Polynômes et fractions rationnelles

Table des matières

1 Construction de l'anneau des polynômes **1**

2 Division euclidienne et conséquences **4**

3 Fonctions polynomiales et dérivation **6**

4 Plus grand commun diviseur et plus petit commun multiple **8**

5 Aspects calculatoires **11**

6 Fractions rationnelles **12**

Notre programme est d'étudier l'arithmétique dans l'anneau $\mathbb{Z}$ des entiers relatifs et dans l'anneau $k[X]$ des polynômes à coefficients dans un corps k. La théorie dans ces deux cas repose sur la division euclidienne et est tout à fait similaire. Nous nous concentrons ici uniquement sur l'anneau $k[X]$.

Tout au long de ce cours, on fixe un corps k.

1 Construction de l'anneau des polynômes

Avant même de donner une définition formelle des polynômes, nous savons bien, ne serait-ce que pour avoir manié le *trinôme* aX^2+bX+c depuis longtemps, qu'un polynôme est une expression de la forme $a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$, où les a_i sont des éléments de k et X est une « indéterminée ». Nous savons aussi comment additionner ou multiplier deux polynômes.

Pour définir l'anneau des polynômes, la seule question qui se pose est de donner un sens mathématique précis à la phrase « une expression de la forme $a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$ ». On résout ce problème en identifiant une telle expression à la suite des coefficients $(a_i)_{i\geqslant 0}$ qui y apparaissent (convenons que $a_i=0$ pour $i>n$). Dans la suite, nous dirons qu'une suite $(a_i)_{i\geqslant 0}$ est *presque nulle* si elle possède un nombre fini de coefficients non nuls.

1.1 Théorème. *L'ensemble A des suites $(a_i)_{i\geqslant 0}$ presque nulles à valeurs dans k est un sous-k-espace vectoriel de l'espace de toutes les suites à valeurs dans k. De plus, la loi interne $\times$ définie par*

$$(a_i)\times(b_i)=(c_i)\quad \text{où}\quad c_i \overset{\text{déf}}{=} \sum_{r+s=i} a_r b_s \text{ pour tout } i\geqslant 0$$

munit A d'une structure d'anneau commutatif dont le neutre pour la loi $\times$ est la suite $1_A \overset{\text{déf}}{=} (1,0,0,\dots)$ et telle que l'application $k\to A$ qui envoie λ sur $\lambda 1_A$ est un morphisme injectif d'anneaux.

Preuve : On doit montrer que A est un sous-espace vectoriel, que le produit $(a_i) \times (b_i)$ est dans A, que la loi $\times$ est associative et commutative d'élément neutre 1_A, et qu'elle est distributive sur $+$.

Le fait que A est un sous-k-espace vectoriel de l'espace $k^{\mathbb{N}}$ des suites à valeurs dans k est un exercice facile. Maintenant, soient (a_i) et (b_i) deux suites dans A. Vérifions que la suite $(c_i) = (a_i) \times (b_i)$ est dans A. Supposons que $a_r = 0$ pour $r > d$ et $b_s = 0$ pour $s > e$. Alors si $a_r b_s \neq 0$, on doit avoir $r \leqslant d$ et $s \leqslant e$ donc $r + s \leqslant d + e$. Par contraposée, si $i > d + e$ alors pour chaque paire (r, s) telle que $r + s = i$ on a $a_r b_s = 0$ donc $c_i = 0$. Ceci montre que la suite (c_i) est presque nulle, donc $\times$ définit une loi interne sur A. Le fait que cette loi est associative revient à voir (nous laissons à la lectrice le soin de le faire en détail) que le coefficient d'incide i dans les deux expressions $((a_i) \times (b_i)) \times (c_i)$ et $(a_i) \times ((b_i) \times (c_i))$ est égal dans les deux cas à

$$\sum_{r+s+t=i} a_r b_s c_t.$$

Il est clair que $\times$ est commutative, car la formule $c_i = \sum a_r b_s$ est symétrique en (a_i) et (b_i). En utilisant la formule qui donne le produit et le fait que 1_A est égal à la suite $(\delta_{i,0})$, on voit immédiatement que 1_A est neutre pour le produit. Enfin, pour montrer que $\times$ est distributive sur $+$ il suffit d'observer que la formule $c_i = \sum a_r b_s$ est bilinéaire, i.e. linéaire en (a_i) (quand (b_i) est fixé) et (b_i) (quand (a_i) est fixé). □

Dans la suite, comme d'habitude, on écrira les produits dans A en omettant le signe « $\times$ ».

1.2 Définition. L'anneau A de la proposition précédente est appelé l'*anneau des polynômes en une variable à coefficients dans k.*

Et l'indéterminée X de notre trinôme fondateur $aX^2 + bX + c$, qu'est-elle devenue ? Sa suite de coefficients est bien sûr $(0, 1, 0, 0, \dots)$ et c'est sous cette forme que nous allons lui (re-)donner vie.

1.3 Lemme. (1) *Soit X le polynôme $(0, 1, 0, 0, \dots)$. Alors $X^k = (0, \dots, 0, 1, 0, \dots)$ pour tout entier $k \geqslant 1$, où le coefficient non nul est à l'indice k. En d'autres termes, on a $X^k = (a_i)$ avec $a_i = \delta_{i,k}$.*
(2) *Soit $P = (a_i)$ un polynôme, avec $a_i = 0$ si $i > n$. Alors, on a $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ où l'on note a_0 au lieu de $a_0 1_A$.*

Preuve : On démontre (1) par récurrence sur k. Pour $k = 1$ il n'y a rien à démontrer. Si l'on suppose que $X^k = (\delta_{i,k})_{i \geqslant 0}$, alors le coefficient d'incide i de $X^{k+1} = X^k \times X$ est égal à la somme des $\delta_{r,k}\delta_{s,1}$, portant sur tous les indices r, s tels que $r + s = i$. Ce terme est non nul seulement si $r = k$ et $s = 1$, donc le seul coefficient non nul de X^{k+1} est celui d'indice $i = r + s = k + 1$, et il vaut 1. Ceci démontre la propriété de récurrence au cran $k + 1$. La preuve de (2) en découle directement en utilisant la loi externe et l'addition dans l'espace des suites, car le polynôme $a_i X^i$ est égal à la suite dont le seul coefficient non nul est a_i en position i. □

1.4 Définitions. On appelle X une *indéterminée*, et on notera dorénavant $k[X]$ l'anneau des polynômes en l'indéterminée X à coefficients dans k. Compte tenu du théorème 1.1, on identifie k au sous-anneau de $k[X]$ des polynômes de la forme $\lambda = \lambda 1_{k[X]}$, que l'on appelle les *polynômes constants*. Enfin, un polynôme de la forme $a_i X^i$ est appelé un *monôme*.

