N° d'ordre :
N° de série :

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Superieur et de la Recherche Scientifique

---

UNIVERSITÉ ECHAHID HAMMA LAKHDAR
EL OUED

FACULTÉ DES SCIENCES ET DE TECHNOLOGIE

Mémoire de fin d'étude

LICENCE ACADEMIQUE

Domaine: Mathématiques et Informatique
Filière: Mathématiques
Spécialité: Modélisation mathématiques & simulation numérique

Thème

Les polynômes

Présenté par:
CHIBANI Djafer
LEKHOUIMES Khaled
SOLTANI Tedjani

Sous la supervision de :

DJEDIDI Mohamed yacine

Année universitaire 2014 – 2015

Remerciement

La louange est à Allah, qui nous a facilité l'accomplisse de ce travail de recherche chose ne peut être qu'avec la volonté de Dieu -à lui la toute puissance et la Majesté- et que la louange initiale et finale appartient à allah,Seigneur des mondes

*Aussi, il nous fait plaisir que nous, au commencement de ce travail, présentons nos grands remerciments, estimations et reconnaissances à notre encadreur puissant " **Djedidi Mohamed Yacine** " de nous avoir encouragé moralement la durée de recherche et que ce travail est le fruit de ces encouragements*

Nous présentons nos véridiques remerciments à toute personne, du proche ou du loin ,qui nous adonnait un coup de main, à fin de términer ce travail de recherche

Enfin, nous remercions vivement notres familles pour l'aide matérielle et morale durant la période de préparation

"Que la grace et la paix soient sur notre profet Muhammad ainsi que sur sa famille et ses compagnons".

Table des matières

Introduction **1**

Notations **2**

1 L'anneau des polynômes à une indéterminée **3**

1.1 structure d'anneau 3

1.1.1 anneaux 3

1.1.2 Sous anneaux 3

1.1.3 Anneau intégre 4

1.2 Corps 4

1.3 L'anneau des polynômes 5

1.4 Opération sur les polynômes 5

1.4.1 Egalité 5

1.4.2 Addition 6

1.4.3 Multiplication 6

1.4.4 Multiplication par un scalaire 6

1.5 Degré et valuation de polynôme 7

1.5.1 Degré de polynôme 7

1.5.2 Valuation de polynôme 8

1.6 Dérivation des polynômes 8

1.7 Division euclidienne des polynômes 10

1.7.1 Proporiétés de la divisibilité 10

1.8 Le PGCD et PPCM des polynômes 12

1.8.1 Le plus grand commun diviseur PGCD 12
1.8.2 Algorithme d'Euclide 14
1.8.3 Polynômes premiers entre eux 15
1.8.4 Pgcd de plusieurs polynômes 15
1.8.5 Plus petit comun multiple des polynomes PPCM 16

2 Factorisation des polynômes **18**
2.1 Racine d'un polynôme 18
2.2 Polynômes irréductibles 19
2.2.1 Critères d'irréductibilité 20
2.3 Théoreme de factorisation 20

3 Résultant et discriminant **24**
3.1 Résultant de deux polynômes 24
3.2 Discriminant 30
3.2.1 Séparation et isolation des racines réelles 31

Bibliographie **33**

Introduction générale

L'objet de ce travail est l'anneau des polynômes à une indétirminé et sa proporieté ,ansi la résolution et l'éxistence des racines de polynôme.

Pour le premier chapitre le sujet d'étude est l'algèbre des structures anneau, sous anneau, anneau intègre, Corps, l'anneau de polynômes, les opérations sur les polynômes, division Euclidienne, P gcd et $PPCM$ des polynômes.

Deuxième chapitre nous étudions la factorisation des polynômes, polynôme irréductible et Critères d'irréductibilité.

Troisième chapitre nous consentirons sur calculer le résultant d'un polynôme, discriminent, séparation et isolation des racines réelles.

.

Notations

K	L'anneau.
$\mathbb{N}$	L'ensemble des nombres entiers naturels.
$\mathbb{Z}$	L'anneau des nombres rationnels.
$\mathbb{R}$	Corps des nombres réels.
$\mathbb{C}$	Corps des nombres complexes.
$\mathbb{N}^*$	L'ensemble des nombres entiers naturels non nul.
$K[X]$	L'anneau des polynômes à une indéterminée X à coefficients dans l'anneau K.
$\mathbb{R}[X]$	L'anneau des polynômes à une indéterminée X à coefficients réels.
$\mathbb{C}[X]$	L'anneau des polynômes à une indéterminée X à coefficients complexes.
$P(X)$	Le polynôme de $K[X]$.
$\deg(P)$	degré de polynôme $P(X)$.
$Val(P)$	Le valuation de polynôme $P(X)$.
$P'(X)$	Le polynôme derive de polynôme.
$A\|B$	A divisibilte sur B.
$p\gcd$	Plus grand commun diviseur.
$PPCM$	Plus petit commun multiple..
$\max(A)$	Maximum l'ensemble A.
$\inf(A)$	L'inferieur de l'ensemble A.
F_n	Le modulo de n.
$S(P,Q)$	La matrice de Sylvester de P et Q.
$Res(P,Q)$	Le résultant de P et Q.
$Disc(P)$	Discriminant de P.

Chapitre 1

L'anneau des polynômes à une indéterminée

1.1 structure d'anneau

1.1.1 anneaux

Définition 1.1.1 *Soit A un ensemble non vide muni de deux lois de compisition interne notée $+$ (addition) et $\cdot$ (multiplication) on dit que $(A, +, \cdot)$ est un anneau si:*

1) $(A, +)$ est un groupe commutatif.

2) la loi $\cdot$ est associative.

3) la loi $\cdot$ est distributive par rapport à la loi $+$,

ce qui signifie que:

$\forall\, (a, b, c) \in A^3$ *alors*

$$a \cdot (b + c) = \ a \cdot b \ + \ a \cdot c$$

$$(b + c) \cdot a \ = \ b.a \ + \ b \cdot c$$

Si la loi $(\cdot)$ est commutative, on dit alors que l'anneau A est commutative.

S'il existe un élement neutre pour la loi $(\cdot)$ on dit que A est un anneau unitaire.

1.1.2 Sous anneaux

Définition 1.1.2 *Soit A anneau, on appelle* ***sous anneau*** *de A tout partie B non vide de A qui vérifie les conditions suivantes:*

1) $\forall x, y \in B$

$$x - y \in B$$

2) $\forall x, y \in B$

$$x.y \in B$$

Remarque 1.1.1 $1_A \in B$ *si* A *unitaire*

1.1.3 Anneau intégre

Définition 1.1.3 *Soit* A *un anneau et* $a \in A$, a *est un diviseur de zéro si et seulement si s'il existe* $b \in A$ *non nul tel que:*

$$a.b = 0 \Longrightarrow (a = 0 \ ou \ b = 0).$$

Exemple 1.1.1 *Dans l'anneau* $\mathbb{Z}/6\mathbb{Z}$ *on a* 2 *et* 3 *sont des diviseurs de zéro.*

Définition 1.1.4 *Un anneau* $(A, +, \cdot)$ *est dit* ***intégre*** *si et seulement si* $A \neq \{0\}$ *et si* A *ne possède pas des diviseurs de zéro.*

Exemple 1.1.2 *L'anneau* $\mathbb{Z}$ *des nombres entiers est un anneau intégre.*

1.2 Corps

Définition 1.2.1 *Soit* $(K, +, \cdot)$ *un anneau unitair, on dit que* K *est un corps si:*

$$(\forall x \in K \setminus \{0\}), (\exists y \in K \setminus \{0\})/xy = 1_{\mathbb{k}}.$$

Exemple 1.2.1 *L'ensemble* $\mathbb{Q}$ *des nombres rationnels, muni de l'addition et de la multiplication ordinaire,*
est un corps de même l'ensemble $\mathbb{R}$ *des nombres réels et l'ensemble* $\mathbb{C}$ *des nombres complexes.*

1.3 L'anneau des polynômes

Définition 1.3.1 *Un polynôme P à coefficient dans K est une expression de la forme:*

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0,$$

avec $n \in \mathbb{N}$ et $a_0, a_1, ..., a_n \in K$.

