Algèbre des polynômes

Table des matières

Dans tout ce chapitre, $\mathbb{K}$ désigne un corps : $\mathbb{R}$ ou $\mathbb{C}$. On trouvera moins d'exercices de cours que d'habitude, mais les exemples non triviaux devront être développés, et la feuille d'exercice contient beaucoup d'applications directes des définitions et résultats de base.

1 Introduction à l'algèbre linéaire

1.1 Espaces vectoriels

Définition 1

Un $\mathbb{K}$-*espace vectoriel* est un ensemble E muni d'une loi de composition interne $+$ et d'une *loi de composition externe* ., c'est-à-dire une application de $\mathbb{K} \times E$ dans E notée de façon infixe, de sorte que $(E, +)$ est un groupe commutatif, et :

- $\forall \lambda_1, \lambda_2 \in \mathbb{K},\ \forall v \in E, \quad (\lambda_1 + \lambda_2).v = \lambda_1.v + \lambda_2.v$
- $\forall \lambda \in \mathbb{K},\ \forall v_1, v_2 \in E, \quad \lambda.(v_1 + v_2) = \lambda.v_1 + \lambda.v_2$
- $\forall \lambda_1, \lambda_2 \in \mathbb{K},\ \forall v \in E, \quad \lambda_1.(\lambda_2.v) = (\lambda_1\lambda_2).v$
- $\forall v \in E, \quad 1_{\mathbb{K}}.v = v$

Les éléments de E sont appelés les *vecteurs* ; ceux de $\mathbb{K}$ les *scalaires*. La loi . est aussi appelée *multiplication externe*.

Exemples 1

- *$E = \mathbb{R}^3$ muni de la somme $(a, b, c) + (a', b', c') = (a + a', b + b', c + c')$ et du produit externe $\lambda.(a, b, c) = (\lambda a, \lambda b, \lambda c)$ est un $\mathbb{R}$-espace vectoriel.*
  Bien entendu, on munit de la même façon $\mathbb{K}^n$ d'une structure de $\mathbb{K}$-espace vectoriel
- *$E = \mathbb{R}^{\mathbb{N}}$ muni de la somme des suites et du produit externe "naturel" $\lambda.u = \lambda u$ (dont le n-ième terme vaut λu_n).*
- *Même chose pour l'ensemble des fonctions de X dans $\mathbb{R}$, où X est un ensemble quelconque donné.*
- *$\mathbb{K}$ peut être vu comme un $\mathbb{K}$-espace vectoriel (on confond ici la multiplication externe et interne).*
- *$\mathbb{C}$ peut être vu comme un $\mathbb{C}$-espace vectoriel, mais aussi comme un $\mathbb{R}$-espace vectoriel. Même chose pour $\mathbb{C}^n$ qui peut être vu comme espace vectoriel sur $\mathbb{C}$, mais aussi sur $\mathbb{R}$.*
- *$E = \mathcal{C}^1([0, 1])$ muni de la somme et du produit externe naturels est un $\mathbb{R}$-espace vectoriel.*

Remarque 1

On montrera soigneusement les trois faits suivants :

- pour tout $v \in E$, $0_{\mathbb{K}}.v = 0_E$;
- pour tout $\lambda \in \mathbb{K}$, $\lambda.0_E = 0_E$;
- $\lambda.x = 0_E$ si et seulement si $\lambda = 0_K$ ou $v = 0_E$ (ce qui s'apparente à de l'intégrité, mais ici il s'agit d'une loi de composition *externe*...).

1.2 Sous-espaces vectoriels

Définition 2

- Un *sous-espace* de E est une partie F de E telle que $(F, +)$ est un sous-groupe de E et F est stable par multiplication externe. $(F, +, .)$ est alors un $\mathbb{K}$-espace vectoriel.
- Les *combinaisons linéaires* de vecteurs $v_1, \ldots, v_n$ sont les vecteurs de la forme $\lambda_1 v_1 + \cdots + \lambda_n v_n$, où les λ_i sont dans $\mathbb{K}$.

Remarques 2

- On montrera sans mal qu'une partie F de E est un sous-espace de E si et seulement si elle est stable par combinaison linéaire : dans un sens, c'est trivial, et dans l'autre, c'est une récurrence facile sur le nombre de vecteurs concernés.
- Il est aisé de vérifier qu'un sous-espace vectoriel est lui-même un espace vectoriel, ce qui fournit un outil pratique pour montrer qu'un ensemble muni de deux lois est un espace vectoriel : on montre qu'il est en fait sous-espace d'un espace déjà connu ; on n'a donc pas à vérifier les propriétés individuelles et croisées des lois.

EXERCICE 1 *Soient F_1 et F_2 deux sous-espaces de E. Montrer qu'il en est de même pour $F_1 \cap F_2$.*

EXEMPLES 2
- $\{(x, y, 0) \mid x, y \in \mathbb{R}\}$ *est un sous-espace de* $\mathbb{R}^3$. *Même chose pour* $\{(x - y, y, x + y) \mid x, y \in \mathbb{R}\}$ *et* $\{(x, y, z) \in \mathbb{R}^3 \mid x + y - 2z = 0\}$.
- *L'ensemble* $\{f \in E \,|\, f(1515) = 0\}$ *est un sous-espace de* $\mathbb{R}^{\mathbb{R}}$, *mais pas* $\{f \in E \,|\, f(0) = 1515\}$.
- E *et* $\{0_E\}$ *sont des sous-espaces (dits triviaux) de* E.
- *Une intersection*[1] *de sous-espaces d'un même espace* E *est un sous-espace de* E.
- $\mathcal{C}^1([0, 1])$ *est un sous-espace de* $\mathcal{C}([0, 1])$ *qui est un sous-espace de* $\mathbb{R}^{[0,1]}$.

