Polynômes

Dans tout ce chapitre, $\mathbb{K}$ désigne les corps $\mathbb{R}$ ou $\mathbb{C}$.

1 Polynômes à une indéterminée à coefficients dans $\mathbb{K}$

1.1 Définition

Définition 1.1 Polynôme

On appelle *polynôme à une indéterminée à coefficients dans* $\mathbb{K}$ toute suite *presque nulle* (i.e. nulle à partir d'un certain rang) d'éléments de $\mathbb{K}$.
Si on choisit de noter X l'indéterminée, une telle suite (a_n) nulle à partir du rang $p+1$ se note alors $a_0+a_1X+\cdots+a_pX^p$ ou encore $\sum_{n=0}^{+\infty} a_nX^n$, cette somme étant en fait finie.
L'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ se note alors $\mathbb{K}[X]$.

Attention ! Contrairement à ce qui se passait auparavant, on ne confondra pas *polynômes* et fonctions polynomiales.

Remarque. L'ensemble des suites presque nulles de $\mathbb{K}^{\mathbb{N}}$ se note $\mathbb{K}^{(\mathbb{N})}$. On peut donc identifier $\mathbb{K}[X]$ et $\mathbb{K}^{(\mathbb{N})}$. ■

Définition 1.2

- On appelle *monôme* tout polynôme du type λX^k avec $\lambda \in \mathbb{K}$.
- On appelle *polynôme constant* tout polynôme du type $\lambda X^0 = \lambda$ avec $\lambda \in \mathbb{K}$.
- On appelle *polynôme nul* le polynôme correspondant à la suite nulle.
- On appelle *coefficient dominant* d'un polynôme le coefficient de son monôme de plus haut degré.
- On appelle *polynôme unitaire* un polynôme dont le coefficient dominant est égal à 1.

Remarque. Si P est un polynôme non nul de coefficient dominant λ, alors $\frac{P}{\lambda}$ est un polynôme unitaire : on dit que c'est le polynôme *normalisé* de P. ■

Proposition 1.1

Deux polynômes sont égaux *si et seulement si* leurs coefficients sont égaux.

Remarque. En particulier, un polynôme est nul *si et seulement si* ses coefficients sont nuls. ■

Attention ! L'indéterminée X n'est pas un élément de $\mathbb{K}$. En particulier, résoudre des équations polynomiales de la manière suivante n'a aucun sens.

$$X^2 - 1 = 0 \iff (X = 1 \text{ ou } X = -1)$$

En effet, $X^2 - 1 = 0$ signifie que $X^2 - 1$ est le polynôme nul i.e. celui dont tous les coefficients sont nuls, ce qui est manifestement faux. Les égalités $X = 1$ et $X = -1$ n'ont pas plus de sens.
Quant on voudra résoudre une équation polynomiale, on prendra garde d'introduire un scalaire. Par exemple, si $z \in \mathbb{R}$, ce qui suit à un sens.

$$z^2 - 1 = 0 \iff (z = 1 \text{ ou } z = -1)$$

Définition 1.3 Opérations sur les polynômes

Soient $P = \sum_{n=0}^{+\infty} a_n X^n$ et $Q = \sum_{n=0}^{+\infty} b_n X^n$ deux polynômes de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

Addition On définit le polynôme $P + Q$ par $\sum_{n=0}^{+\infty} (a_n + b_n) X^n$.

Multplication On définit le polynôme $P \times Q$ par $\sum_{n=0}^{+\infty} c_n X^n$ avec $c_n = \sum_{k+l=n} a_k b_l$.

Multiplication par un scalaire On définit le polynôme $\lambda.P$ par $\sum_{n=0}^{+\infty} \lambda a_n X^n$.

Composition de polynômes On définit le polynôme $P \circ Q = P(Q)$ par $\sum_{n=0}^{+\infty} a_n Q^n$.

Remarque. Dans la définition du produit, on vérifie que la suite (c_n) est presque nulle. De plus, cette définition du produit est telle que $X^n \times X^p = X^{n+p}$ pour tout $(n, p) \in \mathbb{N}^2$. ■
Remarque. Dans le cas particulier où $Q = X$, le polynôme $P \circ Q$ vaut $P(X)$. Le polynôme P peut donc aussi bien être noté P ou $P(X)$. ■

Exemple 1.1

La composition consiste simplement à remplacer l'indéterminée X par un polynôme.
Par exemple, si $P = X^2 + X + 1$, alors $P(X - 1) = (X - 1)^2 + (X - 1) + 1$, $P(X^2) = X^4 + X^2 + 1$ ou encore $P(X^3 - 1) = (X^3 - 1)^2 + (X^3 - 1) + 1$.
Si $(P, Q) \in \mathbb{K}[X]^2$ vérifie $(X^2 + 1)P = XQ$, alors $(X^4 + 1)P(X^2) = X^2 Q(X^2)$, en substituant X^2 à X.

Définition 1.4

- Un polynôme P est dit *pair* si $P(-X) = P(X)$.
- Un polynôme P est dit *impair* si $P(-X) = -P(X)$.

Exercice 1.1

Soit $P = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{K}[X]$.

1. Montrer que P est pair *si et seulement si* $a_{2n+1} = 0$ pour tout $n \in \mathbb{N}$.
2. Montrer que P est impair *si et seulement si* $a_{2,n} = 0$ pour tout $n \in \mathbb{N}$.

Proposition 1.2 Structures de $\mathbb{K}[X]$

- $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.
- $(\mathbb{K}[X], +, .)$ est un $\mathbb{K}$-espace vectoriel.

Remarque. $(\mathbb{K}[X], +, ., \times)$ est en fait une $\mathbb{K}$-algèbre commutative. ■
Remarque. Le fait que $\mathbb{K}[X]$ soit une $\mathbb{K}$-algèbre commutative, combiné au fait que $X^n \times X^p = X^{n+p}$ pour tout $(n, p) \in \mathbb{N}^2$, nous dit qu'on peut calculer avec les polynômes comme on en avait l'habitude. ■

Remarque. $(\mathbb{K}[X], \circ)$ est un monoïde non commutatif, c'est-à-dire que la loi $\circ$ est une loi interne associative mais non commutative sur $\mathbb{K}[X]$, d'élément neutre le polynôme X. ■

Définition 1.5 Base canonique de $\mathbb{K}[X]$

La famille $(X^n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$ appelée la *base canonique* de $\mathbb{K}[X]$.