_ L'ensemble des polynômes est noté $K[X]$.

– Les a_i sont appelés les coefficients du polynôme.

– Si tous les coefficients a_i sont nuls, P est appelé le polynôme nul, il est noté $P_0(X) = 0, \ \forall X \in K$.

Remarque 1.3.1 *Les polynômes comportant un seul terme non nul (du type $a_k X^k$) sont appelés **monômes**.*

Définition 1.3.2 *Soit $P(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$, un polynôme avec $a_n \neq 0$. On appelle **terme dominant** le monôme $a_n X^n$, le coefficient a_n est appelé **le coefficient dominant** de P.*
*Si le coefficient dominant est $a_n = 1$, on dit que P est **un polynôme unitaire**.*

Remarque 1.3.2 *Tout polynôme est donc une somme finie de monôme.*

Exemple 1.3.1 *Soit P est un polynôme tell que: $P(X) = X^n - 1$*
$P(X)$ est unitaire et il est somme de deux monômes: X^n et -1,
telque X^n est le terme dominant.

1.4 Opération sur les polynômes

1.4.1 Egalité

Définition 1.4.1 *Soient $P(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$*
et $Q(X) = b_n X^n + b_{n-1} X^{n-1} + ... + b_1 X + b_0$
deux polynômes à coefficients dans K.
Alors $P = Q$ si et seulement si $a_i = b_i$ pour tout $i \in \{1...n\}$ et on dit que P et Q sont égaux.

1.4.2 Addition

Définition 1.4.2 *Soient* $P(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$
et $Q(X) = b_nX^n + b_{n-1}X^{n-1} + ... + b_1X + b_0$
deux polynômes à coefficients dans K.
On définit:

$$\begin{aligned} P(X) + Q(X) &= (P+Q)(X) \\ &= (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + ... + (a_1 + b_1)X + (a_0 + b_0) \\ &= \sum_{i=1}^{n}(a_i + b_i)X^i \end{aligned}$$

1.4.3 Multiplication

Définition 1.4.3 *Soient* $P(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$
et $Q(X) = b_mX^m + b_{m-1}X^{m-1} + ... + b_1X + b_0$ *deux polynômes à coefficients dans* K. *On définit:*

$$P(X) \times Q(X) = c_rX^r + c_{r-1}X^{r-1} + ... + c_1X + c_0$$

tellque $c_k = \sum_{k=i+j} a_ib_j$ *pour* $k \in (0....r)$.

1.4.4 Multiplication par un scalaire

Définition 1.4.4 *Soient* $P(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 = \sum_{i=1}^{n} a_iX^i$ *polynômes à coefficients dans* K *et Soit* $\lambda \in K$ *alors:*
$\lambda \cdot P(X\ ) = \lambda.\sum_{i=1}^{n} a_iX^i = \sum_{i=1}^{n} \lambda.a_iX^i$ *est le polynôme dont le i-ème coefficients est* λa_i

Exemple 1.4.1 *Soient* $P(X) = aX^3 + bX^2 + cX + d$ *et* $Q(X) = \alpha X^2 + \beta X + \gamma$ *Alors:*
1) $P = Q$ *si et seulement si* $a = 0, b = \alpha, c = \beta$ *et* $d = \gamma$.
2) $P + Q = aX^3 + (a+\alpha)X^2 + (c+\beta)X + (d+\gamma)$.
3) $P \times Q = a\alpha X^5 + (a\beta + b\alpha)X^4 + (a\gamma + b\beta + c\alpha)X^3 + (b\gamma + c\beta + d\alpha)X^2 + (c\gamma + d\beta)X + d\gamma$.

1.5 Degré et valuation de polynôme

1.5.1 Degré de polynôme

Définition 1.5.1 *Soient* $P(X) = \sum_{i=1}^{n} a_i X^i$ *un polynôme à coefficients dans* K*.On appelle le degré de* P*, on le note* $\deg P$ *le plus grand entier* i *tel que* $a_i \neq 0$*.*

Définition 1.5.2 *Pour le degré du polynôme nul (* $P_0(X) = 0$ *) on pose par convention* $\deg(P_0(X) = 0) = -\infty$*.*
Un polynôme de la forme $P(X) = a_0$ *avec* $a_0 \in K$ *est appelé un polynôme constant.*
Si $a_0 \neq 0$*, son degré est* 0*.*

Proposition 1.5.1 *Soient* P, Q *deux polynômes à coefficients dans* K*.*
Alors:

$$\deg(P+Q) \leqslant max(degP, degQ) \tag{1}$$

$$\deg(P \times Q) \leqslant degP + degQ \tag{2}$$

Preuve.

1) On a:
$deg(P+Q) = degP$ si $degP > degQ$,
$deg(P+Q) = degQ$ si $degQ > degP$,
et que si $degP = degQ$, alors $deg(P+Q) \leqslant degP$.
Il peut cependant n'a pas avoir égalité (prendre par exemple $P(X) = X^2$ et $Q(x) = -X^2$).
2) Supposant P et Q non nuls.
(pour que cet énoncé soit valable si l'un des deux polynômes est nul).
$P = (a_p)_{p\geqslant 0}$, $Q = (b_q)_{q\geqslant 0}$ et posant $m = \deg(P)$, $n = \deg(Q)$.
pour $p > m$ (resp. $q > n$) on a: $a_p = 0$ (resp. $b_q = 0$).
Donc, pour $p + q > m + n$, on a: $a_p b_q = 0$.
Cela prouve que le terme $c_M = \sum_{p+q=M} a_p b_q$ du polynôme $PQ = (c_n)_{n\geqslant 0}$ est nul pour $M > m + n$, donc (2) est établie.

■

Exemple 1.5.1 *Soient* P, Q *et* H *des polynômes à coefficients dans* K*.*
1) $P(X) = X^3 - 5X + 2$ *est un polynôme de degré* 3*.*

2) $Q(X) = X^n + 1$ *est un polynôme de degré* n.

3) $H(X) = 2$ *est un polynôme constant de degré* 0.

1.5.2 Valuation de polynôme

Définition 1.5.3 *Soient* $P(X) = \sum_{i=1}^{n} a_i X^i$ *un polynôme à coefficients dans* K.
On appelle le valuation de P *On le noté* $V(P) = k$ *le plus petite entier* k *telque* $a_k \neq 0$.

Proposition 1.5.2 *Soient* $P(X)$ *et* $Q(X)$ *deux polynômes à coefficients dans* K.

$$\begin{aligned} V(P+Q) &\geqslant \inf(V(P), V(Q)) \\ V(P-Q) &\geqslant V(P) + V(Q) \end{aligned}$$

Exemple 1.5.2 *Soit* $P \in K[X]$ *telque*
$P(X) = X^5 + 4X^3 + 2X$ *alors:* $V(P) = 1$

1.6 Dérivation des polynômes

Définition 1.6.1 *Soit* $P(X) = \sum_{i=0}^{n} a_i X^i$ *un polynôme à coefficients dans* K.
On appelle ***polynôme dérivé*** *de* P *le polynôme:*

$$P' = \sum_{i=1}^{n} i a_i X^{i-1}$$

On a en particulier:

$$\forall p \in \mathbb{N}, (X^p)' = \begin{cases} pX^{p-1} & si \;\; p \geqslant 1 \\ 0 & si \; p = 0 \end{cases}$$

Remarque 1.6.1 *On rappelle que si* K *est un corps quelconque et* $a \in K$, *alors pour* $n \in \mathbb{N}$, *l'expression* na *ne représente pas un produit dans ce corps* K, *mais l'addition de* n *termes égaux à* a.

ie $na = a + a + ... + a$.

