Chapitre 15

Arithmétique des polynômes

15.1 Arithmétique des polynômes

15.1.1 Multiples et diviseurs

Rappel

- Le théorème de division euclidienne indique que pour tout couple (A, B) de polynômes, B non nul,
  il existe un unique couple (Q, R) de polynômes
  tels que $\boxed{A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B)}$
- $A \cdot \mathbb{K}[X]$ désigne l'ensemble des multiples de A
- A divise $B \Leftrightarrow B$ est multiple de $A \Leftrightarrow B \in A \cdot \mathbb{K}[X]$

Remarque : $\boxed{A|B \Leftrightarrow B \cdot \mathbb{K}[X] \subset A \cdot \mathbb{K}[X]}$

Th. ▷ **Polynômes associés**

A et B sont deux polynômes de $\mathbb{K}[X]$:

$$A|B \text{ et } B|A \quad \Leftrightarrow \quad \exists\, \lambda \in \mathbb{K}^*,\ A = \lambda B$$

On dit que A et B sont **associés** .

Corollaire : $\boxed{A \cdot \mathbb{K}[X] = B \cdot \mathbb{K}[X] \Leftrightarrow A \text{ et } B \text{ sont associés}}$

Test 415

On reprend la notation habituelle $F + G = \left\{ f + g \mid f \in F \text{ et } g \in G \right\}$.
Ecrire la forme des éléments de $A \cdot \mathbb{K}[X] + B \cdot \mathbb{K}[X]$ et de $(A + B) \cdot \mathbb{K}[X]$.
En déduire que ces deux ensembles ne sont pas toujours égaux.

Th. ▷ **Caractérisation des ensembles de la forme $A \cdot \mathbb{K}[X]$**

Soit $E \subset \mathbb{K}[X]$, $E \neq \varnothing$.

$$\exists\, A \in \mathbb{K}[X],\ E = A \cdot K[X] \Leftrightarrow \begin{cases} E \text{ est un sous-groupe de } \mathbb{K}[X] \\ \forall\, P \in E,\ \forall\, Q \in \mathbb{K}[X],\ PQ \in E \end{cases}$$

On dit que A est un **générateur** du groupe E.

De plus

$A \cdot \mathbb{K}[X] = B \cdot \mathbb{K}[X] \Leftrightarrow A$ et B sont associés.

Si $E \neq \left\{ \mathbf{0} \right\}$, il existe un unique générateur normalisé.

Test 416 Montrer que $G = \left\{ P \in \mathbb{R}[X] \mid \tilde{P}(1) = 0 \right\}$ admet un unique générateur normalisé.
Pour cela on montrera que G est un sous-groupe "super-stable" de $\mathbb{K}[X]$.
Déterminer ce générateur.

15.1.2 PPCM de deux polynômes

Le **PPCM** [1] de $A, B \in \mathbb{K}[X]$ est l'unique polynôme $M \in \mathbb{K}[X]$, normalisé ou nul, qui vérifie $\boxed{A \cdot \mathbb{K}[X] \cap B \cdot \mathbb{K}[X] = M \cdot \mathbb{K}[X]}$

On le note $\boxed{\text{PPCM}(A, B)}$ ou $\boxed{A \vee B}$

Justification et caractérisation

- $M = \text{PPCM}(A, B)$ existe et est unique.
- M est un multiple commun de A et B
- tout multiple commun à A et B est multiple de M

$$\boxed{\forall\ P \in \mathbb{K}[X],\ \left.\begin{array}{l} A|P \\ B|P \end{array}\right\} \quad \Leftrightarrow \quad \text{PPCM}(A, B)|P}$$

Test 417 λ et μ sont des scalaires non nuls.
Comparer $\text{PPCM}(A, B)$ et $\text{PPCM}(\lambda A, \mu B)$

Propriétés : $\forall\ A, B, C \in \mathbb{K}[X]$

- $\lambda, \mu \in \mathbb{K}^* \Rightarrow A \vee B = (\lambda A) \vee (\mu B)$
- $A \vee B = B \vee A$
- $A \vee (B \vee C) = (A \vee B) \vee C$
- $A \neq \mathbf{0} \Rightarrow A \vee 1 = \text{norm}(A)$
- $C \neq \mathbf{0} \Rightarrow (C\,A \vee C\,B) = \text{norm}(C)\,(A \vee B)$

Test 418 Peut-on parler de loi de composition interne ? d'associativité ? de commutativité ? d'élément neutre ?

