CH4) Polynômes à une indéterminée sur un anneau

Dans ce texte, A désigne un anneau (commutatif, unitaire). On supposera parfois que c'est un corps, auquel cas on adoptera la notation K.

Les polynômes sont un peu hybrides. Par analogie avec les fonctions polynômiales sur $\mathbb{R}$ (mais il ne faut ne pas confondre les notions !) ils jouissent d'un statut de fonction. Mais ils ont aussi une nature éminemment arithmétique, comme s'ils étaient des nombres (notion de pgcd, ppcm, théorème de Bezout,...). En outre, comme nous l'avons déjà observé, l'ensemble des polynômes admet une structure naturelle d'espace vectoriel ; et nous verrons plus tard qu'ils jouent un rôle fondamental dans l'étude des endomorphismes d'un espace vectoriel !

Cette versalité font des polynômes, sur un anneau ou un corps quelconque, des objets centraux en algèbre.

1. Anneau des polynômes $A[X]$

Définition 1.1. *Un polynôme à une indéterminée est une suite presque nulle d'éléments de A. Le n-ième élément de la suite est appelé* ***coefficient de degré*** *n.*

Un polynôme est donc un élément de $A^{(\mathbb{N})}$. Un tel polynôme peut donc être noté $(a_i)_{i\in\mathbb{N}}$. Comme les a_i doivent être nuls à partir d'un certain rang, on peut aussi le noter $(a_0, a_1, ..., a_n)$, en convenant $a_i = 0$ si $i > n$.

Le plus pratique, et la notation la plus fréquente pour représenter un polynôme, est :

$$P = \sum_{i=0}^{n} a_i X^i$$

(Dans cette écriture, il n'est pas exigé que le «coefficient» a_n soit non-nul).

On peut aussi écrire :

$$P = \sum_{i\geq 0} a_i X^i$$

en gardant à l'esprit que les a_i doivent être nul à partir d'un certain rang.

La lettre X ne correspond à rien (pas un élément de A, où je ne sais quoi), juste une «indéterminée», un artifice de notation. Cette notation a l'avantage de rendre très lisible la loi interne de multiplication que nous allons (re)définir. C'est cette notation, si pratique, qui amène à écrire $A[X]$, et non $A^{(\mathbb{N})}$, l'ensemble des polynômes sur A.

Nota Bene : Il est fréquent de «confondre» le polynôme avec la fonction de A dans A qui envoie chaque x de A sur $\sum_{i=0}^{n} a_i x^i$; c'est du reste ce que suggère la notation. C'est une (mauvaise) habitude venant de l'étude des fonctions polynômiales sur $\mathbb{R}$ ou $\mathbb{C}$. **Il faut bien se garder de confondre les deux notions !**

1.1. Addition, multiplication Nous avons déjà vu, lorsque A est un corps K, que $K^{(I)}$ est naturellement muni d'une structure de groupe additif (et même de K-espace vectoriel). La même chose reste vrai (pour ce qui est de la loi de groupe) lorsque A n'est pas forcément un corps :

Théorème - Définition 1.2. *Soient P, Q deux polynômes, $P = \sum_{i\geq 0} a_i X^i$, $Q = \sum_{i\geq 0} b_i X^i$. On note $P+Q$ le polynôme $\sum_{i\geq 0}(a_i+b_i)X^i$. Pour tout entier $n \geq 0$, on définit $d_n = \sum_{p+q=n} a_p b_p$; alors la suite $(d_n)_{n\in\mathbb{N}}$ est presque-nulle, donc un polynôme, qui est noté $P.Q$, et appelé produit de P et Q.* □

Théorème 1.3. *Le triplet $(A[X], +, .)$ est un anneau commutatif non-nul.*

Démonstration. : Similaire à celle quand A est un corps. □

1.2. Plongement de l'anneau A dans $A[X]$.

Théorème - Définition 1.4. *L'application de A dans $A[X]$ qui envoie un élément a de A sur aX^0 (ie. le polynôme dont tous les coefficients sont nuls sauf celui de degré nul, qui vaut alors a) est un morphisme d'anneaux injectif.* □

Il est convenu d'identifier l'anneau A avec son image dans $A[X]$ par ce morphisme injectif. Ainsi, on écrit tout simplement a au lieu de aX^0.