Dans des cas trés particuliers, ce terme peut être nul alors que a et n sont tous deux non nuls,
ce qui peut conduire à des resultats surprenants.

Proposition 1.6.1 *Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans K et $\lambda \in \mathbb{R}$ on a:*
1) $(P+Q)' = P' + Q'$.
2) $(\lambda P)' = \lambda P'$
3) $(PQ)' = P'Q + PQ'$

Preuve.
(1) et (2) evident.
3) On pose $P(X) = \sum_{n\geqslant 1} a_n X^n, Q(X) = \sum_{n\geqslant 1} b_n X^n$
Le n-ième coefficient de $P'Q + PQ'$ est:

$$\begin{aligned} V_n &= \sum_{k=0}^{n} a_k \cdot (n-1+k) b_{n-1+k} + \sum_{k=0}^{n} (k+1) a_{k+1} \cdot b_{n-k} \\ &= \sum_{k=0}^{n} a_k (n-k+1) b_{n-1+k} + \sum_{k=0}^{n+1} k a_k b_{n-k+1} \\ &= (n+1) a_0 b_{n+1} + \sum_{k=0}^{n} [(n-k+1)+k] a_k b_{n+1-k} + (n+1) a_{n+1} b_0 \\ &= (n+1) \sum_{k=0}^{n+1} a_k b_{n+1-k} \end{aligned}$$

■

Proposition 1.6.2 *Soient $P(X)$ et $Q(X)$ deux polynômes à coefficients dans K.*
1) Les polynômes constants sont ceux dérivé est nul.
2) Si $P, Q \in K[X]$. Alors $P' = Q'$ si et seulement si: $P - Q = c$ telque c est un constant.

Preuve. 1) Soit P est un polynôme telque $p = \sum_{i=1}^{n} a_n X^n$ vérifié $P' = 0$,
on a $\forall n \in \mathbb{N} : (n+1) a_{n+1} = 0$, d'où $a_{n+1} = 0$. Les coefficients de P sont tous nuls à partir du rang 1 et le resultat en découle.
2) Result de 1. ■

1.7 Division euclidienne des polynômes

Dans ce qui suit nous supposerons que l'anneau $K = \mathbb{R}$ où $\mathbb{C}$.

Définition 1.7.1 *Soient A et B deux polynômes à coefficients dans K, s'il y a un polynôme $C \in K$ qui vérifié:*

$$A = B \cdot C$$

On dit que A est divisible par B ou que B divise A ou aussi A est un multiplie de B et on note $B|A$

Définition 1.7.2 *On dit que A et B sont des polynômes associé lorsque $A = \alpha B$, avec $\alpha \in K^*$.*

1.7.1 Proporiétés de la divisibilité

Soient A et B deux polynômes à coefficients dans K,telque $A = B \cdot C$.

1) Si C existe il est unique car:

En effet $A = BC = BC' \Longrightarrow B(C - C') = 0$ ou $B \neq 0$ alors $C = C'$ parce que $K[X]$ est intégre.

où $B = 0$ et C est indeterminé, ce qui ne présente aucun intérèt.

où suppose donc que $B \neq 0$. Ce qui implique l'unicité de C.

2) On a les résultats suivants:

a) $\forall A \in K[X] - \{0\}, A|A$.

b) $(A|B$ et $B|C) \Longrightarrow A|C$.

c) $(A|B$ et $A|C) \Longrightarrow A|(B + C)$.

d) $(A|B$ et $C|D) \Longrightarrow AC|BD$.

3) L'ensemble I des polynômes BC quand C d'écrit $K[X]$ est un idéal principal de $K[X]$ qui contient bien entendu B et le polynômes O.

Remarque 1.7.1 *1) Si $A \in I$ et $A \neq o$, alors $B|A \Longrightarrow \deg A \geqslant \deg B$; donc le degré de B est minimum dans I.*

2) Si par contre B ne divise pas A il n'existe pas de polynômes C tel que $A = BC$ mais

nous allons alors essayer de trouver un polynôme Q telque $A - BQ$ ait le plus petit dégré possible.

Théorème 1.7.1 *Soit A un polynôme quelconque de $K[X]$ et B un polynôme, dont le coefficient du terme de plus haut degré est inversible dans K: il existe des polynômes Q et R, déterminés de façon unique, tels que:*

$$A = BQ + R \tag{1}$$

$$\deg(R) < \deg(B) \tag{2}$$

Q s'appelle le quotient, R le reste de la divison euclidienne de A par B.

Preuve.

a) **Unicité**.

Si les couples de polynômes $(Q, R), (Q', R')$ satisfont à (1) et (2), on a par soustraction membre à membre,

$$B(Q - Q) = R - R' \tag{3}$$

Le coefficient du terme de plus haut degré de B est inversible, donc régulier dans K.
En reprenant la démonstration de proposition la relation (3) implique donc

$$\deg[B(Q' - Q)] = \deg(B) + \deg(Q' - Q)$$

Si $R \neq R'$, on en déduit $Q' - Q \neq 0$, d'où $\deg[B(Q' - Q)] \geq \deg(B)$; mais d'autre part,

$$\deg[B(Q' - Q)] = \deg(R - R') \leq \sup[\deg(R), \deg(R')] < \deg(B)$$

d'où une contradiction. donc $R = R'$. on établit enfin que $Q = Q'$ en tenant compte du fait que B n'est pas diviseur de zéro dans $K[X]$ (le coefficient de son terme de plus haut degré est inversible).

b) Existence.

Si $A = 0$, il suffit de poser $Q = R = 0$. sinon, on raisonne par récurrence sur $n = \deg(A)$.

Posons $B = b_p X^p + ... + b_0$, avec $P = \deg(B)$.

Par hypothèse, b_p est inversible dans K. Lorsque $n < p$, on pose $Q = 0$, $R = A$.

Supposons la proporiété vraie pour tous les polynômes A de degré $\leqslant n$, et montronts-la pour

$A = a_{n+1}X^{n+1} + ... + a_0$, $(n + 1 = \deg A,\ a_{n+1} \neq 0)$. Le polynôme $A_1 = A - BQ_1$, ou $Q_1 = \frac{a_{n+1}}{b_q} X^{n+1-p}$, est de degré$\leqslant n$.

Par l'hypothèse de recurrence, il existe des polynômes Q_2 et R_2, avec $\deg R_2 < p_1$ telsque $A_1 = BQ_1 + R_2$. On a:

$$A = A_1 + BQ_1 = B(Q_1 + Q_2) + R_2$$

Il suffi donc de poser $R = R_2$, $Q = Q_1 + Q_2$ pour avoir (1) et (2).

La disposition pratique classique de la division s'inspire du raisonnement par récurrence ci-dessus. ■

Exemple 1.7.1 *Soient A et B deux polynômes de $K[X]$ telque:*

$A = X^3 + X^2 - X - 1$ *et* $B = X^2 - 1$

A divise par B car

$$\begin{array}{rll} X^3 + X^2 - X & -1 & |\underline{X^2 - 1} \\ X^2 & -1 & |X + 1 \\ & 0 & \end{array}$$

donc $R = 0$

1.8 Le PGCD et PPCM des polynômes

1.8.1 Le plus grand commun diviseur PGCD

Soient A et B deux polynômes de $K[X]$ et soient $\text{div}(A)$ et $\text{div}(B)$ les deux ensembles formés chacun de tous les diviseurs de A et B respictivement donc tout élément de $\text{div}(A) \cap \text{div}(B)$ est un diviseur commun à A et B.

