Algèbre 3
Chapitre 9
Arithmétique des Polynômes

Licence 2 MAE 2020-2021

Université de Paris - Paris Descartes

Marc Briant

(Fortement inspiré des cours de MM. G. Roussel et R. Lounès)

Table des matières

Avant-propos : En construisant l'ensemble des polynômes sur un corps commutatif, il est apparu que la division jouait un rôle important. Dans $\mathbb{Z}$ grâce à la division euclidienne, tous les nombres s'écrivent avec des "briques élémentaires" : les nombres premiers. Essayons alors de voir si de telles écritures existent pour les polynômes.

Dans tout ce cours, $(\mathbb{K}, +, .)$ désigne un corps commutatif.

1 Divisibilité dans $\mathbb{K}[X]$

1.1 Division euclidienne

Nous rappelons la définition de divisibilité dans $\mathbb{K}[X]$.

Définition 1.1. Soient P et Q deux polynômes de $\mathbb{K}[X]$. Nous disons que Q **divise** P ou Q **est un diviseur de** P ou P **est un multiple de** Q dans $\mathbb{K}[X]$ si et seulement si

$$\exists R \in \mathbb{K}[X], \quad P = QR.$$

Nous le notons alors $Q|P$.

Exemple : **1) Le polynôme nul.** Le polynôme $0_{\mathbb{K}[X]}$ est divisible par tous les polynômes de $\mathbb{K}[X]$.

2) $(X-1)$ et $X+2$ divisent $-2+X+X^2$ dans $\mathbb{R}[X]$.

3) Dépendance du corps $\mathbb{K}$. Dans la définition ci-dessus la mention du corps $\mathbb{K}$ est importante puisque $(X+i)|(X-1)(X^2+1)$ dans $\mathbb{C}[X]$ mais pas dans $\mathbb{R}[X]$ alors que $(X^2+1)|(X-1)(X^2+1)$ dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Remarque 1.2

Remarquons que pour tout $\alpha \neq 0_{\mathbb{K}}$, $\alpha P|P$. En réalité dans $\mathbb{K}[X]$ nous avons que $P|Q$ et $Q|P$ si et seulement si $Q = \alpha P$ avec $\alpha \neq 0_E$. Nous dirons alors que P et Q sont **associés**.

Théorème 1.3 (*Division euclidienne*)

Soient A et B dans $\mathbb{K}[X]$ avec $B \neq 0$. Alors

$$\exists!(Q,R) \in \mathbb{K}[X]^2, \quad \begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$$

Remarque 1.4 (*Hors Programme*)

Lorsque l'on a une division euclidienne alors il est très facile de trouver les sous-ensembles stables par soustraction et multiplication externe (on les appelle des **idéaux**) : ce sont les $D\mathbb{K}[X]$ - ce que montre le prochain corollaire. On dit alors que l'anneau des polynômes est **principal** (de la même manière les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$).

Corollaire 1.5

Soit $F \subset \mathbb{K}[X]$ un idéal de $(\mathbb{K}[X], +, \cdot)$; c'est-à-dire que $0 \in F$ et

(i) $\forall (P,Q) \in F^2, \quad P - Q \in F$

(ii) $\forall P \in F, \forall Q \in \mathbb{K}[X], \quad PQ \in F$.

Il existe $D \in \mathbb{K}[X]$ tel que $F = D\mathbb{K}[X]$. De plus s'il existe $D' \in \mathbb{K}[X]$ tel que $F = D'\mathbb{K}[X]$ alors D et D' sont associés.

1.2 PGCD et algorithme d'Euclide

Comme toujours lorsque l'on a de la division nous pouvons définir un PGCD . Pour éviter les polynômes associés nous demanderons que ces derniers soient unitaires.

Définition 1.6. Soient A et B deux polynômes de $\mathbb{K}[X]$. On appelle **Plus Grand Commun Diviseur (PGCD) de** A **et** B un polynôme unitaire $D \in \mathbb{K}[X]$ tel que

(i) $D|A$ et $D|B$,

(ii) $\forall P \in \mathbb{K}[X]$, $(P|A$ et $P|B) \Rightarrow P|D$.

Exemple : Soit P un polynôme de $\mathbb{K}[X]$ de coefficient dominant $a \neq 0$. Alors $pgcd(P,0) = \frac{1}{a}P$.

Bien entendu, la définition n'implique pas qu'un tel PGCD existe, et si c'est le cas qu'il est unique ! Mais il se trouve que dans $\mathbb{K}[X]$ c'est le cas.

Théorème 1.7 (*Existence du PGCD*)

Soient A et B dans $\mathbb{K}[X]$ tels que A ou B soit non nul. Alors

$$\exists! D \in \mathbb{K}[X] \text{ unitaire}, \quad A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X].$$

D est alors le PGCD de A et B, noté $D = pgcd(A,B)$.

Définition 1.8. Nous dirons que deux polynômes que $\mathbb{K}[X]$ sont **premiers entre eux** si et seulement si leur PGCD vaut $1_{\mathbb{K}[X]}$.

Remarque 1.9

Puisque dans $\mathbb{K}[X]$ les seuls polynômes inversibles sont les polynômes constants non nuls il vient que deux polynômes sont premiers entre eux si et seulement si leurs seuls diviseurs communs dans $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Corollaire 1.10 (*Théorème de Bezout*)

Soient A et B dans $\mathbb{K}[X]$ tels que A ou B soit non nul. Alors

$$\exists (U,V) \in \mathbb{K}[X]^2, \quad pgcd(A,B) = AU + BV.$$

De plus, A et B sont premiers entre eux si et seulement si

$$\exists (U,V) \in \mathbb{K}[X]^2, \quad 1_{\mathbb{K}[X]} = AU + BV.$$

Corollaire 1.11 (*Théorème de Gauss*)

Soient A, B et C dans $\mathbb{K}[X]$. Alors si $(B|A$ et $C|A)$ et que $pgcd(B,C)=1$ alors $BC|A$.