1.5 Définitions. Soit $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ un polynôme en X.

(1) Si $P \neq 0$, on appelle *degré de P* et l'on note $\deg(P)$ le plus grand des indices i tels que $a_i \neq 0$. Si $P = 0$, on pose $\deg(P) = -\infty$.

(2) Si $P \neq 0$, on appelle *valuation de* P et l'on note $\mathrm{val}(P)$ le plus petit des indices i tels que $a_i \neq 0$. Si $P = 0$, on pose $\mathrm{val}(P) = +\infty$.

(3) Supposons que $\deg(P) = n \neq -\infty$. Alors $a_n X^n$ est appelé le *monôme dominant* de P et a_n est appelé le *coefficient dominant* de P.

1.6 Remarques. (1) Il est souvent commode, lorsqu'on n'a pas explicitement besoin du degré, de noter $P = \sum a_i X^i$ ou $P = \sum_{i=0}^{\infty} a_i X^i$. Ce n'est là qu'une convention d'écriture, qui ne porte pas à conséquence tant que l'on n'oublie pas que seul un nombre fini des a_i est non nul.

(2) Il faut prendre garde au fait que si, dans l'écriture $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, on n'a pas précisé que $a_n \neq 0$, alors le degré de P n'est pas égal à n a priori. De même, la valuation de P n'est pas égale à 0 a priori.

1.7 Lemme. *Soient P et Q deux polynômes. Alors, on a :*

(1) $\deg(PQ) = \deg(P) + \deg(Q)$,

(2) $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$ *avec égalité si* $\deg(P) \neq \deg(Q)$,

(3) $\mathrm{val}(PQ) = \mathrm{val}(P) + \mathrm{val}(Q)$,

(4) $\mathrm{val}(P+Q) \geqslant \min(\mathrm{val}(P), \mathrm{val}(Q))$ *avec égalité si* $\mathrm{val}(P) \neq \mathrm{val}(Q)$.

Preuve : Notons $P = \sum a_i X^i$, $Q = \sum b_j X^j$, $p = \deg(P)$, $q = \deg(Q)$.

(1) Si P et Q sont non nuls, la formule donnant le coefficient d'incide i de PQ montre que ce coefficient est égal à $a_p b_q$ si $i = p+q$ et à zéro si $i > p+q$. Ceci montre que $\deg(PQ) = p+q$. Si P ou Q est nul, les deux termes à examiner sont égaux à $-\infty$ et l'égalité est vérifiée.

(2) Si P et Q sont non nuls et si $i > \max(p,q)$, on a $a_i + b_i = 0+0 = 0$ donc $\deg(P+Q) \leqslant \max(p,q)$. Si de plus $p \neq q$, disons par exemple que $p > q$, alors le coefficient d'incide p de $P+Q$ est égal à a_p donc il y a égalité. Si P ou Q est nul, par exemple disons que $P = 0$, alors $\max(\deg(P), \deg(Q)) = \deg(Q)$ et l'inégalité est une égalité.

(3) et (4) se démontrent de la même façon. □

1.8 Proposition. *L'anneau $k[X]$ est intègre : si P et Q sont deux polynômes non nuls de $k[X]$, alors leur produit PQ est non nul.*

Preuve : Si P, Q ne sont pas nuls, leurs coefficients dominants a_p, b_q sont des éléments non nuls de k. Le coefficient dominant de PQ est $a_p b_q$ qui est non nul, donc $PQ \neq 0$. □

1.9 Proposition. *Les éléments inversibles de $k[X]$ sont les polynômes constants non nuls.*

Preuve : Si P inversible dans $k[X]$, il existe Q tel que $PQ = 1$. En particulier, P et Q sont non nuls, et $\deg(P) + \deg(Q) = \deg(1) = 0$. Ceci n'est possible que si $\deg(P) = \deg(Q) = 0$ donc P et Q sont constants. Réciproquement, il est clair qu'un polynôme constant non nul est inversible. □

2 Division euclidienne et conséquences

La suite du cours consiste à étudier l'arithmétique dans $k[X]$. L'Arithmétique est l'activité qui consiste à explorer les relations de divisibilité dans un anneau intègre fixé, et il n'est pas inutile de décrire brièvement la situation générale. (Rappel : A est *intègre* si $ab = 0 \Rightarrow a = 0$ ou $b = 0$.)

2.1 Définitions. Soient A un anneau commutatif unitaire intègre et p, a, b des éléments de A.

(1) On dit que a *divise* b, et on écrit $a \mid b$, s'il existe $c \in A$ tel que $b = ac$. On dit aussi que a *est un diviseur de* b, ou que b *est un multiple de* a.

(2) On appelle *idéal principal engendré par* a, et on note (a), l'ensemble des multiples de a.

(3) On dit que a et b sont *associés*, et on écrit $a \sim b$, s'il existe $\lambda \in A$ inversible tel que $a = \lambda b$.

(4) On dit que p est *irréductible* s'il est non nul, non inversible et si pour tous a, b, on a : $p = ab$ entraîne que a ou b est inversible.

2.2 Remarques. (1) Au contraire de l'ensemble (a) des multiples de a, qui est un idéal, l'ensemble de ses diviseurs ne possède pas de structure additive simple.

(2) Par définition, $a \mid b$ si et seulement si $b \in (a)$.

(3) ($a \mid b$ et $b \mid a$) si et seulement si a et b sont associés. La relation $\sim$ est une relation d'équivalence sur $k[X]$, et aussi sur $k[X] \setminus \{0\}$.

(4) Les générateurs d'un idéal principal sont tous associés entre eux.

(5) On a $(a) = A$ si et seulement si a est inversible dans A.

(6) Une écriture $p = ab$, avec a et b non inversibles, est parfois appelée une *factorisation non triviale*. Ainsi, p est irréductible si et seulement s'il ne possède pas de factorisation non triviale.

Toutes les propriétés arithmétiques de $k[X]$ découleront du résultat fondamental suivant.

2.3 Théorème de division euclidienne. *Soient A et B deux polynômes avec $B \neq 0$. Alors, il existe un unique couple de polynômes (Q, R) tel que :*

(1) $A = BQ + R$,

(2) $\deg(R) < \deg(B)$.