Etudions ce dernier ensemble. On a:
Si un polynôme P divise A et B alors P divise tout les polynômes $D = AU + BV$, quelque soit $U, V \in K[X]$.
D'où:

$$\mathrm{div}(A) \cap \mathrm{div}(B) \subset \mathrm{div}(AU + BV).$$

Soient alors J l'ensemble des polynômes de la forme $AU + BV$, sachant que U et V décrivent $K[X]$.
Il manifeste que J est idéal de $K[X]$ parce que:

$$\begin{cases} D = AU + BV \\ D' = AU' + BV' \end{cases} \Longrightarrow D + D' = A(U + U') + B(V + V')$$

et

$$\alpha D = (\alpha A)U + (\alpha B)V.$$

Comme $K[X]$ est principal alors J est idéal principal c'est à dire que
les éléments de J sont les multiples d'un même élément noté d
(il est défini à un scalaire λ multiplicatif prés) qui a le plus petit degré possible; en d'autres termes $J = d.K[X]$
Comme d est un diviseur de tout polynôme $D = AU+BV$ alors d divise $D_1 = A\cdot 1+B\cdot 0 = A$ et $D_2 = A.0 + B.1 = B$
donc d est un élément $\mathrm{div}(A) \cap \mathrm{div}(B)$; d'où $\mathrm{div}(AU + BV) \subset \mathrm{div}(A) \cap \mathrm{div}(B)$ or $\mathrm{div}(AU + BV) = \mathrm{div}(d)$; donc:

$$\mathrm{div}(d) = \mathrm{div}(A) \cap \mathrm{div}(B)$$

Définition 1.8.1 *Le polynôme d s'appelle le plus grand commun diviseur à A et B et on le note $p\gcd(A, B) = d$.*

Remarque 1.8.1 – *$p\gcd(A, B)$ est un polynôme unitaire.*
– *Si $A|B$ et $A \neq 0$, $p\gcd(A, B) = \frac{1}{\lambda}A$, où λ est le coefficient dominant de A.*

– *Pour tout* $\lambda \in K^*$, $p\gcd(\lambda A, B) = p\gcd(A, B)$.

– *Comme pour les entiers: si* $A = BQ + R$ *alors* $p\gcd(A, B) = p\gcd(B, R)$.

1.8.2 Algorithme d'Euclide

Soient A et B des polynômes, $B \neq 0$.

On calcule les divisions euclidiennes successives,

$A = BQ_1 + R_1 \qquad \deg R_1 < \deg B$

$B = R_1Q_2 + R_2 \qquad \deg R_2 < \deg R_1$

$R_1 = R_2Q_3 + R_3 \qquad \deg R_3 < \deg R_2$

.

.

.

$R_{k-2} = R_{k-1}Q_k + R_k \qquad \deg R_k < \deg R_{k-1}$

$R_{k-1} = R_kQ_{k+1}$

Le degré du reste diminue à chaque division. On arrête l'algorithme lorsque le reste est nul.

Le $p\gcd$ est le dernier reste non nul R_k (rendu unitaire).

Exemple 1.8.1 *Soient* $P_1(X) = 3X^5 + X^3 - 6X^2 - 2$
et $P_2(X) = 3X^4 - 2X^2 - 1$ *deux polynômes de* $K[X]$.
On trouve le $p\gcd(P_1, P_2)$ *avec la méthode l'algorithme d'Euclide:*
$P_1(X) = P_2(X).Q_1(X) + R_1(X)$ *avec* $R_1(X) = 3X^3 - 6X^2 + X - 2$.
$P_2(X) = R_1(X).Q_2(X) + R_2(X)$ *avec* $R_2(X) = 9X^2 + 3$.
$R_1(X) = R_2(X).Q_3(X) + R_3(X)$ *avec* $R_3(X) = -6X^2 - 2$.
$R_2(X) = R_3(X).Q_4(X) + R_4(X)$ *avec* $R_4(X) = -3/2$.
Le rest final est nul. Donc $R_3(X) = -6X^2 - 2$ *est un* $P\gcd$ *de* $P_1(X)$ *et* $P_2(X)$.

1.8.3 Polynômes premiers entre eux

Définition 1.8.2 *Deux polynômes A, B sont dite premiers entre eux si leur $p\gcd$ est une constante*

(que nous pouvons choisir égale à 1).

Théorème 1.8.1 *(de bezout)*

Deux polynômes A, B sont premiers entre eux si et seulement si il existe deux polynômes U et V tels que:

$$AU + BV = 1.$$

Preuve. Nous avons en effet établir que: $\mathrm{div}(d) = \mathrm{div}(A) \cap \mathrm{div}(B) = \mathrm{div}(AU + BV)$
Donc d étant le $p\gcd$ de A et B, il existe un polynômes U et un polynôme V tel que $d = AU + BV$.
Et si A et B sont premiers entre eux. alors d est une constante que nous avons
choisie égale 1. Réciproquement si $AU + BV = d$, tout polynôme qui divise A et B divise d, en particulier, le $p\gcd$ de A, B. comme d a pour degré le degré du $p\gcd$ alors $d = p\gcd(A, B)$ en particulier si $d = 1$. ■

1.8.4 Pgcd de plusieurs polynômes

Définition 1.8.3 *Soient $A_1, A_2, ..., A_n$. n polynômes de $K[X]$ et soit J l'idéal de $K[X]$ engandré par les polynômes A_i ie $P \in J \Leftrightarrow \exists U_1 \in K[X], ..., \exists U_n \in K[X]$:*

$$p = u_1A_1 + u_2A_2 + ... + u_nA_n$$

comme J est un idéal principal, alors tout élément P de J est multiple d'un même polynômes d non-nul

et qui a le plus petit degré possible donc, il existe n polynôme $u_1, u_2, ..., u_n$ de $K[X]$ tels que $d = \sum u_iA_i$

Ce polynôme d qui existe mais qui est défini à une constante multiplicative prés non-nulle est par définition

le $p\gcd$ des polynômes A_i Observons que tout polynôme qui divise tous les A_i divise d et réciproquement tout polynômes $u_1 = u_2 = ... = u_n = 0$ sauf $u_i = 1$; donc $A_i \in J$ $\forall_i$ est par conséquent d est un diviseur de chaque A_i.

1.8.5 Plus petit comun multiple des polynomes PPCM

Etant donnés deux polynômes $A, B \in \Bbbk[X]$, on note $\mathcal{M}(A, B)$ l'ensemble des multiples communs à A, B.

Proposition 1.8.1 *Soient* $A, B \in K[X]$.
1· Il existe $M \in K[X]$ *tel que* $\mathcal{M}(A, B)$ *soit l'ensemble des multiples de* M*:*

$$\forall P \in K[X] : P \in \mathcal{M}(A, B) \Leftrightarrow M|P.$$

2· Un autre polynôme vérifie la condition ci–dessus si et seulement s'il associé à M*.*
le polynôme M *est donc unique à association prés.*

Preuve.
1. Si l'un des deux polynômes A, B est nul, on a $\mathcal{M}(A, B) = \{0\}$ et donc $M = 0$ convient.
Supposons A et B non nuls. On note $D = p\gcd(A, B)$ et on écrit $A = DA_1$, $B = DB_1$.
Montrons que le polynôme $M = DA_1B_1$ convient. Il est clair que M est un multiple commun à A et B.
L'ensemble des multiples de M est donc inclus dans $\mathcal{M}(A, B)$. Réciproquement, soit $P \in \mathcal{M}(A, B)$ et écrivons par exemple $P = AQ$. Alors $B|AQ$,soit aprés simplification:
$B_1|A_1Q$. Comme A_1et B_1sont premier entre eux, le théoréme de gauss permet de conclure que $B_1|Q$. En écrivant $Q = RB_1$.
Il vient $P = AB_1R$, ce qui montre que P est un multiple du polynôme $AB_1 = M$.
2. Immédiat puisque deux polynômes sont associés si et seulement s'ils ont les mémes multiples. ■

Définition 1.8.4 *Soient* $A, B \in K[X]$.*Tout polynome* M *vérifiant la condition du théoréme ci- dessus est un plus petit commun multiple ou plus simplement un* $PPCM$ *des polynômes* A *et* B*.*
On a donc pour A,B,M $\in K[X]$:

$$M \text{ est un } PPCM \text{ de } A \text{ et } B \Leftrightarrow \begin{cases} A|M \text{ et } B|M \\ \forall M_1 \in K[X], (A|M_1 \text{ et } B|M_1) \Rightarrow M|M_1 \end{cases}$$

D'aprés l'assertion 2. du théoréme, les $PPCM$ de A et B sont deux à associés,
et il y a parmi eux un unique polynôme M unitaire.
On dit que c'est le $PPCM$ de A, B et on note $M = PPCM(A, B)$.

