ordre sur E, alors :
 - a) on dit que l'ordre est total si on peut toujours comparer deux éléments de E: pour tous $x,y \in E$, on a x < y ou y < x. Dans le cas contraire, on dit que l'ordre est partiel.
 - b) si A est une partie de E et M est un élément de E, on dit que M est un majorant de A si, pour tout $x \in A$, on a x < M.

6 Polynômes

\mathbb{K} désigne le corps \mathbb{R} ou \mathbb{C} .

- A/ On appelle polynôme à coefficients dans \mathbb{K} une suite finie $(a_0,...,a_N)$ d'éléments de \mathbb{K} . On note ce polynôme $\sum_{n\geq 0}a_nX^n$, où X est appelée l'indéterminée. On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} .
- B/ On définit sur $\mathbb{K}[X]$ les opérations suivantes : $Si\ P(X) = \sum_{n\geq 0} a_n X^n$ et $Q(X) = \sum_{n\geq 0} b_n X^n$ (où les suites (a_n) et (b_n) sont nulles à partir d'un certain rang), on pose

 $(P+Q)(X) = \sum_{n>0} (a_n + b_n)X^n$

$$(PQ)(X) = \sum_{n>0} c_n X^n \text{ où } c_n = \sum_{k=0}^n a_k b_{n-k}.$$

Ces deux opérations font de $\mathbb{K}[X]$ un anneau.

C/ Soient $A, B \in \mathbb{K}[X]$, avec $B = \sum_{n=0}^{N} b_n X^n$. Alors on appelle composé de A par B le polynôme de $\mathbb{K}[X]$

$$B \circ A = \sum_{n=0}^{N} b_n A^n.$$

- D/ Si $P = \sum_{n \geq 0} a_n X^n$ n'est pas nul, il existe un plus grand indice $n \in \mathbb{N}$ tel que $a_n \neq 0$. Cet entier s'appelle le degré de P, noté $\deg(P)$. Le coefficient a_n correspondant s'appelle le coefficient dominant de P. Par convention, si P est nul, son degré vaut $-\infty$.
- E/ Un polynôme de coefficient dominant égal à 1 est appelé unitaire.
- F/ Pour tous polynômes $P, Q \in \mathbb{K}[X]$ non nuls, on a

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

$$deg(PQ) = deg(P) + deg(Q)$$

$$deg(P \circ Q) = deg(P) \times deg(Q).$$

On note $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} de degré inférieur ou égal à n.

G/ Dérivation:

Pour $P = \sum_{n\geq 0} a_n X^n$, on note $P' = \sum_{n\geq 1} n a_n X^{n-1}$ appelé polynôme dérivé de P. Si $\deg(P) \geq 1$, alors $\deg(P') = \deg(P) - 1$.

i) Formule de Leibniz: Pour $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$, alors

$$(PQ)^{(n)} = \sum_{k=0}^{n} {n \choose k} P^{(k)} Q^{(n-k)}.$$

- ii) Formule de Taylor : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors $P(X) = \sum_{n \geq 0} \frac{P^{(n)}(a)}{n!} (X a)^n$.
- H/ Divisibilité, division euclidienne
 - 1) Soit $P,Q \in \mathbb{K}[X]$ avec Q non nul. On dit que Q divise P s'il existe $A \in \mathbb{K}[X]$ tel que P = AQ. On dit aussi que Q est un diviseur de P ou que P est un multiple de Q.
 - 2) Deux polynômes non nuls P et Q de $\mathbb{K}[X]$ sont dits associés si P divise Q et si Q divise P. Ceci revient à dire qu'il existe $\alpha \in \mathbb{K}^*$ tel que $P = \alpha Q$.
 - 3) Théorème (division euclidienne des polynômes) : Soit $P,Q \in \mathbb{K}[X]$ avec Q non nul. Il existe un unique couple $(A,R) \in \mathbb{K}[X]$ tel que P = AQ + R et $\deg(R) < \deg(Q)$.
 - 4) Fonction polynomiale, racine: Un polynôme $P = \sum_{n=0}^{N} a_n X^n \in \mathbb{K}[X]$ définit une fonction polynomiale $\tilde{P} : \mathbb{K} \to \mathbb{K}$ par $\tilde{P}(z) = \sum_{n=0}^{N} a_n z^n$. Le plus souvent, on identifie polynôme et fonction polynomiale. On dit que a est une racine de P si P(a) = 0. Ceci est équivalent à dire que (X a) divise P.
 - i) Si a_1, \ldots, a_p sont des racines distinctes de P, alors $(X a_1) \cdots (X a_p)$ divise P.

