1. Cours 1: Arithmétique dans $\mathbb{Z}$

2. Cours 2: Fonctions et Applications

3. Cours 3: Relations

4. Cours 4: Quelques structures algébriques

5. Cours 5: Homomorphismes de structures algébriques

6. Cours 6: Anneau des polynômes

6.1. L'ensemble des polynômes à une indéterminée

6.1.1.Définitions: *Soit* $(A, +, .)$ *un anneau unitaire et commutatif*

On appelle polynôme à une indéterminée à coefficients dans A *toutes écriture algebrique de la forme* $a_0 + a_1X^1 + ... + a_{n-1}X^{n-1} + a_nX^n + ...$

où les a_i *sont des éléments de* A*, et sont nuls sauf un nombre fini.*

Si on note P *ce polynôme, alors:*

** X est appelé l'indéterminée et les a_i sont appelés les coefficients de P.*

** Le plus grand indice* n *vérifiant* $a_n \neq 0$ *(s'il existe) est appelé degré de* P *et est noté* $\deg P$ *et dans ce cas le terme* a_nX^n *est appelé terme dominant de* P*.*

** Si le coefficient du terme dominant d'un polynôme est égal à* 1 *le polynôme est dit unitaire*

** Si tous les coefficients sont nuls le polynôme est appelé polynôme nul et est noté* 0 *et par convention* $\deg 0 = -\infty$

** Chaque élément* a_0 *de* A *est un polynôme, appelé polynôme constant.*

L'ensemble des polynômes à une indéterminée à coefficients dans A *est noté* $A[X]$

6.1.2.Remarques: 1) Dans un polynôme, on omet souvent les a_iX^i pour les a_i nuls et on l'écrit suivant les puissances décroissantes de X.

2) On écrit souvent, X au lieu de X^1 et X^n au lieu de $1X^n$.

3) Deux polynômes $P = a_0 + a_1X^1 + ... + a_{n-1}X^{n-1} + a_nX^n + ...$ *et* $Q = b_0 + b_1X^1 + ... + b_{n-1}X^{n-1} + b_nX^n + ...$ sont égaux s'ils ont les mêmes coefficients. C.à.d: $P = Q$ ssi pour tout $i \in \mathbb{N} : a_i = b_i$.

Exemple 1: $P = X^n - 1$ (où $n \in \mathbb{N}^*$) est un polynôme unitaire de degré n à coefficients dans $\mathbb{Z}$, c.à.d $P \in \mathbb{Z}[X]$. Le terme dominant de P est X^n et

ses coefficients sont $(-1, 0, ..., 0, 1, 0, ..., 0, ...)$ tous les coefficients sont nuls sauf $a_0 = -1$ et $a_n = 1$.

Exemple 2: $Q = 2X^3 - \sqrt{5}X$ est un polynôme non unitaire de degré 3 à coefficients dans $\mathbb{R}$, c.à.d $Q \in \mathbb{R}[X]$. Le terme dominant de Q est $2X^3$ et ses coefficients sont $\left(0, -\sqrt{5}, 0, 2, 0, ..., 0, ...\right)$ tous les coefficients sont nuls sauf $a_1 = -\sqrt{5}$ et $a_3 = 2$.

Exemple 3: $S = 4 + 2i$ est un polynôme non unitaire de degré 0 (polynôme constant) à coefficients dans $\mathbb{C}$, c.à.d $S \in \mathbb{C}[X]$. Le terme dominant de S est $4 + 2i$ et ses coefficients sont $(4 + 2i, 0, ..., 0, ...)$ tous les coefficients sont nuls sauf $a_0 = 4 + 2i$.