Test 419 Si A divise B, que vaut $A \vee B$?

15.1.3 PGCD de deux polynômes

Le **PGCD** [2] de $A, B \in \mathbb{K}[X]$ est l'unique polynôme $D \in \mathbb{K}[X]$, normalisé ou nul, qui vérifie $\boxed{A \cdot \mathbb{K}[X] + B \cdot \mathbb{K}[X] = D \cdot \mathbb{K}[X]}$

On le note $\boxed{\text{PGCD}(A, B)}$ ou $\boxed{A \wedge B}$

Justification et caractérisation

- $D = \text{PGCD}(A, B)$ existe et est unique.
- D est un diviseur commun de A et B
- tout diviseur commun de A et B divise D.

$$\boxed{\forall\ P \in \mathbb{K}[X],\ \left.\begin{array}{l} P|A \\ P|B \end{array}\right\} \quad \Leftrightarrow \quad P|\,\text{PGCD}(A, B)}$$

1. **PPCM** est l'acronyme de **P**lus **P**etit **C**ommun **M**ultiple.
2. **PGCD** est l'acronyme de **P**lus **G**rand **C**ommun **D**iviseur.

Définition : si $A \wedge B = 1$, alors A et B sont **premiers entre eux** .

Propriétés : $\forall\, A, B, C \in \mathbb{K}[X]$

- $\boxed{D = A \wedge B \;\Rightarrow\; \exists\, P, Q \in \mathbb{K}[X] \quad D = A\,P + B\,Q}$

Attention : la réciproque est fausse
P et Q ne sont pas uniques.

- $\lambda, \mu \in \mathbb{K}^* \;\Rightarrow\; A \wedge B = (\lambda A) \wedge (\mu B)$
- $A \wedge B = B \wedge A$
- $A \wedge (B \wedge C) = (A \wedge B) \wedge C$
- $A \neq \mathbf{0} \;\Rightarrow\; A \wedge \mathbf{0} = \mathrm{norm}(A)$
- $C \neq \mathbf{0} \;\Rightarrow\; (C\,A \wedge C\,B) = \mathrm{norm}(C)\,(A \wedge B)$

Test 420

Si les polynômes A, B, P, Q et R vérifient $R = A\,P + B\,Q$,
que peut-on dire du PGCD $A \wedge B$?
Application : Montrer que $(X^3 - 4\,X + 3) \wedge (X^4 - 4\,X^2 + X + 2) = X - 1$

Test 421

a et b sont deux entiers non nuls. Notons d leur PGCD.
On peut identifier ces entiers aux polynômes constants. Le polynôme constant d est-il le PGCD des polynômes constants a et b ? Pourquoi ?

15.1.4 Algorithme d'euclide

Lemme :

Si $A = B\,Q + R$ est la division euclidienne de A par $B \neq \mathbf{0}$, alors

$$\mathrm{PGCD}\,(A, B) = \mathrm{PGCD}\,(B, R)$$

L'algorithme d'euclide (pour le calcul du PGCD)

Si A et B sont deux polynômes non nuls, le PGCD de A et B est le normalisé du dernier reste non nul dans la suite des divisions euclidiennes :

$$\begin{array}{rcll} A & = & B\,Q_1 + R_1 & \\ B & = & R_1\,Q_2 + R_2 & \\ R_1 & = & R_2\,Q_3 + R_3 & \\ \dots & \dots & \dots & \\ R_{n-2} & = & R_{n-1}\,Q_n + \boxed{R_n} & \leftarrow \text{ dernier reste non nul} \\ R_{n-1} & = & R_n\,Q_{n+1} + \mathbf{0} & \end{array}$$

Note : on peut alléger les calculs en multipliant un reste par un scalaire non nul.