- ii) Un polynôme de degré $n \ge 0$ admet au plus n racines.
- iii) Soit $P \in \mathbb{K}[X]$, soit $a \in \mathbb{K}$ et soit $m \in \mathbb{N}$. On dit que a est racine d'ordre de multiplicité m si

$$P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$$
 et $P^{(m)}(a) \neq 0$.

Les assertions suivantes sont équivalentes :

- i) a est racine de P de multiplicité m.
- ii) $(X-a),...,(X-a)^m$ divisent P, et $(X-a)^{m+1}$ ne divise pas P.
- iv) Un polynôme $P \in \mathbb{K}[X]$ de degré m est dit scindé s'il se factorise en

$$P(X) = a_m \prod_{j=1}^{m} (X - z_j)$$

5) Arithmétique des polynômes

Soit P,Q dans $\mathbb{K}[X]$ non nuls. Tout diviseur commun à P et Q de degré maximal est appelé pgcd de P et Q. Tous les pgcd de P et Q sont associés. En particulier, un seul est unitaire, on l'appelle parfois le pgcd de P et Q. Il est noté $P \wedge Q$. Comme pour les entiers, le pgcd de deux polynômes peut se calculer à l'aide de divisions euclidiennes successives et de l'algorithme d'Euclide.

On dit que P et Q sont premiers entre eux si $P \wedge Q = 1$.

- i) Théorème de Bézout : Soient $P, Q \in \mathbb{K}[X]$ non-nuls. Alors $P \wedge Q = 1$ si et seulement s'il existe $U, V \in \mathbb{K}[X]$ tels que PU + QV = 1.
- ii) Lemme de Gauss : Soient $P, Q, T \in \mathbb{K}[X]$ non-nuls. On suppose que $P \wedge Q = 1$. Alors si P|QT, on a P|T.

Soient P,Q dans $\mathbb{K}[X]$ non-nuls. Tout multiple commun à P et Q de degré minimal est appelé ppcm de P et Q. Tous les ppcm de P et Q sont associés. En particulier, un seul est unitaire, on l'appelle parfois le ppcm de P et Q. Il est noté $P \vee Q$.

- 6) Polynômes irréductibles
 - a) Théorème de d'Alembert-Gauss : Tout polynôme de $\mathbb{C}[X]$ non-constant admet une racine dans \mathbb{C} . Par conséquent, tout polynôme non-constant de $\mathbb{C}[X]$ est scindé.
 - b) Un polynôme $P \in \mathbb{K}[X]$ est irréductible s'il est de degré supérieur ou égal à 1 et si tous ses diviseurs sont les polynômes constants ou les polynômes associés à P (c'est-à-dire les polynômes qui s'écrivent λP avec $\lambda \in \mathbb{K}$).
 - c) Décomposition en produit d'irréductibles sur $\mathbb{C}[X]$:
 - i) Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
 - ii) Tout polynôme non nul est produit de son coefficient dominant et de polynômes irréductibles unitaires. Cette décomposition est unique à l'ordre des termes près. En particulier, tout polynôme $P \in \mathbb{C}[X]$ non-constant se factorise en

$$P(X) = a_N \prod_{k=1}^{r} (X - z_k)^{\mu_k}$$

où $z_1,...,z_r$ sont les racines distinctes de Pdans $\mathbb C$ de multiplicités respectives $\mu_1,...,\mu_r$.

Corollaire :Soit $P,Q \in \mathbb{K}[X]$ avec Q non nul. Alors Q divise P si et seulement si toutes les racines de Q sont des racines de P, et leur multiplicité en tant que racine de P est supérieure ou égale à leur multiplicité en tant que racine de Q.

En particulier, deux polynômes non nuls de $\mathbb{C}[X]$ sont premiers entre eux si et seulement s'ils n'ont pas de racines communes.

- d) Décomposition en produit d'irréductibles sur $\mathbb{R}[X]$:
 - i) Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.
 - ii) Tout polynôme non nul est produit de son coefficient dominant et de polynômes irréductibles unitaires. Cette décomposition est unique à l'ordre des termes près.

