Chapitre 17

Arithmétique des polynômes

Sommaire

I DIVISIBILITÉ

1) La division euclidienne

Théorème 17.1
Soient $A \in \mathbb{K}[X]$ *et* $B \in \mathbb{K}[X]$ ***non nul****, il existe un unique couple de polynômes* (Q,R) *tel que* $A = BQ + R$ *avec* $\deg(R) < \deg(B)$, Q *est appelé le quotient, et* R *le reste.*

Définition 17.1
Soient $A, B \in \mathbb{K}[X]$, *on dit que* B *divise* A *lorsqu'il existe un polynôme* Q *tel que* $A = Q \times B$, *notation* $B|A$.

Remarque 17.1 – *On définit ainsi une relation dans* $\mathbb{K}[X]$, *on peut vérifier que celle - ci est réflexive, transitive, mais elle n'est ni symétrique, ni antisymétrique. Plus précisément,* $B|A$ *et* $A|B$ *ssi il existe* $\lambda \in \mathbb{K}^*$ *tel que* $A = \lambda B$ *(on dit que* A *et* B *sont* ***associés****).*

Théorème 17.2
- *Si* $B \neq 0$, *alors* $B|A$ *si et seulement si le reste de la division euclidienne de* A *par* B *est nul.*
- *Si* $A \neq 0$ *et* $B|A$, *alors* $\deg(B) \leqslant \deg(A)$.
- *Si* $B|A$ *et* $B|C$, *alors* $\forall\, U,V \in \mathbb{K}[X], B|A\times U + C\times V$.

Preuve : Celle-ci est simple et laissée en exercice. □

Remarque 17.2 – *Il découle du dernier point que si* $B|A-C$ *et* $B|D-E$, *alors* $B|(A+D)-(C+E)$ *et* $B|AD-EC$, *en particulier, si* $B|A-C$ *alors* $\forall\ n \in \mathbb{N}, B|A^n - C^n$.

Notation : Soit $P \in \mathbb{K}[X]$, on note $P\mathbb{K}[X]$ l'ensemble des multiples de P : $P\mathbb{K}[X] = \{P\times Q \ /\ Q \in \mathbb{K}[X]\}$.

On vérifie facilement la propriété suivante :
$(P\mathbb{K}[X], +)$ est un groupe commutatif et $\forall B \in \mathbb{K}[X], \forall U \in P\mathbb{K}[X], BU \in P\mathbb{K}[X]$.

2) Congruences

Définition 17.2 (congruences)
Soient $A,B,P \in \mathbb{K}[X]$, *on dit que* A *est congru à* B *modulo* P *lorsque* $P \mid A-B$.
Notation : $A \equiv B \pmod{P}$.

Théorème 17.3
- *La relation de congruence modulo* P *est une relation d'équivalence.*
- *Soient* $A,B,C,D,P \in \mathbb{K}[X]$, *si* $A \equiv B \pmod{P}$ *et* $C \equiv D \pmod{P}$ *alors :*
$$AC \equiv BD \pmod{P} \text{ et } A+C \equiv B+D \pmod{P}.$$

On dit que la relation de congruence est compatible avec les opérations.

3) Diviseurs communs

Définition 17.3 (polynôme normalisé)
Soit A *un polynôme non nul, on appelle* A *normalisé le polynôme noté* $\tilde{A}$ *obtenu en divisant* A *par son coefficient dominant, ce polynôme est donc unitaire et associé à* A. *C'est l'unique polynôme unitaire associé à* A.

Définition 17.4 (diviseurs communs)
Pour $A \in \mathbb{K}[X]$, *on note* D_A *l'ensemble des diviseurs de* A. *Cet ensemble contient toujours* $\mathbb{K}^*$. *On notera* $D_{A,B} = D_A \cap D_B$ *l'ensemble des diviseurs communs à* A *et* B.

Remarque 17.3 –
- *Si* $A \neq 0$, *alors* D_A *est un ensemble infini, mais* $\{\deg(P) \ /\ P \in D_A\}$ *est fini car inclus dans* $[\![0;\deg(A)]\!]$.
- $D_0 = \mathbb{K}[X]$, *si* $\lambda \in \mathbb{K}^*$, $D_\lambda = \mathbb{K}^*$.
- *Si* A *est non nul,* $D_A = D_{\tilde{A}}$.