Utilisation de l'algorithme pour déterminer P et Q

Si $D = \mathrm{PGCD}\,(A, B)$, nous savons que : $\exists\, P, Q \in \mathbb{K}[X]$, $D = A\,P + B\,Q$
On peut déterminer un des couples $(P\,, Q)$ en "remontant l'algorithme d'euclide".

Test 422

Utiliser l'algorithme d'euclide pour déterminer le
PGCD de $X^4 + X^2 + 1$ et $X^3 + 2\,X^2 + 2\,X + 1$

Test 423

$A = X^6 + 5\,X^4 - X^3 + 8\,X^2 - 3\,X + 6$, $B = X^5 + 4\,X^3 + X^2 + 3\,X + 3$.
Calculer $\mathrm{PGCD}\,(A, B)$ et le mettre sous la forme $A\,P + B\,Q$.

Algorithme d'Euclide étendu dans $\mathbb{K}[X]$
Entrées : les polynômes A et B avec $A \neq 0$ ou $B \neq 0$.
Variables : U_0, V_0, U_1, V_1, Q et λ.
Résultat : PGCD unitaire et coefficients de Bezout
début
$(U_0, V_0) \leftarrow (1, 0)$
$(U_1, V_1) \leftarrow (0, 1)$
tant que $B \neq 0$ **faire**
$Q \leftarrow$ quotient de la division de A par B
$(A, B) \leftarrow (B, A - QB)$
$(U_0, U_1) \leftarrow (U_1, U_0 - QU1)$
$(V_0, V_1) \leftarrow (V_1, V_0 - QV1)$
$\lambda \leftarrow$ coefficient dominant de A
$A \leftarrow A/\lambda$, $U_0 \leftarrow U_0/\lambda$, $V_0 \leftarrow V_0/\lambda$
Retourner (A, U_0, V_0)

15.1.5 Théorèmes d'arithmétique

Ce qui suit est une généralisation à $\mathbb{K}[X]$ des théorèmes d'arithmétique dans $\mathbb{Z}$.

Th. ▷ **Théorème de Bézout** [3]

Les polynômes A et B de $\mathbb{K}[X]$ sont premiers entre eux
ssi $\exists\, P, Q \in \mathbb{K}[X] \quad A \cdot P + B \cdot Q = 1$

Corollaire : $A, B, C \in \mathbb{K}[X]$. $A \wedge C = 1 \Rightarrow A \wedge (BC) = A \wedge B$.

Test 424 Calculer $(X^3 + X^2 - X + 1)(2X + 3) - (X^2 + X + 1)(2X^2 + 3X - 4)$. Conclusion ?

Th. ▷ **Théorème de Gauss** [4]

$A, B, C \in \mathbb{K}[X]$

$$\left.\begin{array}{ll} A \text{ divise } BC & A|BC \\ A \text{ premier avec } B & A \wedge B = 1 \end{array}\right\} \Rightarrow A|C \quad (A \text{ divise } C)$$

Th. ▷ **Trois théorèmes indispensables :**

- Si deux polynômes premiers entre eux divisent P, alors leur produit divise P

$$\left.\begin{array}{l} A|P \\ B|P \\ A \wedge B = 1 \end{array}\right\} \Rightarrow AB|P$$

- Le PPCM de deux polynômes premiers entre eux est leur produit (normalisé)

$$A \wedge B = 1 \quad \Rightarrow \quad A \vee B = \text{norm}(AB)$$

- Si A est premier avec deux polynômes, alors A est premier avec leur produit.

$$\left.\begin{array}{l} A \wedge B_1 = 1 \\ A \wedge B_2 = 1 \end{array}\right\} \Rightarrow A \wedge (B_1 B_2) = 1$$

3. Etienne BÉZOUT (1730-1783) mathématicien Français. L'égalité portant son nom était destinée à étudier l'intersection de deux courbes algébriques.
4. Carl Friedrich GAUSS (1777-1855) mathématicien allemand

Test 425

Les polynômes non nuls A, B, P_1 et Q_1 vérifient $A\,P_1 + B\,Q_1 = 1$.
Trouver tous les polynômes P et Q tels que $A\,P + B\,Q = 1$.

