$\mathbb{K}[X]$

Contexte : dans ce chapitre, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ (mais en pratique on prendra $\mathbb{K}=\mathbb{R}$ ou $\mathbb{K}=\mathbb{C}$).

Objectifs du chapitre :

— Définir rigoureusement les objets rencontrés en TACMAS.

— Démontrer les théorèmes admis en TACMAS.

— Décrire l'arithmétique de $\mathbb{K}[X]$.

I Construction. Structure.

I.1 Algèbre $\mathbb{K}[X]$

Définition 1 .

- On appelle indéterminée la lettre X.
- On appelle polynôme en X à coefficients dans $\mathbb{K}$ toute combinaison linéaire formelle de puissances de l'indéterminée X.
- On appelle monôme tout polynôme de la forme a_nX^n.

Définition 2 .

On appelle degré de P l'élément de $\mathbb{N}\cup\{-\infty\}$ suivant : $\deg(P)=\sup_{\overline{\mathbb{R}}}\{i,\ a_i\neq 0\}$.

Ainsi un polynôme est nul si et seulement si son degré est $-\infty$ et, si $a_n\neq 0$, alors $\deg(a_0+a_1X+\cdots+a_nX^n)=n$.

Notation 1

- On note $\mathbb{K}[X]$ l'ensemble de tous les polynômes à coefficients dans $\mathbb{K}$.
- On note $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré $\leqslant n$.

Remarque 1

On peut donc agréablement noter un polynôme $\sum_{k=0}^{+\infty}a_kX^k$, où la suite $(a_k)_{k\in\mathbb{N}}$ est nulle à partir d'un certain rang (on dit aussi qu'elle est presque nulle). Le polynôme nul correspond alors à la suite $(a_k)_{k\in\mathbb{N}}$ telle que $a_k=0$ pour tout $k\in\mathbb{N}$.

Théorème 1 : Identification.

Deux polynômes sont égaux si et seulement si les suites presque nulles $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ sont identiques.

Dit autrement : $P=Q\Leftrightarrow\forall k\in\mathbb{N},\ a_k=b_k$.

I.2 Structure d'algèbre

Définition 3 .

On définit une loi de composition interne $+$ sur $\mathbb{K}[X]$ de la manière suivante :

si $P=\sum_{k=0}^{+\infty}a_kX^k$ et $Q=\sum_{k=0}^{+\infty}b_kX^k$ sont deux éléments de $\mathbb{K}[X]$, on note $P+Q$ le polynôme :

$P+Q=(a_0+b_0)+(a_1+b_1)X+\cdots+(a_n+b_n)X^n$.

Proposition 1 .

$(\mathbb{K}[X],+)$ forme un groupe de neutre le polynôme nul.

Remarque 2

$\Psi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}^{\mathbb{N}} \\ P = a_0 + a_1 X + \cdots + a_n X^n & \mapsto & (a_0, a_1, \cdots, a_n, 0, 0, \ldots, 0, \ldots) \end{array} \right.$ est un morphisme de groupe.

$Im(\Psi) = \mathbb{K}^{(\mathbb{N})}$ (les suites presque nulles). La corestriction $\Psi : \mathbb{K}[X] \to \mathbb{K}^{(\mathbb{N})}$ est un isomorphisme de groupe.

Définition 4 .

On définit une loi de composition externe $\cdot : \left\{ \begin{array}{ccc} \mathbb{K} \times \mathbb{K}[X] & \to & \mathbb{K}[X] \\ (\lambda, P) & \mapsto & \lambda \cdot P \end{array} \right.$ par : si $P = \sum_{k=0}^{+\infty} a_k X^k$ alors

$\lambda \cdot P = (\lambda a_0) + (\lambda a_1) X + \cdots + (\lambda a_n) X^n$

Proposition 2 .

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

Remarque 3

$\Psi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}^{(\mathbb{N})} \\ P = a_0 + \cdots + a_n X^n & \mapsto & (a_0, \cdots, a_n, 0, \ldots, 0, \ldots) \end{array} \right.$ est un isomorphisme de $\mathbb{K}$-ev.