Théorème 17.4
Soient $A,B,Q,R \in \mathbb{K}[X]$, *si* $A = BQ+R$, *alors* $D_A \cap D_B = D_B \cap D_R$.

Application – Le théorème ci-dessus fournit un algorithme pour la recherche des diviseurs communs à A et B basé sur la division euclidienne : c'est **l'algorithme d'***Euclide*, rappelons son principe :

On remarque que si $B = 0$ alors $D_{A,B} = D_A$. On peut supposer désormais que $B \neq 0$ et on cherche à calculer $D = D_{A,B}$:

Étape 1 : on effectue la division euclidienne de A par B : $A = BQ_1 + R_1$ avec $\deg(R_1) < \deg(B)$. On a $D = D_{B,R_1}$, donc si $R_1 = 0$ alors $D = D_B$, sinon on passe à l'étape 2 :

Étape 2 : on effectue la division euclidienne de B par R_1 : $B = R_1Q_2 + R_2$ avec $\deg(R_2) < \deg(B)$. On a $D = D_{R_1,R_2}$, donc si $R_2 = 0$ alors $D = D_{R_1}$, sinon on passe à l'étape 3 ...

La suite des degrés des restes obtenus est une suite strictement décroissante d'entiers positifs, elle est donc nécessairement finie, *i.e.* il existe nécessairement un entier $n \geqslant 1$ tel que $R_n = 0$, l'ensemble cherché est donc $D = D_{R_{n-1}}$ (avec la convention $R_0 = B$).

II ÉLÉMENTS PREMIERS ENTRE EUX

1) Théorème de Bézout

Définition 17.5
Soient $A, B \in \mathbb{K}[X]$*, on dit que* a *et* b *sont premiers entre eux (ou* A *est premier avec* B*) lorsque le seul diviseur commun unitaire est* 1*, i.e.* $D_{A,B} = \mathbb{K}^*$.

Remarque 17.4 –
- *Dire que* A *est premier avec* B *revient à dire que le dernier reste non nul dans l'algorithme d'Euclide est égal à* 1 *une fois normalisé.*
- *Si* A *est premier avec* B*, alors au moins un des deux est non nul (sinon l'ensemble des diviseurs communs est* $\mathbb{K}[X]$*).*
- A *est premier avec* A *si et seulement si* $A \in \mathbb{K}^*$.

Théorème 17.5 (théorème de Bézout)
Soient $A, B \in \mathbb{K}[X]$*, alors* A *et* B *sont premiers entre eux si et seulement si il existe* $U, V \in \mathbb{K}[X]$ *tels que* $AU + BV = 1$*. Les polynômes* U *et* V *sont appelés coefficients de Bézout (non uniques en général).*

Preuve : C'est l'algorithme d'Euclide étendu, comme dans $\mathbb{Z}$. □

★**Exercice 17.1** *Soient* $A = X^3 + 1$ *et* $B = X^2 + 1$*. Montrer que* A *et* B *sont premiers entre eux, et déterminer une relation de Bézout.*

2) Conséquences

Théorème 17.6
- *Si* A *est premier avec* B *et si* A *est premier avec* C*, alors* A *est premier avec le produit* BC*. On en déduit que si* A *est premier avec* $C_1, \dots, C_n$*, alors* A *est premier avec le produit* $C_1 \times \dots \times C_n$.
- *Si* A *est premier avec* C*, si* $A \mid B$ *et si* $C \mid B$*, alors* $AC \mid B$.
- *Si* $A \mid BC$ *et si* A *est premier avec* C*, alors* $A \mid B$.

Preuve : Identique à celle dans $\mathbb{Z}$. □

III LE PLUS GRAND DIVISEUR COMMUN

1) Définition

Soient $A, B \in \mathbb{K}[X]$ non tous deux nuls, on sait que $D_{A,B} = D_R$ où R est le dernier reste non nul dans l'algorithme d'Euclide, on voit que les diviseurs communs à A et B ont un degré inférieur ou égal à celui de R. Soit D un diviseur commun de même degré que R, alors comme $D \mid R$ on a $R = \lambda Q$ avec $\lambda \in \mathbb{K}^*$, on en déduit que les polynômes R et D **normalisés** sont égaux.