Test 426

A connaître . . .
Montrer que $A \wedge B = 1 \quad \Leftrightarrow \quad A^2 \wedge B^2 = 1$
Généralisation : $n, m \in \mathbb{N}^*, \quad A \wedge B = 1 \quad \Leftrightarrow \quad A^n \wedge B^m = 1$

15.1.6 PGCD de n polynômes

Soient P_1, P_2, …, P_n n polynômes non tous nuls. Alors il existe un unique polynôme normalisé D dans $\mathbb{K}[X]$ tel que
— D divise les P_k pour $1 \leqslant k \leqslant n$.
— pour tout M polynôme divisant les P_k, M divise D.
D est appelé **PGCD** des P_k, et est noté

$$D = \bigwedge_{k=1}^{n} P_k$$

Soit $(P_k)_{1\leqslant k\leqslant n}$ une famille finie de polynômes.
— Les P_k sont *premiers dans leur ensemble* si leur PGCD est 1.
— Les P_k sont *premiers deux à deux* si pour tout $k \neq k'$, P_k et $P_{k'}$ sont premiers entre eux.

Th. ▷ **Relation de Bézout**

Si $(P_k)_{1\leqslant k\leqslant n}$ est une famille finie de polynômes de PGCD noté D, il existe une famille de polynômes $(R_k)_{1\leqslant k\leqslant n}$ telle que

$$\sum_{k=1}^{n} R_k P_k = D$$

On peut généraliser aussi le PPCM à une famille de polynômes de la même manière.

Test 427

Calculer le PPCM de la famille $\Big(X-1\,,\ X-2\,,\ X-3\Big)$.
Ce PPCM est-il égal au produit de la famille ?
Même question avec la famille $\Big(X(X-1)\,,\ (X-1)(X-2)\,,\ X(X-2)\Big)$.

Voir l'exercice "Equation $A\,P + B\,Q = C$"

15.2 Polynômes irréductibles

Pour un polynôme, être irréductible est l'équivalent d'être premier pour un entier

15.2.1 Définition et propriétés

$P \in \mathbb{K}[X]$ est **irréductible** [5]

ssi
- ▶ P est non constant
- ▶ les seuls diviseurs de P sont
  - ▷ les polynômes de degré 0 $\quad (\lambda \in \mathbb{K}^*)$
  - ▷ les polynômes associés $\quad (\lambda\,P\,,\ \lambda \in \mathbb{K}^*)$

Propriétés :

- Tout polynôme de degré 1 est irréductible
- P irréductible, $\lambda \in \mathbb{K}^* \quad \Rightarrow \quad \lambda\,P$ irréductible
- Un polynôme irréductible est premier avec tout polynôme, sauf ses multiples.
- Deux polynômes irréductibles non associés sont premiers entre eux.

5. On peut dire **premier** (qu'il ne faut pas confondre avec "premiers entre eux").

C'est donc le cas de deux polynômes irréductibles normalisés distincts.

Test 428 | Que peut-on dire des polynômes A et B si le produit AB est irréductible ?

Test 429

Attention : *la notion d'irréductibilité dépend du corps* $\mathbb{K}$

Justifier que X^2+1 est réductible dans $\mathbb{C}[X]$
mais irréductible dans $\mathbb{R}[X]$.

15.2.2 Décomposition primaire

Th. ▷ **Décomposition en polynômes irréductibles**

Tout polynôme non constant de $\mathbb{K}[X]$ se décompose
en produit d'un scalaire et de polynômes irréductibles normalisés.
Cette décomposition est unique, à l'ordre prés.

(C'est la décomposition **primaire** du polynôme.)

Corollaire : tout polynôme non constant admet un diviseur irréductible.