Cette écriture s'appelle la division euclidienne *de A par B. On dit que A est le* dividende, *B le* diviseur, *Q le* quotient *et R le* reste.

Preuve : Commençons par démontrer l'existence du couple (Q, R). Si $\deg(A) < \deg(B)$, on peut prendre $Q = 0$ et $R = A$. On suppose désormais que $\deg(A) \geqslant \deg(B)$. Notons $A = a_n X^n + \cdots + a_0$ et $B = b_m X^m + \cdots + b_0$, avec $b_m \neq 0$. La preuve consiste en un algorithme de construction du polynôme Q, qui n'est pas que théorique : c'est celui que l'on met en pratique sur les exemples. On construit par récurrence, que pour tout $i \in \{0, \ldots, n-m+1\}$, un polynôme Q_i tel que $\deg(A - BQ_i) \leqslant n - i$. Pour $i = 0$, on peut choisir $Q_0 = 0$. Supposons maintenant que $Q_0, \ldots, Q_i$ sont construits pour $i \leqslant n - m$. Alors, on peut écrire $A - BQ_i = c_{n-i}X^{n-i} + \cdots + c_0$ avec $\deg(A - BQ_i) \geqslant n - i \geqslant m$. Posons $Q_{i+1} = Q_i + c_{n-i}b_m^{-1}X^{n-i-m}$. On a :

$$\begin{aligned} A - BQ_{i+1} &= A - BQ_i - Bc_{n-i}b_m^{-1}X^{n-i-m} \\ &= (c_{n-i}X^{n-i} + \cdots + c_0) - (b_m X^m + \cdots + b_0)c_{n-i}b_m^{-1}X^{n-i-m} \\ &= \underbrace{c_{n-i}X^{n-i} - b_m c_{n-i}b_m^{-1}X^{n-i}}_{=0} + (\text{termes de degré } \leqslant n-i-1) \end{aligned}$$

de sorte que $\deg(A - BQ_{i+1}) \leqslant n - (i+1)$. Ceci termine la démonstration par récurrence. Pour $i = n-m+1$, on obtient un polynôme $Q = Q_{n-m+1}$ vérifiant $\deg(A-BQ) \leqslant m-1$. Il suffit de poser $R = A - BQ$ pour obtenir un couple vérifiant les conditions du théorème.

Montrons maintenant que le couple (Q, R) est unique. Si l'on dispose d'un second couple solution (Q', R'), alors $A = BQ + R = BQ' + R'$ entraîne que $B(Q'-Q) = R - R'$. Ainsi le polynôme $R - R'$ est multiple de B, or par hypothèse $\deg(R-R') \leqslant \max(\deg(R), \deg(R')) \leqslant \deg(B) - 1$. Ceci n'est possible que si $R - R' = 0$. On en déduit $B(Q'-Q) = 0$ donc $Q' - Q = 0$. □

2.4 Remarque. Dans l'énoncé du théorème, les notations sont choisies pour être harmonieuses avec les notations usuelles de la division euclidienne dans $\mathbb{Z}$. Dans la suite, nous reviendrons aux notations $P, Q, \ldots$ pour les polynômes. C'est le cas dès la preuve du corollaire 2.5. Attention de ne pas vous y perdre !

Voici des conséquences extrêmement importantes du théorème de division euclidienne.

2.5 Corollaire. *Tout idéal de l'anneau $k[X]$ est* principal.

Preuve : Soit I un idéal de $k[X]$. Si $I = \{0\}$, il est principal engendré par 0. Sinon, il existe un polynôme P non nul dans I. Choisissons un P de plus petit degré parmi tous les éléments non nuls de I, et montrons que tout élément $F \in I$ est multiple de P. La division euclidienne de F par P s'écrit $F = PQ + R$ avec $\deg(R) < \deg(P)$. Comme P et F sont dans I, les propriétés d'un idéal font que $R = F - PQ \in I$. Comme R est de degré $< \deg(P)$ et P est de degré minimal parmi les éléments non nuls de I, on doit avoir $R = 0$. Ceci montre que P divise F. □

2.6 Lemme d'Euclide. *Soient P, A, B trois polynômes. Si P est irréductible et $P \mid AB$, alors $P \mid A$ ou $P \mid B$.*

Preuve : Supposons que $P \nmid A$ et montrons que $P \mid B$. Considérons l'idéal $I = (A, P)$ engendré par A et P. D'après le corollaire 2.5, cet idéal est principal : $I = (D)$ pour un certain polynôme D. Comme $A \in I$ et $P \in I$, il existe A', P' tels que $A = DA'$ et $P = DP'$. Comme $P \nmid A$, la première de ces deux égalités nous dit que $D \not\sim P$. Comme P est irréductible, la seconde nous dit que $D \sim 1$. Ceci signifie que D est inversible, si bien que $I = (D) = A$. Il en découle que $1 \in I$, donc il existe deux polynômes U, V tels que $1 = UA + VP$. Or par hypothèse il existe Q tel que $AB = PQ$. On a donc $B = BUA + BVP = UPQ + BVP = (UQ + BV)P$ qui est multiple de P. □

2.7 Théorème de décomposition en facteurs irréductibles. *Pour tout polynôme non nul F, il existe une factorisation*

$$F = \lambda P_1^{\alpha_1} \ldots P_r^{\alpha_r}$$

où $\lambda \in k^*$, les P_i sont des polynômes unitaires irréductibles distincts et les α_i sont des entiers $\geqslant 1$. Cette factorisation est unique à l'ordre des facteurs près, i.e. si on a deux factorisations

$$F = \lambda P_1^{\alpha_1} \ldots P_r^{\alpha_r} = \mu Q_1^{\beta_1} \ldots Q_s^{\beta_s}$$

alors $\lambda = \mu$, $r = s$, et il existe une permutation $\sigma \in S_r$ telle que $P_i = Q_{\sigma(i)}$ et $\alpha_i = \beta_{\sigma(i)}$.

Preuve : Démontrons d'abord l'existence. Notons $F = \lambda F_1$, où λ est le coefficient dominant de F. En prenant les degrés, on voit que dans une factorisation $F_1 = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ en produit de polynômes unitaires éventuellement non irréductibles, le nombre de facteurs $\alpha_1 + \cdots + \alpha_r$ est borné par $\deg(F)$. Considérons une factorisation dans laquelle le nombre de facteurs est maximal. Si un seul des P_i n'était pas irréductible, il possèderait une factorisation non triviale $P_i = QR$ et ceci ferait augementer le nombre de facteurs, ce qui n'est pas possible. Donc une telle factorisation maximale est bien une factorisation en irréductibles, comme demandé.