Définition 17.6
Soient $A, B \in \mathbb{K}[X]$ *non tous deux nuls, le pgcd de* A *et de* B *le plus grand diviseur commun* ***unitaire****. Notation :* $\text{pgcd}(A, B)$ *ou* $A \wedge B$*, c'est le dernier reste non nul dans l'algorithme d'Euclide,* ***une fois normalisé****.*

Remarque 17.5 – *Il en découle que deux éléments* A *et* B *de* $\mathbb{K}[X]$*, non tous deux nuls, sont premiers entre eux si et seulement si* $\text{pgcd}(A, B) = 1$*. On remarquera au passage qu'un pgcd entre deux polynômes est unitaire.*

Théorème 17.7
Soient $A, B \in \mathbb{K}[X]$ *non tous deux nuls, et* D *un polynôme unitaire, alors* $D = \text{pgcd}(A, B)$ *si et seulement si* $D \mid A$, $D \mid B$ *et il existe deux polynômes* U *et* V *tels que* $D = AU + BV$.

Preuve : Si $D = \text{pgcd}(A, B)$ cela découle de l'algorithme d'Euclide étendu.
Si D est diviseur commun et si on a la relation, alors tout diviseur commun de A et B divise D et a donc un degré inférieur ou égal à celui de D, comme D est unitaire, c'est le pgcd de A et B. □

Théorème 17.8 (Calcul pratique d'un pgcd)
Si $A, B \in \mathbb{K}[X]$ *sont non tous deux nuls alors* $\forall Q \in \mathbb{K}[X], \text{pgcd}(A,B) = \text{pgcd}(A - BQ, B)$.

★**Exercice 17.2** *Calculer le pgcd entre* $X^4 - 1$ *et* $X^{10} - 1$.

2) Propriétés

Théorème 17.9 (caractérisations du pgcd)
Soient $A, B \in \mathbb{K}[X]$ *non tous deux nuls, et soit* $D \in \mathbb{K}[X]$ *non nul et unitaire. On a alors :*
$$D = \text{pgcd}(A,B) \iff \exists\, U, V \in \mathbb{K}[X] \text{ ***premiers entre eux*** } \textit{tels que } A = DU \textit{ et } B = DV.$$

Preuve : Si $D = \text{pgcd}(A,B)$ alors il existe $U, V \in \mathbb{K}[X]$ tels que $A = DU$ et $B = DV$, de plus il existe des polynômes U_1 et V_1 tels que $D = AU_1 + BV_1$, *i.e.* $D = DUU_1 + DVV_1$, D étant non nul et $\mathbb{K}[X]$ intègre, on en déduit que $1 = UU_1 + VV_1$ et donc U et V sont premiers entre eux.

Si $A = DU, B = DV$ avec $U \wedge V = 1$, alors D est un diviseur commun à A et B, d'après le théorème de Bézout, il existe $\alpha, \beta \in \mathbb{K}[X]$ tels que $\alpha U + \beta V = 1$, d'où $D = \alpha A + \beta B$, comme D est unitaire, on a $D = A \wedge B$. □

Théorème 17.10 (quelques propriétés du pgcd)
Soient $A, B \in \mathbb{K}[X]$ *non tous deux nuls :*

a) $\forall\, P \in \mathbb{K}[X]$, *si* $P \mid A$ *et* $P \mid B$, *alors* $P \mid \text{pgcd}(A,B)$.

b) $\text{pgcd}(A,B) = \text{pgcd}(\tilde{A}, \tilde{B})$.

c) $\forall\, K \in \mathbb{K}[X]$, *unitaire,* $\text{pgcd}(KA, KB) = K\,\text{pgcd}(A,B)$.

d) $\forall\, n \in \mathbb{N}$, $\text{pgcd}(A^n, B^n) = \text{pgcd}(A,B)^n$.

e) *Si* A *et* C *sont premiers entre eux, alors* $\text{pgcd}(A, BC) = \text{pgcd}(A,B)$.

Preuve : Pour le premier point : soit $D = \text{pgcd}(A,B)$, alors $D_{A,B} = D_D$ donc tout diviseur commun à A et B est un diviseur de D.

Pour le deuxième point : soit $D = \text{pgcd}(A,B)$, alors il existe $U, V \in \mathbb{K}[X]$ premiers entre eux tels que $A = DU$ et $B = DV$, d'où $KA = KAU$ et $KB = KDV$, donc $KD = \text{pgcd}(KA, KB)$ (KD est unitaire).

Pour le reste la preuve est identique à celle dans $\mathbb{Z}$. □

Théorème 17.11
Soient A *et* B *deux polynômes non tous deux nuls :*
- *les racines communes à* A *et* B *dans* $\mathbb{K}$, *sont exactement les racines dans* $\mathbb{K}$ *de* $\text{pgcd}(A,B)$.
- A *et* B *sont premiers entre eux si et seulement si ils n'ont pas de racine commune dans* $\mathbb{C}$.