Proposition 1.3

Soient $(P, Q, R) \in \mathbb{K}[X]^3$ et $(\lambda, \mu) \in \mathbb{K}^2$. Alors

$$(\lambda P + \mu Q) \circ R = \lambda P \circ R + \mu Q \circ R \qquad (PQ) \circ R = (P \circ R)(Q \circ R)$$

Attention ! En général, $R \circ (\lambda P + \mu Q) \neq \lambda R \circ P + \mu R \circ Q$ et $R \circ (PQ) \neq (R \circ P)(R \circ Q)$.

1.2 Degré d'un polynôme

Définition 1.6 Degré d'un polynôme

Soit $P = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{K}[X]$. Le degré de P, noté $\deg P$, est défini par :

$$\deg P = \begin{cases} \max\{n \in \mathbb{N} \mid a_n \neq 0\} \text{ si } P \neq 0 \\ -\infty \text{ si } P = 0 \end{cases}$$

Proposition 1.4 Degré et opérations

Soient $(P, Q) \in \mathbb{K}[X]^2$ et $(\lambda, \mu) \in \mathbb{K}^2$.

(i) $\deg(\lambda P + \mu Q) \leqslant \max(\deg P, \deg Q)$.

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

(iii) $\deg P \circ Q = \deg P \times \deg Q$ si $Q \neq 0$.

Remarque. On adopte la convention $n + (-\infty) = (-\infty) + n = -\infty$ pour tout $n \in \mathbb{N} \cup \{-\infty\}$. ■
Remarque. Si P et Q sont des polynômes de degrés distincts, $\deg(P + Q) = \max(\deg P, \deg Q)$. ■

Corollaire 1.1 Intégrité de $\mathbb{K}[X]$

L'anneau $\mathbb{K}[X]$ est *intègre*.

Corollaire 1.2 Éléments inversibles de $\mathbb{K}[X]$

Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0.

Définition 1.7 Polynômes de degré inférieur ou égal à n

Soit $n \in \mathbb{N}$. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.

Proposition 1.5 Structure de $\mathbb{K}_n[X]$

Soit $n \in \mathbb{N}$. $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$. La famille $(X^k)_{0 \leqslant k \leqslant n}$ est une base de $\mathbb{K}_n[X]$ appelée la *base canonique* de $\mathbb{K}_n[X]$.

Attention ! $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$.

Définition 1.8 Famille finie de polynômes à degrés échelonnés

Soit $(P_0, P_1, \dots, P_n)$ une famille de polynômes de $\mathbb{K}[X]$. On dit que la famille $(P_0, P_1, \dots, P_n)$ est à *degrés échelonnés* si :

$$\forall i \in [\![0, n-1]\!],\ \deg P_i < \deg P_{i+1}$$

Définition 1.9 Famille dénombrable de polynômes à degrés échelonnés

Soit $(P_n)_{n\in\mathbb{N}}$ une famille de polynômes de $\mathbb{K}[X]$. On dit que la famille $(P_n)_{n\in\mathbb{N}}$ est à *degrés échelonnés* si la suite $(\deg P_n)$ est strictement croissante.

Proposition 1.6

Une famille de polynômes à degrés échelonnés est libre *si et seulement si* elle ne contient pas le polynôme nul.

Remarque. Une famille $(P_0, \dots, P_n)$ de $\mathbb{K}[X]$ telle que $\deg P_i = i$ pour tout $i \in [\![0, n]\!]$ est une base de $\mathbb{K}_n[X]$.
Une famille $(P_n)_{n\in\mathbb{N}}$ de $\mathbb{K}[X]$ telle que $\deg P_n = n$ pour tout $i \in \mathbb{N}$ est une base de $\mathbb{K}[X]$. ■

Exercice 1.2 **Valuation d'un polynôme**

Soit $P = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{K}[X]$. La valuation de P, noté $\operatorname{val} P$, est définie par :

$$\operatorname{val} P = \begin{cases} \min\{n \in \mathbb{N} \mid a_n \neq 0\} \text{ si } P \neq 0 \\ +\infty \text{ si } P = 0 \end{cases}$$

1. Montrer que $\operatorname{val}(P+Q) \geqslant \min(\operatorname{val} P, \operatorname{val} Q)$.
2. Montrer que $\operatorname{val}(PQ) = \operatorname{val} P + \operatorname{val} Q$.

1.3 Fonctions polynomiales et racines

Définition 1.10 Fonction polynomiale

Soit $P = \sum_{n=0}^{+\infty} a_n X^n$. Pour $x \in \mathbb{K}$, on note $P(x) = \sum_{n=0}^{+\infty} a_n x^n$.

L'application $\tilde{P} : \left\{ \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & P(x) \end{array} \right.$ est appelée la *fonction polynomiale* associée au polynôme P.

Attention ! On ne dira *jamais* que l'on prend $X = x$ dans $P(X)$. En effet, x et X ne sont pas des objets du même type, la relation $X = x$ n'a aucun sens. On dira plutôt que l'on *substitue* x à X dans $P(X)$, ou que l'on remplace X par x dans $P(X)$, ou bien encore que l'on évalue P en x.

Remarque. L'application $\left\{\begin{array}{ccc}\mathbb{K}[X] & \longrightarrow & \mathbb{K}^{\mathbb{K}} \\ P & \longmapsto & \tilde{P}\end{array}\right.$ est un morphisme de $\mathbb{K}$-algèbres pour les lois $+, ., \times$ et un morphisme de monoïdes pour la loi $\circ$. ■

Remarque. On verra plus tard qu'on peut justifier d'un point de vue théorique l'identification entre polynôme et fonction polynomiale que vous acceptiez sans broncher jusqu'à maintenant. ■

Remarque. Il faut bien faire la différence entre le fait qu'un polynôme s'annule (son évaluation en un scalaire est nulle) et le fait qu'un polynôme est nul (tous ses coefficients sont nuls).
Par exemple, si $(X-a)P = 0$, alors $P = 0$ par intégrité bien que $X - a$ s'annule en a. Ce qui compte, c'est que $X - a$ n'est pas le polynôme nul. ■

Exercice 1.3

Soit $a \in \mathbb{K}$. Montrer que $\left\{\begin{array}{ccc}\mathbb{K}[X] & \longrightarrow & \mathbb{K} \\ P & \longmapsto & P(a)\end{array}\right.$ est une forme linéaire sur $\mathbb{K}[X]$.