Remarque 1.8.2 *Soient $A, B, C \in K[X]$ on a:*
1) Lorsque $A|B$ (et en particulier si $B = 0$),alors B est un $PPCM$ de A et B.
2) $PPCM(A, B) = PPCM(B, A)$.
3) $C.PPCM(A, B) = PPCM(CA, CB)$.
4) On obtenue la relation suivante entre $PGCD$ et $PPCM$:

$$\forall A, B \in K[X], PGCD(A, B).PPCM(A, B) \text{ est associé à } AB.$$

5) Si A et B sont prémiers entre eux, alors:
$AB = PPCM(A,B)$.

Chapitre 2

Factorisation des polynômes

On suppose toujours que K est un unitaire commutatif.

2.1 Racine d'un polynôme

Définition 2.1.1 *Soit $P \in K[X]$ et $a \in K$. On dit que a est une racine de P si et seulement si $P(a) = 0$.*

Proposition 2.1.1 *Soit $P \in K[X]$ et $a \in K$. a est racine de P si et seulement si P est divisible par $X - 1$ dans $K[X]$*
ie:

$$P(a) = 0 \Longleftrightarrow (X - a)|P.$$

Preuve.
Si $(X - a)|P$, on peut écrire $P = (X - a)Q$ avec $Q \in K[X]$.
On a donc:

$$P(a) = (a - a)Q(a) = 0.$$

Réciproquement, supposons $P(a) = 0$ et écrivons la division euclidienne de P par $X - a$:

$$P = (X - a)Q + \lambda, \lambda \in K.$$

En prenant la valeur en a, il vient $\lambda = 0$ et donc $(X - a)|P$. ■

Exemple 2.1.1 *Soit* $P(X) = X^2 - 2X + 1 \in K[X]$
1 *est un racine de* P *car* $P(1) = 0$.

Théorème 2.1.1 *Soit* $P \in K[X]$ *un polynôme de degré* $d \geqslant 0$. *alors* P *posséde au plus* d *racines dans* K.
En particulier tout polynôme non nul posséde un nombre fini des racines.

Preuve.

Notons $a_1, ..., a_r$ des racines distinctes de P. D'aprés ce qui précéde,
P est divisible par chacun des polynômes $X - a_i$. Par aillaurs, ces polynômes sont irréductiblies,
donc deux à deux premiers entre eux.
On en déduit que P est divisible par le produit $\prod_{i=1}^{r}(X - a_i)$.
En comparant les degrés, il vient: $r \leqslant d$, et le résultat en découle. ■

2.2 Polynômes irréductibles

Définition 2.2.1 *Un polynôme* $P \in K[X]$ *est dit irréductible dans* $K[X]$ *si* P *n'est pas constant et si ses seuls diviseurs dans* $K[X]$ *sont les constantes et les polynômes proportionnels à* P *non nuls,*
ou, de manière équivalente, s'il n'existe pas $Q, R \in K[X]$ *avec* $\deg Q \geqslant 1$ *et* $\deg R \geqslant 1$ *tel que* $P = QR$.

Remarque 2.2.1 *1) Si* P *est irréductible, tout les polynômes associés à* P *le sont aussi.*
2) L'irréductibilité dépend du corps K.
Prenons par exemple $P(X) = X^2 + 2$, *dons* $\mathbb{C}[X]$, $P(X)$ *est divisible par le polynôme* $X - i\sqrt{2}$ *qu'est ni constant, ni associé à* P. P *n'est donc pas irréductible dans* $\mathbb{C}[X]$.
Etudions la situation dans $\mathbb{R}[X]$. *si* P *n'est pas irréductible dans* $\mathbb{R}[X]$, *on peut écrire* $P = QR$ *où* Q *et* R *sont non constants tous les deux. On a alors nécessairement*

$\deg(Q) = \deg(R) = 1$ *et donc* P *se factorise sous la forme* $P(X) = (X-a)(X-b)$ *avec* a, $b \in R$.
En identifiant, il vient $a + b = 0$ *et* $ab = 2$, *d'où* $a^2 = -2$; *or ceci est impossible dans* R.
P *est donc irréductible dans* $\mathbb{R}[X]$.

Théorème 2.2.1 *Soit* $A \in K[X]$ *un polynôme non constant, alors l'ensemble des diviseurs irréductibles unitaire de* A *est non vide et fini. Cet ensemble sera noté* $\varphi_K(A)$

2.2.1 Critères d'irréductibilité

Nous allons donner quelques exemples de critères d'irréductibilité pour les polynômes de $\mathbb{Z}[X]$.

Proposition 2.2.1 *Soit* P *unitaire dans* $\mathbb{Z}[X]$. *S'il existe* n *tel que sa réduction modulo* n *est irréductible, alors* P *est irréductible dans* $\mathbb{Z}[X]$.

Exemple 2.2.1 $P(X) = X^2 + X + 3$ *se réduit modulo* 2 *à* $\bar{P}(X) = X^2 + X + 1$
qui est irréductible: parceque n'admet pas des racines dans F_2
$\bar{P}(0) = 1 \neq 0,\ \bar{P}(1) = 3 \neq 0$

Proposition 2.2.2 *(Critère d'Eisenstein)*
Soit $P(X) = \sum_{i=0}^{n} a_i X_i \in \mathbb{Z}[X]$ *alors, s'il existe un nombre premier* p *tel que:*
$p|a_0,\ p|a_1, ...,\ p|a_{n-1},\ p \nmid a_n$ *et* $p^2 \nmid a_0$
alors P *est irréductible dans* $\mathbb{Q}[X]$.

Preuve. Cf [1] ■

Exemple 2.2.2 *Le polynôme* $P(X) = X^5 + 6X^4 - 3X^2 + 3X - 12$ *est irréductible pour* $p = 3$ *d'après critère d'Eisenstein.*

2.3 Théoreme de factorisation

On dans $K[X]$ un analogue du théoréme de décomposition en facteurs premiers dans $\mathbb{Z}$.

Définition 2.3.1 *Soit $P \in \varphi$ et A un polynôme non nule. On appelle $P-$valuation de A l'entier $val_p(A)$ défini par:*

$$val_P(A) = \max\left\{k \in \mathbb{N} : P^k | A\right\}$$

on a en particulier:

$$P|A \Leftrightarrow val_p(A) \geqslant 1.$$

Théorème 2.3.1 *Soit $A \in K[X]$ un polynôme non constant, A s'écrit de façon unique sous la forme:*

$$A = u\prod_{i=1}^{r} P_i^{\alpha_i}$$

où

1) *$u \in K^*$ (K^* les éléments inversible de K).*

2) *Pour $1 \leqslant i \leqslant r$ les P_i sont des polynomes irréductibles unitaire deux à deux distincts.*

3) *Pour $1 \leqslant i \leqslant r$ les α_i sont des entiers $\geqslant 1$.*

Preuve. D'aprés le proposition du nombre fini seulement de polynômes irréductibles unitaire $p_1, ..., p_r$ divisent A.
Notons $\alpha_i = val_P(A) \geqslant 1$. les $p_i^{\alpha_i}$ sont premiers entre eux et divisent A, donc leur produit divise A.
Notons:

$$A = u\prod_{i=1}^{r} P_i^{\alpha_i} \in K[X].$$

Si u n'est pas constant, alors il admet au moins un diviseur irréductible, ce qui est contradictoire avec la définition des p_i et des α_i, d'où l'existence de la décomposition. Supposons maintenant:

$$A = u\prod_{i=1}^{r} P_i^{\alpha_i} = v\prod_{i=1}^{s} Q_j^{\beta_j}$$

où $v \in K^*$, les Q_j sont des polynômes irréductibles unitaire et les β_j des entiers $\geqslant 1$.
On a $u = v = cd(A)$. Les $Q_J^{\beta_J}$ sont premiers entre eux donc pour tout i, chaque p_i divise l'un des Q_J et un seul; comme Q_j est irréductible et que p_i n'est pas constant,
on en déduit que $\{P_1, ..., P_r\} \subset \{Q_1, ..., Q_S\}$.