Remarque 4

- Par définition, $\mathbb{K}[X]$ a une base canonique : $(1, X, X^2, \ldots, X^n, \ldots)$.
- $\mathbb{K}_n[X]$ est clairement un sev de $\mathbb{K}[X]$ qui a aussi une base canonique : $(1, X, X^2, \ldots, X^n)$.

Définition 5 .

Soit $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{j=0}^{m} b_j X^j$.

On définit le polynôme noté $P \times Q$ par : $P \times Q = \sum_{k=0}^{n+m} c_k X^k$ avec $c_k = \sum_{i+j=k} a_i b_j = \sum_{r=0}^{k} a_r b_{k-r}$.

Notation 2 Pour un polynôme P quelconque, on note évidemment $P^2 = P \times P$, $P^3 = P^2 \times P$, etc.

Théorème 2 .

$(\mathbb{K}[X], +, \times)$ est un anneau commutatif, d'élément unité le polynôme constant 1.

Corollaire 1 : Structure de $\mathbb{K}$-algèbre.

$(\mathbb{K}[X], +, \times, \cdot)$ forme une $\mathbb{K}$-algèbre.

Remarque 5

$\mathbb{K}_n[X]$ **n'**est **pas** un sous-anneau de $\mathbb{K}[X]$ pour $n \geqslant 1$!

Proposition 3 .

L'anneau $\mathbb{K}[X]$ est intègre, c'est-à-dire qu'un produit de deux polynômes est nul si et seulement si un des deux facteurs est nul.

I.3 Applications polynomiales

Définition 6 .

Soit $(\mathcal{A}, +, \times, \cdot)$ une $\mathbb{K}$-algèbre. Pour tout polynôme $P = \sum_{k=0}^{d} a_k X^k$ de $\mathbb{K}[X]$ on peut considérer l'application polynomiale associée à P dans $\mathcal{A}$, simplement définie par : $\widetilde{P}^{\mathcal{A}} \left\{ \begin{array}{ccc} \mathcal{A} & \to & \mathcal{A} \\ A & \mapsto & \sum_{k=0}^{d} a_k A^k \end{array} \right.$,

la somme et les multiplications considérées dans cette expression étant celles de l'algèbre $\mathcal{A}$.

Théorème 3 : Lien polynôme/application polynomiale.

Si $\mathcal{A} \neq \{0\}$ alors $P \mapsto \tilde{P}$ est un morphisme d'algèbres injectif, c'est-à-dire :

1. $\forall (P,Q) \in \mathbb{K}[X]^2,\ \forall (\lambda,\mu) \in \mathbb{K}^2\ \widetilde{\lambda P + \mu Q}^{\mathcal{A}} = \lambda \widetilde{P}^{\mathcal{A}} + \mu \widetilde{Q}^{\mathcal{A}}$ (linéarité) ;
2. $\forall (P,Q) \in \mathbb{K}[X]^2,\ \widetilde{PQ}^{\mathcal{A}} = \widetilde{P}^{\mathcal{A}}\,\widetilde{Q}^{\mathcal{A}}$ (préservation des produits) ;
3. $\forall (P,Q) \in \mathbb{K}[X]^2,\ \widetilde{P}^{\mathcal{A}} = \widetilde{Q}^{\mathcal{A}} \Rightarrow P = Q$ (injectivité).

Remarque 6

On a vu dans le corollaire 1 que $(\mathbb{K}[X], +, \times, \cdot)$ est justement une $\mathbb{K}$-algèbre.

À tout polynôme P, on peut donc associer une application $\widetilde{P}^{\mathbb{K}[X]} : \mathbb{K}[X] \to \mathbb{K}[X]$! **Remarque 7**

On a donc toujours : $P(X) = P$!

Définition 7 .

Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q \in \mathbb{K}[X]$.

On définit le polynôme composé $P \circ Q$, noté parfois simplement $P(Q)$, par : $P \circ Q = \widetilde{P}^{\mathbb{K}[X]}(Q) = \sum_{k=0}^{+\infty} a_k Q^k$.