Définition 1.11 Racine

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est une *racine* de P (dans $\mathbb{K}$) si $P(a) = 0$.

Attention ! La précision «dans $\mathbb{K}$» peut avoir de l'importance : le polynôme $X^2 + 1$ admet des racines dans $\mathbb{C}$ mais pas dans $\mathbb{R}$.

Méthode **Montrer qu'un polynôme à coefficients réels admet une racine réelle**

On peut employer des techniques d'analyse pour montrer qu'un polynôme admet une racine réelle.

1. Le théorème des valeurs intermédiaires assure l'existence d'une racine de $P \in \mathbb{R}[X]$ si P change de signe.
2. Le théorème de Rolle montre que P' s'annule si P prend deux fois la même valeur.

Exemple 1.2

Un polynôme à coefficients réels de degré *impair* admet nécessairement une racine réelle d'après le théorème des valeurs intermédiaires.

Proposition 1.7

Soient $P \in \mathbb{K}[X]$ pair ou impair et $a \in \mathbb{K}$. Alors a est une racine de P *si et seulement si* $-a$ est également une racine de P.

1.4 Conjugaison

Définition 1.12 Conjugué d'un polynôme

Soit $P = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{C}[X]$. On appelle *polynôme conjugué* de P le polynôme $\overline{P} = \sum_{n=0}^{+\infty} \overline{a}_n X^n$.

Remarque. En particulier, $P \in \mathbb{R}[X]$ *si et seulement si* $P = \overline{P}$. ■

Proposition 1.8

Soient $P \in \mathbb{C}[X]$ et $a \in \mathbb{C}$. Alors a est une racine de P *si et seulement si* $\overline{a}$ est une racine de $\overline{P}$.
En particulier, si $P \in \mathbb{R}[X]$, les racines complexes non réelles de P sont conjuguées deux à deux.

Proposition 1.9

Soient $(P, Q) \in \mathbb{C}[X]^2$ et $(\lambda, \mu) \in \mathbb{C}^2$. Alors

$$\overline{\lambda P + \mu Q} = \overline{\lambda}\,\overline{P} + \overline{\mu}\,\overline{Q} \qquad \overline{PQ} = \overline{P}\,\overline{Q}$$

En particulier, si $(\lambda, \mu) \in \mathbb{R}^2$, $\overline{\lambda P + \mu Q} = \lambda\overline{P} + \mu\overline{Q}$.

1.5 Dérivation

Définition 1.13 Polynôme dérivé

Soit $P = \sum_{k=0}^{+\infty} a_k X^k$. Le polynôme $P' = \sum_{k=1}^{+\infty} k a_k X^{k-1}$ est appelé le *polynôme dérivé* de P. On définit par récurrence les polynômes dérivés successifs $P^{(n)}$ de P pour $n \in \mathbb{N}$.

Remarque. La dérivation des polynômes «coïncide» avec la dérivation des fonctions.
Si $\mathbb{K} = \mathbb{R}$, $\widetilde{P'} = \left(\tilde{P}\right)'$.
Si $\mathbb{K} = \mathbb{C}$, $\left(\widetilde{P'}\right)_{|\mathbb{R}} = \left(\tilde{P}_{|\mathbb{R}}\right)'$.

En fait, on peut établir des notions de dérivabilité et de dérivée pour les fonctions de $\mathbb{C}$ dans $\mathbb{C}$. On a alors $\widetilde{P'} = \left(\tilde{P}\right)'$, que le corps soit $\mathbb{R}$ ou $\mathbb{C}$. ■

Définition 1.14 Dérivées successives

Soit $P \in \mathbb{K}[X]$. On définit les dérivées successives de P en posant $P^{(0)} = P$ et $P^{(n+1)} = \left(P^{(n)}\right)'$ pour tout $n \in \mathbb{N}$.

Proposition 1.10 Degré de la dérivée

Soit $P \in \mathbb{K}[X]$. Si $n \leqslant \deg P$, $\deg P^{(n)} = \deg P - n$. Sinon $P^{(n)} = 0$.
De manière générale, $\deg P^{(n)} \leqslant \deg P - n$.

Exemple 1.3

Pour $k \leqslant n$, $(X^n)^{(k)} = \frac{n!}{(n-k)!} X^{n-k}$ et pour $k > n$, $(X^n)^{(k)} = 0$.

Proposition 1.11 Linéarité de la dérivation

Soient $(P, Q) \in \mathbb{K}[X]^2$ et $(\lambda, \mu) \in \mathbb{K}^2$. Alors $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.
Pour tout $n \in \mathbb{N}$, $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$.

Remarque. Si on note $D : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ P & \longmapsto & P' \end{array} \right.$, $D \in \mathcal{L}(\mathbb{K}[X])$. D n'est pas injectif puisque $\operatorname{Ker} D = \mathbb{K}_0[X]$.
De manière générale, $\operatorname{Ker} D^n = \mathbb{K}_{n-1}[X]$ pour tout $n \in \mathbb{N}^*$. ■

Proposition 1.12 Dérivée d'un produit

Soit $(P,Q)\in\mathbb{K}[X]^2$.

- $(PQ)'=P'Q+PQ'$.
- Formule de Leibniz : $(PQ)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n-k)}$

Proposition 1.13 Formule de Taylor pour les polynômes

Soient $P\in\mathbb{K}[X]$ et $a\in\mathbb{K}$.

$$P=\sum_{n=0}^{+\infty}\frac{P^{(n)}(a)}{n!}(X-a)^n \qquad P(a+X)=\sum_{n=0}^{+\infty}\frac{P^{(n)}(a)}{n!}X^n$$

Proposition 1.14 Dérivée d'une composée

Soit $(P,Q)\in\mathbb{K}[X]^2$. Alors $(P\circ Q)'=(P'\circ Q)Q'$.

Exemple 1.4

Soit $P\in\mathbb{K}[X]$. Alors $P(-X)'=-P'(-X)$ et $P(X^2)'=2XP'(X^2)$.