De manière plus générale, un terme du polynôme dont le coefficient vaut 1 est noté tout simplement X^i au lieu de $1.X^i$. Si le coefficient est nul, il est tout simplement omis !

Définition 1.5. *Un monôme est un polynôme dont tous les coefficients sont nuls, sauf un qui vaut* 1.

Il n'y a donc qu'un monôme de degré i, on le note X^i.
Ainsi, l'anneau A s'identifie au sous-anneau des monômes de degré nul.

En résumé, un élément typique de $A[X]$ est noté :

$$X^7 + aX^5 + bX^4 + X^2 - X + c$$

où a, b et c sont des éléments de A.

1.3. Anneaux intègres

Certaines propriétés de l'anneau A (pas toutes) restent vraies dans $A[X]$. Par exemple :

Proposition 1.6. *A est intègre si et seulement si $A[X]$ est intègre.*

Démonstration. Si $A[X]$ est intègre, A aussi puisque A est un sous-anneau de $A[X]$.

Inversement, supposons A intègre. Supposons par l'absurde qu'il existe deux polynômes non-nuls $P = \sum_{i\geq 0} a_i X^i$, $Q = \sum_{i\geq 0} b_i X^i$ dont le produit $P.Q$ est nul. Soit n le plus grand indice tel que $a_n \neq 0$ et m le plus grand indice tel que $b_m \neq 0$. Le coefficient de degré $m+n$ de $P.Q$ est nul, donc :

$$0 = \sum_{p+q=n+m} a_p b_p = a_0.0 + a_1.0 + ... + a_n.b_m + 0.b_{m-1} + ... + 0.b_0 = a_n b_m$$

Contradiction. □

Exercice 1. Montrer que $A[X]$ n'est jamais un corps, même si A l'est.

1.4. Degré

Définition 1.7. *Le degré d'un polynôme $P = \sum_{i\geq 0} a_i X^i$* ***non-nul*** *est le plus grand entier i pour lequel a_i est non-nul. Il est noté* $\deg P$.

Par convention :

$$\deg 0 = -\infty$$

Désormais, on s'en tient à l'écriture $P = \sum_{i=0}^{n} a_i X^i$, où il est sous-entendu que n est plus grand que le degré de P (mais pas forcément égal).

Proposition 1.8. *Pour tout P,Q dans $A[X]$ on a :*

$$\deg(P+Q) \leq \sup[\deg P, \deg Q] \qquad \deg(P.Q) \leq \deg P + \deg Q$$

Si A est intègre :

$$\deg(P.Q) = \deg P + \deg Q$$

□

Corollaire 1.9. *Si A est intègre, les unités (ie. éléments inversibles de $A[X]$) sont les éléments de A (polynômes de degré nuls) inversibles dans A.* □

1.5. Polynôme unitaire

Définition 1.10. *Un polynôme P de $A[X]$ est* ***unitaire*** *si le coefficient de son terme de plus haut degré est* 1.

1.6. Dérivation de polynôme

Définition 1.11. *Le polynôme dérivé d'un polynôme $P = \sum_{i=0}^{n} a_i X^i$ de $A[X]$ est le polynôme $\sum_{i=0}^{n-1}(i+1)a_{i+1}X^i$ de $A[X]$. On le note P'.*

Proposition 1.12. *Le polynôme dérivé P' d'un polynôme P de $A[X]$ est de degré strictement inférieur à celui de P.* □

Remarque 1.13. *Attention ! On n'a pas toujours* $\deg P' = \deg P - 1$ *(cf. exo suivant). En fait, cette égalité a lieu si et seulement si, notant n le degré de P et a_n son coefficient dominant, $na_n \neq 0$.*

Exercice 2. Calculer le polynôme dérivé de X^n dans $(\mathbb{Z}/n\mathbb{Z})[X]$.