6.2. Opérations sur l'ensemble $A[X]$

6.2.1.Définitions: *Soient* $P = a_0 + a_1X^1 + ... + a_{n-1}X^{n-1} + a_nX^n + ...$ *et* $Q = b_0 + b_1X^1 + ... + b_{n-1}X^{n-1} + b_nX^n + ...$ *deux polynômes de* $A[X]$

On définit la somme $P + Q$ *et le produit* $P.Q$ *par:*

$$P + Q = (a_0 + b_0) + (a_1 + b_1)X^1 + ... + (a_{n-1} + b_{n-1})X^{n-1} + (a_n + b_n)X^n + ...$$

$$P.Q = \left(\sum_{i+j=0} a_i.b_j\right) + \left(\sum_{i+j=1} a_i.b_j\right)X^1 + ... + \left(\sum_{i+j=n-1} a_i.b_j\right)X^{n-1} + \left(\sum_{i+j=n} a_i.b_j\right)X^n + ...$$

6.2.2.Remarque: 1) $c_0 = \sum_{i+j=0} a_i.b_j = a_0.b_0 = \sum_{i=0}^{0} a_i.b_{0-i}$

$c_1 = \sum_{i+j=1} a_i.b_j = a_0.b_1 + a_1.b_0 = \sum_{i=0}^{1} a_i.b_{1-i}$

.....

$c_{n-1} = \sum_{i+j=n-1} a_i.b_j = a_0.b_{n-1} + a_1.b_{n-2} + ... + a_{n-1}.b_0 = \sum_{i=0}^{n-1} a_i.b_{n-1-i}$

$c_n = \sum_{i+j=n} a_i.b_j = a_0.b_n + a_1.b_{n-1} + ... + a_n.b_0 = \sum_{i=0}^{n} a_i.b_{n-i}$

.....

2) Pour énoncer la proposition suivante, on adopte la convention suivante:
Pour tout $n \in \mathbb{N}$: $n + (-\infty) = (-\infty) + n = -\infty$, $\quad -\infty < n$
et $(-\infty) + (-\infty) = -\infty$

6.2.3.Proposition: *Soient* P *et* Q *deux polynômes de* $A[X]$, *alors:*
$\deg(P + Q) \leq \max(\deg P, \deg Q)$ *et* $\deg(P.Q) \leq \deg P + \deg Q$
et si A *est intègre, alors* $\deg(P.Q) = \deg P + \deg Q$

Preuve: Notons $n = \deg P$ et $m = \deg Q$ et $P = a_0 + a_1X^1 + ... + a_{n-1}X^{n-1} +$

a_nX^n *et* $Q = b_0 + b_1X^1 + ... + b_{m-1}X^{m-1} + b_mX^m$

1) Si l'un des polynômes est nul, par exemple $P = 0$, alors $P + Q = Q$ et $P.Q = 0$ ainsi $\deg(P+Q) = \deg Q = \max(-\infty, \deg Q) = \max(\deg P, \deg Q)$

$\deg(P.Q) = -\infty = -\infty + \deg Q = \deg P + \deg Q$

2) Si aucun des polyômes P et Q n'est nul, alors

2.1) Les coefficients de $P + Q$ sont tous nuls après le rang $\max(n, m)$ donc $\deg(P+Q) \leq \max(n, m) = \max(\deg P, \deg Q)$

2.2) Les coefficients $c_k = \sum_{i+j=k} a_i.b_j$ de $P.Q$ vérifient pour tout $k \in \mathbb{N}^*$:

$$c_{(n+m)+k} = \sum_{i+j=n+m+k} a_ib_j = \underbrace{a_0b_{n+m+k} + ... + a_nb_{m+k}}_{\text{dans ce terme tous les } b_j \text{ sont nuls}} + \underbrace{a_{n+1}b_{m+k-1} + ... + a_{n+m+k}b_0}_{\text{dans ce terme tous les } a_i \text{ sont nuls}}$$

$$= 0$$

Ainsi $\deg(P.Q) \leq n + m = \deg P + \deg Q$.

$$c_{n+m} = \sum_{i+j=n+m} a_i.b_j = \underbrace{a_0.b_{n+m} + ... + a_{n-1}.b_{m+1}}_{\text{dans ce terme tous les } b_j \text{ sont nuls}} + a_n.b_m + \underbrace{a_{n+1}.b_{m-1} + ... + a_{n+m}.b_0}_{\text{dans ce terme tous les } a_i \text{ sont nuls}}$$

$$= a_n.b_m$$

Si A est un anneau intègre, alors $c_{n+m} = a_n.b_m \neq 0$ car $a_n \neq 0$ et $b_m \neq 0$.