2 Arithmétique de $\mathbb{K}[X]$

2.1 Divisibilité dans $\mathbb{K}[X]$

Définition 2.1 Divisibilité dans $\mathbb{K}[X]$

Soit $(P,Q)\in\mathbb{K}[X]^2$. On dit que P divise Q ou que Q est un multiple de P s'il existe $A\in\mathbb{K}[X]$ tel que $Q=AP$. On note $P|Q$.

Proposition 2.1 Propriétés de la divisibilité

Soit $(A,B,C,D)\in\mathbb{K}[X]^4$.

Réflexivité $A|A$.

Transitivité Si $A|B$ et $B|C$ alors $A|C$.

«Pseudo-antisymétrie» Si $A|B$ et $B|A$, alors il existe $\lambda\in\mathbb{K}^*$ tel que $B=\lambda A$. On dit alors que les polynômes A et B sont *associés*.

«Combinaison linéaire» Si $D|A$ et $D|B$, alors $D|AU+BV$ pour tout $(U,V)\in\mathbb{K}[X]^2$.

Produit Si $A|B$ et $C|D$, alors $AC|BD$.
En particulier, si $A|B$ alors $A^n|B^n$ pour tout $n\in\mathbb{N}$.

Multiplication/division par un polynôme Si $D\neq 0$, $A|B\iff AD|BD$.

Remarque. On pourrait introduire la notion de congruence pour les polynômes comme pour les entiers mais ce n'est pas au programme... ■

2.2 Division euclidienne

Proposition 2.2 Division euclidienne

Soit $(A, B) \in \mathbb{K}[X]^2$ avec $B \neq 0$. Alors il *existe un unique* couple d'entiers $(Q, R) \in \mathbb{K}[X]^2$ vérifiant :

$$\text{(i)} \quad A = BQ + R \qquad\qquad \text{(ii)} \quad \deg R < \deg B$$

A s'appelle le *dividende*, B le *diviseur*, Q le *quotient*, et R le *reste*.

Remarque. Soit $(A, B) \in \mathbb{R}[X]^2$. La division euclidienne de A par B est la même dans $\mathbb{R}[X]$ ou dans $\mathbb{C}[X]$. ■

Exemple 2.1

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le reste de la division euclidienne de P par $X - a$ est $P(a)$.

Méthode **Calculer le reste d'une division euclidienne**

Pour calculer le reste de la division euclidienne de A par B, on écrit $A = BQ + R$ avec $R = \sum_{k=0}^{\deg B - 1} a_k X^k$. On évalue ensuite en les racines de B. En effet, si a est une racine de B, alors $P(a) = R(a)$. Ceci nous permet de déterminer les coefficients de R.

Exemple 2.2

Déterminer le reste de la division euclidienne de $X^{10} - X^5$ par $X^2 - 3X + 2$.

Proposition 2.3

Soit $(A, B) \in \mathbb{K}[X]^2$ avec $B \neq 0$. Alors B divise A *si et seulement si* le reste de la division euclidienne de A par B est nul.

Remarque. Soient $(A, B) \in \mathbb{R}[X]^2$. Si B divise A dans $\mathbb{C}[X]$, alors B divise également A dans $\mathbb{R}[X]$. ■

Proposition 2.4 Racine et divisibilité

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est une racine de P *si et seulement si* $X - a$ divise P.

Méthode **Division euclidienne de P par $(X - a)^p$**

La formule de Taylor nous donne directement le quotient est le reste de la division euclidienne de P par $(X - a)^p$. En effet, $P = (X - a)^p Q + R$ avec

$$Q = \sum_{n \geqslant p} \frac{P^{(n)}(a)}{n!}(X - a)^{n-p}$$

$$R = \sum_{n < p} \frac{P^{(n)}(a)}{n!}(X - a)^n$$

Algorithme de la division euclidienne

$$\begin{array}{rrrrrrr|l}
X^3 & + & & & X & + & 1 & X+1 \\
\cline{8-8}
-(X^3 & + & X^2) & & & & & X^2-X+2 \\
\cline{1-3}
 & & -X^2 & + & X & & & \\
 & & -(-X^2 & - & X) & & & \\
\cline{3-5}
 & & & & 2X & + & 1 & \\
 & & & & -(2X & + & 2) & \\
\cline{5-7}
 & & & & & & -1 & \\
\end{array}$$

Exercice 2.1

Soit $B \in \mathbb{K}[X]$ avec $\deg B \geqslant 1$. Montrer que l'application qui à un polynôme P associe le reste de la division euclidienne de P par B est un projecteur de $\mathbb{K}[X]$. Déterminer son noyau et son image.

2.3 PGCD

Définition 2.2 PGCD

Soit $(P, Q) \in \mathbb{K}[X]^2$. On appelle *plus grand commun diviseur (PGCD)* du couple (P, Q) tout polynôme $D \in \mathbb{K}[X]$ vérifiant :

(i) D est multiple commun de P et Q i.e. $D|P$ et $D|Q$;

(ii) tout diviseur commun de P et Q divise D.

Proposition 2.5 Existence et «unicité» du PGCD

Soit $(P, Q) \in \mathbb{K}[X]^2$. Deux PGCD de (P, Q) sont associés.
Il existe un unique PGCD *unitaire* ou nul de (P, Q). On le note $P \wedge Q$.

Remarque. Le PGCD de deux polynômes est nul *si et seulement si* ces deux polynômes sont nuls. ■
Remarque. Soit $P \in \mathbb{K}[X]$ avec $P \neq 0$. $P \wedge 0 = \widehat{P}$ où $\widehat{P}$ est le polynôme normalisé de P. ■

Lemme 2.1

Soit $A = BQ + R$ la division euclidienne de $A \in \mathbb{K}[X]$ par $B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors $A \wedge B = B \wedge R$.

L'algorithme suivant permet de déterminer le PGCD de deux polynômes par une succession de divisions euclidiennes.

Algorithme d'Euclide

On reprend l'idée de l'algorithme d'Euclide vu dans le cadre de l'arithmétique dans $\mathbb{Z}$. On définit donc une suite (R_n) de la manière suivante :

1. On pose $R_0 = A$ et $R_1 = B$.
2. Pour $n \geqslant 1$, R_{n+1} est le reste de la division euclidienne de R_{n-1} par R_n.