Preuve : Soit $a \in \mathbb{K}$, alors $A(a) = B(a) = 0 \iff X - a \mid A$ et $X - a \mid B \iff X - a \mid \text{pgcd}(A,B)$. Si A et B sont premiers entre eux, alors $\text{pgcd}(A,B) = 1$ qui est sans racine dans $\mathbb{C}$, donc A et B n'ont pas de racine commune dans $\mathbb{C}$.

Si A et B n'ont pas de racine commune dans $\mathbb{C}$, alors leur pgcd n'a pas de racine dans $\mathbb{C}$, or $\mathbb{C}$ est algébriquement clos (théorème de D'Alembert Gauss), donc D est nécessairement constant, comme il est unitaire, $D = 1$. □

3) Généralisation

Soient A, B, C trois polynômes non tous nuls, l'ensemble des diviseurs communs à A, B et C est :

$$D_{A,B,D} = D_A \cap D_B \cap D_C = (D_A \cap D_B) \cap D_C = D_A \cap (D_B \cap D_C)$$

or on sait que $D_A \cap D_B = D_{A \wedge B}$, donc $D_{A,B,C} = D_{(A \wedge B) \wedge C} = D_{A \wedge (B \wedge C)}$. Ces deux polynômes étant unitaires, on a $(A \wedge B) \wedge C = A \wedge (B \wedge C)$ et ce polynôme est le plus grand (en degré) diviseur unitaire commun à A, B et C. Par définition ce nombre est le pgcd de A, B et C, on le note : $\text{pgcd}(A,B,C)$.

Théorème 17.12 (associativité du pgcd)
Soient A, B, C *trois polynômes avec* B *non nul, alors* $\text{pgcd}(A,B,C) = (A \wedge B) \wedge C = A \wedge (B \wedge C)$.

À retenir

L'associativité du pgcd permet de ramener le calcul au cas de deux polynômes.

Notons $D_1 = A \wedge B$ et $R = \text{pgcd}(A,B,C)$, alors $R = D_1 \wedge C$, donc il existe deux polynômes U_1 et W tels que $R = D_1U_1 + CW$, de même, il existe deux polynômes U_2 et V_1 tels que $D_1 = AU_2 + BV_1$, d'où en remplaçant, $R = AU_2U_1 + BV_1U_1 + cW = AU + BV + CW$ avec $U,V,W \in \mathbb{K}[X]$.

Réciproquement, si R est un diviseur commun unitaire, et si $R = AU + BV + CW$, alors il est facile de voir que tout diviseur commun à A, B et C est un diviseur de R et donc $R = \text{pgcd}(A,B,C)$, d'où le théorème :

Théorème 17.13

Soient A, B, C *trois polynômes non tous nuls et* R *unitaire, alors :*

$$R = \text{pgcd}(A,B,C) \iff R \in D_{A,B,C} \text{ et } \exists U,V,W \in \mathbb{K}[X],\ R = AU + BV + CW.$$

Définition 17.7

Soient A, B, C *trois polynômes non tous nuls, on dira que ces trois polynômes sont :*

- ***premiers entre eux dans leur ensemble*** *lorsque* $\text{pgcd}(A,B,C) = 1$.
- ***premiers entre eux deux à deux*** *lorsque* $\text{pgcd}(A,B) = \text{pgcd}(B,C) = \text{pgcd}(A,C) = 1$.

Attention!

Les deux notions ne sont pas équivalentes, ***la deuxième entraîne la première mais la réciproque est fausse*** *comme le montre l'exemple suivant :*

$\text{pgcd}((X+1)X,(X+1)(X+2),X(X+2)) = 1$ *mais* $\text{pgcd}(X(X+1),(X+1)(X+2)) = X+1$, $\text{pgcd}(X(X+1),X(X+2)) = X$ *et* $\text{pgcd}((X+1)(X+2),X(X+2)) = X+2$.