Par un raisonnement symétrique, on montre que les deux ensembles sont égaux et $r = s$, ouitte à réindexer les polynômes, on peut supposer $p_i = Q_i$, pour tout $i \in [1, r]$:

$$\prod_{i=1}^{r} P_i^{\alpha_i} = \prod_{i=1}^{r} P_i^{\beta_i}$$

par définition des α_i, on a $\beta_i \leq \alpha_i$. L'egalité des degrés montre alors que $\beta_i = \alpha_i$, pour tout $i \in [1, r]$,
d'ou l'unicité de la décomposition. ■

Remarque 2.3.1 *Avec les notations ci-dessus les diviseurs irréductibles unitaire de A sont exactement $P_1, P_2, ..., P_r$ et on a: $\forall i \in \{1...r\}$:*

$$\alpha_i = val_{p_i}(A).$$

Corollaire 2.3.1 *Tout polynôme non nul $A \in K[X]$ s'écrit de façon unique sous la forme:*

$$A = u \prod_{P \in \varphi_k} p^{\alpha_P}$$

oú $u \in K^*$ et $(\alpha_p)_{p \in \varphi_K}$ est une famille presque nulle d'entiers naturels.

Théorème 2.3.2 ***(Polynôme scindé)***
Un polynôme $P \in K[X]$ de degré n, est scindé s'il s'écrit comme produit de polynômes de degré 1,
ie:

$$P = a_n \prod_{i=1}^{r} (X - \alpha_i)^{k_i}$$

avec $a_n \neq 0$ et $\alpha_i \in K$ pour tout $i = 1...r$.

Proposition 2.3.1 *Pour tout $a \in A$, $X - a$ est irréductible.*

Preuve. on commence par observer qu'un polynôme est une
unité si et seulement si c'est un polynôme constant égal à une unité de A. Ensuite,
puisque $\deg QR = \deg Q + \deg R$, les diviseurs de $X - a$ sont de degré 0 ou 1,
ce sont les unités ou les associés de $X - a$. Il est un cas où on obtient ainsi tous les irréductibles. ■

Définition 2.3.2 *Le corps K est algébriquement clos si tout polynôme non constant admet au moins une racine.*

Corollaire 2.3.2 *1) Si K est algébriquement clos, tous les polynômes de $K[X]$ se factorisent*
en polynômes du premier degré. On dit qu'ils sont scindés.!!
2) Les polynômes irréductibles de $K[X]$ sont les polynômes du premier degré.

Théorème 2.3.3 ***(Albert -Gauss)***
Le corps $\mathbb{C}$ est algébriquement clos.

Théorème 2.3.4 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes du second degré sans racines réelles.*

Preuve.

Tout polynôme P de $\mathbb{R}[X]$ peut être considéré comme un polynôme de $\mathbb{R}[X]$. De plus, si α est une racine non réelle de P, on a $\bar{P}(\alpha) = P(\bar{\alpha}) = 0$, donc $\bar{a}$ est racine de P avec la même multiplicité. On termine en observant que $(X - \bar{\alpha})(X - \bar{\alpha})$ est alors un polynôme du second degré à coefficient réels, sans racine réelle. ■

Chapitre 3

Résultant et discriminant

3.1 Résultant de deux polynômes

Définition 3.1.1 *Soient* $P(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ *et* $Q(X) = b_mX^m + b_{n-1}X^{n-1} + ... + b_1X + b_0$ *deux polynômes à coefficients dans un anneau commutatif.*

On appelle matrice de Sylvester de P *et* Q *la matrice carrée suivante:*

$$S(P;Q) = \begin{pmatrix} a_n & . & . & . & . & . & a_0 & 0 & . & . & 0 \\ 0 & . & & & & & & . & . & & \\ . & . & . & & & & & & . & . & \\ . & & . & . & & & & & & . & 0 \\ 0 & . & . & 0 & a_n & . & . & . & . & . & a_0 \\ b_m & . & . & . & . & b_0 & 0 & . & . & . & 0 \\ 0 & . & & & & . & . & . & & & . \\ . & . & . & & & . & & . & . & & . \\ . & & . & . & & . & & & . & . & . \\ . & & & . & . & . & & & & . & 0 \\ 0 & . & . & . & 0 & b_m & . & . & . & . & b_0 \end{pmatrix} \begin{matrix} \\ - \\ - \\ n\ ligne \\ - \\ \\ \\ - \\ - \\ m\ ligne \\ - \\ - \\ \end{matrix}$$

Définition 3.1.2 *On définit le résultant* $Res(P,Q)$ *est le déterminant de la matrice dite de Sylvester:*

$$R(P,Q) = \det(S(P,Q)).$$

Proposition 3.1.1 *On suppose que*
$P(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ *et* $Q(X) = b_mX^m + b_{n-1}X^{n-1} + ... + b_1X + b_0$ *sont deux polynômes à coefficients dans le corps commutatif* K*. Si* $b_m \neq 0$ *alors:*

$$Res(P, Q) = b_m^{\deg(p)} \det(\varphi_p)$$

où

$$\varphi_p : \Bbbk[X]/(Q) \longrightarrow \Bbbk[X]/(Q)$$
$$\overline{U} \longmapsto \overline{UP}.$$

Théorème 3.1.1 *Soient* $P(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$
et $Q(X) = b_mX^m + b_{n-1}X^{n-1} + ... + b_1X + b_0$ *sont deux polynômes à coefficients dans un corps commutatif* K *.*
Si $b_n \neq 0$ *alors le résultant de* P *et* Q *est non nul si et seulement si* P *et* Q *sont premiers entre eux.*

Proposition 3.1.2 *Soient* $P(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$
et $Q(X) = b_mX^m + b_{n-1}X^{n-1} + ... + b_1X + b_0$ *sont deux polynômes à coefficients dans un corps commutatif* K *donc:*
a) $Res(P, Q) = (-1)^{nm}Res(Q, P)$*.*
b) $Res(P_1P_2, Q) = Res(P_1, Q)Res(P_2, Q)$*.*
c) Si le polynômes Q *est de degré* m *et scindé:* $Q(X) = b_m \prod_{j=1}^{m}(X - y_j)$*.*
Alors:

$$Res(P, Q) = b_m^{\deg(p)} \prod_{i=1}^{n} P(y_i).$$

d) Si P *est de degré* n *et également scindé:* $P = a_n \prod_{i=1}^{n}(X - x_i)$*.*
Alors:

$$Res(P, Q) = a_n^m b_m^n \prod_{i=1}^{m} \prod_{j=1}^{n} (y_j - x_i).$$

Lemme 3.1.1 *Soient* $P(X) = a_0 + ... + a_nX^n$ *et* $Q(X) = b_0 + ... + b_mX^m$ *sont deux polynômes à coefficients dans un corps* K*.*

1) Si Q divise P, on a $R(P,Q)=0$.

2) Si Q ne divise pas P, soient R le reste de la division de P par Q, r le degré de R.