REMARQUE 3 ***IMPORTANT***
Dans bien des cas, on peut décrire un même espace d'un point de vue "*énumération*" (l'ensemble des ... pour ... décrivant ...), ou bien d'un point de vue "*vérification*" (l'ensemble des ... tels que ...). Par exemple :

$$\{(x, y, 0) \mid x, y \in \mathbb{R}\} = \{(u, v, w) \in \mathbb{R}^3 \mid w = 0\}.$$

1.3 Applications linéaires

DÉFINITION 3
Soient E et F deux $\mathbb{K}$-espaces vectoriels.
- Une application $u : E \to F$ est dite *linéaire* lorsque :

$$\forall \lambda \in \mathbb{K},\ \forall v_1, v_2 \in E, \qquad u(\lambda v_1 + v_2) = \lambda u(v_1) + u(v_2).$$

- On reprend au langage des groupes les termes d'endomorphisme, automorphisme, isomorphisme.
- $\mathcal{L}(E, F)$ désigne l'ensemble des applications linéaires de E dans F. L'ensemble des endomorphismes de E est noté $\mathcal{L}(E)$ plutôt que $\mathcal{L}(E, E)$.

REMARQUE 4 Si u est linéaire, alors u est un morphisme entre les groupes additifs E et F ; en particulier $u(0_E) = 0_F$. Pour montrer que u est linéaire, on peut alors séparer les problèmes, en montrant que $u(\lambda v) = \lambda u(v)$ et $u(w_1 + w_2) = u(w_1) + u(w_2)$.

EXEMPLES 3
- *L'application identité réalise un automorphisme de* E.
- $u : \mathbb{R}^3 \to \mathbb{R}^2,\ (a, b, c) \mapsto (a + b, c - b)$ *est une application linéaire de* $\mathbb{R}^3$ *dans* $\mathbb{R}^2$ *non injective mais surjective.*
- *La dérivation est une application linéaire de* $\mathcal{C}^1([0, 1])$ *dans* $\mathcal{C}([0, 1])$ *non injective (facile) mais surjective : pourquoi ?*
- *L'application de* $E = \mathbb{R}^{\mathbb{R}}$ *dans lui-même qui à* f *associe sa partie paire est un endomorphisme de* E *ni injectif ni surjectif.*
- $\varphi : \mathbb{C}^{\mathbb{N}} \to \mathbb{C},\ u \mapsto u_{1515}$ *est une application linéaire surjective et non injective de* $\mathbb{C}^{\mathbb{N}}$ *sur* $\mathbb{C}$.

EXERCICE 2 *Munir* $\mathcal{L}(E, F)$ *d'une structure d'espace vectoriel.*

SOLUTION : Que faut-il faire au juste ? Quelle est la seule façon raisonnable de le faire ? Montrer qu'en faisant ainsi, ça marche effectivement !

PROPOSITION 1 *Soit* $\varphi \in \mathcal{L}(E, F)$.
- *Si* E_1 *(resp.* F_1*) est un sous-espace de* E *(resp.* F*), alors* $\varphi(E_1)$ *(resp.* $\varphi^{-1}(F_1)$ *) est un sous-espace de* F *(resp.* E*).*
  Le noyau $\ker \varphi = \{x \in E \mid \varphi(x) = 0\} = \varphi^{-1}(\{0_F\})$ *est donc un sous-espace de* E *et l'image* $\operatorname{Im} \varphi = \varphi(E)$ *est un sous-espace de* F.

[1] même d'une infinité

- φ *est injective si et seulement si* $\ker \varphi = \{0_E\}$.

PREUVE : Le premier point se montre sans problème en suivant les définitions, et le second n'est qu'un cas particulier de la caractérisation des morphismes de groupe injectifs. Une application linéaire induisant en effet un morphisme entre les groupes $(E, +)$ et $(F, +)$.

Bien que conséquence d'un résultat antérieur, la preuve du dernier résultat doit être refaite dans ce cas précis. ■

1.4 Familles libres, génératrices ; bases

INTERDICTION D'ABORDER LA SUITE AVANT DE LIRE ET COMPRENDRE CE PARAGRAPHE

Si $v_1, \dots, v_n \in E$, la combinaison linéaire $0.v_1 + 0.v_2 + \cdots + 0.v_n$ est appelée "combinaison linéaire triviale", et est clairement égale au vecteur nul.

Une combinaison linéaire triviale est donc nulle.

Maintenant, si on prend $E = \mathbb{R}^2$, $u = (1, 0)$, $v = (0, 1)$ et $w = (-2, -3)$, alors $2.u + 3.v + 1.w = 0_E$.

Une combinaison linéaire nulle n'est donc pas nécessairement triviale.

DÉFINITION 4
Soient $v_1, \dots, v_n$ des vecteurs d'un $\mathbb{K}$-espace vectoriel E. On dit que la famille $(v_1, \dots, v_n)$ est :
- *génératrice* si tout vecteur de E peut s'écrire comme combinaison linéaire de $v_1, \dots, v_n$;
- *libre* si la **seule** combinaison linéaire des v_i qui est nulle est la combinaison linéaire triviale ;
- une *base* de E si elle est libre et génératrice.