$(\deg R_n)$ est une suite strictement décroissante d'éléments de $\mathbb{N} \cup \{-\infty\}$ (à partir du rang 1) : elle est donc égale à $-\infty$ à partir d'un certain rang. La suite (R_n) est donc nulle à partir d'un certain rang. Soit N l'indice du dernier terme non nul de cette suite. Le lemme précédent montre que $\widehat{R_N} = A \wedge B$ où $\widehat{R_N}$ est le polynôme normalisé de R_N.

Exemple 2.3

Déterminons le PGCD de $6X^4+8X^3-7X^2-5X-2$ et $6X^3-4X^2-X-1$.

$$\begin{aligned}6X^4+8X^3-7X^2-5X-2 &= (X+2)\times(6X^3-4X^2-X-1)+2X^2-2X\\ 6X^3-4X^2-X-1 &= (3X+1)\times(2X^2-2X) &&+X-1\\ 2X^2-2X &= 2X\times(X-1) &&+0\end{aligned}$$

On a donc $(6X^4+8X^3-7X^2-5X-2)\wedge(6X^3-4X^2-X-1)=X-1$.

Théorème 2.1 Bézout

Soit $(A,B)\in\mathbb{K}[X]^2$. Il existe $(U,V)\in\mathbb{K}[X]^2$ tels que $AU+BV=A\wedge B$. On appelle (U,V) un couple de *coefficients de Bézout*. Une égalité du type précédent s'appelle une *identité de Bézout*.

Attention ! Ces coefficients ne sont pas uniques. Si (U_0,V_0) est un couple de coefficients de Bezout, tous les couples de la forme (U_0+KB,V_0-KA) avec $K\in\mathbb{K}[X]$ le sont aussi.
La réciproque de ce théorème est fausse.

Algorithme d'Euclide étendu

On reprend à nouveau l'idée de l'algorithme d'Euclide étendu vu dans le cadre de l'arithmétique dans $\mathbb{Z}$. On reprend les notations de l'algorithme d'Euclide. Pour tout $n\geqslant 1$, on a $R_{n+1}=R_n-Q_nR_{n-1}$. Le dernier reste non nul R_N est le PGCD D de A et B. On abrégera combinaison linéaire à coefficients polynomiaux en CLP. On peut ainsi exprimer D comme une CLP de R_{N-1} et R_{N-2}. Puis comme on peut exprimer R_{N-1} comme une CLP de R_{N-2} et R_{N-3}, on peut exprimer D comme une CLP de R_{N-2} et R_{N-3}, etc... Finalement on peut exprimer D comme une CLP de $R_0=A$ et $R_1=B$. Plutôt qu'un long discours, reprenons l'exemple traité pour l'algorithme d'Euclide standard.

Exemple 2.4

Réécrivons les divisions euclidiennes de l'algorithme d'Euclide standard sous une autre forme :

$$\begin{aligned}2X^2-2X &= (6X^4+8X^3-7X^2-5X-2)-(X+2)\times(6X^3-4X^2-X-1)\\ X-1 &= (6X^3-4X^2-X-1) &&-(3X+1)\times(2X^2-2X)\end{aligned}$$

On part ensuite du PGCD (c'est-à-dire $X-1$) et on remonte les lignes de la manière suivante :

$$\begin{aligned}X-1 &= (6X^3-4X^2-X-1)-(3X+1)\times(2X^2-2X)\\ &= (6X^3-4X^2-X-1)-(3X+1)\Big[(6X^4+8X^3-7X^2-5X-2)-(X+2)\times(6X^3-4X^2-X-1)\Big]\\ &= -(3X+1)\times(6X^4+8X^3-7X^2-5X-2)+(3X^2+7X+3)\times(6X^3-4X^2-X-1)\end{aligned}$$

Et voilà notre identité de Bézout.

2.4 Polynômes premiers entre eux

Définition 2.3 Polynômes premiers entre eux

Soit $(P,Q)\in\mathbb{K}[X]^2$. On dit que P et Q sont premiers entre eux si leurs seuls diviseurs communs sont les polynômes constants non nuls i.e. si leur PGCD vaut 1.

Théorème 2.2 Bézout

Soit $(P, Q) \in \mathbb{K}[X]^2$. Alors P et Q sont premiers entre eux *si et seulement si* il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $UP + VQ = 1$.

Remarque. Contrairement au premier théorème de Bézout, on a bien ici une *équivalence.* ■

Théorème 2.3 Gauss

Soit $(A, B, C) \in \mathbb{K}[X]^3$. Si $A|BC$ et $A \wedge B = 1$ alors $A|C$.

Proposition 2.6

Soit $(P_1, \dots, P_r) \in \mathbb{K}[X]^r$ et $Q \in \mathbb{K}[X]$.

1. Si $P_1, \dots, P_r$ sont tous premiers avec Q, alors le produit $P_1 \dots P_r$ est également premier avec Q.
2. Si $P_1, \dots, P_r$ sont premiers entre eux deux à deux et divisent Q, alors le produit $P_1 \dots P_r$ divise également Q.

Lemme 2.2

Soit $(a, b) \in \mathbb{K}^2$ avec $a \neq b$. Alors $(X - a) \wedge (X - b) = 1$.

Théorème 2.4

Un polynôme de degré $n \in \mathbb{N}$ de $\mathbb{K}[X]$ possède au plus n racines dans $\mathbb{K}$.

Méthode **Prouver qu'un polynôme est nul**

Pour prouver qu'un polynôme est nul, il suffit de prouver qu'il possède une infinité de racines.

Exercice 2.2

Soit $P \in \mathbb{K}[X]$ tel que $P(X + 1) = P(X)$. Montrer que P est constant.

Exercice 2.3

Déterminer les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{R}) \subset \mathbb{R}$.

Proposition 2.7

Si le corps $\mathbb{K}$ est infini, l'application qui à un polynôme $P \in \mathbb{K}[X]$ associe la fonction polynomiale $\tilde{P} \in \mathbb{K}^{\mathbb{K}}$ est une application linéaire injective.

Remarque. C'est même un morphisme injectif de $\mathbb{K}$-algèbres. ■
Remarque. Autrement dit, toute fonction polynomiale est associée à un unique polynôme, ce qui justifie la fait que l'on confonde polynôme et fonction polynomiale. Cette identification repose sur le fait que $\mathbb{R}$ et $\mathbb{C}$ sont des corps infinis. Mais tous les corps ne sont pas infinis comme vous le verrez l'année prochaine. ■

Méthode **Identification de coefficients**

Si deux fonctions polynomiales coïncident sur un ensemble infini (typiquement $\mathbb{R}$), leurs coefficients sont égaux.

