Chapitre 19 — "L'essentiel" sur les polynômes

Préambule. Ce document est un résumé du chapitre sur les polynômes. Malgré son nombre de pages relativement grand, ce résumé est réduit à sa plus simple expression (par rapport aux attentes du programme) ; ce qui implique qu'aucune définition, aucune propriété de ce document ne doit être tenue pour négligeable.

Comme d'habitude, ce résumé ne contient aucune démonstration ; les preuves sont présentes dans le cours fait en classe. Je vous encourage très chaleureusement à essayer de comprendre ces démos, et à les faire par vous-mêmes. C'est par ce biais que vous vous approprierez les propriétés des polynômes, et que vous gagnerez en efficacité à l'écrit sur ce thème.

Table des matières

1. Polynômes - Généralités

1.1. L'anneau des polynômes.

Définition 1 - Un **polynôme (formel)** à coefficients dans un corps $\mathbb{K}$ est une suite d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang.

Notations : un polynôme P à coefficients dans $\mathbb{K}$ sera en général noté $P = \sum_{k=0}^{n} a_k X^k$.

Explicitement, cela signifie que l'on notera $P = X^2 - 2$ plutôt que $P = (-2, 0, 1, 0, 0, \ldots, 0, \ldots)$.

L'ensemble des polynômes en l'indéterminée X et à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$:

$$\mathbb{K}[X] = \{a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad , \quad (a_0, \ldots, a_n) \in \mathbb{K}^{n+1}\}$$

Le polynôme nul est celui dont tous les coefficients sont nuls : il est noté $0_{\mathbb{K}[X]}$ ou $\widetilde{0}$.

Définition 2 - (Addition dans $\mathbb{K}[X]$). Soient $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$ deux polynômes. La **somme** de P et Q est le polynôme noté $P + Q$ défini en posant :

$$P + Q = \sum_{k=0}^{n} (a_k + b_k) X^k$$

Muni de cette lci, il est aisé de vérifier que $(\mathbb{K}[X], +)$ est un **groupe abélien** [1].

Définition 3 - (Multiplication dans $\mathbb{K}[X]$). Soient $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$ deux polynômes. Le **produit** de P et Q est le polynôme noté PQ défini en posant :

$$PQ = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$$

Application. Considérons les polynômes $P = (1+X)^n$ et $Q = (1+X)^m$. En comparant le coefficient de X^n dans les deux expressions [2] du produit PQ, on peut établir la très classique **formule de Vandermonde** :

$$\forall\, (n, m) \in \mathbb{N}^2, \quad \sum_{k=0}^{n} \binom{n}{k} \binom{m}{n-k} = \binom{n+m}{n}$$

➢ Par ailleurs, il résulte de la définition que la multiplication est une lci associative et commutative, possédant un élément neutre (le polynôme constant $\widetilde{1}$ ou $1_{\mathbb{K}[X]}$), et distributive par rapport à l'addition.

1. L'addition est une loi de composition interne, associative, possédant un élément neutre (le polynôme nul $\widetilde{0}$), et pour laquelle tout polynôme P admet un inverse (son opposé $-P$ défini de manière évidente).
2. Celle donnée par la formule précédente, et celle donnée par le binôme de Newton.

Finalement :

Propriété 1 - (Anneau des polynômes).
$(\mathbb{K}[X], +, \times)$ est un anneau commutatif et intègre.

L'intégrité [3] de $\mathbb{K}[X]$ sera prouvée à l'aide des propriétés du degré, faisant l'objet de la section suivante.

1.2. Degré d'un polynôme.

Définition 4 - Soit $P = \sum_{k=0}^{n} a_k X^k$ non nul de $\mathbb{K}[X]$. Le **degré de** P est l'entier :

$$\deg(P) = \max\{k \in \mathbb{N},\ a_k \neq 0\}$$

Par convention : $\deg\left(\widetilde{0}\right) = -\infty$.

Sans transition :

Propriété 2 - (Propriétés du degré). Soient P et Q dans $\mathbb{K}[X]$. On a :

1/ $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$

2/ $\deg(PQ) = \deg(P) + \deg(Q)$

3/ $\forall \lambda \in \mathbb{K}^*, \deg(\lambda P) = \deg(P)$

4/ $\deg(P \circ Q) = \deg(P) \times \deg(Q)$

Premières applications des propriétés du degré :
- Résolution d'équations polynomiales
- Intégrité de $\mathbb{K}[X]$
- Inversibles de $\mathbb{K}[X]$ pour la multiplication

Remarque. La propriété concernant le degré de la somme de deux polynômes peut être précisée, comme indiqué ci-dessous.