7 Corps des fractions, opérations, degré

- a) Une fraction rationnelle à coefficients dans \mathbb{K} est le quotient $\frac{P}{Q}$ de deux polynômes de $\mathbb{K}[X]$ avec $Q \neq 0$. Par définition, $\frac{P}{Q} = \frac{R}{S}$ si et seulement si PS = QR. On note $\mathbb{K}(X)$ l'ensemble des fractions à coefficients dans \mathbb{K} .
- b) On définit l'addition et la multiplication de fractions rationnelles de façon naturelle :

$$\frac{P}{Q} + \frac{R}{S} = \frac{PS + RQ}{QS}, \qquad \frac{P}{Q} \times \frac{R}{S} = \frac{PR}{QS}.$$

Muni de ces deux opérations, $\mathbb{K}(X)$ est un corps.

- c) Le degré d'une fraction rationnelle $\frac{P}{Q}$ est par définition $\deg(P) \deg(Q)$. C'est un élément de $\mathbb{Z} \cup \{-\infty\}$.
- e) Fraction irréductible, zéros, pôles
 - i) Une fraction rationnelle $F \in \mathbb{K}(X)$ s'écrit $\frac{P}{Q}$ où $P,Q \in \mathbb{K}[X]$ sont premiers entre eux. Cette écriture est unique, à un facteur multiplicatif près. Elle s'appelle la représentation irréductible de F.
 - ii) Si $F \in \mathbb{K}(X)$ s'écrit sous forme irréductible $\frac{P}{Q}$, alors les zéros de F sont les zéros de F, les pôles de F sont les zéros de F. La multiplicité d'un zéro ou d'un pôle de F est par définition sa multiplicité en tant que zéro de F ou de F.
- c) Décomposition en éléments simples
 - i) Si $F = \frac{P}{Q} \in \mathbb{K}(X)$, on appelle partie entière de F le quotient dans la division euclidienne de P par Q.
 - ii) Théorème : Soit $F \in \mathbb{K}(X)$ une fraction rationnelle non-nulle. Alors il existe un unique polynôme $E \in \mathbb{K}[X]$, des uniques polynômes irréductibles H_1, \ldots, H_p des uniques polynômes $J_{i,k}$ pour $1 \le i \le p$ et $1 \le k \le n_i$ avec $\deg(J_{i,k}) < \deg(H_i)$ tels que

$$F = E + \sum_{i=1}^{p} \left(\frac{J_{i,1}}{H_i} + \frac{J_{i,2}}{H_i^2} + \dots + \frac{J_{i,n_i}}{H_i^{n_i}} \right).$$

De plus, E est la partie entière de F, et si $\frac{P}{Q}$ est une représentation irréductible de F, alors on a

$$Q=\lambda H_1^{n_1}\cdots H_p^{n_p},\ \lambda\in\mathbb{K}\backslash\{0\}.$$

iii) Décomposition en éléments simples sur \mathbb{C} : Soit $F = \frac{P}{Q} \in \mathbb{C}(X)$ non-nulle écrite sous forme irréductible et soit E la partie entière de la fraction rationnelle. Si Q se factorise dans \mathbb{C} sous la forme $\prod_{k=1}^{r} (X - z_k)^{\mu_k}$, alors il existe une unique famille $(\lambda_{k,j})$ de complexes telle que

$$F(X) = E(X) + \sum_{k=1}^{r} \left(\sum_{j=1}^{\mu_k} \frac{\lambda_{k,j}}{(X - z_k)^j} \right).$$

iv) Décomposition en éléments simples sur \mathbb{R} : Soit $F = \frac{P}{Q} \in \mathbb{R}(X)$ non-nulle écrite sous forme irréductible et soit E la partie entière de la fraction rationnelle. Si Q se factorise dans \mathbb{R} sous la forme $\prod_{k=1}^r (X-z_k)^{\mu_k} \prod_{k=1}^s (X^2+\beta_k X+\gamma_k)^{\nu_k}$ avec $\beta_k^2-4\gamma_k<0$, alors il existe trois uniques familles $(\lambda_{k,j})$, $(\theta_{k,j})$ et $(\tau_{k,j})$ de réels telle que

$$F(X) = E(X) + \sum_{k=1}^{r} \left(\sum_{j=1}^{\mu_k} \frac{\lambda_{k,j}}{(X - z_k)^j} \right) + \sum_{k=1}^{s} \left(\sum_{j=1}^{\nu_k} \frac{\theta_{k,j} X + \tau_{k,j}}{(X^2 + \beta_k X + \gamma_k)^j} \right).$$