REMARQUE 5 Lorsque la famille est une base, on montre facilement[2] que tout vecteur de E s'écrit **de façon unique** comme combinaison linéaire des v_i.

EXEMPLE 4 *Dans* $E = \mathbb{R}^3$, *on pose* $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ *et* $e_3 = (0, 0, 1)$. *Alors :*
- $(2e_1 + e_3, e_2 - e_1)$ *est libre et non génératrice ;*
- $(e_1 + e_2, e_1 + e_3, e_2 + e_3, e_1 + e_2 + e_3 + e_4)$ *est génératrice mais n'est pas libre ;*
- (e_1, e_2, e_3) *est une base de* E *(on parle de* base canonique*).*
- *A VOTRE AVIS (en vous fiant à votre "expérience" : on ne demande pas de preuve), que peut-on dire de* p *si* $(v_1, \dots, v_p)$ *est libre (resp. génératrice) dans* $\mathbb{R}^3$ *?*

DÉFINITION 5
Soient $v_1, \dots, v_k \in E$. Le "sous-espace engendré par les v_i" est l'ensemble des combinaisons linéaires des v_i. On montre sans mal que c'est un sous-espace de E (ouf !), et même qu'il est inclus dans tout sous-espace contenant les v_i (c'est même parfois comme cela qu'on le définit). Ce sous-espace engendré est noté $\mathrm{Vect}(v_1, \dots, v_k)$, et, *par définition*, les v_i en constituent une famille génératrice.

EXEMPLE 5 *Avec les notations de l'exemple 4 :*
- $\mathrm{Vect}(e_1, e_2) = \mathrm{Vect}(e_1, e_1 + e_2) = \{(x, y, 0) \mid x, y \in \mathbb{R}\}$;
- $\mathrm{Vect}(e_2) = \mathrm{Vect}(2e_2) = \{(0, t, 0) \mid t \in \mathbb{R}\}$;
- $\mathrm{Vect}(e_3, e_2 - 2e_3, e1 + e_2, e_1 + e_3) = \mathrm{Vect}(e_3, e_2 - 2e_3, e1 + e_2) = E$.

Dans ce chapitre, on considérera parfois des familles infinies. On est donc amené à étendre les définitions précédentes :

DÉFINITION 6
On considère une famille de vecteurs $\mathcal{F} = (v_i)_{i \in I}$. On dit que $\mathcal{F}$ est :
- génératrice si tout vecteur de E peut s'écrire comme combinaison linéaire d'éléments de $\mathcal{F}$;
- libre si les seules combinaisons linéaires d'éléments de $\mathcal{F}$ qui sont nulles sont les combinaisons triviales ;

[2] Le vérifier !

- une base si elle est libre et génératrice.

REMARQUE 6 BIEN ENTENDU, on ne parlera JAMAIS de "combinaisons linéaires infinies" : quand on parle d'une combinaison linéaire des $(v_i)_{i\in I}$, il s'agit d'un vecteur de la forme $\sum_{k=1}^{n} \lambda_k v_{i_k}$, avec $\lambda_k \in \mathbb{K}$ et $i_k \in I$ pour tout $k \in [\![1, n]\!]$.

EXERCICE 3 *Dans $E = \mathbb{C}^{\mathbb{R}}$, montrer que les applications $f_n : t \mapsto e^{nit}$ ($n \in \mathbb{Z}$) forment une famille libre non génératrice.*

SOLUTION : Pour la liberté, on pourra partir d'une combinaison linéaire nulle, multiplier par e^{-kit} et intégrer entre 0 et 2π. Pour montrer que la famille n'est pas génératrice, on pourra considérer une fonction non bornée.

2 L'algèbre $\mathbb{K}[X]$

Algèbre ? Cékoadonc ?

DÉFINITION 7
Une $\mathbb{K}$-*algèbre* est un ensemble E muni de deux lois de composition interne $+$ et $*$ et d'une loi de composition externe . de sorte que $(E, +, *)$, est un anneau[3], $(E, +, .)$ est un $\mathbb{K}$-espace vectoriel, et "les lois . et $*$ se comportent bien entre elles" c'est-à-dire plus précisément :

$$\forall \lambda \in \mathbb{K},\ \forall x, y \in E, \qquad (\lambda.x) * y = \lambda.(x * y) = x * (\lambda.y).$$

REMARQUE 7 En pratique, dès qu'on a une structure naturelle d'anneau et d'espace vectoriel, la relation de "compatibilité" des lois . et $*$ est en général évidente. A l'usage, on ne note ni . ni $*$!

EXEMPLES 6
- *L'ensemble des suites complexes, muni de la somme, des produits externe et interne naturels est une $\mathbb{K}$-algèbre commutative.*
- *Même chose avec l'ensemble des fonctions continues de $\mathbb{R}$ dans lui-même, qui est une $\mathbb{R}$-algèbre (pour les lois définissant $f + g$, $f.g$ et λf). Par contre, si on prend comme seconde loi de composition interne la composition des applications, on n'obtient pas une algèbre car $f \circ (g + h)$ n'est pas en général égal à $(f \circ g) + (f \circ h)$, de sorte que $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ n'est pas un anneau.*
- *Par contre, si E est un $\mathbb{K}$-espace vectoriel, alors $(\mathcal{L}(E), +, \circ, .)$ est une $\mathbb{K}$-algèbre (le vérifier).*
- *$\mathbb{K}$ peut être vu comme une $\mathbb{K}$-algèbre...*

2.1 "Définition" de $\mathbb{K}[X]$

Dans la suite, X va désigner ce qu'on appelle une "indéterminée" : il ne s'agit pas d'une variable, mais d'un symbole nouveau[4].