Il découle du théorème précédent :

Théorème 17.14 (de Bézout)

Soient A, B, C *trois polynômes non tous nuls, alors* A, B *et* C *sont premiers entre eux dans leur ensemble si et seulement si :*

$$\exists U,V,W \in \mathbb{K}[X],\ AU + BV + CW = 1.$$

Théorème 17.15 (caractérisation)

Soient A, B, C *trois polynômes non tous nuls et* R *unitaire, alors :*

$$R = \text{pgcd}(A,B,C) \iff \exists U,V,W \in \mathbb{K}[X],\ A = RU,\ B = RV \text{ et } C = RW \text{ avec } \text{pgcd}(U,V,W) = 1.$$

Preuve : Si $R = \text{pgcd}(A,B,C)$ alors il existe $\exists U,V,W \in \mathbb{K}[X]$, $A = RU$, $B = RV$ et $C = RW$. Il existe également des polynômes U_1,V_1 et W_1 tels que $R = AU_1 + BV_1 + CW_1$ d'où $1 = UU_1 + VV_1 + WW_1$ et donc $\text{pgcd}(U,V,W) = 1$.

Réciproquement, si $A = RU$, $B = RV$ et $C = RW$ avec $\text{pgcd}(U,V,W) = 1$. Il existe des polynômes U_1,V_1 et W_1 tels $1 = UU_1 + VV_1 + WW_1$, en multipliant par R il vient alors que $R = RUU_1 + RVV_1 + RWW_1 = AU_1 + BV_1 + CW_1$, ce qui entraîne que $R = \text{pgcd}(A,B,C)$ (car R est unitaire et diviseur commun à A, B et C). □

Remarque 17.6 – *La notion de pgcd s'étend de la même manière à n polynômes.*

IV LE PLUS PETIT MULTIPLE COMMUN

1) Définition

Théorème 17.16

Si A *et* B *sont non nuls, il existe un unique polynôme* M *unitaire dans* $\mathbb{K}[X]$ *tel que :*

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X].$$

Preuve : $\{\deg(P) \ /\ P \in A\mathbb{K}[X] \cap B\mathbb{K}[X],\ P \neq 0\}$ contient $\deg(AB)$, il existe donc un multiple commun non nul de degré minimal, quitte à le normaliser, on peut le supposer unitaire, et on le note M. Il est facile de voir que $M\mathbb{K}[X] \subset A\mathbb{K}[X] \cap B\mathbb{K}[X]$. Si $P \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$, on effectue la division de P par M, $P = MQ + R$ avec $\deg(R) < \deg(M)$, d'où $R = P - MQ$, on vérifie alors que R est aussi dans $A\mathbb{K}[X] \cap B\mathbb{K}[X]$. Si $R \neq 0$ alors $\deg(R) \geqslant \deg(M)$ car M est de degré minial, ceci est absurde, donc $R = 0$ et $P = MQ$, d'où $A\mathbb{K}[X] \cap B\mathbb{K}[X] \subset M\mathbb{K}[X]$, et finalement on a bien l'inégalité.

Si $M'\mathbb{K}[X] = M\mathbb{K}[X]$ avec M' unitaire, alors M et M' se divisent mutuellement, ils sont donc associés et unitaires d'où $M = M'$. □

Il découle de ce théorème que C est un multiple commun à A et B si et seulement si $C \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$, ce qui équivaut à $C \in M\mathbb{K}[X]$, c'est à dire $M \mid C$. Ceci entraîne en particulier : $\deg(M) \leqslant \deg(C)$.

Définition 17.8

Soit $A, B \in \mathbb{K}[X]$, *non nuls, et soit* $M \in \mathbb{K}[X]$ ***unitaire***, *on dit que* M *est le ppcm de* A *et* B *lorsque* $A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$. *Notation :* $M = \text{ppcm}(A, B)$ *ou encore* $M = A \vee B$.

Théorème 17.17 (caractérisation du ppcm)

Soient $A, B \in \mathbb{K}[X]$, *non nuls, et soit* $M \in \mathbb{K}[X]$ *unitaire alors :*

$$M = \text{ppcm}(A, B) \iff \exists\, U, V \in \mathbb{K}[X] \text{ ***premiers entre eux*** } \textit{tels que } M = AU = BV.$$

Preuve : On suppose $A, B \in \mathbb{K}[X]$, non nuls.

Si $M = \text{ppcm}(A, B)$: alors $A \mid M$ et $B \mid M$. Donc il existe $U, V \in \mathbb{K}[X]$ tels que $M = AU = BV$, soit $D = \text{pgcd}(U, V)$ alors il existe $\alpha, \beta \in \mathbb{K}[X]$ premiers entre eux tels que $U = D\alpha$ et $V = D\beta$, d'où $M = AD\alpha = BD\beta$, mais alors $M_0 = A\alpha = B\beta$ est un multiple commun à A et B donc $\deg(M) \leqslant \deg(M_0)$ ce qui entraîne $D = 1$ (car D est unitaire et $M = M_0 D$).