Proposition 1.14. *Soit K un corps. L'application de $K[X]$ dans lui-même qui à un polynôme P associe le polynôme dérivé P' est un endomorphisme de K-espace vectoriel.* □

On peut définir par récurrence la dérivée d'ordre n d'un polynôme :

Définition 1.15. *Le **polynôme dérivé (itéré) d'ordre** k d'un polynôme P de $A[X]$ est le polynôme dérivée du polynôme dérivé d'ordre $(k-1)$ de P. On le note $P^{(k)}$.*

Théorème 1.16 (Règle de Leibniz)**.** *Pour toute paire d'éléments P, Q de $A[X]$ et pour tout entier n on a :*

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

En particulier, pour $n = 1$:

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

□

1.7. Composition de polynômes

Définition 1.17. *Soient $P = \sum_{i=0}^{n} a_i X^i$, $Q = \sum_{i=0}^{n} b_i X^i$ deux éléments de $A[X]$. On appelle **polynôme composé de P et Q** le polynôme :*

$$\sum_{i=0}^{n} a_i Q^i$$

On le note $P \circ Q$ ou aussi $P(Q)$.

Proposition 1.18. *La composition est une loi associative. Elle vérifie :*
- $P_1 \circ Q + P_2 \circ Q = (P_1 + P_2) \circ Q$
- $P \circ X = P$
- $X \circ P = P$

Ainsi, comme $P \circ X = P$, la notation $P = P(X)$ n'est pas si abusive qu'elle en a l'air...

1.8. Fonction polynôme

Définition 1.19. *Soit $P = \sum_{i=0}^{n} a_i X^i$ un élément de $A[X]$. L'application $\widetilde{P} : A \to A$ définie par :*

$$\widetilde{P}(x) = \sum_{i=0}^{n} a_i x^i$$

*est appelée **fonction polynôme associée à P.***

Proposition 1.20. *Pour tout a dans A, et tout P, Q dans $A[X]$, on a :*

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}, \quad \widetilde{P.Q} = \widetilde{P}.\widetilde{Q}, \quad \widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}, \quad \widetilde{aP} = a.\widetilde{P}$$

□

L'application qui à un polynôme associe sa fonction polynôme est donc un morphisme d'anneaux entre $(A[X], +, .)$ et $(A^A, +, .)$. C'est même un morphisme d'algèbres lorsque A est un corps. *Mais elle n'est pas injective !*

Exercice 3. Considérons le cas où A est le corps $\mathbb{F}_p$ à p éléments (où p est un nombre premier). Montrer que la fonction polynôme associée à $X^p - X$ est la fonction nulle.

Nous verrons plus loin qu'elle est bien injective lorsque A est un anneau intègre infini. En particulier, lorsque A est le corps des nombres rationnels, réels et complexes : c'est ce qui «justifie» le point de vue professé auparavant lors de vos études, confondant un peu polynômes et fonctions polynômes (sur $\mathbb{R}$ ou $\mathbb{C}$).

Définition 1.21. *Une* ***racine*** *d'un polynôme $P \in A[X]$ est un élément de A sur lequel la fonction polynôme $\widetilde{P}$ associée s'annule.*

Remarque 1.22. *Lorsque $A = \mathbb{R}$, la fonction polynôme $\widetilde{P'}$ associée au polynôme dérivé P' de P est la dérivée $\widetilde{P}'$ de la fonction polynôme $\widetilde{P}$. C'est l'origine de la terminologie. Mais ceci n'a plus de sens lorsque A est un anneau quelconque : par exemple, lorsqu'il s'agit de $\mathbb{Z}/n\mathbb{Z}$, la fonction polynôme est une fonction définie sur un ensemble fini, et çà n'a pas de sens de dériver une telle fonction (même si $\mathbb{Z}/n\mathbb{Z}$ est un corps, ie. si n est premier). Que signifie qu'une suite de points dans $\mathbb{Z}/n\mathbb{Z}$ tend vers 0 ?*

2. Division, idéaux, éléments irréductibles dans $A[X]$

Comme dans tout anneau :

Définition 2.1. *Soient P, Q deux éléments de $A[X]$. On dit que Q* ***divise*** *P s'il existe un élément D de $A[X]$ tel que $P = D.Q$.*

2.1. Division euclidienne

Théorème - Définition 2.2. *Soit A un anneau commutatif, et P, D deux éléments de $A[X]$ tel que* ***le coefficient de D de plus haut degré soit inversible dans A.*** *Alors, il existe un et un seul couple (Q, R) de polynômes de $A[X]$ tels que :*

$$P = D.Q + R \text{ et } \deg R < \deg D$$

Q est appelé quotient et R est appelé reste de la division euclidienne de P par D.