Propriété 3 - (Degré d'une somme, cas d'égalité). Soient P et Q dans $\mathbb{K}[X]$. On a :

$$\deg(P+Q) = \max(\deg(P), \deg(Q)) \quad \text{SSI} \quad \begin{cases} \deg(P) \neq \deg(Q) \\ \quad \text{ou} \\ [\deg(P) = \deg(Q)] \wedge [\mathrm{cd}(P) + \mathrm{cd}(Q) \neq 0] \end{cases}$$

Exemples d'exercices d'application : 3, 4 et 9.

3. Dans $\mathbb{K}[X]$, le produit PQ est nul SSI P ou Q est le polynôme nul.

1.3. **Coefficient dominant d'un polynôme non nul.**

Définition 5 - Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme non nul de $\mathbb{K}[X]$. Le **coefficient dominant de** P est le scalaire : $a_{\deg(P)}$.

Remarque. Le coefficient dominant n'est pas défini pour le polynôme nul $\widetilde{0}$.

Terminologie. Un polynôme P est **unitaire** si $\mathrm{cd}(P) = 1$.

➤ Le cofficient dominant peut se révéler un outil plus fin que le degré pour résoudre certaines équations polynomiales, par exemple :

"Déterminer tous les polynômes $P \in \mathbb{K}[X]$ tels que : $X^2P'' = P^2$."

Exemples d'exercices d'application : énoncé ci-dessus, et exo 10.

2. Arithmétique dans $\mathbb{K}[X]$

Les anneaux des entiers et des polynômes possèdent un grand nombre de propriétés communes. L'objectif de ce chapitre est de passer en revue une partie de ces propriétés, en reprenant exactement le même plan que pour le chapitre d'arithmétique dans $\mathbb{Z}$.

2.1. **Diviseurs et multiples dans $\mathbb{K}[X]$.**

Définition 6 - Soient P et Q dans $\mathbb{K}[X]$.
On dit que P **divise** Q s'il existe un polynôme $R \in \mathbb{K}[X]$ tel $Q = PR$.
Dans ce cas, on note : $P|Q$.
On dit aussi que P est **un diviseur** de Q, ou que Q est **un multiple** de P.

Exemples. Pour tout entier n non nul, le polynôme $X^n - 1$ est multiple du polynôme $\sum_{k=0}^{n-1} X^k$. Le polynôme nul ne divise que le polynôme nul, mais est multiple de tout polynôme. Un polynôme constant non nul divise tout polynôme. Le polynôme $X - \mathrm{j}$ divise $X^2 + X + 1$. Le polynôme $X + 1$ divise $X^{2n} - 1$.

Propriétés de la relation de divisibilité. Comme son analogue dans $\mathbb{Z}$, la relation de divisibilité dans $\mathbb{K}[X]$ est réflexive, transitive, mais pas antisymétrique.

2.2. **Polynômes associés dans $\mathbb{K}[X]$.**

La notion de polynômes associés dans $\mathbb{K}[X]$ généralise celle d'entiers égaux ou opposés dans $\mathbb{Z}$.

Définition 7 - Soient P et Q dans $\mathbb{K}[X]$.
On dit que P et Q **sont associés** s'ils se divisent mutuellement, càd $P|Q$ et $Q|P$.

Exemples. $2X + 2$ et $X + 1$ sont associés ; X^2 et X ne le sont pas.

Propriété 4 - Soient P et Q dans $\mathbb{K}[X]$.

$$[P \text{ et } Q \textbf{ sont associés}] \iff [\exists\, \lambda \in \mathbb{K}^*,\ Q = \lambda P]$$

En d'autres termes deux polynômes sont associés SSI ils sont égaux à une constante multiplicative non nulle près, càd à la multiplication par un inversible de $\mathbb{K}[X]$ près (puisque : $\mathbb{K}[X]^* = \mathbb{K}^*$).

2.3. Division euclidienne dans $\mathbb{K}[X]$.

Théorème 1 - (Division euclidienne dans $\mathbb{K}[X]$)

$$\forall (A,B) \in \mathbb{K}[X]^2,\ B \neq \tilde{0},\ \exists!\ (Q,R) \in \mathbb{K}[X]^2,\ A = BQ + R \text{ et } \deg(R) < \deg(B)$$

Corollaire 1 - P divise Q SSI le reste dans la division euclidienne de Q par P est nul.