Comme pour les entiers, la décomposition en polynômes irréductibles de A et B permet

- *de savoir si A divise B*
- *d'obtenir tous les diviseurs de A*
- *d'obtenir le PPCM et le PGCD des deux polynômes*

Th. ▷ **Diviseurs, PGCD et PPCM**

Soit A et B deux polynômes non nuls tels que :

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_k^{\alpha_k} \quad \text{et} \quad B = \mu P_1^{\beta_1} P_2^{\beta_2} \cdots P_k^{\beta_k}$$

où $P_1, P_2, \cdots, P_k$ sont des polynômes irréductibles normalisés distincts deux à deux, $\alpha_1, \alpha_2, \cdots, \alpha_k, \beta_1, \beta_2, \cdots, \beta_k$ des entiers naturels éventuellement nuls. Alors, on a :

- $A|B \Leftrightarrow \forall i \in [\![1,k]\!] \quad \alpha_i \leqslant \beta_i$
- $A \wedge B = \prod_{i=1}^{k} P_i^{\min(\alpha_i,\beta_i)}$ et $A \vee B = \prod_{i=1}^{k} P_i^{\max(\alpha_i,\beta_i)}$

15.2.3 Cas de $\mathbb{C}[X]$

Th. ▷ **Théorème de d'Alembert [6]-Gauss**

Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins un zéro dans $\mathbb{C}$.

On dit que $\mathbb{C}$ est algébriquement clos.

(La démonstration est hors programme.)

Conséquences :

- Dans $\mathbb{C}[X]$, un polynôme est irréductible ssi il est du premier degré
- Dans $\mathbb{C}[X]$, tout polynôme non constant est scindé.

donc, dans $\mathbb{C}[X]$, tout polynôme de degré $n \geqslant 1$ admet exactement n zéros
(en comptant leur ordre de multiplicité)

Ainsi, la décomposition primaire de P non constant de $\mathbb{C}[X]$ est

$$P = \lambda \prod_{i=1}^{p} (X - a_i)^{\alpha_i}$$

avec

$\lambda \in \mathbb{C}$ coefficient dominant de P
$a_1, a_2, \cdots, a_p \in \mathbb{C}$ deux à deux distincts
$\alpha_1, \cdots, \alpha_p \in \mathbb{N}^*$

6. Jean Le Rond D'ALEMBERT (1717-1783) mathématicien français.

Test 430 Décomposer dans $\mathbb{C}[X]$: X^2+X+1 X^4+X^2+1

Cas particulier : décomposition de X^n-1 dans $\mathbb{C}[X]$

$$\forall\, n\in\mathbb{N}^*,\quad X^n-1=\prod_{k=0}^{n-1}\left(X-e^{i\,k\,\frac{2\,\pi}{n}}\right)$$

Test 431 Décomposer dans $\mathbb{C}[X]$: X^6-1 X^6+1

15.2.4 Cas de $\mathbb{R}[X]$

Th. ▷ **Zéros complexes de $P\in\mathbb{R}[X]$**

$P\in\mathbb{R}[X]$, $z\in\mathbb{C}$:

z zéro complexe de $P \Leftrightarrow \overline{z}$ zéro de P

z zéro d'ordre k de $P \Leftrightarrow \overline{z}$ zéro d'ordre k de P

Test 432 Soit $P=2X^4+7X^2-8X^3+12X-15$.
Montrer que $2-i$ est un zéro complexe de P. (Pensez à Horner)
En déduire la décomposition de P dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.

Conséquence : les polynômes irréductibles de $\mathbb{R}[X]$ sont
- les polynômes du 1er degré
- les polynômes du 2ème degré de discriminant strictement négatif

Ainsi, la décomposition primaire de P non constant de $\mathbb{R}[X]$ est

$$P=\lambda\prod_{i=1}^{p}(X-a_i)^{\alpha_i}\prod_{j=1}^{q}(X^2+b_j\,X+c_j)^{\beta_j}$$

avec
$\lambda\in\mathbb{R}$ coefficient dominant de P
$a_1,a_2,\cdots,a_p\in\mathbb{R}$ deux à deux distincts
$(b_1,c_1),(b_2,c_2),\cdots,(b_q,c_q)\in\mathbb{R}^2$, couples distincts
deux à deux $\alpha_1,\cdots,\alpha_p,\beta_1,\cdots,\beta_q\in\mathbb{N}^*$

Test 433 Décomposer dans $\mathbb{R}[X]$: $X^{2n}-1$

Test 434 Décomposer X^4-1 dans $\mathbb{C}[X]$ et en déduire la décomposition dans $\mathbb{R}[X]$.
Ne pouvait-on pas obtenir directement ce résultat ?
Faire de même avec X^4+X^2+1.