I.4 Dérivation des polynômes

Définition 8 .

Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$.

On appelle polynôme dérivé de P le polynôme $P' = \sum_{k=1}^{d} a_k k X^{k-1}$ i. e. $P' = \sum_{k=0}^{d-1} (k+1) a_{k+1} X^k$.

Théorème 4 : Propriétés de la dérivation.

- $P \mapsto P'$ est linéaire, donc $P \mapsto P^{(n)}$ est linéaire ;
- $\forall (P,Q) \in \mathbb{K}[X],\ (PQ)' = P'Q + PQ'$, donc $\forall (P,Q) \in \mathbb{K}[X],\ (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$;
- $\forall (P,Q) \in \mathbb{K}[X],\ (P \circ Q)' = Q' \times P' \circ Q$, donc $\forall P \in \mathbb{K}[X],\ \forall (\alpha,\beta) \in \mathbb{K}^2,\ P^{(n)}(\alpha X + \beta) = \alpha^n P^{(n)}(\alpha X + \beta)$.

Théorème 5 : Taylor pour les polynômes.

- En 0 : $P(X) = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(0)}{k!} X^k$.
- En λ : $P(X+\lambda) = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(\lambda)}{k!} X^k$.
- En λ (v2) : $P(X) = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(\lambda)}{k!} (X-\lambda)^k$.

I.5 Propriétés du degré

Proposition 4 : Degré d'une dérivée.

Soit P un polynôme. Alors on a :

- $\deg(P') = \begin{cases} \deg(P) - 1 \text{ si } \deg(P) \geqslant 1 \\ -\infty \text{ sinon.} \end{cases}$
- $\deg(P^{(n)}) = \begin{cases} \deg(P) - n \text{ si } \deg(P) \geqslant n \\ -\infty \text{ sinon.} \end{cases}$

Théorème 6 : Degré d'une CL.

Soient P et Q deux polynômes, λ un scalaire. Alors on a :

1. $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$;
2. si $\deg(P) \neq \deg(Q)$, alors $\deg(P+Q) = \max(\deg P, \deg Q)$;
3. si $\lambda \neq 0$, alors $\deg(\lambda P) = \deg(P)$.

Théorème 7 : Degré d'un produit.

Soient P et Q deux polynômes. Alors on a : $\deg(P \times Q) = \deg(P) + \deg(Q)$.

Remarque 8

La proposition précédente montre à nouveau que $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$ pour $n \geqslant 1$.

On peut aussi l'utiliser pour retrouver l'intégrité de $\mathbb{K}[X]$ en une demi-ligne !

Corollaire 2 : Degré d'une puissance.

Soit P un polynôme et $n \in \mathbb{N}$. Alors on a : $\deg(P^n) = n\deg(P)$.

Théorème 8 : Degré d'une composée.

Soient P un polynôme **et** Q **un polynôme non constant**. Alors on a : $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Remarque 9

Si Q est constant il peut se produire qu'il soit une racine de P et dans ce cas on a $P \circ Q = 0$...

II Racines

II.1 Division euclidienne

Théorème 9 : Division euclidienne.

Soit $(A, B) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$.
Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que : $A = BQ + R$ et $\deg(R) < \deg(B)$.

Proposition 5 : Invariance par extension de corps.

Soit $(A, B) \in \mathbb{R}[X] \times (\mathbb{R}[X] \setminus \{0\})$ $\Big($ en particulier on a $(A, B) \in \mathbb{C}[X] \times (\mathbb{C}[X] \setminus \{0\})$ $\Big)$.

Le quotient et le reste de la division euclidienne de A par B sont les mêmes pour la division euclidienne dans $\mathbb{C}[X]$ que pour la division euclidienne dans $\mathbb{R}[X]$.

II.2 Racines

Proposition-Définition 9 .

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Sont équivalentes :

1. $P(\alpha) = 0$.
2. Le polynôme $(X - \alpha)$ divise P.

On dit alors que α est une racine de P dans $\mathbb{K}$.