Notons bien que ce théorème est valable dans un anneau (commutatif) quelconque, même pas intègre ! Comme il s'agit de «division», on pourrait croire que lors de la preuve on soit amené à diviser un élément de A par un autre élément, mais justement, le seul élément par lequel on doit diviser est le coefficient dominant de D, qui est supposé inversible.

Évidemment, lorsque A est un corps, la condition $D \neq 0$ suffit pour pouvoir appliquer le théorème.

Plutôt que refaire la preuve - que vous avez déjà du voir dans le cas réel et/ou complexe - revoyons comment la division s'effectue sur un exemple, qu'on va prendre dans $\mathbb{Z}/4\mathbb{Z}$ (anneau fini pas intègre !).

Exemple 2.3. *Le reste de la division euclidienne (dans $\mathbb{Z}/4\mathbb{Z}$) de $2X^5 + 3X^2 + 2$ par $3X^2 + 1$ est $2X + 1$; le quotient est $2X^3 + 2X + 1$.*

Exercice 4. Quel est le résultat de la division euclidienne dans $\mathbb{Z}/4\mathbb{Z}$ de $2X^5 + 3X^2 + 2$ par $2X^2 + 1$? Que se passe-t'il ?

Une méthode pour calculer le reste de la division euclidienne : Soit P, $Q \neq 0$ deux polynômes dans $K[X]$. Le reste de la division euclidienne de P par Q est l'unique polynôme de degré $< \deg Q$ qui est congru à P modulo Q, ie. dont la projection dans l'anneau $K[X]/(Q)$ coincide avec la projection de P dans le même anneau.

Ceci est pratique dans certaines situations, notamment lorsque P est une puissance n-ième d'un polynôme P_0 dont on connait déjà le reste R_0 modulo Q : il suffit de calculer la puissance n-ième de du projeté $\overline{R}_0$ de R_0 dans $K[X]/(Q)$. Ceci est avantageux lorsque n est très grand et $\deg P$ très petit.

Exercice 5. Calculer le reste de la division euclidienne dans $\mathbb{Q}[X]$ de X^{10000} par $X^4 - 1$.

2.2. Caractérisation des racines par division euclidienne. Anneaux intègres infinis

Proposition 2.4. *Soit A un anneau (commutatif) quelconque, P un élément de $A[X]$, et a un élément de A. Alors, le reste de la division euclidienne de P par $X - a$ est $\widetilde{P}(a)$.*

Démonstration. Le reste de cette division euclidienne doit être de degré $< \deg(X - a) = 1$, donc de degré nul : c'est un élément b de A. Donc :

$$P = (X - a).D + b$$

La fonction polynôme associée à P est donc :

$$\widetilde{P} = \widetilde{(X - a)}.\widetilde{D} + \tilde{b}$$

La valeur qu'elle prend en a est donc $\widetilde{P}(a) = 0.\widetilde{D}(a) + b = b$. □

Corollaire 2.5. *Les assertions suivantes sont équivalentes :*

(1) a est racine de P,

(2) $X - a$ divise P.

Corollaire 2.6. *Supposons que l'anneau A est intègre. Alors, tout polynôme non-nul de $A[X]$ de degré n admet au plus n racines.*

Démonstration. On va le montrer par récurrence sur n.

- **Le cas $n = 0$:** Un polynôme non nul de degré 0 est toujours de la forme a avec $a \in A \setminus \{0\}$. Il admet 0 racine(s).
- **Hérédité :** On suppose le corollaire démontré pour les polynômes de degré $\leq n$. Soit P un polynôme de degré $n+1$. Si P n'a pas de racines, il n'y a rien à démontrer (car $0 \leq n+1$!). Sinon, soit a une racine de P. D'après le corollaire **??**, il existe un polynôme D de $A[X]$ tel que $P = D.(X - a)$. Si b est une racine de P, on doit avoir $0 = \widetilde{D}(b).(b - a)$. Comme A est intègre, ceci signifie que b est soit égal à a, soit une racine de D. Or, d'après la Proposition **??** (dans le cas intègre) le degré de D est n, il n'admet donc, par hypothèse de récurrence, qu'au plus n racines. Donc P n'a qu'au plus $n + 1$ racines. cqfd.