Montrons maintenant l'unicité à l'ordre près, par récurrence sur $\deg(F)$. Si $\deg(F) = 0$, la seule décomposition de F ne possède aucun facteur irréductible et il n'y a rien à démontrer. Si $\deg(F) \geqslant 1$, soient deux factorisations en irréductibles unitaires :

$$F = \lambda P_1^{\alpha_1} \dots P_r^{\alpha_r} = \mu Q_1^{\beta_1} \dots Q_s^{\beta_s}.$$

Alors $\lambda = \mu =$ le coefficient dominant de F. De plus, P_1 divise $Q_1^{\beta_1} \dots Q_s^{\beta_s}$ donc d'après le lemme d'Euclide 2.6, P_1 divise l'un des Q_j. Quitte à réordonner, on peut supposer que $j = 1$. Comme P_1 et Q_1 sont irréductibles unitaires, en fait $P_1 = Q_1$. On peut donc simplifier de part et d'autre par P_1, et en appliquant l'hypothèse de récurrence pour les décompositions

$$\lambda P_1^{\alpha_1 - 1} \dots P_r^{\alpha_r} = \lambda Q_1^{\beta_1 - 1} \dots Q_s^{\beta_s},$$

on obtient le résultat. □

Dans la suite, on utilisera parfois le sigle DFI comme raccourci pour l'expression « décomposition en facteurs irréductibles ». Dans une DFI comme ci-dessus, l'entier α_i est appelé la *multiplicité* du facteur P_i ; on le note parfois aussi $\alpha_i(F)$.

3 Fonctions polynomiales et dérivation

Dans cette partie, nous formalisons le lien entre un polynôme P, la fonction $\widetilde{P}$ qu'il définit et sa dérivée P'. Puis nous nous intéressons aux racines de ces polynômes (les zéros de $\widetilde{P}$ et de $\widetilde{P'}$) et à leurs relations avec l'irréductibilité.

Notons $\mathcal{F}(k,k)$ l'ensemble des applications de k dans k. Il est naturellement muni d'une structure de k-espace vectoriel et d'une structure d'anneau, telles que pour tous $\lambda \in k$ et $(f,g) \in \mathcal{F}(k,k)^2$, on a :

$$(f+g)(x) \stackrel{\text{déf}}{=} f(x) + g(x) \quad , \quad (\lambda f)(x) \stackrel{\text{déf}}{=} \lambda f(x) \quad , \quad (fg)(x) \stackrel{\text{déf}}{=} f(x)g(x).$$

3.1 Définition. Soit $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ un polynôme à coefficients dans k. La *fonction polynomiale associée à* P est la fonction $\widetilde{P}$ définie par

$$\widetilde{P}(x) \stackrel{\text{déf}}{=} a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Dans la pratique, si $x \in k$, on note en fait bien souvent $P(x)$ au lieu de $\widetilde{P}(x)$.

3.2 Proposition. *L'application $k[X] \to \mathcal{F}(k,k)$ qui à P associe $\widetilde{P}$ est un morphisme de k-espaces vectoriels et d'anneaux.*

Preuve : C'est presque évident, et laissé au lecteur. □

Pour les fonctions suffisamment régulières définies sur le corps des réels $k = \mathbb{R}$, on dispose de l'opération de dérivation. Celle-ci est définie par un procédé analytique, mais dans le cas des polynômes, les formules bien connues montrent qu'elle peut être définie pour n'importe quel corps k. Elle est tout aussi importante dans ce degré de généralité.

3.3 Définition. Soient $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$ un polynôme à coefficients dans k. On définit le *polynôme dérivé de P* par

$$P'(X) \overset{\text{déf}}{=} na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + 2a_2X + a_1.$$

3.4 Remarque. Sur les corps $\mathbb{R}$ ou $\mathbb{C}$ (ou plus généralement sur un corps de caractéristique 0), on peut aussi définir la *primitive de P qui s'annule en 0* par

$$(\textstyle\int_0^X P)(X) \overset{\text{déf}}{=} \frac{1}{n+1}a_nX^{n+1} + \frac{1}{n}a_{n-1}X^n + \cdots + \frac{1}{3}a_2X^3 + \frac{1}{2}a_1X^2 + a_0X.$$

Sur un corps de caractéristique égale à un nombre premier p, tel que le corps à p éléments $k = \mathbb{F}_p$, on ne peut cependant pas définir d'intégration : ainsi, le polynôme X^{p-1} n'a pas de primitive. La raison en est que la dérivée d'un monôme de la forme X^{kp} ($k \geqslant 0$ entier) est nulle, si bien que la dérivée d'un polynôme ne possède aucun monôme de la forme X^{kp-1}.

3.5 Proposition. *L'opérateur de dérivation $D : k[X] \to k[X]$ défini par $D(P) = P'$ est une application linéaire. De plus, pour tout entier $n \geqslant 0$, le sous-espace $E_n = k[X]_{\leqslant n}$ des polynômes de degré inférieur ou égal à n est D-stable et $D|_{E_n}$ est nilpotent d'indice n.*

Preuve : Ces faits sont bien connus et faciles à vérifier. □

3.6 Théorème (Formule de Taylor). *Soit $k = \mathbb{R}$ ou $\mathbb{C}$, ou plus généralement un corps de caractéristique 0. Alors pour tout polynôme P de degré n et pour tout $h \in k$, on a :*

$$P(X+h) = P(X) + hP'(X) + \frac{h^2}{2}P''(X) + \cdots + \frac{h^n}{n!}P^{(n)}(X),$$

où $P^{(i)}$ désigne la dérivée i-ème de P, pour tout entier i.

Preuve : Comme D est linéaire, il suffit d'établir la formule pour un monôme $P(X) = X^n$. Dans ce cas, un calcul direct montre que pour un entier $i \leqslant n$, on a $P^{(i)}(X) = n(n-1)\dots(n-i+1)X^{n-i}$. En utilisant la formule du binôme de Newton, on a donc :

$$P(X+h) = (X+h)^n = \sum_{i=0}^{n} \binom{n}{i} h^i X^{n-i} = \sum_{i=0}^{n} \frac{h^i}{i!}P^{(i)}(X),$$

ce qu'il fallait démontrer. □

3.7 Proposition. *Soient $P \in k[X]$ et $r \in k$. Alors :*

(1) *$(X-r)$ divise P si et seulement si $P(r) = 0$,*

(2) *$(X-r)^2$ divise P si et seulement si $P(r) = P'(r) = 0$.*

Preuve : (1) La division euclidienne de P par $X - r$ s'écrit $P = (X-r)Q + R$ avec $\deg(R) < 1$, c'est-à-dire que R est constant. En évaluant cette égalité en r, on voit que $P(r) = 0$ si et seulement si $R = 0$, ou encore, si et seulement si $X - r$ divise P.