PROPOSITION 2 *On admet l'existence d'une algèbre commutative, notée $\mathbb{K}[X]$, appelée algèbre des polynômes à coefficients dans $\mathbb{K}$, qui est une $\mathbb{K}$-algèbre contenant un élément noté X, et tel que la famille $(1, X, X^2, \ldots, X^n, \ldots)$ est une base de $\mathbb{K}[X]$.*

REMARQUES 8
- De même qu'on peut *construire* $\mathbb{C}$ à partir de $\mathbb{R}^2$, on peut *construire* $\mathbb{K}[X]$ à partir de $\mathbb{K}^{(\mathbb{N})}$, c'est-à-dire les suites complexes "presque nulles", c'est-à-dire n'admettant qu'un nombre fini de termes non nuls.

[3] pas forcément commutatif

[4] Un peu comme pour construire $\mathbb{C}$, on part de $\mathbb{R}$, et on introduit un symbole nouveau noté i. L'analogie s'arrête là, puisque dans le cas qui nous intéresse, X ne vérifiera pas de relation algébrique contrairement à i qui vérifie $i^2 + 1 = 0$

- Si $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$, alors les rêgles de calculs dans les anneaux et espaces vectoriels font que $PQ = \sum_{k=0}^{p+q} c_k X^k$, avec :

$$\forall k \in [\![0, p+q]\!], \qquad c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j.$$

  En fait, dans la formule précédente, on pose $a_i = 0$ lorsque $i < 0$ ou $i > p$, et $b_j = 0$ lorsque $j < 0$ ou $j > q$.
- X s'appelle "*l'indéterminée*", à ne pas confondre avec une *variable* : un polynôme n'est pas une *fonction*, même si à tout polynôme $P \in \mathbb{K}[X]$ on peut associer une fonction $\widetilde{P}$, comme on le verra plus tard.

DÉFINITION 8
- On définit le *degré* d'un polynôme *non nul* $P = \sum_{k=0}^{n} a_k X^k$ comme le plus grand des $k \in [\![0, n]\!]$ tel que $a_k \neq 0$. Par convention, le degré du polynôme nul est $-\infty$.
- Si $P = \sum_{k=0}^{n} a_k X^k \neq 0$, le *coefficient dominant* est a_p, où $p = \deg P$.
- Un polynôme non nul est dit *unitaire* lorsque son coefficient dominant vaut 1.

EXEMPLES 7
- $X^{1515} - 1$ *est unitaire de degré* 1515 *;*
- *si* $n \in \mathbb{N}^*$, $(X^2+1)^{2n} - (X^2-1)^{2n}$ *est de degré* $2n-2$ *et de coefficient dominant* $4n$.

PROPOSITION 3 *Soient P et Q deux polynômes non nuls. Alors :*
- $\deg(PQ) = \deg P + \deg Q$ *;*
- $\deg(P+Q) \leq \mathrm{Max}(\deg P, \deg Q)$.

COROLLAIRE 1 $\mathbb{K}[X]$ *est un anneau intègre ($PQ = 0$ implique $P = 0$ ou $Q = 0$), dont les éléments inversibles sont les polynômes de degré* 0*, c'est-à-dire les polynômes constants non nuls.*

DÉFINITION 9
Si $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré $\leq n$. D'après la proposition précédente, il s'agit d'un sous-espace vectoriel de $\mathbb{K}[X]$. Par contre, il ne s'agit pas d'une sous-algèbre (sauf pour $n = 0 \ldots$) : pourquoi ?

EXERCICE 4 *Déterminer le degré et le coefficient dominant de* $\prod_{k=12}^{18} \frac{X-k}{\sqrt{k}}$.

2.2 Division euclidienne

Comme dans tout anneau, on dit que B divise A (et on note $B|A$) lorsqu'il existe $Q \in \mathbb{K}[X]$ tel que $A = QB$. Le résultat suivant permet de *décider* (au sens informatique du terme) si B divise A.

THÉORÈME 1 *Soient $A, B \in \mathbb{K}[X]$, avec $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$, avec* $\deg R < \deg B$.

PREUVE : Pour l'unicité, on suppose $A = BQ_1 + R_1 = BQ_2 + R_2$, avec R_1 et R_2 de degré strictement inférieur au degré de B, on écrit $R_1 - R_2 = B(Q_2 - Q_1)$, et on suppose par l'absurde $Q_1 \neq Q_2$. Le degré de $R_1 - R_2$ vaut alors $\deg B + \deg(Q_2 - Q_1) \geq \deg B$, alors que par ailleurs :

$$\deg(R_1 - R_2) \leq \mathrm{Min}(\deg R_1, \deg R_2) < \deg B \ldots$$

Pour l'existence, on procède par récurrence sur le degré de A, ce qui est d'ailleurs le procédé *effectif* (algorithmique) pour réaliser une division euclidienne. ■

REMARQUE 9 **BIEN ENTENDU**, on n'oubliera *jamais* la condition sur le degré de R dans la conclusion...