15.3 Interpolation de Lagrange

On considère n scalaires distincts a_1, a_2, …, a_n.

Lemme de Lagrange

Pour tout $i\in[\![1,n]\!]$, il existe un unique polynôme $L_i\in\mathbb{K}_{n-1}[X]$ tel que pour tout $j\in[\![1,n]\!]$, $L_i(a_j)=\delta_i^j$. C'est

$$L_i(X)=\prod_{\substack{1\leq j\leq n\\ j\neq i}}\frac{X-a_j}{a_i-a_j}$$

Th. ▷ **Polynôme d'interpolation de Lagrange**

Soient $(b_1, b_2, \dots, b_n) \in \mathbb{K}^n$. Il existe un unique polynôme P de $\mathbb{K}_{n-1}[X]$ tel que $P(a_j) = b_j$ pour tout $j \in [\![1, n]\!]$. C'est

$$P = \sum_{i=1}^{n} b_i L_i$$

où les L_i sont ceux définis dans le lemme de Lagrange.

Test 435 Avec les notations précédentes, quels sont *tous* les polynômes P tels que $P(a_j) = b_j$ pour tout $j \in [\![1, n]\!]$?

Test 436 Avec les notations précédentes, simplifier $\displaystyle\sum_{i=1}^{n} L_i$.

15.4 Exercices

Exercice 1

$P, Q \in \mathbb{R}[X]$. Montrer que $\text{PGCD}(P, Q) = \text{PGCD}(P+Q, P-Q)$
Déterminer $A, B \in \mathbb{R}[X]$ normalisés qui vérifient

$$\text{PGCD}(A, B) = X + 2 \quad \text{et} \quad A^2 - B^2 = X^4 + 4X^3 + 3X^2 - 4X - 4$$

Exercice 2

"héritage du PGCD"...

1. Appliquer l'algorithme d'euclide pour trouver le PGCD de $A = X^6 - 1$ et $B = X^4 - 1$,
2. Refaire de même pour $A = X^{18} - 1$ et $B = X^{12} - 1$.

Exercice 3

Soient a et b deux entiers naturels.

1. Montrer que le reste de la division euclidienne (dans $K[X]$) de $X^a - 1$ par $X^b - 1$ est $X^r - 1$, où r est le reste de la division euclidienne (dans $\mathbb{Z}$) de a par b.
2. En déduire, à l'aide de l'algorithme d'Euclide que

$$(X^a - 1) \wedge (X^b - 1) = X^{a \wedge b} - 1$$

Exercice 4

Soient $P \in \mathbb{K}[X]$, $a, b \in \mathbb{K}$ distincts, et $\alpha = P(a)$, $\beta = P(b)$.

1. Quel est le reste de la division euclidienne de P par $(X-a)(X-b)$?
2. Trouver le reste de la division euclidienne de $(\cos\theta + X\sin\theta)^n$ par $X^2 + 1$.

Exercice 5

Déterminer les polynômes $P \in \mathbb{Q}_3[X]$ divisibles par $X+1$ et dont les restes des divisions par $X+2, X+3, X+4$ sont égaux.

Exercice 6

Calculer le pgcd de P et Q pour :

1. $P = X^4 + X^3 - 3X^2 - 4X - 1$ et $Q = X^3 + X^2 - X - 1$.
2. $P = X^4 - 10X^2 + 1$ et $Q = X^4 - 4X^3 + 6X^2 - 4X + 1$.
3. $P = X^5 - iX^4 + X^3 - X^2 + iX - 1$ et $Q = X^4 - iX^3 + 3X^2 - 2iX + 2$.