*Théorème 10 : **très important**.*

1. Un polynôme de degré $n \geqslant 0$ a au plus n racines.
2. Si $P \in \mathbb{K}[X]$ a une infinité de racines alors $P = 0$.
3. Si $P \in \mathbb{K}_n[X]$ a $n+1$ racines alors $P = 0$.

Définition 10 .

Un polynôme P de degré n est dit :

- scindé lorsqu'il peut s'écrire $P(X) = a_n(X - \lambda_1)\cdots(X - \lambda_n)$.
- scindé à racines simples lorsqu'il peut s'écrire $P(X) = a_n(X - \lambda_1)\cdots(X - \lambda_n)$ avec les λ_i distincts.

Théorème 11 : de d'Alembert-Gauss (rappel).

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

II.3 Relations coefficients-racines

Proposition 6 : Cas $n = 3$.

Supposons $a_3X^3 + a_2X^2 + a_1X + a_0$ scindé de racines $\lambda_1, \lambda_2, \lambda_3$. Alors :

$$\begin{cases} \frac{a_2}{a_3} = -(\lambda_1 + \lambda_2 + \lambda_3) \\ \frac{a_1}{a_3} = +(\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3) \\ \frac{a_0}{a_3} = -\lambda_1\lambda_2\lambda_3 \end{cases}$$

Théorème 12 : Cas général.

Supposons $a_nX^n + \cdots + a_1X + a_0$ scindé de racines $\lambda_1, \lambda_2, \ldots, \lambda_n$.

On appelle k^e expression symétrique élémentaire le scalaire $\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} \lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_k}$.

Supposons $a_nX^n + \cdots + a_1X + a_0$ scindé de racines $\lambda_1, \lambda_2, \ldots \lambda_n$. Alors :

Pour tout $0 \leqslant i \leqslant n$ on a $\dfrac{a_i}{a_n} = (-1)^{n-i}\sigma_{n-i}$

II.4 Multiplicité

Proposition-Définition 11 : Racines multiples.

Soit $P \in \mathbb{K}[X] \setminus \{0\}$, $\alpha \in \mathbb{K}$ et $r \in \mathbb{N}$. Les trois propositions suivantes sont équivalentes :

i. $r = \max\{k \in \mathbb{N} \setminus \{0\},\ (X-\alpha)^k \text{ divise } P\}$.
ii. On peut écrire $P = (X-\alpha)^r Q$ avec $Q(\alpha) \neq 0$.
iii. $P(\alpha) = 0,\ P'(\alpha) = 0, \ldots,\ P^{(r-1)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$.

Lorsqu'elles sont vérifiées, on dit que α est une racine de multiplicité r de P.

Pour $r = 1$ on parle de racine simple, pour $r = 2$ de racine double, pour $r = 3$ de racine triple, etc.

On parle de racine multiple dès qu'on a $r \geqslant 2$.

Remarque 10

L'exercice CCINP $n°85$ consiste essentiellement en cette question de cours ! **Remarque 11**

Avec la définition précédente, on peut donc dire que α est racine de multiplicité 0 de P si et seulement si ce n'est pas une racine de P (c'est dans le programme). On peut aussi dire que tout scalaire est racine de multiplicité infinie du polynôme nul. **Remarque 12**

Si P est un polynôme admettant des racines distinctes α_i, pour $i \in \{1, \ldots, s\}$, de multiplicités respectives r_i, alors P est divisible par $(X-\alpha_1)^{r_1}(X-\alpha_2)^{r_2}\ldots(X-\alpha_s)^{r_s} = \prod_{i=1}^{s}(X-\alpha_i)^{r_i}$.

Corollaire 3 .

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

1. P a au plus n racines **comptées avec leur multiplicité**.
2. P est scindé si et seulement si il a n racines **comptées avec leur multiplicité**.
3. Si P a au moins $n+1$ racines **comptées avec multiplicité**, c'est le polynôme nul.

II.5 Racines complexes d'un polynôme de $\mathbb{R}[X]$

Définition 12 .

Pour $P \in \mathbb{C}[X]$, on appelle **polynôme conjugué** de $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ le polynôme $\overline{P}$ défini par $\overline{P}(X) = \overline{a_0} + \overline{a_1}X + \overline{a_2}X^2 + \cdots + \overline{a_n}X^n$.