(2) Si $P(X) = (X-r)^2Q(X)$, un calcul direct montre que $P(r) = P'(r) = 0$. Réciproquement, considérons la division euclidienne de P par $(X-r)^2$, qui s'écrit $P = (X-r)^2Q + aX + b$, avec a, b dans k. On a alors $P(r) = ar + b$ et $P'(r) = a$, donc si $P(r) = P'(r) = 0$, on trouve $a = b = 0$ et le polynôme $(X-r)^2$ divise P. □

3.8 Définitions. Une *racine* de P est un élément $r \in k$ tel que $P(r) = 0$. La *multiplicité de r dans P* est la multiplicité de $(X - r)$ dans la décomposition en facteurs irréductibles de P. On la note parfois $\mathrm{mult}_P(r)$. Une racine de P est dite *multiple* si sa multiplicité est au moins égale à 2.

3.9 Lemme. *Dans l'anneau $k[X]$, on a :*

(1) *Un polynôme irréductible est de degré au moins* 1.

(2) *Tout polynôme de degré* 1 *est irréductible.*

(3) *Un polynôme irréductible possède une racine si et seulement s'il est de degré* 1.

(4) *Un polynôme de degré* 2 *ou* 3 *est irréductible si et seulement s'il n'a pas de racine.*

Preuve : (1), (2), (3) sont clairs. Passons à (4). Soit P un polynôme de degré 2 ou 3. S'il n'est pas irréductible, il possède une factorisation non triviale $P = AB$, et A ou B doit être de degré 1 donc posséder une racine. Réciproquement, si P possède une racine r, la proposition 3.7 nous dit que $X - r$ divise P, qui n'est donc pas irréductible. □

3.10 Définition. Un corps k est dit *algébriquement clos* si tout polynôme $P \in k[X]$ non constant possède une racine.

Ainsi, dans un corps algébriquement clos, les polynômes irréductibles sont les polynômes de degré 1.

3.11 Théorème. *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Preuve : Admise. □

4 Plus grand commun diviseur et plus petit commun multiple

Dans toute la suite, notons $\{P_i\}_{i \in I}$ la famille de tous les irréductibles unitaires de $k[X]$. Il est souvent commode d'utiliser une écriture

$$F = \lambda \prod_{i \in I} P_i^{\alpha_i}$$

où *tous les α_i sont nuls, sauf un nombre fini.* L'unicité dans le théorème 2.7 signifie maintenant que $\lambda \in k^*$ et les multiplicités $\alpha_i \geqslant 0$ sont uniquement déterminés.

4.1 Lemme. *Soient F, G deux polynômes non nuls et $F = \lambda \prod_{i \in I} P_i^{\alpha_i}$, $G = \mu \prod_{i \in I} P_i^{\beta_i}$ leurs décompositions en irréductibles dans $k[X]$. Alors F divise G si et seulement si $\alpha_i \leqslant \beta_i$ pour tout i.*

Preuve : Si F divise G, il existe H tel que $G = FH$. Notons $H = \nu \prod_{i \in I} P_i^{\gamma_i}$ sa décomposition en irréductibles. On a donc :

$$\mu \prod_{i \in I} P_i^{\beta_i} = \left(\lambda \prod_{i \in I} P_i^{\alpha_i} \right) \left(\nu \prod_{i \in I} P_i^{\gamma_i} \right).$$

Par unicité dans la DFP, on obtient $\beta_i = \alpha_i + \gamma_i \geqslant \alpha_i$. Réciproquement, si $\alpha_i \leqslant \beta_i$ pour tout i, alors $\gamma_i = \beta_i - \alpha_i \geqslant 0$. Le polynôme $H = \lambda^{-1} \mu \prod_{i \in I} P_i^{\gamma_i}$ vérifie évidemment $G = FH$, donc $F \mid G$. □

4.2 Proposition. *Soient F, G deux polynômes non nuls et $F = \lambda \prod_{i\in I} P_i^{\alpha_i}$, $G = \mu \prod_{i\in I} P_i^{\beta_i}$ leurs décompositions en irréductibles. Soit D un polynôme. Alors, les conditions suivantes sont équivalentes :*

(1) *D divise F et G, et tout diviseur de F et G divise D,*

(2) *D est un générateur de l'idéal (F, G),*

(3) *D est associé au polynôme $\prod_{i\in I} P_i^{\min(\alpha_i,\beta_i)}$.*

Preuve : (1) $\Rightarrow$ (2). D'après le corollaire 2.5, l'idéal (F, G) est principal ; notons E un de ses générateurs. Comme F et G appartiennent à $(F, G) = (E)$, il existe F', G' tels que $F = EF'$ et $G = EG'$. Comme par hypothèse tout diviseur de F et G divise D, on trouve que E divise D. Par ailleurs D divise F et G, donc il existe F'', G'' tels que $F = DF''$ et $G = DG''$. Ceci montre que F et G sont dans (D), donc $(E) = (F, G) \subset (D)$. On en déduit que D divise E. Finalement, D est associé à E donc c'est un générateur de (F, G).

(2) $\Rightarrow$ (1). Comme $(F, G) = (D)$, en particulier F et G sont dans (D) donc multiples de D. Par ailleurs, le fait que $D \in (F, G)$ montre qu'il existe U, V tels que $D = UF + VG$. Si E est un diviseur de F et G, il existe F', G' tels que $F = EF'$ et $G = EG'$ donc $D = UF + VG = E(UE' + VG')$. Ceci montre que tout diviseur de F et G divise D.

(1) $\Rightarrow$ (3). Notons D_0 le polynôme $\prod_{i\in I} P_i^{\min(\alpha_i,\beta_i)}$. D'après le lemme, les polynômes $E = \nu \prod_{i\in I} P_i^{\gamma_i}$ qui sont diviseurs communs de F et G vérifient $\gamma_i \leqslant \alpha_i$ et $\gamma_i \leqslant \beta_i$ pour tout i, donc $\gamma_i \leqslant \min(\alpha_i, \beta_i)$. Donc, un tel diviseur commun divise D_0. En particulier D divise D_0. Comme D_0 lui-même est un diviseur de F et G, d'après l'hypothèse sur D, il divise D. Finalement D et D_0 sont associés.