Si $\exists U, V \in \mathbb{K}[X]$ premiers entre eux tels que $M = AU = BV$, alors $A \mid M$ et $B \mid M$, il existe $\alpha, \beta \in \mathbb{K}[X]$ tels que $U\alpha + V\beta = 1$, soit M_0 un multiple commun non nul, alors $M_0 = M_0 U\alpha + M_0 V\beta$, on en déduit que $M \mid M_0$ et donc $\deg(M) \leqslant \deg(M_0)$, ce qui prouve que $M = \text{ppcm}(A, B)$. □

2) Propriétés

Théorème 17.18

Soient $A, B \in \mathbb{K}[X]$, *non nuls :*

a) $\forall\, P \in \mathbb{K}[X]$, *si* $A \mid P$ *et* $B \mid P$ *alors* $\text{ppcm}(A, B) \mid P$.

b) Si A *et* B *sont premiers entre eux, alors* $\text{ppcm}(A, B) = \tilde{A}\tilde{B}$.

c) $\forall\, K \in \mathbb{K}[X]$, *unitaire,* $\text{ppcm}(KA, KB) = K\,\text{ppcm}(A, B)$.

d) $\text{ppcm}(A, B) \times \text{pgcd}(A, B) = \tilde{A}\tilde{B}$.

e) $\forall\, n \in \mathbb{N}, \text{ppcm}(A^n, B^n) = \text{ppcm}(A, B)^n$.

Preuve : Analogue au cas des entiers. □

V POLYNÔMES IRRÉDUCTIBLES, DÉCOMPOSITION

1) Définition

Définition 17.9

Un polynôme $P \in \mathbb{K}[X]$ *est dit* ***irréductible*** *sur* $\mathbb{K}$ *lorsque* P *est non constant et que ses seuls diviseurs unitaires sont* 1 *et* $\tilde{P}$. *L'ensemble des éléments irréductibles normalisés de* $\mathbb{K}[X]$ *est noté* $\mathscr{I}_{\mathbb{K}[X]}$.

☞**Exemples** :

- Tout polynôme de degré 1 est irréductible, donc $\forall\, \lambda \in \mathbb{K}, X + \lambda \in \mathscr{I}_{\mathbb{K}[X]}$.
- Tout polynôme de degré 2 **sans racine dans** $\mathbb{K}$ est irréductible dans $\mathbb{K}[X]$. Cependant cette propriété ne se généralise pas au delà du degré 2, par exemple : $X^4 + 1$ est sans racine dans $\mathbb{R}$, mais ce polynôme est réductible car $X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$.
- La notion de polynôme irréductible dépend du corps $\mathbb{K}$, par exemple, $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais pas dans $\mathbb{C}[X]$. De même, le polynôme $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{R}[X]$.

Théorème 17.19

Dans $\mathbb{C}[X]$, *les polynômes irréductibles unitaires sont les polynômes unitaires de degré* 1, *c'est à dire :*

$$\mathscr{I}_{\mathbb{C}[X]} = \{X + a \;/\; a \in \mathbb{C}\}.$$

Dans $\mathbb{R}[X]$, *les polynômes irréductibles sont les polynômes unitaires de degré* 1, *plus les polynômes unitaires de degré* 2 ***sans racines réelles***. *C'est à dire :*

$$\mathscr{I}_{\mathbb{R}[X]} = \{X + a \;/\; a \in \mathbb{R}\} \cup \left\{X^2 + pX + q \;/\; p, q \in \mathbb{R}, p^2 - 4q < 0\right\}.$$

Preuve : Pour $\mathbb{C}[X]$ cela découle du théorème de *D'Alembert*.