Remarque 13

La conjugaison étant un automorphisme de corps involutif sur $\mathbb{C}$ elle induit un automorphisme d'anneau involutif sur $\mathbb{C}[X]$. Elle est de plus compatible avec la dérivation et avec $P \mapsto \tilde{P}$.

III Arithmétique dans $\mathbb{K}[X]$

III.1 Divisibilité des polynômes

III.2 Propriétés algébriques de la divisibilité

III.3 PGCD

III.4 Polynômes premiers entre eux

Remarque 14 $\overline{P} = P \Leftrightarrow P \in \mathbb{R}[X]$. **C'est à ça que sert à la conjugaison des polynômes.**

Corollaire 4 .

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

1. α racine de $P \Leftrightarrow \overline{\alpha}$ racine de P.
2. α racine de P de multiplicité $k \Leftrightarrow \overline{\alpha}$ racine de P de multiplicité k.

Démonstration.

1. Il suffit de montrer l'implication directe par involutivité de la conjugaison.
   Supposons $P(\alpha) = 0$. On a $P \in \mathbb{R}[X]$ donc $\overline{P} = P$.
   On conjugue : $\overline{P(\alpha)} = \overline{0}$ *i. e.* $\overline{P}(\overline{\alpha}) = 0$ *i. e.* $P(\overline{\alpha}) = 0$. Youpie.

2. Il suffit de montrer l'implication directe par involutivité de la conjugaison.
   α est racine de P de multiplicité k signifie que α est racine de P, P', …, $P^{(k-1)}$ mais pas de $P^{(k)}$.
   On utilise le point 1. sur P, P', …, $P^{(k-1)}$ et sa contraposée sur $P^{(k)}$.

□

Corollaire 5 .

Soit $P \in \mathbb{R}_{2n+1}[X]$. Alors P a une racine **réelle**.

Démonstration. D'après d'Alembert-Gauss, P a $2n+1$ racines complexes comptées avec multiplicité.
Or P est à coefficients réels donc ses racines vont par paires avec leur conjugué qui a la même multiplicité.
Montrons que l'une est réelle par l'absurde : si ce n'était pas le cas on aurait un nombre pair de racines comptées avec leur multiplicité. C'est une contradiction. □

On aurait aussi pu utiliser le TVI !

Lorsqu'on a un anneau, on a une arithmétique (qui consiste, essentiellement, en l'étude de sa relation de divisibilité). L'arithmétique d'un anneau dans lequelle on a un théorème de division euclidienne est essentiellement la même que celle de $\mathbb{Z}$: nous allons l'illustrer ici, en prenant notre sur cours sur $\mathbb{Z}$ et en le recopiant. Recopier, c'est le bien. Avec l'ordinateur en plus ça va vite.

Définition 13 .

On dit d'un polynôme B de $\mathbb{K}[X]$ qu'il divise un polynôme A de $\mathbb{K}[X]$, et on écrit $B \mid A$, lorsqu'il existe un polynôme C de $\mathbb{K}[X]$ vérifiant $A = BC$. On dit alors de B qu'il est un diviseur de A, et de A qu'il est un multiple de B.

Notation 3

- L'ensemble des multiples de P dans $\mathbb{K}[X]$ se note $P\mathbb{K}[X]$.
- On pourra, comme dans $\mathbb{Z}$, noter $D(P)$ l'ensemble des diviseurs de P.

Proposition 7 : Inversibles de $\mathbb{K}[X]$. L'ensemble des inversibles de $\mathbb{K}[X]$ est $\mathbb{K}[X]^\times = \mathbb{K}^*$

Démonstration. $\boxed{\supset}$ Si $c \in \mathbb{K}^*$ alors c est inversible puisque son inverse est c^{-1}.

$\boxed{\subset}$ Soit P un polynôme inversible et notons Q son inverse. On a $PQ = 1$ donc $\deg(PQ) = 0$.
D'après la formule des degrés $\deg(P) + \deg(Q) = 0$. Donc $\deg(P) = \deg(Q) = 0$ et en particulier $P \in \mathbb{K}^*$. □

Proposition 8 .