Alors:

$$R(P,Q)=(-1)^{mn}b_m^{n-r}R(Q,R) \qquad (*)$$

Preuve.

1) Multiplions la i-ième colonne de la matrice $S(P,Q)$ par X^{n+m-i}.

On obtient la matrice $\tilde{S}(P,Q)(X)$ suivante:

$$\left(\begin{array}{cccccccccc}
a_nX^{n+m-1} & . & . & . & . & . & a_0X^{m-1} & 0 & . & 0 \\
0 & . & & & & & & . & . & \\
. & . & . & & & & & & . & . \\
. & & . & . & & & & & & 0 \\
0 & . & . & 0 & a_nX^n & . & . & . & . & a_0 \\
b_mX^{n+m-1} & . & . & . & . & b_0X^{n-1} & 0 & . & . & 0 \\
0 & . & & & & . & . & . & & . \\
. & . & . & & & . & & . & . & . \\
. & & . & . & & . & & & . & . \\
. & & & . & . & . & & & . & 0 \\
0 & . & . & . & 0 & b_mX^m & . & . & . & b_0
\end{array}\right)
\begin{array}{c}
- \\ - \\ \\ n\ ligne \\ - \\ \\ - \\ \\ m\ ligne \\ - \\ -
\end{array}$$

telle que $\tilde{S}(P,Q)(1)=S(P,Q)$.

Remarquons que dans la matrice $\tilde{S}(P,Q)(X)$, la ligne l_i est formée des monômes du polynôme $X^{m-i}P(X)$ pour $1\leqslant i\leqslant m$ et des monômes du polynôme $X^{m+n-i}Q(X)$

pour $m+1\leqslant i\leqslant m+n$.

2) Si $m>n$, on a $R=P$, et le lemme est vrai par la formule:

$$Res(P,Q)=(-1)^{nm}Res(Q,P) \qquad (1)$$

Si $n\geqslant m$, considérons la division euclidienne:

$P=QA+R$ $\deg(R)<\deg(Q)$ ou $R=0$. Posons:

$$A(X)=\alpha_0+\alpha_1X+\cdots+\alpha_{n-m}X^{n-m} \qquad (2)$$

on a donc:

$$QA = \alpha_0 Q + \alpha_1 (XQ) + \cdots + \alpha_{n-m}(X^{n-m}Q) \tag{3}$$

1. Si Q divise P, on voit ainsi en utilisant (3) que la relation $P = QA$ s'interprète en disant que la ligne l_q de la matrice $\tilde{S}(P,Q)(X)$ est une combinaison linéaire des lignes $l_{n+m}, l_{n+m-1}, ..., l_{2m}$ avec coefficients $\alpha_0, ..., \alpha_{n-m}$. Le déterminant de la matrice $\tilde{S}(P,Q)(X)$ est donc nul, ce qui implique que $R(P,Q) = 0$.

2. Dans le cas général, posons:

$$R(X) = c_0 + c_1 X + \cdots + c_r X^r$$

avec $c_r \neq 0$. On voit alors en utilisant (3) que la relation $P = QA + R$ s'interprète en disant que la ligne l_q de la matrice $\tilde{S}(P,Q)(X)$ est la somme de la ligne $(0, ..., 0, c_r X^r, ..., c_0)$ correspondant au polynôme $R(X)$, et d'une combinaison linéaire des lignes $l_{n-m}, l_{n-m+1}, ..., l_{2m}$ avec coefficients $\alpha_0, ..., \alpha_{n-m}$.
On peut donc remplacer la ligne l_q de $\tilde{S}(P,Q)(X)$ par la ligne $(0, ..., 0, c_r X^r, ..., c_0)$ sans changer son déterminant.
En procédant de même avec les relations:

$$X^i P = X^i QA + X^i R$$

pour $0 \leqslant i \leqslant m-1$, on voit que l'on peut remplacer les m premières lignes de $\tilde{S}(P,Q)(X)$ par les lignes formées des zéros et des monômes des polynômes $X^i R$, $0 \leqslant i \leqslant m-1$, la ligne l_{m-i} étant remplacée par la ligne $(0, ..., 0, c_r X^{r+i}, ..., c_0 X^i, 0, ..., 0)$, cela sans changer le déterminant. En faisant $X = 1$ on voit alors que le déterminant de

$S(P,Q)$ est égal au déterminant de la matrice:

$$\left(\begin{array}{ccccccccccc}
0 & . & . & . & c_r & . & . & . & c_0 & 0 & . & . & . \\
 & & & & & . & & & & & & & \\
 & & & & & & . & & & & & & \\
 & & & & & & & . & & & & & \\
0 & . & . & . & & & & & c_r & & & & c_0 \\
b_m & . & . & . & & & & b_0 & 0 & & & & \\
0 & . & & & & & & & & & & & \\
. & & . & & & & & & & & & & \\
. & & & . & & & & & & & & & \\
. & & & & & & & & & & & & \\
 & . & . & . & & . & & & & & & & \\
 & & & & & & . & & & & & & \\
0 & & & & & & b_m & . & . & . & & & b_0
\end{array}\right) \quad m+n \text{ lignes}$$

d'où relation $(*)$ ■

Corollaire 3.1.1 *Soit K un corps. Avec les notations ci-dessus, les conditions suivantes sont équivalentes:*

1. $R(P,Q)=0$.

2. les polynômes P et Q ont un facteur commun de degré >0 dans $K[X]$.

Preuve.

1. $\Rightarrow$ 2. Supposons que 2. soit faux, i.e. que P et Q n'aient pas de facteur commun dans $K[X]$. Le $p\,\mathrm{gcd}$ de P et Q (dernier reste non nul dans l'algorithme d'Euclide) est alors une constante $c \neq 0$. Recursivement donne:

$$R(P,Q) = \alpha R(R_s, c)$$

avec $\alpha \neq 0, c \neq 0$ et R_s un reste de degré $r_s > 0$. Mais on voit tout de suite (enregardant la matrice de Sylvester) que $R(R_s,c) = c^{r_s} \neq 0$, et donc que $R(P,Q) \neq 0$.

2. $\Rightarrow$ 1. Si P et Q ont un facteur commun non trivial A dans $K[X]$, supposons d'abord que $P = QA$ avec A de degré $n-m>0$. que $R(P,Q)=0$. Dans le cas général, on

se retrouve

dans la situation ci-dessus en considérant le dernier reste non nul dans l'algorithme d'Euclide.

■

Proposition 3.1.3 *Soient P et Q sont deux polynômes à coefficients dans $K[X]$, on ait:*

$$P(X) = a_n(X-\alpha_1)...(X-\alpha_n).$$

$$Q(X) = b_m(X-\beta_1)...(X-\beta_m).$$

Alors:

$$R(P,Q) = a_n^m b_m^n \prod_{i,j}(\alpha_i - \beta_j) = a_n^m \prod_{1\leqslant i\leqslant n} Q(\alpha_i) = (-1)^{nm} b_m^n \prod_{1\leqslant j\leqslant m} P(\beta_j).$$

Preuve.

Les égalités:

$$a_n^m b_m^n \prod(\alpha_i - \beta_j) = a_n^m \prod Q(\alpha_i) = (-1)^{nmb_m^n} \prod P(\beta_j)$$

sont immédiates.

Posons $R_2(P,Q) = a_n^m \prod Q(\alpha_i) = (-1)^{nmb_m^n} \prod P(\beta_j)$.