(3) $\Rightarrow$ (1). Ce qui vient d'être dit montre clairement que si $D = \nu \prod_{i\in I} P_i^{\min(\alpha_i,\beta_i)}$ alors D divise F et G, et que tout diviseur de F et G divise D. □

4.3 Définition. Tout polynôme D vérifiant l'une des propriétés équivalentes de la proposition 4.2 est appelé un *plus grand commun diviseur de F et G*, et on note par abus $D = \mathrm{pgcd}(F, G)$. On dit que F et G sont *premiers entre eux* si $\mathrm{pgcd}(F, G) = 1$.

La notation $D = \mathrm{pgcd}(F, G)$ est bien sûr abusive car « le » pgcd n'est défini qu'à un élément inversible près. Si on le souhaite, on peut éviter cet abus en choisissant le pgcd unitaire par définition. Par ailleurs, on peut noter que dans la démonstration de 4.2, le fait que F et G soient non nuls est utile surtout pour pouvoir considérer leurs DFI. Si l'un des deux polynômes F ou G est nul (mais pas les deux), on peut encore définir le pgcd comme générateur de l'idéal (F, G).

4.4 Remarque. On peut généraliser la notion de pgcd au cas d'un nombre fini de polynômes $F_1, \ldots, F_k$. Notons $F_j = \lambda_j \prod_{i\in I} P_i^{\alpha_{j,i}}$ les DFI. On montre que les conditions suivantes sont équivalentes :

(1) D divise chacun des F_j, et tout diviseur commun des F_j divise D,

(2) D est un générateur de l'idéal $(F_1, \ldots, F_k)$,

(3) D est associé au polynôme $\prod_{i\in I} P_i^{\min(\alpha_{1,i},\ldots,\alpha_{k,i})}$.

On note alors par abus $D = \mathrm{pgcd}(F_1, \ldots, F_k)$. On dit que les F_j sont *premiers entre eux dans leur ensemble* si $\mathrm{pgcd}(F_1, \ldots, F_k) = 1$. Attention : si $F_1, \ldots, F_k$ sont premiers entre eux dans leur ensemble, deux polynômes pris au hasard parmi eux ne sont pas nécessairement premiers entre eux. Ainsi, si P, Q, R sont trois polyômes irréductibles non associés, les polynômes PQ, PR et QR sont premiers entre eux dans leur ensemble alors qu'aucune paire ne donne deux polynômes premiers entre eux.

4.5 Proposition. *Soient F, G deux polynômes non nuls et $F = \lambda \prod_{i\in I} P_i^{\alpha_i}$, $G = \mu \prod_{i\in I} P_i^{\beta_i}$ leurs décompositions en irréductibles. Soit M un polynôme. Alors, les conditions suivantes sont équivalentes :*

(1) *M est multiple de F et G, et tout multiple de F et G est multiple de M,*

(2) *M est un générateur de l'idéal $(F) \cap (G)$,*

(3) *M est associé au polynôme $\prod_{i\in I} P_i^{\max(\alpha_i,\beta_i)}$.*

Preuve : La démonstration est similaire à celle de la proposition 4.2, et nous l'omettrons. □

4.6 Définition. Tout polynôme M vérifiant l'une des propriétés équivalentes de la proposition 4.5 est appelé un *plus petit commun mutiple de F et G*, et on note par abus $M = \text{ppcm}(F, G)$.

Comme dans la remarque 4.4, on peut généraliser la notion de ppcm au cas d'un nombre fini de polynômes $F_1, \ldots, F_k$.

Il existe une relation fondamentale entre le pgcd et le ppcm :

4.7 Proposition. *Soient F et G deux polynômes non nuls, D leur pgcd, M leur ppcm. Alors, on a :*

$$DM \sim FG.$$

Preuve : Notons $F = \lambda \prod_{i\in I} P_i^{\alpha_i}$ et $G = \mu \prod_{i\in I} P_i^{\beta_i}$ les DFI. En utilisant les propositions 4.2, 4.5 et la formule élémentaire $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$, on trouve :

$$DM \sim \left(\prod_{i\in I} P_i^{\min(\alpha_i,\beta_i)}\right)\left(\prod_{i\in I} P_i^{\max(\alpha_i,\beta_i)}\right) = \prod_{i\in I} P_i^{\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)} = \prod_{i\in I} P_i^{\alpha_i+\beta_i} \sim FG.$$

□

4.8 Théorème de Bézout. *Soient P, Q deux polynômes non nuls et D leur pgcd. Alors, il existe deux polynômes U et V tels que $D = UP + VQ$. De plus, P et Q sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $1 = UP + VQ$.*

Un couple (U, V) comme dans le théorème est appelé un *couple de Bézout* pour P et Q.

Preuve : On a vu dans la proposition 4.2 qu'un pgcd est un générateur de l'idéal (P, Q). En particulier $D \in (P, Q)$ d'où l'existence annoncée de U et V. Si P et Q sont premiers entre eux, on a donc $1 = UP + VQ$, et réciproquement s'il existe U et V tels que $1 = UP + VQ$ alors $1 \in (P, Q)$ donc $(P, Q) = A$ et cet idéal est engendré par 1. Donc 1 est un pgcd de P et Q. □

4.9 Lemme de Gauss. *Soient A, B, C trois polynômes. Si A est premier avec B, alors $A \mid BC$ implique $A \mid C$.*

Preuve : L'hypothèse que A est premier avec B signifie que A et B n'ont aucun facteur irréductible commun. En écrivant les DFI de A, B et C, le résultat en découle aussitôt. □

4.10 Proposition. *Soient P, Q, D des polynômes non nuls. Alors*

$$D = \mathrm{pgcd}(P,Q) \iff \exists (P',Q') \in k[X]^2 \text{ t.q. } \begin{cases} P = DP',\ Q = DQ' \\ \mathrm{pgcd}(P',Q') = 1. \end{cases}$$

Preuve : C'est un exercice facile, en utilisant les DFI de P, Q et D. □

4.11 Proposition. *Soient G un polynôme et $F_1, \ldots, F_k$ des polynômes premiers entre eux deux à deux. Si chaque F_j divise G, alors le produit $F_1 \ldots F_k$ divise G.*

Preuve : Pour $1 \leqslant j \leqslant k$, soit $\mathcal{E}_j$ l'ensemble des facteurs irréductibles de F_j. Ici encore, par hypothèse, les ensembles $\mathcal{E}_1, \ldots, \mathcal{E}_k$ sont disjoints. En écrivant les DFI de tous les polynômes en jeu, le résultat en découle. □

5 Aspects calculatoires

En arithmétique, décider si un polynôme donné P est ou non irréductible, et a fortiori calculer la décomposition en facteurs irréductibles de P, sont des questions très difficiles à résoudre en pratique. Nous ne dirons presque rien à ce sujet. Certaines questions reliées, comme le calcul du pgcd ou le calcul du ppcm, sont plus faciles à traiter, grâce à un outil très puissant : l'algorithme d'Euclide.