La relation de divisibilité sur $\mathbb{K}[X]$ est réflexive et transitive mais n'est pas antisymétrique.

Si on la restreint à l'ensemble $\mathcal{U}$ des polynômes unitaires de $\mathbb{K}[X]$, elle devient alors antisymétrique et est par conséquent une relation d'ordre sur $\mathcal{U}$. Idem sur $\mathcal{U} \cup \{0\}$ si on ne veut pas se priver du polynôme nul.

Démonstration.
- Réflexivité : soit $P \in \mathbb{K}[X]$. On a $1 \in \mathbb{K}[X]$ et $P = 1 \times P$ donc $P \mid P$.
- Transitivité : soient $P, Q, R \in \mathbb{K}[X]$ et supposons $P \mid Q$ et $Q \mid R$. Il existe donc $S, T \in \mathbb{K}[X]$ tels que $Q = PS$ et $R = QT$, donc $R = P(ST)$ et donc $P \mid R$.
- La relation de divisibilité n'est pas antisymétrique sur $\mathbb{K}[X]$: $3X^2 \mid X^2$ et $X^2 \mid 3X^2$ mais $X^2 \neq 3X^2$.
- Plaçons-nous maintenant dans $\mathcal{U} \cup \{0\}$: soit $(P, Q) \in \left(\mathcal{U} \cup \{0\}\right)^2$ et supposons $P \mid Q$ et $Q \mid P$. Il existe $S \in \mathbb{K}[X]$ tel que $Q = SP$ et il existe $T \in \mathbb{K}[X]$ tel que $P = TQ$. On en déduit $P = STP$ et donc on a soit $P = 0$, soit $ST = 1$ par intégrité.
- Évidemment, restreindre une relation antisymétrique donne une relation antisymétrique, donc la divisibilité est aussi un ordre sur $\mathcal{U}$. □

On retiendra donc que $\mathcal{U}$ **joue dans** $\mathbb{K}[X]$ **le rôle joué dans** $\mathbb{Z}$ **par** $\mathbb{N} \setminus \{0\}$.

Proposition-Définition 14 .

On dit de deux polynômes P et Q qu'ils sont associés lorsqu'une des propositions suivantes est vérifiées :
- $P \mid Q$ et $Q \mid P$;
- il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$.

L'association est donc la relation d'équivalence canoniquement associée à la divisibilité. La multiplication par un scalaire non nul joue dans $\mathbb{K}[X]$ le rôle joué par la multiplication par ± 1 dans $\mathbb{Z}$. On retrouve bien que $\mathcal{U}$ joue dans $\mathbb{K}[X]$ le rôle joué dans $\mathbb{Z}$ par $\mathbb{N} \setminus \{0\}$. On voit en particulier que tout polynôme non nul est associé à un unique polynôme unitaire.

Démonstration. $\boxed{\Rightarrow}$ Soit $(P, Q) \in \mathbb{K}[X]^2$ tels que $P|Q$ et $Q|P$.
Ainsi il existe $C \in \mathbb{K}[X]$ tel que $P = QS$ et $T \in \mathbb{K}[X]$ tel que $Q = PT$.
On a en particulier les relations $\deg(P) = \deg(Q) + \deg(S)$ et $\deg(Q) = \deg(P) + \deg(T)$, dont on déduit en réinjectant : $\deg(S) + \deg(T) = 0$. Et donc $\deg(S) = \deg(T) = 0$. Ainsi S est un polynôme constant non nul ; en posant $\lambda = S$, on a bien $P = \lambda Q$ avec $\lambda \in \mathbb{K}^*$.
$\boxed{\Leftarrow}$ λ et $\frac{1}{\lambda}$ sont dans $\mathbb{K}[X]$ donc lol. □

Proposition 9 .