EXEMPLE 8 *Pour la division euclidienne de X^4+3X^2-2X+1 par X^2+X+1, on écrit successivement :*

$$\begin{aligned} X^4+3X^2-2X+1 &= X^2(X^2+X+1)+(-X^3+2X^2-2X+1)\\ -X^3+2X^2-2X+1 &= (-X)(X^2+X+1)+3X^2-X+1\\ 3X^2-X+1 &= 3(X^2+X+1)-4X-2 \end{aligned}$$

De sorte que $X^4+3X^2-2X+1=(X^2+X+1)(X^2-X+3)+(-4X-2)$. Dans la pratique, on pourra présenter le calcul comme une division euclidienne d'entiers :

$$\begin{array}{r|l} X^4+3X^2-2X+1 & X^2+X+1 \\ \cline{2-2} -(X^4+X^3+X^2) & X^2-X+3 \\ \cdots\cdots\cdots & \\ -X^3+2X^2-2X+1 & \\ -(-X^3-X^2-X) & \\ \cdots\cdots\cdots & \\ 3X^2-X+1 & \\ -(3X^2+3X+3) & \\ \cdots\cdots\cdots & \\ -4X-2 & \end{array}$$

On appréciera la prouesse typographique...

2.3 Racines d'un polynôme

DÉFINITION 10

- Si $P=a_0+a_1X+\cdots+a_nX^n$, on définit une application $\widetilde{P}:\mathbb{K}\to\mathbb{K}$ par :

$$\forall t\in\mathbb{K},\qquad \widetilde{P}(t)=a_0+a_1t+\cdots+a_nt^n.$$

  $\widetilde{P}$ est la *fonction polynômiale* associée à P.
- On dit que $x_0\in\mathbb{K}$ est une *racine* de P lorsque $\widetilde{P}(x_0)=0$.

REMARQUE 10 Partant de P, la valeur de $\widetilde{P}(t)$ se trouve en substituant (au sens lexical) t à X : on remplace toutes les occurences de X par t. En Maple, partant d'un polynôme en X, on peut obtenir $\widetilde{P}(2)$ en écrivant `subs(X=2,P)`, et non pas $P(2)$:

```
> P:=X^2+5;
                                  2
                          P := X  + 5
> P(2);
                                  2
                           X(2)  + 5
> subs(X=2,P);
                                  9
> fonction_P:=t->subs(X=t,P);
                fonction_P := t -> subs(X = t, P)
> fonction_P(2);
                                  9
```

Le fait suivant et ses corollaires sont tout à fait fondamentaux.

PROPOSITION 4 *x_0 est racine de P si et seulement si $X-x_0$ divise P.*

PREUVE : Ecrire la division euclidienne de P par $X-x_0$. ■

Corollaire 2
- *Si* $\deg P = n \in \mathbb{N}$*, alors* P *a au plus* n *racines distinctes.*
- *Si* P *a une infinité de racines, alors* $P = 0$
- *L'application* $P \mapsto \widetilde{P}$ *est injective.*
- *Si* P *est de degré* n*, de coefficient dominant* a*, et admet* n *racines distinctes* $x_1, \ldots, x_n$*, alors* $P = a(X - x_1)(X - x_2)\ldots(X - x_n)$.

Preuve : Le premier point s'établit par récurrence sur n et division euclidienne, le second en est une conséquence immédiate. Pour le troisième, on suppose $\widetilde{P} = 0$, de sorte que P admet une infinité de racines[5]. Le dernier point s'établit également par récurrence. ■

Remarque 11 Si $P, Q \in \mathbb{K}[X]$ et $t \in \mathbb{K}$, la relation $\widetilde{P}(t) = \widetilde{Q}(t)$ n'implique certainement pas $P = Q$. Par contre, si cette relation est valable **pour tout** $t \in \mathbb{K}$, cela signifie que $\widetilde{P} = \widetilde{Q}$ donc $P = Q$, et "on peut *identifier* les coefficients de P et Q" (en utilisant le fait que les X^k forment une famille libre).

Dans ce type de situation, il est donc *essentiel* de savoir si la relation $\widetilde{P}(t) = \widetilde{Q}(t)$ est vérifiée pour un t donné ou bien pour tout t. Toute formulation ambigûe de la forme "$\widetilde{P}(t) = \widetilde{Q}(t)$, $t \in \mathbb{R}$" sera donc rejetée ("avec effets de bords sur la copie"...) la virgule avant le "$t \in \mathbb{R}$" laissant le doute quant à la quantification.

3 Dérivation

3.1 Dérivées d'un polynôme, formule de Leibnitz

Définition 11
Si $P = \sum_{k=0}^{n} a_k X^k$, on définit le polynôme dérivé de P, noté P', par :

$$P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{i=0}^{n-1} (i+1) a_{i+1} X^i.$$

Remarque 12 Il s'agit d'une dérivation FORMELLE : elle n'est pas définie à partir de la fonction dérivée de $\widetilde{P}$ (cela n'aurait d'ailleurs pas de sens lorsque $\mathbb{K} = \mathbb{C}$). Cela dit, heureusement, si $P \in \mathbb{R}[X]$, on a $\widetilde{P'} = (\widetilde{P})'$ (la dérivation dans le membre de droite correspondant à la dérivation des fonctions numériques d'une variable réelle) : OUF !