Premières applications :
- Déterminer si un polynôme en divise un autre
- Calcul de A^n connaissant un polynôme annulateur de $A \in \mathrm{M}_n(\mathbb{K})$
- Déterminer la partie entière et la partie polaire d'une fraction rationnelle

Exemples d'exercices d'application : 8, 12, 14, 15, 16 et 17.

2.4. PGCD de deux polynômes.

Notation. Pour tout polynôme $P \in \mathbb{K}[X]$, on note $\mathrm{Div}(P)$ l'ensemble des diviseurs de P dans $\mathbb{K}[X]$.

Définition 8 - Soient P et Q dans $\mathbb{K}[X]$ non nuls. On appelle **PGCD de P et Q** l'unique polynôme unitaire Δ tel que : $\mathrm{Div}(P) \cap \mathrm{Div}(Q) = \mathrm{Div}(\Delta)$.

Notation. On note $P \wedge Q$ le PGCD des polynômes P et Q.

Remarques. La preuve de l'existence et de l'unicité du polynôme Δ satisfaisant les conditions de la définition précédente est loin d'être triviale (elle est détaillée dans cours, et le "gros pdf"). Par ailleurs, on peut montrer sans trop de difficultés que $P \wedge Q$ est le polynôme unitaire de plus grand degré divisant à la fois P et Q. Cette propriété le rapproche du PGCD dans $\mathbb{Z}$: $n \wedge m$ étant le plus grand entier naturel divisant à la fois n et m.

Théorème 2 - (de Bezout dans $\mathbb{K}[X]$). Soient P et Q dans $\mathbb{K}[X]$.
Il existe un couple $(U,V) \in \mathbb{K}[X]^2$ tel que : $PU + QV = P \wedge Q$.

Cet énoncé, que l'on obtient comme conséquence de la propriété permettant de définir le PGCD, est surtout utile théoriquement. En effet, en pratique, si un couple (U,V) peut être déterminé comme dans $\mathbb{Z}$ via l'algorithme d'Euclide, son utilisation mène très vite à des calculs assez lourds (que l'on ne vous demanderait certainement pas de faire), et d'un intérêt assez limité.

Pour finir ce paragraphe, on dispose comme dans $\mathbb{Z}$ d'une propriété caractérisant les couples de polynômes premiers entre eux (càd les couples de polynômes de PGCD égal à 1).

Propriété 5 - Soient P et Q dans $\mathbb{K}[X]$.

$$\left[\exists (U,V) \in \mathbb{K}[X]^2,\quad PU + QV = 1\right] \iff [P \text{ et } Q \text{ premiers entre eux}]$$

Exemple fondamental. Si α et β sont deux scalaires distincts, alors $(X-\alpha)$ et $(X-\beta)$ sont premiers entre eux.

C'est une conséquence de la propriété précédente, et de l'observation ci-dessous :

$$\frac{1}{\beta-\alpha}(X-\alpha)-\frac{1}{\beta-\alpha}(X-\beta)=1$$

2.5. Arithmétique dans $\mathbb{K}[X]$ - la suite.

Arrivé à ce point du cours, on peut reprendre paragraphe après paragraphe le chapitre sur l'arithmétique des entiers, et construire par analogie celui sur l'arithmétique des polynômes. C'est ce qui a été fait dans le "gros pdf" ; mais de fait, certaines notions - au programme - ne sont pratiquement jamais utilisées ni évaluées au concours : c'est notamment le cas de la notion du PPCM dans $\mathbb{K}[X]$ (mais pas seulement).

Prenons donc le "risque" de se concentrer sur l'essentiel (c'est l'objectif de ces notes), en énonçant deux résultats qui s'appliqueront un peu plus loin à la factorisation des polynômes.

Lemme de Gauss dans $\mathbb{K}[X]$. Soient P, Q et R dans $\mathbb{K}[X]$.

$$[P|QR \quad \text{et} \quad P\wedge Q=1] \Longrightarrow [P|R]$$

Propriété 6 - Soient P, Q et R dans $\mathbb{K}[X]$.

$$[P|R, \quad Q|R \quad \text{et} \quad P\wedge Q=1] \Longrightarrow [PQ|R]$$

Conséquence. Soient P un polynôme, α et β sont deux scalaires distincts.

Si $(X-\alpha)|P$ et $(X-\beta)|P$, alors $(X-\alpha)(X-\beta)|P$. [4]

Cet ingrédient justifiera le fait que l'on peut factoriser un polynôme par $(X-\alpha)(X-\beta)$ dès lors que l'on sait que α et β sont racines de P.