□

Corollaire 2.7. *Soit A un anneau intègre infini. L'application qui à un polynôme de $A[X]$ associe sa fonction polynômiale est injective.*

Démonstration. On sait que cette application est un morphisme d'anneaux ; il s'agit donc de montrer que son noyau est réduit à $\{0\}$. Or, dire qu'un polynôme est dans le noyau, c'est dire que la fonction polynôme associée s'annule sur A tout entier, ie. que tous les éléments de A sont racines de P. Comme A est infini, ceci n'est possible d'après le Corollaire **??** que si le polynôme est nul. □

2.3. Idéaux de $K[X]$ Rappelons qu'un idéal I d'un anneau, par exemple $A[X]$, est un sous-groupe additif de l'anneau, qui est invariant par multiplication par les éléments de l'anneau.

Pour tout élément P de l'anneau, le sous-ensemble formé par les multiples de P (ie. les polynômes dont P est un diviseur...) est un idéal, qu'on note (P).

Désormais, dans ce texte, on ne considère que le cas où A est un corps K.

Théorème 2.8. *Soit K un corps. L'anneau $K[X]$ est principal. Plus précisément, pour tout idéal non-nul I de $K[X]$, il existe un unique polynôme unitaire P tel que I soit l'idéal (P) engendré par P.*

Démonstration. Si $I = \{0\}$, l'idéal I est engendré par le polynôme nul.

Sinon, soit P un élément de I dont le degré soit minimal parmi l'ensemble des degrés pris par les éléments non-nuls de I. Tout élément B de I est de la forme $B = P.Q + R$ où $\deg R < \deg P$. Or, $R = B - P.D$ appartient à I ; comme P est de degré minimal, ceci n'est possible que si R est nul. Donc P divise B : $I = (P)$. Nous avons déjà montré que $K[X]$ est principal.

Écrivons P sous la forme $P = \sum_{i=0}^{n} a_n X^n$ où pour une fois $n = \deg P$, ie. $a_n \neq 0$. Alors $P = a_n(P_0)$ où P_0 est unitaire, et il est évident que les multiples de P sont exactement les multiples de P_0 : quitte à le remplacer par P_0, on peut donc supposer P unitaire.

Reste à montrer l'unicité : soit Q un autre polynôme unitaire tel que $(P) = (Q)$. Alors P et Q se divisent l'un l'autre : il existe deux polynômes B, C tels que $Q = B.P$ et $P = C.Q$. Alors $P = C.Q = C.B.P$, donc $(1 - BC).P = 0$. Comme P est non-nul et que K est intègre, on a $BC = 1$. D'après le Corollaire **??**, B et C sont des éléments inversibles de K, c'est-à-dire des éléments non-nuls de K. Or, le seul élément non-nul B de K pour lequel $B.P$ soit unitaire est l'élément 1. D'où $P = Q$. □

Exercice 6. Pourquoi cette preuve ne montre-t'elle pas que $A[X]$ est principal pour tout anneau intègre A ?

2.4. Plus grand commun diviseur Comme dans tout anneau principal, et le fait que les inversibles de $K[X]$ sont les éléments non-nuls de K :

Théorème 2.9. *Pour toute famille P_1, ... , P_k de polynômes de $K[X]$, il existe un polynôme qui divise tous les P_i et qui est multiple de tout polynôme de $K[X]$ qui divise tous les P_i. Ce polynôme est unique au produit près par un élément de $K \setminus \{0\}$ près, et est appelé le **plus grand commun diviseur des** P_i, noté $P_1 \wedge ... \wedge P_k$.* □

Rappelons que l'existence et unicité (à inversibles près) s'obtient en observant qu'être un pgcd équivaut à être un générateur de l'idéal $(P_1) + ... + (P_k)$.