La divisibilité est stable par :
- CL : si $C \mid A$ et $C \mid B$ alors $C \mid AU + BV$.
- Produit : $\begin{cases} \text{si } A \mid B \text{ alors } AC \mid BC\,; \\ \text{si } A \mid B \text{ et } P \mid Q \text{ alors } AP \mid BQ. \end{cases}$
- Puissances : si $n \in \mathbb{N}$ et $A \mid B$ alors $A^n \mid B^n$.

Démonstration. Fastoche (recopier le cours sur $\mathbb{Z}$). □

Proposition 10 .

La divisibilité est invariante par extension de corps : si $P,\ Q \in \mathbb{R}[X]$ alors $P \mid Q$ dans $\mathbb{R}[X]$ si et seulement si $P \mid Q$ dans $\mathbb{C}[X]$.

Démonstration. Immédiat car il suffit d'utiliser le lien divisibilité/division euclidienne et l'invariance de la division euclidienne par extension de corps. □

Définition 15 .

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

1. On dit que D est **un** pgcd de P et Q lorsque c'est un plus grand diviseur de P et de Q (pour la divisibilité).
2. Il existe un unique pgcd unitaire (ou nul), on l'appelle **le** pgcd et on le note $\mathrm{PGCD}(P,Q)$ ou $P \wedge Q$.

Exercice 1. Reformuler cette définition.

— — $D|P$ et $D|Q$
— $\forall R \in \mathbb{K}[X], (R|P \text{ et } R|Q) \implies R|D$
— $P \wedge Q = \inf_{(\mathcal{U}\cup\{0\},\ |)}\{P,Q\}$
— $\mathcal{D}(D) = \mathcal{D}(P) \cap \mathcal{D}(Q)$

Proposition 11 : Propriétés immédiates du PGCD.

- Homogénéité : si K est unitaire alors $KA \wedge KB = K(A \wedge B)$;
- Commutativité : $B \wedge A = A \wedge B$;
- Associativité : $(A \wedge B) \wedge C = A \wedge (B \wedge C)$.

Pour montrer l'existence, ne faisons pas comme dans $\mathbb{Z}$ (on pourrait), mais utilisons l'algorithme d'Euclide.

Lemme 1 : Lemme préparatoire à l'algorithme d'Euclide.

1. Si R est le reste dans la division euclidienne de A par B alors $A \wedge B = B \wedge R$.
2. Si D est unitaire, $D \wedge 0 = D$.

Démonstration.
1. Il suffit de montrer que les diviseurs communs à A et B sont les mêmes que les diviseurs communs à B et R. Cela provient de la stabilité par CL avec les deux CL $A = BQ + R$ et $R = A - BQ$.
2. Les diviseurs communs à D et 0 sont juste les diviseurs de D d'où le résultat.

□

L'existence du PGCD est assurée par l'algorithme d'Euclide :

- On pose $R_0 = A$ et $R_1 = B$.
- Tant que $R_{n+1} \neq 0$ on définit R_{n+2} comme le reste dans la DE de R_n par R_{n+1}.
- Le PGCD est le dernier reste non nul R_n (au coefficient dominant près).

Reste à montrer la terminaison et la correction de cet algorithme.

Démonstration. On copie le cours sur $\mathbb{Z}$.

- Terminaison : par division euclidienne, pour tout $n \geqslant 1$ tel que $R_n \neq 0$, on a $\deg(R_{n+1}) < \deg(R_n)$. On a donc $\deg(B) = \deg(R_1) > \deg(R_2) > \deg(R_3) > \cdots$. Comme il n'y a qu'un nombre fini d'éléments dans $\{-\infty\} \cup \{0, \ldots, \deg(B)\}$, il existe nécessairement un rang $N \geqslant 2$ tel que $\deg(R_N) = -\infty$, c'est-à-dire $R_N = 0$ et $\deg(R_{N-1}) \geqslant 0$. D'où la terminaison.
- Correction : on a alors, par le lemme préparatoire, $R_{n-1} \wedge R_n = R_n \wedge R_{n+1}$ pour tout $n \in \{1, \ldots, N-1\}$. Donc : $A \wedge B = R_0 \wedge R_1 = R_1 \wedge R_2 = \cdots = R_{N-2} \wedge R_{N-1} = R_{N-1} \wedge R_N = R_{N-1} \wedge 0$. Le PGCD est donc associé à R_{N-1}. □

Exercice 2. Calculons par exemple $\left(X^6+1\right) \wedge \left(X^4+1\right)$.