D'où $\deg(P.Q) = n + m = \deg P + \deg Q$. ■

Exemple 1: Dans $\mathbb{Q}[X]$, soient les polynômes:

$P = 3X^2 - 1 \quad = \quad 3X^2 + 0X - 1$ et

$Q = \frac{1}{2}X^3 + 4X = \frac{1}{2}X^3 + 0X^2 + 4X + 0$ alors

$P + Q = \left(0 + \frac{1}{2}\right)X^3 + (3+0)X^2 + (0+4)X + (-1+0)$ et

$= \frac{1}{2}X^3 + 3X^2 + 4X - 1$

$$\begin{aligned} P.Q = & \left(((-1)\times 0) + (0\times 0) + \left(3\times\tfrac{1}{2}\right) + (0\times 0) + (0\times 4) + (0\times 0)\right)X^5 \\ & + \left(((-1)\times 0) + \left(0\times\tfrac{1}{2}\right) + (3\times 0) + (0\times 4) + (0\times 0)\right)X^4 \\ & + \left(\left((-1)\times\tfrac{1}{2}\right) + (0\times 0) + (3\times 4) + (0\times 0)\right)X^3 \\ & + (((-1)\times 0) + (0\times 4) + (3\times 0))X^2 \\ & + ((-1)\times 4 + 0\times 0)X \\ & + ((-1)\times 0) \\ = & \ \tfrac{3}{2}X^5 + 0X^4 - \tfrac{23}{2}X^3 + 0X^2 - 4X + 0 \quad = \tfrac{3}{2}X^5 - \tfrac{23}{2}X^3 - 4X \end{aligned}$$

Exemple 2: Dans $\mathbb{Z}/_{6\mathbb{Z}}[X]$, soient les polynômes:

$P = \dot{3}X^2 - \dot{1} \quad = \dot{3}X^2 + \dot{0}X - \dot{1}$ et

$Q = \dot{4}X^2 + \dot{2}X = \dot{4}X^2 + \dot{2}X + \dot{0}$ alors

$P + Q = \left(\dot{3} + \dot{4}\right)X^2 + \left(\dot{0} + \dot{2}\right)X + \left(-\dot{1} + \dot{0}\right)$ et

$= X^2 + \dot{2}X - \dot{1}$

$$
\begin{aligned}
P.Q = \quad & \left(\left(\left(\overset{\bullet}{-1}\right)\times\overset{\bullet}{0}\right)+\left(\overset{\bullet}{0}\times\overset{\bullet}{0}\right)+\left(\overset{\bullet}{3}\times\overset{\bullet}{4}\right)+\left(\overset{\bullet}{0}\times\overset{\bullet}{2}\right)+\left(\overset{\bullet}{0}\times\overset{\bullet}{0}\right)\right)X^4 \\
& +\left(\left(\left(\overset{\bullet}{-1}\right)\times\overset{\bullet}{0}\right)+\left(\overset{\bullet}{0}\times\overset{\bullet}{4}\right)+\left(\overset{\bullet}{3}\times\overset{\bullet}{2}\right)+\left(\overset{\bullet}{0}\times\overset{\bullet}{0}\right)\right)X^3 \\
& +\left(\left(\left(\overset{\bullet}{-1}\right)\times\overset{\bullet}{4}\right)+\left(\overset{\bullet}{0}\times\overset{\bullet}{2}\right)+\left(\overset{\bullet}{3}\times\overset{\bullet}{0}\right)\right)X^2 \\
& +\left(\left(\left(\overset{\bullet}{-1}\right)\times\overset{\bullet}{2}\right)+\left(\overset{\bullet}{0}\times\overset{\bullet}{0}\right)\right)X \\
& +\left(\left(\overset{\bullet}{-1}\right)\times\overset{\bullet}{0}\right) \\
& =\overset{\bullet}{0}X^4+\overset{\bullet}{0}X^3-\overset{\bullet}{4}X^2-\overset{\bullet}{2}X=-\overset{\bullet}{4}X^2-\overset{\bullet}{2}X
\end{aligned}
$$