Pour montrer que $R_2(P,Q) = R(P,Q)$, on peut supposer $n \geqslant m > 0$ (car on a évidemment $R(P,Q) = R_2(P,Q) = b_m^n$ si $m = 0$). Il suffit alors de montrer que R_2 satisfait à la même relation de récurrence $(*)$

que $R(P,Q)$. Si $P = QA + R$, on a $P(\beta j) = R(\beta j)$ pour toute racine β_j de Q, et donc:

$$R_2(P,Q) = (-1)^{nm} b_m^n \prod P(\beta_j) = (-1)^{nmb_m^n} \prod R(\beta_j) = (-1)^{nm} b_m^{n-r} R_2(Q,R)$$

ce qui est bien la même relation que $(*)$. ■

Exemple 3.1.1 *Soit $P(X) = aX^2 + bX + c$ et $Q(X) = a2X + b$ deux polynômes à coefficients dans un anneau commutatif intégre A.*

On a:

$$S(P,Q) = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}$$

d'ou

$$R(P) = a(4ac - b^2)$$

3.2 Discriminant

Soit $P(X) = a_0 + ... + a_n X^n$ un polynôme de degré n à coefficients dans un anneau commutatif intégre A.

Définition 3.2.1 *Le discriminant de P, noté $Disc(P)$ est défini par:*

$$Disc(P) = (-1)^{\frac{n(n-1)}{2}} \begin{vmatrix} a_0 & & & & & a_1 & & & & & \\ a_1 & a_0 & & & & 2a_2 & a_1 & & & & \\ . & a_1 & . & & & . & 2a_2 & . & & & \\ . & . & . & . & & . & . & . & . & & \\ . & . & . & . & & . & . & . & . & & \\ & . & & . & a_0 & & . & & . & . & \\ & & & & a_1 & na_n & & & . & . & \\ & & & & . & & na_n & & & . & a_1 \\ a_n & & & & . & & & na_n & & & 2a_2 \\ & . & & & . & & & & . & & \\ & & . & & & & & & . & & \\ & & & . & & & & & & . & \\ & & & & a_n & a_{n-1} & & & & na_n & (n-1)a_{n-1} \\ & & & & & 1 & & & & & n \end{vmatrix}$$

Notons que:

$$a_n Disc(P) = (-1)^{\frac{n(n-1)}{2}} Res(P, P').$$

Théorème 3.2.1 *Soit $P(X) = a_0 + ... + a_n X^n$ un polynôme de degré n à coefficients dans un anneau commutatif intégre A.*
Si $P(X) = a_n(X - \alpha_i)...(X - \alpha_n)$, alors:

$$Disc(P) = (-1)^{-\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{i \neq j} (\alpha_i - \alpha_j) = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Preuve.

On a:

$$P'(X) = a_n \sum_{i=1}^{n} (X - \alpha_1)...(\widehat{X - \alpha_i})...(X - a_n)$$

la notation $(\widehat{X-\alpha_i})$ signifiant que l'on omet le terme $(X-\alpha_i)$ dans le produit.
Comme $P'(\alpha_i) = a_n(\alpha_i-\alpha_1)...(\alpha_i-\alpha_n)$ (sans le terme $(\alpha_i-\alpha i)$), cela entraîne le résultat

■

Exemple 3.2.1 *Soit $P(X) = aX^2+bX+c$ un polynôme à coefficients dans un anneau commutatif intégre A.*
Alors: $P'(X) = a2X+b$, on a:

$$S(P,P') = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}$$

d'ou

$$R(P) = a(4ac-b^2)$$

et

$$Disc(P) = b^2-4ac.$$

3.2.1 Séparation et isolation des racines réelles

Définition 3.2.2 *Soit $P \in \mathbb{C}[X]$, $P(X) = a_0+a_1X^1+...+a_dX^d$, avec $a_d \neq 0$, α_i les racines de P.*
On pose:

$$sep(P) = \inf_{\alpha_i \neq \alpha_j} |\alpha_i-\alpha_j|.$$

Proposition 3.2.1 *On suppose que $P \in \mathbb{Z}[X]$. Alors, en posant $C = |a_d| + \sup_{1 \leqslant i \leqslant d-1} |a_i|$, on a pour $d \geqslant 3$:*

$$sep(P) \geqslant (2C)^{-\frac{d(d-1)}{2}+1}.$$

Preuve.

1) Supposons d'abord que les racines de P sont simples.
On peut supposer, quitte à changer les indices, que $sepP = |\alpha_1-\alpha_2|$.

Soit $D(P)$ le discriminant de P. $D(P) \in \mathbb{Z}$ puisque par hypothèse $P \in \mathbb{Z}[X]$.
On a donc $1 \leqslant |D(P)|$ puisque l'hypothèse (1) implique que $D(P) \neq 0$.
On a donc d'après la théorème 3.2.1:

$$1 \leqslant |a_d|^{2d-2i} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

soit

$$\frac{1}{(\alpha_{1-}\alpha_2)^2} \leqslant |a_d|^{2d-2} \prod_{i<j \ (i,j)\neq(1,2)} |\alpha_i - \alpha j|^2.$$

Mais $|\alpha_i - \alpha_j| \leqslant |\alpha_i| + |\alpha_j| \leqslant 2\frac{C}{|a_d|}$, et il y a $\frac{d(d-1)}{2} - 1 = \frac{d^2-d-2}{2}$ facteurs $|\alpha_i - \alpha_j|^2$,
ce qui donne:

$$\frac{1}{|\alpha_{1-}\alpha_2|^2} \leqslant \frac{(2C)^{d^2-d-2}}{|a_d|^{d^2-3d}} \leqslant (2C)^{d^2-d-2}$$

(car $|a_d| \geqslant 1$ et $d^2 - 3d \geqslant 0$), d'où le résultat.
2) Dans le cas général (i.e. lorsque les racines de $P \in \mathbb{Z}[X]$ ne sont pas nécessairement simples), on peut supposer P primitif quitte à le diviser par son contenu (qui est un entier).
On considère le polynôme $R = p\gcd(P, P')$ que l'on
peut supposer dans $\mathbb{Z}[X]$ et primitif; on a alors $P = QR$ dans $\mathbb{Z}[X]$, P et R étant primitifs.
On peut alors appliquer la méthode de (1) au polynôme Q qui a les mêmes racines que P, mais avec multiplicité 1.
On trouve donc, en notant d le degré de Q, et en utilisant que $d' \leqslant d$:

$$\frac{1}{(sepP)^2} = \frac{1}{(sepQ)^2} \leqslant (2C)^{d'^2-d'-2} \leqslant (2C)^{d^2-d-2}$$

■

Bibliographie

[1] *Guy AULIAC, Jean, DELCOURT, Rémy GOBLOT, Mathématiques Algèbre et géométrie;* Dunod, Paris, 2005.

[2] *Jean-Pierre ESCOFIER, toute l'algebre de la licence, $2^{éme}$ édition.*

[3] *Daniel FREDON, Myriam MAUMY-BERTRAND; Mathématiques Algèbre et géométrie;* Dunod, Paris, 2009.

[4] *H.HENICHE L'Algébre lineaire polynome et fraction rationelles;* office des publications universitaires; 1993.

[5] *Amara HITTA; cours d'algèbre et exercices corriges;* publication univercitaires, 07-2006.

[6] *Jacqueline LELONG-FERRAND, Jean-Marie ARNAUDIÈS; cours de mathématiques, Algèbre.*

[7] *Jean-Marie MONIER, ALGEBRE MPSI.*Dunod, Paris; 1996.

[8] *Jean-Jacques RISLER, Pascal BOYER; algèbre pour la licence 3, Groupe, anneau, corps.*

Résumé

Nous avons discuté dans notre mémoire de l'anneau des polynômes, sa propriété avec la définition de la défirent opérations, la division Euclidienne , PGCD et PPCM en se concentrons sur résultant et discriminants des polynômes.

الملخص

تطرقنا في مذكرتنا حول حلقة كثيرات الحدود وخصائصها مع تعريف مختلف العمليات عليها وكذلك القسمة الاقليدية والقواسم والمضاعفات المشتركة لكثيرات الحدود مركزين على التحليل وقابلية الحل باستخدام الناتج والتمايز .