Remarque. La réciproque est évidemment vraie. ■

Proposition 2.8 Polynôme interpolateur de Lagrange

Soient $(x_0,\dots,x_n)$ et $(y_0,\dots,y_n)$ deux n-uplets de $\mathbb{K}^{n+1}$ où les x_i sont distincts deux à deux. Il existe un unique polynôme de $\mathbb{K}_n[X]$ tel que $P(x_i)=y_i$ pour tout $i\in[\![0,n]\!]$.
Le polynôme en question est $\sum_{i=0}^{n} y_i L_i$ où

$$L_i=\prod_{j\neq i}\frac{X-x_j}{x_i-x_j}$$

Remarque. Il suffit en effet de montrer que l'application $\left\{\begin{array}{ccc}\mathbb{K}_n[X] & \longrightarrow & \mathbb{K}^{n+1}\\ P & \longmapsto & (P(x_0),\dots,P(x_n))\end{array}\right.$ est un isomorphisme. ■

Remarque. Les polynômes $Q\in\mathbb{K}[X]$ tels que $Q(x_i)=y_i$ pour tout $i\in[\![0,n]\!]$ (sans contrainte de degré) sont les polynômes $P+M\prod_{i=0}^{n}(X-x_i)$ avec $M\in\mathbb{K}[X]$. ■

2.5 PPCM

Définition 2.4 PPCM

Soit $(P,Q)\in\mathbb{K}[X]^2$. On appelle *plus petit commun multiple* du couple (P,Q) tout polynôme $M\in\mathbb{K}[X]$ vérifiant :

(i) M est un multiple commun de P et Q i.e. $P|M$ et $Q|M$;

(ii) tout multiple commun de P et Q est multiple de M.

Proposition 2.9 Existence et «unicité» du PPCM

Soit $(P,Q)\in\mathbb{K}[X]^2$. Deux PPCM de P et Q sont associés.
Il existe un unique PPCM *unitaire* ou nul de (P,Q). On le note $P\vee Q$.

Remarque. Le PPCM de deux polynômes est nul *si et seulement si* l'un des deux est nul. ■

Proposition 2.10 Lien entre PGCD et PPCM

Soit $(P,Q)\in\mathbb{K}[X]^2$. Alors $(P\wedge Q)(P\vee Q)$ et PQ sont associés.

3 Racines multiples

3.1 Définition

Définition 3.1 Racines multiples

Soient $P\in\mathbb{K}[X]$ et $a\in\mathbb{K}$. On dit que a est une racine de P d'ordre (de multiplicité) p si p est le plus grand entier k tel que $(X-a)^k$ divise P.
On dit que a est une racine multiple de P si a est une racine d'ordre au moins 2.

Remarque. Si $P \neq 0$, cet entier p existe puisque $\left\{k \in \mathbb{N} \;\middle|\; (X-a)^k | P\right\}$ est une partie non vide (elle contient 0) et majorée (par $\deg P$) de $\mathbb{N}$. ■
Remarque.

- Dire que a est une racine d'ordre p de a signifie que $(X-a)^p | P$ mais que $(X-a)^{p+1} \not| P$.
- Dire que a est une racine d'ordre *au moins* p signifie que $(X-a)^p | P$.
- Une racine de P est une racine d'ordre au moins 1.
- Une racine d'ordre 0 n'est pas une racine de P.

■

Lemme 3.1

Soit $(a,b) \in \mathbb{K}^2$ avec $a \neq b$. Soit $(p,q) \in \mathbb{N}^2$. Alors $(X-a)^p \wedge (X-b)^q = 1$.

Théorème 3.1

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}$. Alors P possède au plus n racines *comptées avec leur multiplicité.*

Exemple 3.1

Le polynôme $(X-1)(X+1)^2(X-2)^3$ possède 3 racines distinctes mais 6 racines comptées avec leur multiplicité.

3.2 Dérivation et ordre de multiplicité

Remarque. Les deux sommes précédentes sont bien entendu finies puisque la suite des dérivées successives de P est nulle à partir d'un certain rang. ■

Proposition 3.1 Caractérisation de la multiplicité d'une racine

Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $r \in \mathbb{N}$. a est une racine de P de multiplicité r *si et seulement si*

$$\forall k \in [\![0, r-1]\!],\ P^{(k)}(a) = 0 \text{ et } P^{(r)}(a) \neq 0$$

Remarque. $P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0$ *si et seulement si* a est racine de P de multiplicité *au moins* égale à r. a est racine multiple de P *si et seulement si* $P(a) = P'(a) = 0$. ■

Méthode **Division euclidienne**

Pour trouver le reste R de la division euclidienne de $P \in \mathbb{K}[X]$ par $(X-a)^r(X-b)^s$, on peut constater que $P - R$ est divisible par $(X-a)^r(X-b)^s$. Autrement dit, a et b sont des racines de $P - R$ d'ordre respectifs au moins r et s. On en déduit les conditions

$$\begin{array}{llll} R(a) = P(a) & R'(a) = P'(a) & \dots & R^{(r-1)}(a) = P^{(r-1)}(a) \\ R(b) = P(b) & R'(b) = P'(b) & \dots & R^{(s-1)}(b) = P^{(s-1)}(b) \end{array}$$

ce qui suffit à déterminer R ($r+s$ conditions pour un polynômes de $\mathbb{K}_{r+s-1}[X]$).

Exercice 3.1 **Calcul d'un reste**

Déterminer de deux manières le reste R dans la division euclidienne d'un polynôme $P \in \mathbb{K}[X]$ par $B = (X-a)^2$ où $a \in \mathbb{K}$.

Proposition 3.2

Soient $P \in \mathbb{K}[X]$ pair ou impair et $a \in \mathbb{K}$. a est une racine de P de multiplicité r *si et seulement si* $-a$ est également une racine de P de multiplicité r.