On remarque dans cet exemple que $\deg(P.Q) < \deg P + \deg Q$, c'est parceque $\mathbb{Z}/_{6\mathbb{Z}}$ n'est pas intègre.

6.2.4.Théoreme: $(A[X],+,.)$ *est un anneau unitaire commutatif.*

Preuve:

1) Montrons que $(A[X],+)$ est un groupe.

L'addition des polyômes + est clairement une lois de composition interne associative et commutative, car l'addition + l'est sur A.

On vérifie facilement que le polynôme nul 0 est l'élément neutre et que $-P = (-a_0)+(-a_1)X^1+...+(-a_{n-1})X^{n-1}+(-a_n)X^n+...$ est le symétrique de $P = a_0+a_1X^1+...+a_{n-1}X^{n-1}+a_nX^n+...$ pour l'addition des polynômes.

Par conséquent $(A[X],+)$ est un groupe commutatif.

2) Pour la multiplication des polynômes qui est cailrement une lois interne, prenons $P = p_0+p_1X^1+...+p_{n-1}X^{n-1}+p_nX^n+...$, $Q = q_0+q_1X^1+...+q_{m-1}X^{m-1}+q_mX^m+...$ *et* $S = s_0+s_1X^1+...+s_{k-1}X^{k-1}+s_kX^k+..$
et notons respectivement les coefficients de $(P.Q).S$, $P.(Q.S)$, $P.Q$, $Q.S$ par $((P.Q).S)_l$, $(P.(Q.S))_l$, $(P.Q)_l$ et $(Q.S)_l$, alors $(P.Q)_l = \sum\limits_{i+j=l} p_i.q_j = \sum\limits_{j+i=l} q_j.p_i = (Q.P)_l$
et $P.Q = Q.P$, car ils ont les mêmes coefficients, d'où la commutativité de la multiplication.

$$
\begin{aligned}
((P.Q).S)_l &= \sum_{r+k=l}(P.Q)_r.s_k = \sum_{r+k=l}\left(\sum_{i+j=r}p_i.q_j\right).s_k \\
&= \sum_{r+k=l}\left(\sum_{i+j+k=r+k}p_i.q_j.s_k\right) = \sum_{i+j+k=l}p_i.q_j.s_k \\
(P.(Q.S))_l &= \sum_{i+r=l}p_i.(Q.S)_r = \sum_{i+r=l}p_i.\left(\sum_{j+k=r}q_j.s_k\right) \\
&= \sum_{i+r=l}\left(\sum_{i+j+k=i+r}p_i.q_j.s_k\right) = \sum_{i+j+k=l}p_i.q_j.s_k
\end{aligned}
$$

alors $(P.Q).S = P.(Q.S)$ car ils ont les mêmes coefficients, d'où l'associativité de la multiplication.

$$\begin{aligned}((P+Q).S)_l &= \sum_{r+k=l}(P+Q)_r.s_k = \sum_{r+k=l}(P_r+Q_r).s_k \\ &= \sum_{r+k=l}P_r.s_k + \sum_{r+k=l}Q_r.s_k = (P.S)_l + (Q.S)_l\end{aligned}$$

alors $(P+Q).S = P.S + Q.S$, car ils ont les mêmes coefficients, d'où la distributivité de la multiplication par rapport à l'addition.