Exercice 7

Coefficients de Bézout

Montrer que les polynômes P et Q suivants sont premiers entre eux. Trouver $U, V \in \mathbb{K}[X]$ tels que $UP + VQ = 1$.

1. $P = X^4 + X^3 - 2X + 1$
   $Q = X^2 + X + 1$
2. $P = X^3 + X^2 + 1$
   $Q = X^3 + X + 1$

Exercice 8

Trouver les restes des divisions euclidiennes :

1. de X^{50} par $X^2 - 3X + 2$.
2. de $\left(X + \sqrt{3}\right)^{17}$ par $X^2 + 1$.
3. de $X^8 - 32X^2 + 48$ par $\left(X - \sqrt{3}\right)^3$.

Exercice 9

Trouver $\lambda, \mu \in \mathbb{C}$ tels que $X^2 + X + 1$ divise $X^5 + \lambda X^3 + \mu X^2 + 1$.

Exercice 10

Congruences

Soit $P \in \mathbb{R}[X]$ tel que les restes des divisions de P par $X^2 + 1$ et $X^2 - 1$ valent respectivement $2X - 2$ et $-4X$. Quel est le reste de la division de P par $X^4 - 1$?

15.5 Exercices Complémentaires

Exercice 1

Equation $A\,P + B\,Q = C$

1. Quelle condition doivent vérifier les trois polynômes A, B et C de $\mathbb{K}[X]$ pour que l'équation $A\,P + B\,Q = C$ admette au moins une solution ?
2. Trouver tous les couples (P, Q) dans les cas
$$A = X^2 + 1\,,\ B = X - 1\,,\ C = 1$$
$$A = X^3 - 1\,,\ B = X^2 - 1\,,\ C = X^2 - X$$

Exercice 2

Montrer que $\text{PGCD}\,(A, B) = 1 \quad \Rightarrow \quad \text{PGCD}\,(A + B, A) = 1$
En déduire que $\text{PGCD}\,(A, B) = 1 \quad \Rightarrow \quad \text{PGCD}\,(A + B, A\,B) = 1$

Exercice 3

$A \circ P | B \circ P \Rightarrow A | B$
Soient $A, B, P \in \mathbb{K}[X]$ avec P non constant. Montrer que si $A \circ P$ divise $B \circ P$, alors A divise B.

Exercice 4

Soit $P \in K[X]$.

1. Déterminer le reste de la division euclidienne de P par $(X-\alpha)(X-\beta)$ $(\alpha \neq \beta)$ connaissant le reste de la division euclidienne de P par $(X - \alpha)$ et $(X - \beta)$.
2. Soient $\alpha_1, \ldots, \alpha_n$ une famille d'éléments de K deux à deux distincts. Déterminer à l'aide de la formule d'interpolation de Lagrange, le reste de la divison euclidienne de P par $(X-\alpha_1)\ldots(X-\alpha_n)$ connaissant les restes de la division euclidienne de P par les $(X-\alpha_i)$.

Exercice 5

Faire la division euclidienne de t^6 par $1 + t^2$, en déduire la valeur de $\displaystyle\int_{-1}^{1} \frac{t^6}{1+t^2}\,dt$.

Exercice 6

Soit $P \in \mathbb{K}[X]$. Démontrer que les polynômes
— $PGCD(P(X), P(-X))$
— $PPCM(P(X), P(-X))$
sont des polynômes pairs ou impairs.

Exercice 7

Trouver l'ensemble des polynômes de $\mathbb{R}[X]$ vérifiant :
$P(1) = P'(1) = 0; P(3) = -8; P(X) + 2$ est divisible par $X - 2$.
Quel polynôme de plus petit degré vérifie ces conditions ?

Exercice 8

Donner une CNS pour que $X^p - 1 | X^n - 1$.
(On pourra regarder les racines.)

Exercice 9

Trouver un polynôme P tel que $x^2 + 1$ divise P et $x^3 + x^2 + 1$ divise $P + 1$.