Remarque. Si P est pair ou impair, a est une racine d'ordre *au moins* r de P *si et seulement si* $-a$ est une racine d'ordre *au moins* r de P. ■

Proposition 3.3

Soient $P \in \mathbb{C}[X]$, $a \in \mathbb{C}$ et $r \in \mathbb{N}$. a est une racine d'ordre r de P *si et seulement si* $\overline{a}$ est une racine d'ordre r de $\overline{P}$.
En particulier, si $P \in \mathbb{R}[X]$, les racines complexes non réelles de P sont conjuguées deux à deux et deux racines complexes non réelles conjuguées sont de même ordre de multiplicité.

Remarque. a est une racine d'ordre *au moins* r de P *si et seulement si* $\overline{a}$ est une racine d'ordre *au moins* r de $\overline{P}$. ■

4 Factorisation

4.1 Polynômes irréductibles

Définition 4.1 Polynômes irréductibles

Soit $P \in \mathbb{K}[X]$. On dit que P est *irréductible* (dans $\mathbb{K}[X]$) si P n'est pas constant et si ses seuls diviseurs sont les polynômes constants et les polynômes associés à P.

Attention ! La précision «dans $\mathbb{K}[X]$» peut avoir de l'importance : le polynôme X^2+1 est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Remarque. Deux polynômes irréductibles distincts sont premiers entre eux. ■

Exemple 4.1

Tout polynôme de degré 1 est irréductible.

Il est important de comprendre que les polynômes irréductibles ont le même rôle dans l'anneau $\mathbb{K}[X]$ que les nombres premiers dans l'anneau $\mathbb{Z}$.

Proposition 4.1 Lemme d'Euclide

Soit $(P, A, B) \in \mathbb{K}[X]^3$ avec P irréductible. Si $P|AB$, alors $P|A$ ou $P|B$.

Remarque. Cette propriété se généralise par récurrence à un produit de plus de deux polynômes. ■

Proposition 4.2

Soit $(A, B) \in \mathbb{K}[X]^2$. A et B sont premiers entre eux *si et seulement si* ils n'admettent aucun diviseur irréductible commun.

Théorème 4.1 Décomposition en facteurs irréductibles dans $\mathbb{K}[X]$

On note $\mathcal{I}$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{K}[X]$.
Soit $P \in \mathbb{K}[X]$ non nul. Il existe un unique $\lambda \in \mathbb{K}^*$ et une unique famille $(\mu_R)_{R\in\mathcal{I}}$ d'entiers naturels presque tous nuls (i.e. nuls sauf un nombre fini d'entre eux) telle que $Q = \lambda \prod_{R\in\mathcal{I}} R^{\mu_R}$.

Comme dans le cas de l'arithmétique dans $\mathbb{Z}$, on peut caractériser la divisibilité, le PGCD et le PPCM à l'aide de cette décomposition en facteurs irréductibles.

Proposition 4.3

Soient $P = \lambda \prod_{R \in \mathcal{I}} R^{\mu_R}$ et $Q = \mu \prod_{R \in \mathcal{I}} R^{\nu_R}$.

(i) $P|Q \iff \forall R \in \mathcal{I}, \mu_R \leqslant \nu_R$.

(ii) $P \wedge Q = \prod_{R \in \mathcal{I}} R^{\min(\mu_R, \nu_R)}$.

(iii) $P \vee Q = \prod_{R \in \mathcal{I}} R^{\max(\mu_R, \nu_R)}$.

4.2 Factorisation dans $\mathbb{C}[X]$

Théorème 4.2 Théorème de d'Alembert-Gauss

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine (dans $\mathbb{C}$).

Proposition 4.4 Irréductibles de $\mathbb{C}[X]$

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

Corollaire 4.1

Tout polynôme non nul de $\mathbb{C}[X]$ admet autant de racines comptées avec multiplicité que son degré.

Corollaire 4.2

Deux polynômes $\mathbb{C}[X]$ sont premiers entre eux *si et seulement si* ils n'ont pas de racine *complexe* commune.

Remarque. C'est a fortiori vrai pour des polynômes de $\mathbb{R}[X]$ à condition de considérer les racines complexes. Par exemple, $(X+1)(X^2+1)$ et $(X+2)(X^2+1)$ n'ont pas de racine réelle commune mais ne sont pas premiers entre eux. ■

Exemple 4.2

Les polynômes X^2+X+1 et X^4-1 sont premiers entre eux.

Corollaire 4.3

Soit $(P, Q) \in \mathbb{C}[X]^2$. Alors P divise Q *si et seulement si* toute racine *complexe* de P est racine de Q avec au moins le même ordre de multiplicité.

Remarque. C'est a fortiori vrai si $(P, Q) \in \mathbb{R}[X]^2$ à condition de considérer les racines complexes. Posons $P = (X+1)(X^2+1)$ et $Q = (X+1)^2(X^4+1)$. Toute racine réelle de P (ici -1) est racine de Q avec au moins le même ordre de multiplicité. Pourtant P ne divise pas Q. ■

Exemple 4.3

Soit $P \in \mathbb{R}[X]$. X^2+X+1 divise P *si et seulement si* $P(j) = 0$.

Proposition 4.5

Pour $n \in \mathbb{N}^*$, la décomposition en facteurs irréductibles de $X^n - 1$ est $X^n - 1 = \prod_{\omega \in \mathbb{U}_n} X - \omega$.

Exercice 4.1

Soit $(m, n) \in (\mathbb{N}^*)^2$. Montrer que $(X^m - 1) \wedge (X^n - 1) = X^{m \wedge n} - 1$.

4.3 Factorisation dans $\mathbb{R}[X]$

Proposition 4.6 Irréductibles de $\mathbb{R}[X]$

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

Méthode **Factorisation dans $\mathbb{R}[X]$**

Pour factoriser un polynôme réel dans $\mathbb{R}[X]$, on le factorise d'abord dans $\mathbb{C}[X]$ puis on regroupe les facteurs comportant des racines complexes non réelles conjuguées deux à deux.

Remarque. Une relation utile à connaître est $X^2 - 2X\cos\theta + 1 = (X - e^{i\theta})(X - e^{-i\theta})$ pour $\theta \in \mathbb{R}$. ■

Exercice 4.2

Donner la décomposition en facteurs irréductibles de $X^4 + 1$ dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Exercice 4.3

Décomposer le polynôme $P = (X+1)^7 - X^7 - 1$ en produit de facteurs irréductibles dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ en sachant que j est une racine multiple de P.