L'anneau A est unitaire d'élément unité 1, alors l'anneau $A[X]$ est aussi unitaire d'élément unité 1.

Par suite $(A[X], +, .)$ est un anneau commutatif et unitaire. ■

6.2.5.Proposition: *Si A est un anneau intègre, alors $(A[X], +, .)$ est un anneau intègre*

Preuve: Si $P.Q = 0$ alors $\deg(P.Q) = \deg 0 = -\infty$, donc d'après **Prop.6.2.3** , on conclut que $\deg P + \deg Q = -\infty$, alors ou bien $\deg P = -\infty$ ou bien $\deg Q = -\infty$, c.à.d $P = 0$ ou $Q = 0$. ■

6.3. Arithmétique dans $A[X]$

Dans la suite, on suppose que A est un anneau commutatif, unitaire et intègre.

6.3.1. Divisibilité:

Soient P , B deux polynômes de $A[X]$
On dit que B divise P , s'il exite $Q \in A[X]$ tel que $P = Q.B$

Exemple 1: Tout élément inversible a de l'anneau A divise tout polynôme P de $A[X]$ En effet: $P = a.(a^{-1}P)$

Exemple 2: Tout polynôme P divise le polynôme nul 0 En effet: $0 = 0.P$

Exemple 3: $X+1$ divise X^2+X En effet: $X^2+X = X(X+1)$

6.3.1.1 Remarques:

R1) 0 ne divise que 0, et les seuls diviseurs de 1 sont les éléments inversibles de A, qui sont aussi les seuls éléments inversibles dans $A[X]$.

(si $1 = QB$, alors $0 = \deg 1 = \deg Q + \deg B$, d'où $\deg Q = \deg B = 0$ donc $Q = q_0$ et $B = b_0$ avec $1 = q_0 b_0$)

R2) Si B divise P , on dit aussi que P est un multiple de B.

R3) Si B divise P et $P \neq 0$, alors $\deg B \leq \deg P$ ($P = Q.B$ et $\deg P = \deg Q + \deg B$)

6.3.1.2 Proposition: *Soient P et B deux polynomes de $A[X]$*
i) B divise P , si et seulement, si $P.A[X] \subset B.A[X]$
ii) $P = \lambda B$ (λ un élément inversible de A) , si et seulement, si $P.A[X] = B.A[X]$
(Les polynômes P et B sont dits associés, si $P = \lambda B$ où λ est un élément inversible de A).

Preuve: i) Evidente

Pour montrer ii), il suffit de remarquer que $P.A[X] = B.A[X]$ et équivalente, d'après i) à $P = Q_1.B$ et $B = Q_2.P$ d'où $P(1 - Q_1.Q_2) = 0$ et comme $A[X]$ est intègre (voir **Prop.6.2.5**), alors $P = 0$ ou $Q_1.Q_2 = 1$

* Si $P = 0$, alors $B = 0$ et $P = 1.B$

* Si $Q_1.Q_2 = 1$, alors Q_1 et Q_2 sont inverse l'un de l'autre, alors $Q_1 = \lambda \in A$ et $Q_2 = \lambda^{-1}$ donc $P = \lambda B$ où λ est un élément inversible de A.

Il est clair que si $P = \lambda B$, alors $B = \lambda^{-1}P$ d'où B divise P et P divise B.

6.3.2. Division euclidienne dans $A[X]$:

Soient P , B deux polynômes de $A[X]$
Si le coefficient du terme dominant de B est inversible dans A, alors il existe un couple $(Q, R) \in A[X]^2$ tels que

$P = QB + R$ *et* $\deg R < \deg B$

Preuve: a) Pour montrer l'existence, on a deux cas.

a.1) Si $P = 0$, alors $P = Q.B + R$ avec $Q = R = 0$, ce qui vérifie $-\infty = \deg R < \deg B$ ($\deg B \geq 0$ car $B \neq 0$)

a.2) Si $P \neq 0$, et $\deg P = n$ et $\deg B = m$, alors $P = p_0 + p_1X + ... + p_nX^n$ et $B = b_0 + b_1X + ... + b_mX^m$

Raisonnons par récurrence sur n.