Remarque 1.12 (*Algorithme d'Euclide*)

Remarquons de suite que si $A = BC + D$ alors $pgcd(A,B) = pgcd(B,D)$. Ceci est l'essence de l'algorithme d'Euclide pour calculer un pgcd. En effet faisons des divisions euclidiennes successives :

$$\begin{aligned} A &= BQ_1 + R_1 \quad \text{avec} \quad \deg(R_1) < \deg(B) \\ B &= R_1Q_2 + R_2 \quad \text{avec} \quad \deg(R_2) < \deg(R_1) \\ R_1 &= R_2Q_3 + R_3 \quad \text{avec} \quad \deg(R_3) < \deg(R_1) \\ &\vdots \\ R_{k-1} &= R_kQ_{k+1} + R_{k+1} \quad \text{avec} \deg(R_{k+1}) < \deg(R_k). \end{aligned}$$

Comme le degré est un entier positif, et que $\deg(R_{k+1}) < \deg(R_k)$ le processus s'arrête forcément à un certain rang $N+1$: $R_N \neq 0$ et $R_{N+1} = 0$. Il vient alors

$$\begin{aligned} pgcd(A,B) &= pgcd(B,R_1) = pgcd(R_1,R_2) = \dots \\ &= pgcd(R_N,0) = \frac{1}{\text{coef dominant}(R_N)} R_N. \end{aligned}$$

2 Décomposition en produit d'irréductibles

2.1 Les polynômes irréductibles

Les "briques élémentaires" de $\mathbb{N}$ sont les nombres premiers p positifs, tandis que celles de $\mathbb{Z}$ sont les $\pm p$. Ce sont donc des nombres divisibles uniquement par eux-même (pour $\mathbb{N}$) ou uniquement par eux-même ou leur opposé (dans $\mathbb{Z}$). Élargissons donc cette définition dans $\mathbb{K}[X]$: dans $\mathbb{K}[X]$ les associés αP de P et les polynômes constants non nuls divisent tous P.

Définition 2.1. Un polynôme P de $\mathbb{K}[X]$ est un **polynôme irréductible de** $\mathbb{K}[X]$ si et seulement si P n'est pas constant et que les seuls diviseurs de P dans $\mathbb{K}[X]$ sont les polynômes constants non nuls et ses associés.

Exemple : 1) Les polynômes de degré 1 sont irréductibles dans $\mathbb{K}[X]$.

2) Si $P \in \mathbb{K}[X]$ est irréductible alors tous ses associés (αP avec $\alpha \neq 0$) le sont également.

3) Irréductibilité et division. Soit $P \in \mathbb{K}[X]$. S'il existe $Q \in \mathbb{K}[X]$ tel que $Q|P$ et $0 < \deg(Q) < \deg(P)$ alors P n'est pas irréductible dans $\mathbb{K}[X]$.

4) Influence du corps $\mathbb{K}$. Le polynôme $X^2 + 121$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$. De même, $X^2 - 3$ est irréductible sur $\mathbb{Q}[X]$ mais pas sur $\mathbb{R}[X]$.

2.2 Écriture en polynômes irréductibles

Proposition 2.2

Soit P un polynôme irréductible de $\mathbb{K}[X]$

1. $\forall A \in \mathbb{K}[X], \quad pgcd(P,A) = 1_{\mathbb{K}[X]} \Leftrightarrow P \nmid A$.
2. Pour tout $A_1,..,A_n$ de $\mathbb{K}[X]$, si P divise $\prod_{1\leqslant i\leqslant n} A_i$ alors P divise l'un des A_i.

Théorème 2.3

Pour tout polynôme A non constant de $\mathbb{K}[X]$ il existe r polynômes distincts P_1,..,P_r irréductibles et unitaires dans $\mathbb{K}[X]$, r entiers non nuls α_1,..,α_r et un scalaire $\lambda \in \mathbb{K}$ tels que

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_r^{\alpha_r}.$$

De plus cette écriture est unique à l'ordre près des facteurs - c'est-à-dire que si A s'écrit comme un produit d'irréductibles unitaires distincts $A = \lambda' Q_1^{\beta_1} \cdot\cdot Q_s^{\beta_s}$ alors $r = s$, $\lambda = \lambda'$ et pour tout i il existe j tel que $Q_i = P_j$ et $\alpha_i = \beta_j$.

Remarque 2.4

Notons que cette histoire d'unicité à l'ordre près des facteurs prend place aussi dans $\mathbb{N}$ et la décomposition en nombres premiers mais c'est moins lourd à écrire puisque dans $\mathbb{N}$ il suffit de demander que $p_1 < p_2 < .. < p_r$ pour avoir unicité. Ordre que nous n'avons pas dans $\mathbb{K}[X]$...

2.3 Les cas spécifiques de $\mathbb{R}$ et $\mathbb{C}$

Nous rappelons le théorème vu au chapitre précédent.

Théorème 2.5 (*Théorème de d'Alembert-Gauss*)

Tout polynôme de $\mathbb{C}[X]$ de degré supérieur ou égal à 1 admet une racine dans $\mathbb{C}$.

Ceci nous permet de connaître tous les polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Théorème 2.6

1. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
2. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant négatif.

Nous pouvons donc écrire les polynômes de $\mathbb{C}[X]$ comme des produits de polynômes de degré 1 et les polynômes de $\mathbb{R}[X]$ comme le produit de polynômes de degré 1 et de degré 2 à discriminant négatif (n'ayant donc pas de racine réelle).