Dans $\mathbb{R}[X]$: les polynômes annoncés sont bien irréductibles unitaires. Soit $P \in \mathscr{I}_{\mathbb{K}[X]}$, avec $\deg(P) \geqslant 2$ alors P admet des racines complexes, et celles-ci sont non réelles (P est irréductible de degré supérieur à 1), soit α l'une d'elles, alors $\overline{\alpha}$ est également racine de P (et distincte de α), donc dans $\mathbb{C}[X]$ le polynôme P est divisible par $(X-\alpha)(X-\overline{\alpha}) = X^2 + pX + q \in \mathbb{R}[X]$ avec $p^2 - 4q < 0$. Mais alors P est divisible dans $\mathbb{R}[X]$ par $X^2 + pX + q$ (unicité du quotient et du reste), or $P \in \mathscr{I}_{\mathbb{K}[X]}$, donc nécessairement $P = X^2 + pX + q$. □

Propriétés élémentaires :

a) Si P est irréductible, alors pour tout polynôme Q, soit $P \mid Q$ soit $\operatorname{pgcd}(P,Q) = 1$.
Preuve : Soit $D = \operatorname{pgcd}(P,Q)$, $D \mid P$ donc $D = 1$ ou $D = \tilde{P}$. □

b) Si $P \in \mathbb{K}[X]$ est non constant, alors P possède au moins un diviseur irréductible.
Preuve : Soit $B = \{\deg(d) \ / \ d \mid P \text{ et } d \notin \mathbb{K}^*\}$, alors B est une partie de $\mathbb{N}$ non vide ($\deg(P) \in B$), soit Q un diviseur de P avec $\deg(P) \in B$ **minimal**, si $D \mid Q$ avec D normalisé et $D \notin \mathbb{K}^*$, alors $D \mid P$ et donc $\deg(D) \in B$, d'où $\deg(D) \geqslant \deg(Q)$, or $D \mid Q$, donc $\deg(D) \leqslant \deg(Q)$ et finalement $\deg(D) = \deg(Q)$, d'où $D = \tilde{Q}$ et donc Q est irréductible. □

c) L'ensemble $\mathscr{I}_{\mathbb{K}[X]}$ est infini, puisque tout polynôme $X + a$ où $a \in \mathbb{K}$ est irréductible unitaire.

d) Si P est irréductible et si $P \mid AB$, alors $P \mid A$ ou $P \mid B$.
Preuve : Supposons que P ne divise pas A, alors $\operatorname{pgcd}(P,A) = 1$ et par conséquent $P \mid B$ (d'après le théorème de Gauss). □

2) Décomposition en facteurs irréductibles

Théorème 17.20 (décomposition en produit de facteurs irréductibles)
Tout élément $Q \in \mathbb{K}[X]$ non constant, est un produit d'éléments irréductibles. Plus précisément, il existe $r \geqslant 1$, il existe $P_1, \ldots, P_r \in \mathscr{I}_{\mathbb{K}[X]}$, il existe des entiers $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$, il existe $\lambda \in \mathbb{K}^*$ tels que :

$$Q = \lambda \times P_1^{\alpha_1} \times P_2^{\alpha_2} \times \ldots \times P_r^{\alpha_r}.$$

Preuve : On a $Q = \lambda \times \tilde{Q}$ avec λ le coefficient dominant de Q. On se ramène ainsi au cas où Q est unitaire.

Par récurrence sur $\deg(Q)$: pour $\deg(Q) = 1$ il n'y a rien à montrer. Supposons le théorème démontré jusqu'au rang k, si $\deg(Q) = k+1$ alors Q admet au moins un diviseur irréductible unitaire P, donc $Q = PR$, si $R = 1$ alors Q est irréductible, sinon R est un produit de facteurs irréductibles (HR), donc Q aussi. □

Théorème 17.21 (unicité de la décomposition)
Si $Q \in \mathbb{K}[X]$ s'écrit sous la forme : $Q = \lambda \times P_1^{\alpha_1} \times \ldots \times P_r^{\alpha_r} = \mu \times Q_1^{\beta_1} \times \ldots \times Q_s^{\beta_s}$,
avec $P_1, \ldots, P_r \in \mathscr{I}_{\mathbb{K}[X]}, \alpha_1, \ldots, \alpha_r \in \mathbb{N}^*, Q_1, \ldots, Q_s \in \mathscr{I}_{\mathbb{K}[X]}, \beta_1, \ldots, \beta_s \in \mathbb{N}^*$, et $\lambda, \mu \in \mathbb{K}^*$, alors $r = s$, $\lambda = \mu$ et il existe une permutation σ de $[\![1;r]\!]$ telle que pour $i \in [\![1;r]\!]$, $P_i = Q_{\sigma(i)}, \alpha_i = \beta_{\sigma(i)}$. La décomposition est unique [à l'ordre près].