4.4 Lien entre coefficients et racines d'un polynôme

Définition 4.2 Polynôme scindé

Soit $P \in \mathbb{K}[X]$. On dit que P est *scindé* (sur $\mathbb{K}$) s'il peut s'écrire comme un produit de polynômes de degré 1 de $\mathbb{K}[X]$.

Attention ! La précision «sur $\mathbb{K}$» peut avoir de l'importance : $X^2 + 1$ est scindé sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.

Proposition 4.7

Tout polynôme de $\mathbb{C}[X]$ de degré supérieur ou égal à 1 est scindé sur $\mathbb{C}$.

Proposition 4.8

Un polynôme de $\mathbb{K}[X]$ de degré $n \in \mathbb{N}^*$ est scindé sur $\mathbb{K}$ *si et seulement si* il possède exactement n racines dans $\mathbb{K}$ comptées avec multiplicité.

Exemple 4.4

Le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$ et

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega)$$

Définition 4.3 Fonctions symétriques élémentaires

Soit $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$. Pour $k \in [\![1, n]\!]$, on définit la $k^{\text{ème}}$ fonction symétrique élémentaire de $\alpha_1, \dots, \alpha_n$ notée σ_k par

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k}$$

Exemple 4.5

Concrètement σ_k est la somme de tous les produits de k éléments parmi $\alpha_1, \dots, \alpha_n$. Si $n = 3$,

$$\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 \qquad \sigma_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 \qquad \sigma_3 = \alpha_1\alpha_2\alpha_3$$

Proposition 4.9 Relations coefficients/racines

Soient $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré $n \in \mathbb{N}^*$, scindé sur $\mathbb{K}$ et $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$.
On note $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires associées à $\alpha_1, \dots, \alpha_n$.
Alors $\alpha_1, \dots, \alpha_n$ sont les n racines de P (comptées avec multiplicité) *si et seulement si* $\forall k \in [\![1, n]\!]$, $\sigma_k = \frac{(-1)^k a_{n-k}}{a_n}$.

Remarque. σ_1 est la somme des racines et σ_n est le produit des racines. On a alors $\sigma_1 = -\frac{a_{n-1}}{a_n}$ et $\sigma_n = (-1)^n \frac{a_0}{a_n}$. ■

Exemple 4.6

Montrer que $\sum_{\omega \in \mathbb{U}_n} \omega = 0$ pour $n \geqslant 2$ et $\prod_{\omega \in \mathbb{U}_n} \omega = (-1)^{n+1}$ pour $n \geqslant 1$.

Exercice 4.4 ✯ **Relations cœfficients-racines, III**

Résoudre dans $\mathbb{C}$ le système suivant :

$$\begin{cases} x + y + z = 1 \\ x^2 + y^2 + z^2 = 9 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1 \end{cases}$$

5 Compléments

5.1 PGCD d'un nombre fini de polynômes

Définition 5.1 PGCD

Soit $(P_1,\dots,P_r)\in\mathbb{K}[X]^r$. On appelle *plus grand commun diviseur (PGCD)* de $(P_1,\dots,P_r)$ tout polynôme $P\in\mathbb{K}[X]$ vérifiant :

(i) P est un diviseur commun des P_i ;

(ii) tout diviseur commun des P_i est un diviseur de P.

Proposition 5.1 Existence et «unicité» du PGCD

Soit $(P_1,\dots,P_r)\in\mathbb{K}[X]^r$. Si les P_i sont non tous nuls, il existe un unique PGCD *unitaire* de $(P_1,\dots,P_r)$. On le note $P_1\wedge\dots\wedge P_r$. L'unique PGCD de $(0,\dots,0)$ est 0.
Deux PGCD de $(P_1,\dots,P_r)$ sont associés.

Théorème 5.1 Bézout

Soit $(P_1,\dots,P_r)\in\mathbb{K}[X]^r$. Il existe $(U_1,\dots,U_r)\in\mathbb{K}[X]^r$ tel que $\sum_{i=1}^{r}U_iP_i=P_1\wedge\dots\wedge P_r$.

5.2 Polynômes premiers entre eux dans leur ensemble

Définition 5.2 Polynômes premiers entre eux dans leur ensemble

Soit $(P_1,\dots,P_r)\in\mathbb{K}[X]^r$. On dit que $P_1,\dots,P_r$ sont premiers entre eux dans leur ensemble si $P_1\wedge\dots\wedge P_r=1$.

Attention ! Si les P_i sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble mais la réciproque est fausse.
Par exemple, $(X-1)(X-2),(X-2)(X-3),(X-3)(X-1)$ sont premiers entre eux dans leur ensemble sans être premiers entre eux deux à deux.

Théorème 5.2 Bézout

Soit $(P_1,\dots,P_r)\in\mathbb{K}[X]^r$. Alors $P_1\wedge\dots\wedge P_r=1$ *si et seulement si* il existe $(U_1,\dots,U_r)\in\mathbb{K}[X]^r$ tel que $\sum_{i=1}^{r}U_iP_i=1$.

Proposition 5.2

Soit $(P_1,\dots,P_r)\in\mathbb{K}[X]^r$. Alors $P_1\wedge\dots\wedge P_r=1$ *si et seulement si* il existe $P_1,\dots,P_r$ n'admettent aucun diviseur irréductible commun.

5.3 PPCM d'un nombre fini de polynômes (hors programme)

Définition 5.3 PPCM (hors programme)

Soit $(P_1, \dots, P_r) \in \mathbb{K}[X]^r$. On appelle *plus petit commun multiple (PPCM)* de $(P_1, \dots, P_r)$ tout polynôme $P \in \mathbb{K}[X]$ vérifiant :

(i) P est un multiple commun des P_i ;

(ii) tout multiple commun des P_i est un multiple de P.

Proposition 5.3 Existence et «unicité» du PPCM (hors programme)

Soit $(P_1, \dots, P_r) \in \mathbb{K}[X]^r$. Si les P_i sont tous non nuls, il existe un unique PPCM *unitaire* de $(P_1, \dots, P_r)$. On le note $P_1 \vee \dots \vee P_r$.
Sinon, l'unique PPCM de $(P_1, \dots, P_r)$ est 0.
Deux PPCM de $(P_1, \dots, P_r)$ sont associés.