Convention : «Le» pgcd n'est donc pas unique ; mais il le devient en adoptant la convention suivante : lorsque $P_1 \wedge ... \wedge P_k$ n'est pas nul, ie. que les P_i ne sont pas tous nuls, on réserve la notation $P_1 \wedge ... \wedge P_k$ à l'unique pgcd **unitaire** des P_i.

Il existe un moyen pratique de calculer le pgcd de deux polynômes : l'*algorithme d'Euclide,* le même que celui utilisé dans l'anneau $\mathbb{Z}$. Il est fondé sur l'observation suivante : **le pgcd de deux polynômes A et B avec $\deg A \geq \deg B$ est aussi le pgcd entre B et le reste de la division euclidienne de A par B.** Ainsi, de proche en proche, on abaisse le degré des polynômes, jusqu'à aboutir à la situation où un des polynômes divise l'autre, ce qui signifie qu'il est pgcd des deux, et donc des deux polynômes A et B initiaux.

Définition 2.10. *Les polynômes P_1, ... , P_k sont premiers entre eux si leur pgcd est* 1.

Ainsi, on peut aussi observer qu'**un polynôme Δ est le pgcd de P_1, ... , P_k si et seulement si il divise tous les P_i et que les polynômes $\frac{P_i}{\Delta}$ sont premiers entre eux.**

Que les P_1, ... , P_k soient premiers entre eux équivaut à ce que leurs seuls diviseurs communs soient les éléments non-nuls de K. D'après la caractérisation du pgcd en terme d'idéaux engendrés :

Théorème 2.11 (Théorème de Bézout)**.** *Les polynômes P_1, ... , P_k sont premiers entre eux si et seulement si il existe k polynômes A_1, ... , A_k tels que :*

$$\sum_{i=1}^{k} A_i P_i = 1$$

□

Théorème 2.12 (Théorème de Gauss)**.** *Si un polynôme P de $K[X]$ divise le produit $B.C$ de deux polynômes de $K[X]$ et qu'il est premier avec B, alors P divise C.* □

2.5. Plus petit commun multiple Comme dans tout anneau principal :

Théorème 2.13. *Pour toute famille P_1, ... , P_k de polynômes de $K[X]$, il existe un polynôme qui est multiple de tous les P_i et qui divise tout polynôme de $K[X]$ qui est multiple de tous les P_i. Ce polynôme est unique au produit près par un élément de $K \setminus \{0\}$ près, et est appelé le **plus petit commun multiple des** P_i, noté $P_1 \vee ... \vee P_k$.* □

En convenant de définir $P_1 \vee ... \vee P_k$ comme étant unitaire (s'il est non-nul, ie. qu'aucun des P_i n'est nul), il est alors unique.

Rappelons qu'on peut aussi définir $P_1 \vee ... \vee P_k$ comme étant le générateur (unitaire) de l'idéal $(P_1) \cap ... \cap (P_k)$.

Théorème 2.14. *Soient P, Q deux polynômes non-nuls de $K[X]$. Alors, à un coefficient multiplicatif près :*

$$PQ = (P \wedge Q)(P \vee Q)$$

□

2.6. Polynômes irréductibles, décomposition en facteurs irréductibles Comme dans tout anneau principal, et comme ici les polynômes inversibles sont les éléments de $K \setminus \{0\}$:

Définition 2.15. *Un polynôme P de $K[X]$ est **irréductible** si ses seuls diviseurs dans $K[X]$ sont les éléments de $K \setminus \{0\}$ et les produits de lui-même par un élément de $K \setminus \{0\}$.*

Il résulte du Théorème de Gauss que cette notion coïncide avec celle de **polynôme premier**, ie. de polynôme premier avec tous les polynômes non-nuls. En particulier, un polynôme irréductible divise un produit de polynômes si et seulement si il divise un des polynômes du produit.

Notons $\mathcal{P}$ l'ensemble des polynômes unitaires irréductibles (ou premiers) de $K[X]$.

Théorème 2.16. *Soit B un polynôme de $K[X]$. Il existe un unique élément a de K et une unique application presque nulle $\nu_B : \mathcal{P} \to \mathbb{N}$ tels que :*

$$B = a. \prod_{P \in \mathcal{P}} P^{\nu_B(P)}$$

*On appelle cette égalité **décomposition du polynôme B en facteurs irréductibles (ou premiers).***