3. Fonctions polynomiales

3.1. Généralités.

A partir de maintenant, nous aurons le droit "d'évaluer en α" des polynômes, qui pourront être interprétés comme des fonctions.

Définition 9 - Soit $P\in\mathbb{K}[X]$, avec : $P=\sum_{k=0}^{n}a_kX^k$.

On appelle **fonction polynomiale associée à** P et on note (abusivement) P la fonction définie sur $\mathbb{K}$ en posant :

$$\forall\, t\in\mathbb{K}, \quad P(t)=\sum_{k=0}^{n}a_kt^k$$

4. C'est une application directe de la propriété, en utilisant l'observation faite précédemment : $(X-\alpha)$ et $(X-\beta)$ sont premiers entre eux.

On commence par une notion déjà bien connue.

Définition 10 - Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

Le scalaire α est **racine du polynôme** P si $P(\alpha) = 0$.

Exemples : j et j^2 sont racines de $X^2 + X + 1$; -1, i et $-\mathrm{i}$ sont racines de $X^3 + X^2 + X + 1$.

On obtient comme application du théorème de la division euclidienne dans $\mathbb{K}[X]$ l'énoncé suivant :

Propriété 7 - Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

$$[\alpha \text{ est racine de } P] \iff [\text{le reste dans la D.E. de } P \text{ par } (X - \alpha) \text{ est nul}]$$

3.2. Racines et factorisation.

En utilisant la propriété énoncée plus haut, et celle énoncée à la fin de la partie consacrée à l'arithmétique dans $\mathbb{K}[X]$, on obtient :

Propriété 8 - Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

$$[\alpha \text{ est racine de } P] \iff [(X - \alpha) \text{ divise } P]$$

Généralisation. Soient $P \in \mathbb{K}[X]$ et $\alpha_1, \ldots, \alpha_n$ des scalaires deux à deux distincts ($n \in \mathbb{N}^*$). Alors :

$$[\alpha_1, \ldots, \alpha_n \text{ sont racines de } P] \iff [\prod_{i=1}^{n} (X - \alpha_i) \text{ divise } P]$$

Application. Soient n, m et p trois entiers naturels. Le polynôme $X^2 + X + 1$ divise le polynôme $X^{3n} + X^{3m+4} + X^{3p+17}$. En effet, on a d'une part $X^2 + X + 1 = (X - \mathrm{j})\left(X - \mathrm{j}^2\right)$.

D'autre part, en notant $P = X^{3n} + X^{3m+4} + X^{3p+17}$, on vérifie aisément que $P(\mathrm{j}) = P\left(\mathrm{j}^2\right) = 0$ (principalement en utilisant les identités $\mathrm{j}^3 = 1$ et $1 + \mathrm{j} + \mathrm{j}^2 = 0$). On en déduit que $(X - \mathrm{j})\left(X - \mathrm{j}^2\right) | P$, ce qu'il fallait établir.

Propriété 9 - (nombre maximal de racines d'un polynôme).

Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}^*$.

Si $\deg P = n$, alors P possède au plus n racines.

De plus, dans le cas où $\alpha_1, \ldots, \alpha_n$ sont n racines (deux à deux distinctes) de P, alors :

$$P = \mathrm{cd}(P) \prod_{i=1}^{n} (X - \alpha_i)$$

Application : factorisation des polynômes de Tchebychev (exercice 50).

Une formulation équivalente de l'énoncé majorant le nombre de racines d'un polynôme par son degré est :

Propriété 10 -

Soient $n \in \mathbb{N}^*$ et $P \in \mathbb{K}_n[X]$.

Si P possède $(n + 1)$ racines 2 à 2 distinctes, alors $P = \widetilde{0}$.

Corollaire 2 - (principe du prolongement algébrique).
Soient $n \in \mathbb{N}^*$, P et Q dans $\mathbb{K}_n[X]$.
S'il existe $(n+1)$ scalaires $(\alpha_i)_{1\leqslant i\leqslant n+1}$ deux à deux distincts tels que :

$$\forall\, i \in[\![\, 1,\ n+1\,]\!], P(\alpha_i) = Q(\alpha_i)$$

alors $P = Q$.