5.1 Calcul du pgcd. Soient A et B deux polynômes dont on veut calculer le pgcd D. Si on dispose des décompositions en facteurs irréductibles de A et B, alors la proposition 4.2 nous donne la réponse. Mais comme on vient de le dire, en général il est difficile de trouver ces décompositions, et on ne peut donc pas conclure ainsi. On peut alors utiliser le résultat suivant.

5.2 Théorème (Algorithme d'Euclide). *Soient A, B deux polynômes non nuls tels que* $\deg(A) \geqslant \deg(B)$. *Posons $R_0 = A$ et $R_1 = B$ et définissons par récurrence le polynôme R_{k+1} comme reste de la division euclidienne de R_{k-1} par R_k :*

$$R_{k-1} = R_k Q_k + R_{k+1} \quad \textit{avec} \quad \deg(R_{k+1}) < \deg(R_k).$$

Alors le pgcd de A et B est le dernier reste non nul de cet algorithme.

Preuve : Comme les degrés des R_k sont strictement décroissants, après un certain nombre d'étapes le reste s'annule. Soit R_n le dernier reste non nul de l'algorithme : on a donc $R_{n-1} = R_n Q_n$ de sorte que R_n divise R_{n-1}. Maintenant, notons que lorsqu'on effectue une division euclidienne $A = BQ + R$ avec $\deg(R) < \deg(B)$, alors on a l'égalité d'idéaux $(A,B) = (BQ+R, B) = (R,B)$, si bien que $\mathrm{pgcd}(A,B) = \mathrm{pgcd}(B,R)$. Il s'ensuit qu'au fil de l'algorithme, on a

$$\mathrm{pgcd}(A,B) = \mathrm{pgcd}(R_0,R_1) = \mathrm{pgcd}(R_1,R_2) = \cdots = \mathrm{pgcd}(R_{n-1},R_n) = R_n$$

puisque R_n divise R_{n-1}. C'est ce qu'on voulait démontrer. □

5.3 Calcul d'un couple de Bézout. Il n'est pas difficile de raffiner l'algorithme d'Euclide pour que celui-ci fournisse en plus un couple (U,V) tel que $UA + VB = D$. Pour cela, parallèlement aux restes successifs R_k, on demande à l'algorithme de fabriquer un couple (U_k, V_k) tel que $U_k A + V_k B = R_k$:

5.4 Théorème (Algorithme d'Euclide étendu). *Dans l'algorithme d'Euclide présenté ci-dessus, définissons deux suites (U_k) et (V_k) par :*

$$\begin{array}{llll} U_0 = 1, & U_1 = 0 & et & U_{k+1} = -Q_k U_k + U_{k-1}, \\ V_0 = 0, & V_1 = 1 & et & V_{k+1} = -Q_k V_k + V_{k-1}. \end{array}$$

Alors on a $U_k A + V_k B = R_k$ pour tout k. En particulier, (U_n, V_n) est un couple de Bézout pour A, B.

Preuve : Comme $R_0 = A$ et $R_1 = B$, il est immédiat que la propriété $U_k A + V_k B = R_k$ est vérifiée pour $k = 0$ et $k = 1$. Par récurrence, on obtient ensuite

$$U_{k+1}A + V_{k+1}B = (-Q_k U_k + U_{k-1})A + (-Q_k V_k + V_{k-1})B = -Q_k R_k + R_{k-1} = R_{k+1},$$

d'où la propriété au rang $k+1$. Le dernier reste non nul R_n est égal au pgcd D, donc $U_n A + V_n B = R_n = D$ et (U_n, V_n) est un couple de Bézout pour A, B. □

5.5 Calcul du ppcm. Soient A et B deux polynômes dont on veut calculer le ppcm M. Comme plus haut, si on dispose des décompositions en facteurs irréductibles de A et B, la réponse est donnée par la proposition 4.5. Dans le cas contraire, on commence par calculer le pgcd en utilisant l'algorithme d'Euclide, puis on déduit le ppcm de la formule $DM \sim AB$ de la proposition 4.7.

6 Fractions rationnelles

6.1 Définition et notions de base. Nous allons construire un corps, c'est-à-dire un anneau dans lequel tout élément non nul est inversible, qui contient $k[X]$ et est le plus petit possible. Pour cela, on considère l'ensemble $\mathcal{E}$ formé des paires de polynômes (F, G) avec $G \neq 0$. On munit cet ensemble de la relation d'équivalence définie par

$$(F_1, G_1) \sim (F_2, G_2) \quad \text{ssi} \quad F_1 G_2 = F_2 G_1.$$

On notera (exercice) que le fait que G_1, G_2 sont non nuls est important pour démontrer que cette relation est transitive. On note $k(X)$ l'ensemble $\mathcal{E}/\sim$ qui est l'ensemble des classes d'équivalence pour cette relation. La classe de (F, G) est notée F/G ou $\frac{F}{G}$. Par définition de la relation $\sim$, pour tout polynôme non nul H on a donc $(FH)/(GH) = F/G$.

6.2 Proposition. *Les opérations $+$ et $\times$ définies par*

$$\frac{F_1}{G_1} + \frac{F_2}{G_2} = \frac{F_1 G_2 + F_2 G_1}{G_1 G_2} \qquad et \qquad \frac{F_1}{G_1} \times \frac{F_2}{G_2} = \frac{F_1 F_2}{G_1 G_2}$$

munissent $k(X)$ d'une structure de corps commutatif, dont l'élément neutre additif est $0/1$ et l'élément neutre multiplicatif est $1/1$. L'application $k[X] \to k(X)$ qui envoie un polynôme F sur $F/1$ est un morphisme injectif d'anneaux.

Preuve : La démonstration est une suite de petites vérifications que l'on invite la lectrice à faire. □

Comme d'habitude, nous omettrons souvent le signe « $\times$ » dans les produits.