Proposition 5
- *L'application* $D : P \mapsto P'$ *est un endomorphisme surjectif de* $\mathbb{K}[X]$ *; son noyau est* $\mathbb{K}_0[X] \neq \{0\}$*, donc* D *n'est pas injective.*
- *Si* $P, Q \in \mathbb{K}[X]$*, on a* $D(PQ) = P.D(Q) + Q.D(P)$.
- *Si* $P, Q \in \mathbb{K}[X]$ *et* $n \in \mathbb{N}$*, on a :*

$$D^n(PQ) = \sum_{k=0}^{n} \mathrm{C}_n^k D^k(P) D^{n-k}(Q),$$

où D^i *désigne l'opérateur* D *itéré* i *fois.*

Preuve : On exploitera au maximum la linéarité de D. En particulier, pour établir une formule $\Phi(P, Q) = 0$ *linéaire* en P et en Q, on peut commencer par établir $\Phi(X^p, X^q) = 0$ pour tout $p, q \in \mathbb{N}$; on étend ensuite par linéarité à $\Phi(P, X^q)$ puis $\Phi(P, Q)$. ■

[5] le fait que le corps de base soit infini est ici essentiel : sur des corps *finis*, on peut trouver des polynômes non nuls dont les fonctions associées sont nulles

3.2 Formule de Taylor

Dans la suite, on verra parfois des "polynômes composés" ; on commence donc par la :

DÉFINITION 12
Soient $P, Q \in \mathbb{K}[X]$, avec $P = a_0 + a_1 X + \cdots + a_n X^n$. On définit le *polynôme composé* de P et Q, noté $P \circ Q$, par :

$$P \circ Q = a_0 + a_1 Q + a_2 Q^2 + \cdots + a_n Q^n = \sum_{k=0}^{n} a_k Q^k.$$

EXEMPLES 9
- $(X^2+1) \circ (X-2) = (X-2)^2 + 1 = X^2 - 4X + 5$;
- $(X-2) \circ (X^2+1) = (X^2+1) - 2 = X^2 - 1$;
- *en général,* $P \circ (X+a)$ *est noté* $P(X+a)$ *; ainsi,* $P(X)$ *désigne... P !*

THÉORÈME 2 *Formule de Taylor algébrique*
Soient $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}_n[X]$ *et* $a \in \mathbb{K}$*. Alors :*

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k, \tag{1}$$

ou encore :

$$P(X+a) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k. \tag{2}$$

PREUVE : Dans chaque cas, on peut commencer par montrer le résultat dans le cas où P est le monôme X^N, puis conclure par linéarité.

Pour (1), on peut utiliser le fait que la famille $1, X-a, (X-a)^2, \ldots, (X-a)^n$ est échelonnée en degré, donc constitue une base de $\mathbb{K}_n[X]$ (exercice de TD). On peut donc écrire $P = X^N = \sum_{k=0}^{n} a_k (X-a)^k$. Pour déterminer a_k, on dérive k fois puis on *évalue*[6] en a ; on trouve alors $P^{(k)}(a) = k! a_k$, d'où le résultat.

Pour (2), le résultat est conséquence directe de la formule du binôme de Newton, justifiée ici puisque $\mathbb{K}[X]$ est commutatif.

Enfin, on peut ne montrer qu'une seule des deux relations puis en déduire la seconde. Dans le sens "(1) implique (2)", on compose (à droite) les polynômes des deux membres par le polynôme $X+a$. Dans l'autre sens, on compose avec $X-a$, en notant que $\big(P \circ (X+a)\big) \circ (X-a) = P \ldots$ ■

3.3 Caractérisation de l'ordre d'une racine

DÉFINITION 13
Soient $P \in \mathbb{K}[X]$, $x_0 \in \mathbb{K}$ une racine de P, et $p \in \mathbb{N}^*$. On dit que x_0 est racine de P de *multiplicité* k lorsque $(X-x_0)^k | P$ mais $(X-x_0)^{p+1}$ ne divise pas P.

Pour déterminer la multiplicité d'une racine, il faudrait donc faire a priori un certain nombre de divisions euclidiennes. En fait, la proposition suivante dit qu'il suffit de dériver et évaluer ces dérivées. On retrouve le vocabulaire habituel concernant les "racines doubles" d'applications polynômiales du second degré.

PROPOSITION 6 $x_0 \in \mathbb{K}$ *est racine de* $P \in \mathbb{K}[X]$ *de multiplicité* p *si et seulement si* $P^{(i)}(x_0) = 0$ *pour tout* $i \in [\![0, p-1]\!]$*, et* $P^{(p)}(x_0) \neq 0$.

PREUVE : Leibnitz dans un sens ; Taylor dans l'autre. ■

[6] au passage, on note que dans la formule de Taylor, on devrait plutôt écrire $\widetilde{P^{(k)}}(a) \ldots$

Exemple 10 *$X^4 - X^2$ admet pour racines 0 (de multiplicité 2), et 1 et -1 (de multiplicité 1) ; on parle de racines double et simples.*

Remarque 13 En cas de doute entre p, $p+1$ et $p-1$ dans l'énoncé du résultat précédent, on peut se ramener à un cas connu : une racine double x_0 pour un trinôme du second degré P est telle que $P(x_0) = P'(x_0) = 0$, mais bien entendu $P''(x_0) eq 0$. Même remarque pour la *définition* de la multiplicité d'une racine.