Application - Construction des polynômes interpolateurs de Lagrange. Soient $\alpha_0,\ldots,\ \alpha_n$ $(n+1)$ scalaires deux à deux distincts. On définit les polynômes interpolateurs de Lagrange $L_0,\ldots,\ L_n$ associés à ces scalaires en posant :

$$\forall\, k \in[\![\, 0, n\,]\!], \qquad L_k = \prod_{j=0,\, j\neq k}^{n} \frac{X-\alpha_j}{\alpha_k-\alpha_j}$$

Pour tout entier k, il est clair que L_k est de degré n.

Par ailleurs :

$$\forall\, k \in[\![\, 0, n\,]\!],\ \forall\, i \in[\![\, 0, n\,]\!],\ L_k(\alpha_i) = \delta_{ik}$$

Chacun des polynômes L_k prend donc la valeur 1 en α_k, et s'annule sur les autres α_i. Ces polynômes ont deux applications principales : en Algèbre, ils sont utilisés pour des problèmes d'interpolation (d'où leur nom !), consistant à déterminer l'équation d'une courbe polynomiale passant par des points donnés. En Analyse par ailleurs, ils sont utiles pour démontrer le théorème de Stone-Weierstrass (un célèbre résultat que vous verrez l'an prochain), qui affirme que toute fonction continue sur un segment peut être approchée "arbitrairement près" par une fonction polynomiale.

Exemples d'exercices d'application : 21, 22 et 33.

3.3. Dérivation formelle dans $\mathbb{K}[X]$.

Définition 11 - Soit $P \in \mathbb{K}[X]$ un polynôme non-constant (càd de degré $\geqslant 1$), que nous noterons : $P = \sum_{k=0}^{\deg(P)} a_k X^k$.
Le **polynôme dérivé** de P est défini en posant :

$$P' = \sum_{k=0}^{\deg(P)} k a_k X^{k-1}$$

Lorsque P est constant, on pose $P' = \tilde{0}$.

Dans le sens où la dérivation possède la propriété de linéarité, on dit que la dérivation est une **application linéaire** (définie sur $\mathbb{K}[X]$ et à valeurs dans $\mathbb{K}[X]$) :

$$\forall\,(\lambda,\mu) \in \mathbb{K}^2,\ \forall\,(P,Q) \in \mathbb{K}[X]^2,\ (\lambda P + \mu Q)' = \lambda P' + \mu Q'$$

Propriété. Si $P \in \mathbb{K}[X]$ et $\deg(P) \geqslant 1$, alors :

$$\deg(P') = \deg(P) - 1$$

En outre, si P est non constant, alors :

$$\mathrm{cd}(P') = \deg(P)\ \mathrm{cd}(P)$$

Bien entendu, on peut itérer la définition de dérivée dans $\mathbb{K}[X]$.

Définition 12 - Soit n un entier naturel, et soit $P \in \mathbb{K}[X]$.

On appelle **dérivée n-ième** du polynôme P et on note $P^{(n)}$ l'élément de $\mathbb{K}[X]$ défini récursivement en posant :

$$P^{(0)} = P, \text{ et pour tout } n \in \mathbb{N}^*,\ P^{(n)} = \left(P^{(n-1)}\right)'$$

Exemple. Si $P = X^3 + 4X^2 + 1$, alors $P' = 3X^2 + 8X$; $P'' = 6X + 8$; $P^{(3)} = 6$ et $P^{(n)} = \widetilde{0}$ pour tout entier $n \geqslant 4$.

Comme précédemment, le fait d'associer à un polynôme son n-ème polynôme dérivé est une **application linéaire** (définie sur $\mathbb{K}[X]$ et à valeurs dans $\mathbb{K}[X]$) :

$$\forall (\lambda, \mu) \in \mathbb{K}^2,\ \forall (P, Q) \in \mathbb{K}[X]^2,\ (\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$$

Par ailleurs, il résulte de la définition (de polynôme et de dérivée successive) que les dérivées successives d'un polynôme seront toutes nulles à partir d'un certain rang. Cette propriété rend particulièrement sympathique (càd exacte) la formule de Taylor dans $\mathbb{K}[X]$ ("pas de petit o").

Théorème 3 - (Formule de Taylor dans $\mathbb{K}[X]$, en α).

Soit $P \in \mathbb{K}[X]$ non nul, et soit $\alpha \in \mathbb{K}$. On a :

$$P = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k$$

soit encore, en notant $n = \deg(P)$:

$$P = P(\alpha) + P'(\alpha)(X - \alpha) + \frac{P''(\alpha)}{2}(X - \alpha)^2 + \cdots + \frac{P^{(n)}(\alpha)}{n!}(X - \alpha)^n$$

Théorème 4 - (Formule de Taylor dans $\mathbb{K}[X]$, en 0).