Théorème 13 : Théorème d'Eudoxe (théorème "sur la relation de Bézout").

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

Formulation moderne : pour D unitaire : $D = A \wedge B \Leftrightarrow A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$.

Démonstration. Il suffit de remonter l'algorithme d'Euclide. □

Exercice 3. Trouvons une relation de Bézout pour $A = X^6 + 1$ et $B = X^4 + 1$.

Proposition 12 .

Le PGCD est invariant par extension de corps : si $P, Q \in \mathbb{R}[X]$ alors le pgcd de P et Q dans $\mathbb{R}[X]$ est le même que dans $\mathbb{C}[X]$.

Démonstration. Immédiat d'après le lien divisibilité/division euclidienne et l'invariance de la division euclidienne par extension de corps. □

Exercice 4. Calculons $\left(X^6 - 1\right) \wedge \left(X^4 - 1\right)$.

Définition 16 .

On dit que deux polynômes P et Q sont premiers entre eux lorsque $P \wedge Q = 1$.

Proposition 13 .

Le caractère "premiers entre eux" est invariant par extension de corps : $P,\ Q \in \mathbb{R}[X]$ sont premiers entre eux dans $\mathbb{R}[X]$ si et seulement si ils le sont dans $\mathbb{C}[X]$.

Remarque 15

L'homogénéïté entraîne que si A et B sont non nuls et D est leur PGCD, alors $\dfrac{A}{D}$ et $\dfrac{B}{D}$ sont premiers entre eux.

Théorème 14 : Théorème de Bézout.

Soient A et B deux polynômes. On a $A \wedge B = 1 \Leftrightarrow \exists (U,V),\ AU + BV = 1$.

Théorème 15 : Lemme de Gauss.

Si $\begin{cases} A \wedge B = 1 \\ A | BC \end{cases}$ alors $A | C$.

III.5 PPCM

Définition 17 .

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

1. On dit que M est **un** ppcm de P et Q lorsque c'est un plus petit multiple de P et de Q.
2. Il existe un unique ppcm unitaire (ou nul), on l'appelle **le** ppcm et on le note $\text{ppcm}(P,Q)$ ou $P \vee Q$.

Proposition 14 : Propriétés immédiates du PPCM.

- Homogénéité : si K est unitaire alors $KA \vee KB = K(A \vee B)$;
- Commutativité : $B \vee A = A \vee B$;
- Associativité : $(A \vee B) \vee C = A \vee (B \vee C)$.

Remarque 16

Si A et B sont unitaires, alors $(A \wedge B) \times (A \vee B) = A \times B$.

Proposition 15 .

Le PPCM est invariant par extension de corps : si $P, Q \in \mathbb{R}[X]$ alors le ppcm de P et Q dans $\mathbb{R}[X]$ est le même que dans $\mathbb{C}[X]$.

III.6 Polynômes irréductibles

Définition 18 .

Un polynôme $P \in \mathbb{K}[X] \setminus \mathbb{K}$ est dit irréductible lorsqu'on a :

$$\forall (U,V) \in \mathbb{K}[X]^2,\ P = UV \ \Rightarrow \ \begin{cases} U \text{ inversible} \\ V \text{ associé à } P \end{cases} \text{ ou } \begin{cases} U \text{ associé à } P \\ V \text{ inversible} \end{cases}$$

Théorème 16 : Théorème de décomposition.

Tout polynôme peut s'écrire comme produit de polynômes irréductibles, de façon unique à l'ordre des facteurs près et à association près.

Théorème 17 : Irréductibles de $\mathbb{C}$.

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

Théorème 18 : Irréductibles de $\mathbb{R}$.

Les irréductibles unitaires de $\mathbb{R}[X]$ sont

- les $X - \lambda,\ \lambda \in \mathbb{R}$;
- les $X^2 + bX + c$, $\Delta < 0$.