6.3 Définition. Les éléments de $k(X)$ sont nommés *fractions rationnelles en X à coefficients dans k.*

6.4 Définition. On définit les fonctions $\deg = \deg_{k(X)}$ et $\mathrm{val} = \mathrm{val}_{k(X)}$ par :

$$\deg(F/G) = \deg(F) - \deg(G) \qquad \text{et} \qquad \mathrm{val}(F/G) = \mathrm{val}(F) - \mathrm{val}(G).$$

Utilisant le lemme 1.7, on montre aisément :

- que ces définitions sont licites, c'est-à-dire que degré et valuation ne dépendent en effet que de F/G, i.e. $\deg(FH/GH) = \deg(F/G)$ et $\mathrm{val}(FH/GH) = \mathrm{val}(F/G)$,

- que les fonctions $\deg_{k(X)}$ et $\mathrm{val}_{k(X)}$ prolongent le degré et la valuation des polynômes, au sens où pour tout polynôme F on a $\deg_{k(X)}(F/1) = \deg_{k[X]}(F)$ et $\mathrm{val}_{k(X)}(F/1) = \mathrm{val}_{k[X]}(F)$,

- que $\deg_{k(X)}$ et $\mathrm{val}_{k(X)}$ vérifient encore toutes les propriétés du lemme 1.7.

6.5 Proposition. *Toute fraction rationnelle $R \in k(X)$ possède une unique écriture de la forme $R = F'/G'$ avec F', G' premiers entre eux et G' unitaire.*

Cette écriture est appelée la *forme irréductible* de R.

Preuve : Soit $R = F/G$ une écriture de R, et soit D le pgcd de F et G dont le coefficient est égal au coefficient dominant de G. On a donc $F = DF'$ et $G = DG'$ avec F', G' premiers entre eux et G' unitaire. Il est clair que $R = F/G = F'/G'$ et que c'est la seule écriture qui répond à la question. □

Nous serons très brefs en ce qui concerne les rappels sur la fonction associée à une fraction rationnelle, la dérivation, etc. Les concepts principaux sont les suivants :

6.6 Définition. Soit $R \in k(X)$ et $r \in k$. On dit que R est *définie en r* s'il existe une écriture $R = F/G$ telle que $G(r) \neq 0$, ou de manière équivalente, si pour la forme irréductible $R = F'/G'$ on a $G'(r) \neq 0$. On dit que R possède un *pôle* en r dans le cas contraire. On note $\mathcal{P}(R)$ l'ensemble des pôles de R.

La fraction rationnelle $R = F'/G'$ définit une fonction associée

$$\begin{array}{rccl} \widetilde{R} : k \setminus \mathcal{P}(R) & \longrightarrow & k \\ r & \mapsto & F'(r)/G'(r). \end{array}$$

Notons qu'il existe une autre façon de détecter les pôles, via la multiplicité (voir définition 3.8). Pour tout $r \in k$, on peut définir la *multiplicité de r dans R* par $\mathrm{mult}_R(r) = \mathrm{mult}_F(r) - \mathrm{mult}_G(r)$ où $R = F/G$. Alors r est un pôle de R si et seulement si $\mathrm{mult}_R(r) < 0$ et r est un zéro de R si et seulement si $\mathrm{mult}_R(r) > 0$.

6.7 Décomposition en éléments simples.

6.8 Proposition. *Le k-espace vectoriel $k(X)$ est somme directe des deux sous-espaces vectoriels $k[X] = k^+(X) = \{R,\, \deg(R) \geqslant 0\} \cup \{0\}$ et $k^-(X) = \{R,\, \deg(R) < 0\}$.*

Preuve : Il est facile de vérifier que $k[X]$ et $k^-(X)$ sont des sous-espaces vectoriels. Par ailleurs, si $R \in k[X] \cap k^-(X)$, comme son degré ne peut être simultanément strictement négatif et positif, on doit avoir $R = 0$. Donc ces sous-espaces sont en somme directe. Enfin, montrons qu'ils engendrent $k(X)$ comme espace vectoriel. Si $R = F/G$, en faisant la division euclidienne de F par G on trouve $F = GE + R$ avec $\deg(R) < \deg(G)$. Il s'ensuit que $R = E + P$ avec une fraction $P = R/G$ de degré strictement négatif, comme désiré. □

6.9 Définition. Dans la décomposition $R = E + P$, avec $E \in k[X]$ et $P \in k^-(X)$, le polynôme E s'appelle la *partie entière* de R et la fraction P s'appelle la *partie polaire* de R.

On peut donner un énoncé de décomposition en éléments simples sur un corps k quelconque, mais il est inutilement compliqué pour nos besoins. Nous nous contenterons d'un énoncé sur le corps des nombres complexes.

6.10 Théorème. *Soit $R \in \mathbb{C}(X)$ une fraction rationnelle à coefficients complexes. Soient $R = E + P$ son écriture en partie entière et partie polaire, $P = F/G$ l'écriture irréductible de P et*

$$G = (X - r_1)^{\alpha_1} \dots (X - r_m)^{\alpha_m}$$

la factorisation de G en polynômes irréductibles. Alors, il existe d'uniques coefficients $c_{ij} \in \mathbb{C}$ avec $1 \leqslant i \leqslant m$ et $1 \leqslant j \leqslant \alpha_i$ tels que

$$R = E + \sum_{i=1}^{m} \sum_{j=1}^{i} \frac{c_{ij}}{(X - r_i)^j} \ .$$

Preuve : Nous renvoyons au cours de Licence. □

6.11 Lemme. *Soit $R = F/G$ une fraction rationnelle mise sous forme irréductible, et soit $r \in \mathbb{C}$ un pôle* simple*, c'est-à-dire de multiplicité $\alpha = 1$. Alors, dans la décomposition de R en éléments simples, la partie polaire relative au pôle r est réduite à $\frac{c}{X-r}$ avec*

$$c = \frac{F(r)}{G'(r)}$$

où G' est le polynôme dérivé de G.

Preuve : D'après les hypothèses, on peut écrire $G = (X - r)H$ avec $H(r) \neq 0$. En dérivant, on trouve $G'(r) = H(r)$. Le fait que la partie polaire relative au pôle r est réduite à $c/(X-r)$ est une conséquence du théorème : on a donc $R = S + \frac{c}{X-r}$ où S est une fraction rationnelle sans pôle en r. En multipliant par $(X - r)$, on trouve $(X - r)R = (X - r)S + c = (X - r)F/G = F/H$. En évaluant en r, on trouve $c = F(r)/H(r) = F(r)/G'(r)$. □