Soit $P \in \mathbb{K}[X]$ non nul. On a :

$$P = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(0)}{k!} X^k$$

soit encore, en notant $n = \deg(P)$:

$$P = P(0) + P'(0)X + \frac{P''(0)}{2} X^2 + \cdots + \frac{P^{(n)}(0)}{n!} X^n$$

Remarque. Naturellement, un seul énoncé aurait suffi, la seconde formule étant un corollaire immédiat de la première.

La volonté de donner ces deux énoncés est motivée par la considération suivante : la formule de Taylor en α, plus générale, est utilisée notamment dans l'étude de la multiplicité d'une racine (voir paragraphe suivant). La formule de Taylor en 0 présente quant à elle l'intérêt de faire le lien entre les coefficients d'un polynôme et ses dérivées successives en 0 ; explicitement, il est équivalent de choisir les coefficients $a_0,\ldots,\ a_n$ d'un polynôme P, ou de choisir ses dérivées successives en 0, puisque :

$$\forall\, k \in [\![\, 0, n\,]\!],\ a_k = \frac{P^{(k)}(0)}{k!} \text{ soit encore : } \forall\, k \in [\![\, 0, n\,]\!],\ P^{(k)}(0) = k!\, a_k$$

3.4. **Racines multiples.**

Définition 13 - Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$.

Le scalaire α est racine de P de **multiplicité au moins** m (*resp.* de **multiplicité** m) si $(X-\alpha)^m$ divise P (*resp.* $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne divise pas P).

Exemples : 2 est racine de multiplicité exactement 3, 0 est racine de multiplicité exactement 4, et 1 est racine simple du polynôme $(X-2)^3(X-1)X^4$.

Théorème 5 - (multiplicité/dérivées successives).

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$.

α est racine de P de multiplicité au moins m SSI $P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$.

α est racine de P de multiplicité exactement m SSI $P(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$.

En résumé, ce théorème fournit une méthode pratique pour calculer la multiplicité d'une racine :

Calcul pratique de la multiplicité d'une racine

Soient $P \in \mathbb{K}[X]$ et α un scalaire.

1/ On vérifie que α est racine de P (*ie* $P(\alpha) = 0$).

2/ On calcule $P'(\alpha)$, $P''(\alpha)$, …, $P^{(p)}(\alpha)$ jusqu'à obtenir une dérivée non nulle.

3/ Le premier entier p pour lequel $P^{(p)}(\alpha) \neq 0$ est la multiplicité de α.

Exemple : $P = X^{2n} - nX^{n+1} + nX^{n-1} - 1$ (avec n entier $\geqslant 3$) est divisible par $(X-1)^3$, car $P(1) = P'(1) = P''(1) = 0$; et pas divisible par $(X-1)^4$ car $P^{(3)}(1) \neq 0$.

Exemples d'exercices d'application : 34, 35 et 38.

4. Polynômes irréductibles

Dans $\mathbb{Z}$, un nombre premier est un entier p différent de 1 et -1 n'admettant pas de diviseur non trivial (càd différent de ± 1 et de $\pm p$). Dans $\mathbb{K}[X]$, la notion correspondante est celle de polynôme irréductible : un tel polynôme sera un polynôme non-constant, n'admettant pas de diviseur non trivial (càd non associé à 1 et à P).

4.1. Généralités.

Définition 14 - Un polynôme $P \in \mathbb{K}[X]$ non-constant (*ie* de degré $\geqslant 1$) est **irréductible dans** $\mathbb{K}[X]$ si les seuls diviseurs de P dans $\mathbb{K}[X]$ sont les polynômes associés à P et à $\tilde{1}$.

Exemples.

- Le polynôme $X - \alpha$ est irréductible dans $\mathbb{K}[X]$, pour tout scalaire α.
- Le polynôme $(X-1)^3$ n'est pas irréductible, tout comme le polynôme $X^4 + 4X^3 + 6X^2 + 4X + 1 = (X+1)^4$.
- Le polynôme $P = X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais pas dans $\mathbb{C}[X]$.
- Posons $P = X^4 - 1$. Dans $\mathbb{C}[X]$, P peut s'écrire comme produit de polynômes irréductibles de la façon suivante :

$$X^4 - 1 = (X-1)(X+1)(X-\mathrm{i})(X+\mathrm{i})$$

Dans $\mathbb{R}[X]$, P peut s'écrire comme produit de polynômes irréductibles de la façon suivante :

$$X^4 - 1 = (X-1)(X+1)(X^2+1)$$

L'énoncé ci-dessous est la traduction dans l'anneau des polynômes du théorème de décomposition en facteurs premiers dans l'anneau des entiers.