4 Factorisation

Les résultats de cette partie seront admis, mais doivent être appris !

4.1 Un peu de vocabulaire

Définition 14

- Un polynôme non constant $P \in \mathbb{K}[X]$ est *scindé* sur $\mathbb{K}$ s'il peut s'écrire comme produit de polynômes de degré 1.
- Un polynôme non constant $P \in \mathbb{K}[X]$ est dit *irréductible* sur $\mathbb{K}$ lorsque dans toute décomposition $P = AB$, l'un des deux polynômes A ou B est constant *(les irréductibles dans $\mathbb{K}[X]$ jouent le rôle des nombres premiers dans $\mathbb{Z}$).*

On méditera longtemps sur les exemples qui suivent.

Exemples 11

- *Les polynômes de degré 1 sont irréductibles.*
- *Les polynômes réels de degré 3 ne sont jamais irréductibles (l'analyse de leur fonction associée assure qu'ils admettent une racine).*
- *$X^2 + 1$ est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$, puisqu'on peut écrire $X^2 + 1 = (X + i)(X - i)$.*
- *Si P admet une racine et $\deg P \geq 2$, alors P n'est pas irréductible.*
- *(IMPORTANT) Le polynôme $P = (X^2 + 1)^2$ n'est pas irréductible dans $\mathbb{R}[X]$, bien qu'il n'admette pas de racine réelle.*

Un problème naturel consiste à factoriser un polynôme P donné en un produit de polynômes irréductibles[7]. Dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$, la situation est simple (les irréductibles sont connus et simples à décrire), et est exposée dans les deux prochains paragraphes. Pour le cas d'un corps quelconque, on sait qu'il y a existence et unicité de la décomposition (en un sens à préciser), mais par contre, les irréductibles peuvent être bien plus compliqués... Cela dit, on sait (et Maple aussi !) traiter le cas où $\mathbb{K} = \mathbb{Q}$, et quelques autres...

On pourra admettre le résultat suivant et son corollaire (ou bien les montrer à partir de la formule de Taylor), qui permettent de factoriser un polynôme, *pour peu qu'on connaisse assez de racines.*

Proposition 7 *Soit $P \in \mathbb{K}[X]$ admettant (au moins) pour racines distinctes x_1 (mult. α_1), ..., x_k (mult. α_k). Alors :*

$$\prod_{i=1}^{k} (X - x_i)^{\alpha_i} \Big| P.$$

Corollaire 3 *Si LES racines de P sur $\mathbb{K}$ sont x_1 (mult. α_1), ..., x_k (mult. α_k), alors P est scindé sur $\mathbb{K}$ si et seulement si $\sum_{i=1}^{k} \alpha_i = \deg P$.*
Si c'est le cas, et si a est le coefficient dominant de P, on a alors :

$$P = a \prod_{i=1}^{k} (X - x_i)^{\alpha_i}.$$

[7] de même qu'on cherche à factoriser les entiers en produits de nombres premiers

4.2 Factorisation sur $\mathbb{C}$

Le résultat qui suit est la "raison d'être" de $\mathbb{C}$:

THÉORÈME 3 D'Alembert-Gauss
Tout polynôme complexe non constant admet (au moins) une racine.

PREUVE : Admis. Les curieux pourront le montrer en Khôlle s'ils le souhaitent ... La version la plus simple (et la plus naturelle de mon point de vue) consiste à raisonner par l'absurde, montrer qu'il existe un z_0 tel que $|P(z_0)|$ est minimal, puis faire un DL de P au voisinage de z_0. ■

COROLLAIRE 4
- *Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
- *Tout polynôme complexe est scindé.*

PREUVE : Le premier point est conséquence directe du théorème, et le second se prouve par une récurrence élémentaire sur le degré du polynôme en question. ■

4.3 Factorisation sur $\mathbb{R}$

On commence par un résultat intervenant souvent, pour des résultats théoriques, mais aussi dans la pratique des factorisations. On le montre à partir de la caractérisation de la multiplicité des racines à l'aide des dérivées.

LEMME 1 *Soit $P \in \mathbb{R}[X]$ admettant une racine $\alpha \in \mathbb{C} \setminus \mathbb{R}$ de multiplicité p. Alors $\overline{\alpha}$ est racine de P de multiplicité p.*

PROPOSITION 8 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1, et ceux de degré deux aX^2+bX+c dont le discriminant $\Delta = b^2-4ac$ est strictement négatif.*

PREUVE : Pour les polynômes de degré 2, on transforme sous forme réduite (où X n'intervient qu'une seule fois). Si deg $P \geq 3$, on considère une racine complexe z_0 : si elle est réelle, c'est fini car $X - z_0$ divise P, et sinon, on sait que $\overline{z_0}$ est également racine, ce qui permet de mettre en facteur $(X-z_0)(X-\overline{z_0})$, qui est un polynôme réel. Il reste à voir pourquoi le quotient est réel : cela vient de l'unicité de la division euclidienne dans $\mathbb{C}[X]$ (c'est un point plus subtil qu'il n'y parait, et il convient de s'y attarder...). ■

REMARQUE 14 Pour factoriser sur $\mathbb{R}$, on peut factoriser sur $\mathbb{C}$, puis regrouper les termes complexes conjugués (comme dans la preuve précédente). Avec un peu d'habitude, on connaît l'allure des termes réels sans écrire explicitement la factorisation sur $\mathbb{C}$.