Preuve : Identique à celle des entiers. □

3) Notion de P-valuation

Si Q est un polynôme non nul et P un polynôme irréductible, alors l'ensemble $\{k \in \mathbb{N} \ / \ P^k \mid Q\}$ est non vide (contient 0) et majoré par $\deg(Q)$, cet ensemble admet donc un maximum :

Définition 17.10
Soit $P \in \mathscr{I}_{\mathbb{K}[X]}$ et Q polynôme non nul, on appelle P-valuation de Q, notée $v_P(Q)$, le plus grand entier k tel que $P^k \mid Q$. La définition s'étend au polynôme nul en posant $v_P(0) = +\infty$.

Remarque 17.7 :

- $v_P(Q) = k \iff P^k \mid Q \text{ et } P^{k+1} \nmid Q \iff \boxed{\exists\, T \in \mathbb{K}[X], Q = P^k T \text{ avec } P \nmid Q}$.
- $v_P(Q) \geqslant 1 \iff P \mid Q$, *auquel cas $v_P(Q)$ est la puissance de P dans la décomposition de Q en facteurs irréductible.*
- $\{k \in \mathbb{N} \ / \ P^k \mid Q\} = [\![0; v_P(Q)]\!]$.

À retenir

Si Q est non constant, la décomposition de Q en produit de facteurs irréductibles s'écrit :

$$Q = \lambda_Q \prod_{P \in \mathscr{I}_{\mathbb{K}[X]}} P^{v_P(Q)}.$$

En effet, seul un nombre fini de valuations sont non nulles (les autres donnent un facteur égal à 1).

Théorème 17.22 (Propriétés)

Soient Q, R *deux polynômes, on a :*

a) $\forall P \in \mathscr{I}_{\mathbb{K}[X]},\ v_P(QR) = v_P(Q) + v_P(R)$.

b) $\forall P \in \mathscr{I}_{\mathbb{K}[X]},\ v_P(Q+R) \geqslant \min(v_P(Q); v_P(R))$.

c) $Q \mid R \iff \forall P \in \mathscr{I}_{\mathbb{K}[X]},\ v_P(Q) \leqslant v_P(R)$.

d) Si Q *et* R *sont non nuls alors* $\forall P \in \mathscr{I}_{\mathbb{K}[X]}$ *:*

$$v_P(Q \wedge R) = \min(v_P(Q); v_P(R)) \text{ et } v_P(Q \vee R) = \max(v_P(Q); v_P(R)).$$

Preuve : Analogue au cas des entiers. □

À retenir : formules du pgcd et du ppcm

Il découle du théorème ci-dessus que :

$$\text{pgcd}(Q,R) = \prod_{P \in \mathscr{I}_{\mathbb{K}[X]}} P^{\min(v_P(Q); v_P(R))} \text{ et } \text{ppcm}(Q,R) = \prod_{P \in \mathscr{I}_{\mathbb{K}[X]}} P^{\max(v_P(Q); v_P(R))}.$$

4) Applications

Comme dans $\mathbb{Z}$:

- Si P est non constant, alors la décomposition de P en produit de facteurs irréductibles permet de trouver tous les diviseurs de P.
- Si P, Q sont non constants, alors à partir de leur décomposition en produit de facteurs irréductibles, on peut calculer pgcd(P, Q) et ppcm(P, Q).

★**Exercice 17.3** *Dans* $\mathbb{C}[X]$, *montrer que pour* $n, m \in \mathbb{N}^*$, *on a* $\text{pgcd}(X^n - 1, X^m - 1) = X^d - 1$ *où* $d = \text{pgcd}(n, m)$.

VI SOLUTION DES EXERCICES

Solution 17.1 *L'algorithme d'Euclide étendu donne un dernier reste non nul égal à* 2 *avec la relation :* $2 = (X+1)A - (X^2 + X - 1)B$, *il suffit de tout diviser par* 2.

Solution 17.2 *En appliquent l'algorithme d'Euclide, le dernier reste non nul normalisé est* $D = X^2 - 1$ *qui est donc le pgcd.*

Solution 17.3 *Il existe* $u, v \in \mathbb{Z}$ *tels que* $nu + mv = d$, *on en déduit que* $z^n = z^m = 1$ *si et seulement si* $z^d = 1$, *les racines du pgcd sont donc les racines* d^{es} *de l'unité, comme les racines de* $X^n - 1$ *sont simples, celles du pgcd le sont aussi, ce qui donne le résultat.*