Théorème 6 - (décomposition en irréductibles dans $\mathbb{K}[X]$).

Tout polynôme non constant de $\mathbb{K}[X]$ peut s'écrire comme un produit de polynômes irréductibles, de manière unique à l'ordre des facteurs et à une constante multiplicative près.

Explicitement, pour tout polynôme $P \in \mathbb{K}[X] \setminus \{\tilde{0}\}$, il existe des polynômes $P_1, \ldots, P_n$ irréductibles unitaires et deux à deux distincts, et des entiers naturels non nuls $\alpha_1, \ldots, \alpha_n$ tels que :

$$P = \mathrm{cd}(P) \prod_{i=1}^{n} P_i^{\alpha_i}$$

Exemples.

- Dans $\mathbb{C}[X]$ ou $\mathbb{R}[X]$, la décomposition en irréductibles du polynôme $X^3 - 3X^2 + 2X$ est $X(X-1)(X-2)$.
- Dans $\mathbb{C}[X]$, la décomposition en irréductibles du polynôme $X^5 + X^4 + X^3$ est $X^3(X-\mathrm{j})(X-\bar{\mathrm{j}})$.

  Dans $\mathbb{R}[X]$, la décomposition en irréductibles du polynôme $X^5 + X^4 + X^3$ est $X^3(X^2+X+1)$.

➢ Dans $\mathbb{C}[X]$, la décomposition en irréductibles du polynôme X^6-1 est $\prod_{\omega\in\mathbb{U}_6}(X-\omega)$, càd plus explicitement :

$$X^6-1=(X-1)(X+\mathrm{j})(X-\mathrm{j})(X+1)\left(X-\bar{\mathrm{j}}\right)\left(X+\bar{\mathrm{j}}\right)$$

En effet, les racines sixièmes de l'unité sont les complexes $\mathrm{e}^{2\mathrm{i}k\pi/6}=\mathrm{e}^{\mathrm{i}k\pi/3}$, avec k variant de 0 à 5. Ces six nombres complexes sont, par "ordre d'apparition" sur le cercle trigo, 1, $-\bar{\mathrm{j}}$, j, -1, $\bar{\mathrm{j}}$ et $-\mathrm{j}$.

Dans $\mathbb{R}[X]$, la décomposition en irréductibles du polynôme X^6-1 s'obtient à partir de la précédente en multipliant les parenthèses faisant intervenir des racines conjuguées :

$$X^6-1=(X-1)\underbrace{\left(X^2+X+1\right)}_{=(X-\mathrm{j})\left(X-\bar{\mathrm{j}}\right)}(X+1)\underbrace{\left(X^2-X+1\right)}_{=(X+\mathrm{j})\left(X+\bar{\mathrm{j}}\right)}$$

Remarques. En pratique, il est très important de connaître la formule suivante (de démonstration immédiate) pour obtenir rapidement la décomposition en irréductibles dans $\mathbb{R}[X]$ à partir de la DPI dans $\mathbb{C}[X]$:

Formule (très) pratique.

$$\forall\, z\in\mathbb{C},\qquad (X-z)(X-\overline{z})=X^2-2\mathrm{Re}(z)+|z^2|$$

Dans le même registre, il est très pratique de connaître l'énoncé suivant, qui affirme que si un complexe z est racine d'un polynôme à coefficients réels, alors son conjugué $\overline{z}$ l'est aussi (la démo de ce fait est un bon petit exercice, pas trop compliqué).

Propriété (très) pratique.

Soient $P\in\mathbb{R}[X]$ et $\alpha\in\mathbb{C}$.

$$[P(\alpha)=0]\Longrightarrow[P(\overline{\alpha})=0]$$

En d'autres termes, si α est racine de P, alors $\overline{\alpha}$ est également racine de P.

Exemple d'application spécifique de cette dernière propriété : 19.

Exemples d'exercices d'application relatifs au paragraphe : 41, 45 et 48.

4.2. Irréductibles de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$.

Les énoncés de ce paragraphe décrivent les polynômes irréductibles lorsque l'on travaille dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$. Il est indispensable de les connaître lorsque l'on vous demande de déterminer la décomposition en irréductibles d'un polynôme, ce que l'on a déjà illustré à la section précédente.