4.4 Quelques exemples

EXEMPLE 12 *X^n-1 est unitaire et admet n racines complexes distinctes qui sont les racines n-èmes de l'unité, de sorte que :*

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{2ik\pi/n}).$$

Pour la factorisation sur $\mathbb{R}$, on commence par faire un dessin où on représente les racines n-èmes de l'unité. Elles se regroupent différemment selon la parité de n : si $n = 2p$, on regroupe $X - e^{2ik\pi/n}$ et $X - e^{-2ik\pi/n} = X - e^{2i(n-k)\pi/n}$ pour $k \in [\![1, p-1]\!]$, et on obtient :

$$X^n - 1 = (X-1)(X+1) \prod_{k=1}^{p-1} \Big(X^2 - 2\cos\frac{ik\pi}{p} X + 1 \Big).$$

Dans le cas où $n = 2p+1$, on trouve :

$$X^n - 1 = (X-1)\prod_{k=1}^{p}\Big(X^2 - 2\cos\frac{2ik\pi}{2p+1}X + 1\Big).$$

EXEMPLE 13 *$P = (X+1)^{2n} - (X-1)^{2n}$ est de degré $2n-1$, de coefficient dominant $4n$, et ses racines $z \in \mathbb{C}$ sont $\neq 1$, donc sont les complexes qui vérifient $\dfrac{z+1}{z-1} \in \mathbb{U}_{2n}$. L'équation $\dfrac{z+1}{z-1} = 1$ n'admet pas de solution, par contre, si $k \in [\![1, 2n-1]\!]$, l'équation $\dfrac{z+1}{z-1} = e^{ik\pi/n}$ admet exactement une solution qui est $\dfrac{e^{ik\pi/n}+1}{e^{ik\pi/n}-1} = -i\operatorname{cotan}\dfrac{k\pi}{2n}$. Mais la fonction* cotan *est injective sur $]0,\pi[$, donc les $\operatorname{cotan}\dfrac{k\pi}{2n}$ sont distincts deux à deux, et P admet $2n-1$ racines distinctes. Ainsi :*

$$P = 4n\prod_{k=1}^{2n-1}\Big(X + i\operatorname{cotan}\frac{k\pi}{2n}\Big).$$

Si $\theta \in]0,\pi[$, $\operatorname{cotan}(\pi-\theta) = -\operatorname{cotan}\theta$, donc $\operatorname{cotan}\dfrac{(2n-k)\pi}{2n} = -\operatorname{cotan}\dfrac{k\pi}{2n}$, et on peut regrouper les termes pour $k \in [\![1, n-1]\!]$ avec les termes pour $k \in [\![n+1, 2n-1]\!]$, pour obtenir :

$$P = 4nX\prod_{k=1}^{n-1}\Big(X^2 + \operatorname{cotan}^2\frac{k\pi}{2n}\Big)$$

(le terme X apparaît pour $k = n$).

4.5 Relations entre coefficients et racines

REMARQUE 15 Si P est un trinôme du second degré de coefficient dominant a et de racines x_1 et x_2, alors on a $P = a(X-x_1)(X-x_2)$. Si par ailleurs $P = aX^2+bX+c$, on a alors en développant l'expression factorisée : $a(x_1+x_2) = -b$ et $ax_1x_2 = c$.

Ainsi, en regardant les coefficients d'un trinôme du second degré, on peut retrouver la somme et le produit de ses racines. La proposition suivante est une simple généralisation de ce fait.

PROPOSITION 9 *Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X]$ un polynôme scindé admettant pour racines comptées avec multiplicité $x_1, \ldots, x_n$. Soit $k \in [\![1, n]\!]$. Alors :*

$$a_{n-k} = a_n(-1)^k \sum_{1\leq i_1<i_2<\cdots<i_k\leq n} x_{i_1}x_{i_2}\ldots x_{i_k}.$$

PREUVE : Regarder le coefficient de X^{n-k} dans $a_n\prod_{k=1}^{n}(X-x_k)$. ∎

REMARQUES 16

- "comptées avec leur multiplicité" signifie qu'on fait apparaître chaque racine autant de fois que sa multiplicité. Sur $\mathbb{C}$, on trouve alors autant de racines que le degré. Par exemple, les racines "comptées avec leur multiplicité" de $X^4 - X^2$ sont 0, 0, -1 et 1.
- La "formule" de la propositon précédente semble bien compliquée. *En pratique*, il faut (et il suffit) d'avoir compris le fait suivant : "en écrivant un polynôme sous forme factorisée PUIS en développant, on obtient ses coefficients en fonction de ses racines". Il faut de plus être capable de retrouver effectivement les formules pour $n = 2$ et $n = 3$.

- Pour $k = 1$, on trouve : $\dfrac{a_{n-1}}{a_n} = -\sum_{i=1}^{n} x_i = -\sigma$.
- Pour $k = n$, on trouve : $\dfrac{a_0}{a_n} = (-1)^n x_1 x_2 \dots x_n = (-1)^n \pi$.

EXERCICE 5 *A l'aide de* $(X+1)^n - e^{2ni\theta}$, *montrer :*

$$\prod_{k=0}^{n-1} \sin\Big(\theta + \frac{k\pi}{n}\Big) = \frac{\sin n\theta}{2^{n-1}}.$$