Théorème 7 - (description des irréductibles de $\mathbb{C}[X]$).

Dans $\mathbb{C}[X]$, les polynômes irréductibles sont exactement les polynômes de degré 1.

Théorème 8 - (description des irréductibles de $\mathbb{R}[X]$).

Dans $\mathbb{R}[X]$, les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif (càd sans racine réelle).

Même si elle est hors-programme, il serait dommage de ne pas dire un mot sur la preuve de ces résultats. Le second est une conséquence un peu technique du premier, largement à votre niveau. En revanche, le premier (description des irréductibles de $\mathbb{C}[X]$) est plus corsé. Dans le détail, cet énoncé est une équivalence :

$$P \text{ irréductible dans } \mathbb{C}[X] \text{ SSI } P \text{ est de degré } 1$$

L'implication de la droite vers la gauche n'est pas trop difficile : c'est même une excellente question de cours, pour vérifier que vous connaissez la définition de polynôme irréductible, et les propriétés du degré.

En revanche, la réciproque ne peut se faire sans le **théorème de d'Alembert-Gauss**[5] ; celui-ci affirme que tout polynôme non constant à coeffs dans $\mathbb{C}$ admet une racine complexe.[6]

On finit ce voyage au pays des polynômes par une définition, qui sera utilisée l'an prochain (MP/PSI) en Algèbre linéaire dans le cadre de la réduction des endomorphismes.

Définition 15 -

Un polynôme de $\mathbb{K}[X]$ est **scindé (dans $\mathbb{K}$)** si toutes ses racines appartiennent à $\mathbb{K}$.

Exemples.

- ➢ Le polynôme $X^2 - 1$ est scindé (dans $\mathbb{R}$ ou $\mathbb{C}$).
- ➢ Le polynôme $X^2 + 1$ est scindé dans $\mathbb{C}$, mais pas dans $\mathbb{R}$ (i est dans $\mathbb{C}\backslash\mathbb{R}$).

5. Parfois appelé **théorème fondamental de l'Algèbre**, c'est dire !

6. Il revient au même de dire que toute équation polynomiale (de degré $\geqslant 1$) à coefficients complexes possède au moins une solution dans $\mathbb{C}$. On traduit cette propriété en disant que $\mathbb{C}$ est un corps **algébriquement clos**.

➢ Le polynôme $X^3 - 1$ est scindé dans $\mathbb{C}$, mais pas dans $\mathbb{R}$ (j est dans $\mathbb{C}\backslash\mathbb{R}$).

Le dernier énoncé de ce chapitre est une conséquence du théorème de d'Alembert-Gauss.

Propriété 11 -
Tout polynôme de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}$.

5. Fractions rationnelles

A venir ! La notion de fraction rationnelle, intimement liée à celle de polynôme, fera l'objet d'un chapitre "à part", dans quelques semaines.

6. Synthèse - A savoir, à savoir faire

Comme évoqué dans le préambule, les définitions et propriétés énoncées dans ce document sont à connaître. Je vous encourage à ne pas faire une impasse totale sur la partie théorique (les preuves des propriétés), qu'il vous faudra avoir assimilée pour pouvoir aller plus loin (dans le cours de cette année, et de la suivante).

Par ailleurs, ce chapitre contient un certain nombre de méthodes permettant de résoudre à des questions pratiques courantes. Ces méthodes pratiques sont liées aux notions suivantes :

- le degré et le coefficient dominant (pour la résolution d'une équation polynomiale par exemple) ;
- le théorème de la division euclidienne (pour calculer les puissances d'une matrice par exemple, cf exos 14/15) ;
- le rôle des racines dans la factorisation d'un polynôme ; notamment pour les **polynômes de Tchebychev** ;
- le principe du prolongement algébrique ; application aux **polynômes interpolateurs de Lagrange**. Concernant ces polynômes en particulier, la formule générale "$L_k = \prod_{j=0,\, j\neq k}^{n} \frac{X-\alpha_j}{\alpha_k-\alpha_j}$" est à savoir retrouver (il suffit d'en avoir compris le principe) ; et 15 secondes doivent vous suffire pour trouver l'expression de l'unique polynôme P de degré 3 admettant 0, 1 et 4 comme racines, et tel que $P(5) = 1$.
- les formules de Taylor dans $\mathbb{K}[X]$;
- le calcul pratique de la multiplicité d'une racine ;
- la décomposition en irréductibles dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.