* Si $n = 0$, on a deux cas

$1^{er}cas$: $m = 0$, alors $P = p_0$ et $B = b_0$ d'où $P = Q.B + R$ avec $Q = p_0b_0^{-1}$ et $R = 0$, ce qui vérifie $-\infty = \deg R < \deg B = 0$)

$2^{ème}cas$: $m > 0$, alors $P = p_0$ d'où $P = Q.B + R$ avec $Q = 0$ et $R = P$, ce qui vérifie $0 = \deg R < \deg B$)

* Supposons le théorème démontré pour tous les polynômes de degré inférieur ou égal à $n - 1$ et montrons qu'il reste vrai pour les polynômes de degré n.

on a deux cas

$1^{er}cas$: $m > n$, alors $P = Q.B + P$ avec $Q = 0$ et $R = P$, ce qui vérifie $n = \deg R < \deg B = m$)

$2^{ème} cas$: $m \leq n$, alors $\overline{P} = P - a_n b_n^{-1} X^{n-m}.B$ est de degré inférieur ou égal à $n-1$, alors d'après l'hypothèse de récurrence $\overline{P} = \overline{Q}B + \overline{R}$ avec $\deg \overline{R} < \deg B$

par conséquent $P = \overline{P} + a_n b_n^{-1} X^{n-m}.B = \left(\overline{Q} + a_n b_n^{-1} X^{n-m}\right) B + \overline{R}$ donc $P = Q.B + R$ avec $Q = \overline{Q} + a_n b_n^{-1} X^{n-m}$ et $R = \overline{R}$, ce qui vérifie $\deg R < \deg B$)

b) Pour montrer l'unicité, on suppose que $P = Q.B + R = Q_1.B + R_1$ tels que $\deg R < \deg B$ et $\deg R_1 < \deg B$.

Alors $(Q - Q_1).B = (R_1 - R)$ et par passage aux degrés, on obtient $\deg (Q - Q_1) + \deg B = \deg (R_1 - R) \leq \max (\deg R_1, \deg R) < \deg B$, d'où $\deg (Q - Q_1) = -\infty$, ainsi $Q - Q_1 = 0$ et par suite $R_1 - R = 0$ ■

6.3.2.1 Remarque: La preuve précédente montre que la division euclidienne de P par B, se ramène à la division euclidienne de $\overline{P}$ par B, avec $\deg \overline{P} < \deg P$, ceci est la base d'un procédé itératif appelé algorithme de la division euclidienne des polynômes.

Exemple 1: Divison $P = 3X^5 - 2X^3 - 5X^2 + 1$ par $B = 2X^3 + \frac{1}{2}X^2 - X$

$3X^5 + 0X^4 - 2X^3 - 5X^2 + 0X + 1$	$\frac{1}{2}X^3 + 2X^2 - X + 0$
$-12X^4 + 4X^3 - 5X^2 + 0X + 1$	$6X^2 - 24X + 104$
$52X^3 - 29X^2 + 0X + 1$	
$-237X^2 + 104X + 1$	

donc le quotient $Q = 6X^2 - 24X + 104$ et le reste $R = -237X^2 + 104X + 1$

6.3.3. Idéaux de $A[X]$

Un idéal de $(A[X], +, .)$ est un sous ensemble non vide I de $A[X]$ vérifiant

1) I contient le polynôme nul 0 et pour tous P,$Q \in I$: $P - Q \in I$

2) Pour tous $P \in A[X]$ et $Q \in I$: $P.Q \in I$

(voir **cours 4.Propo.4.2.6.1**)

Exemple 1: On peut facilement vérifier que les ensembles $B.A[X]$ sont des idéaux de $(A[X], +, .)$ (où B est un polynôme)

6.3.3.1.Théorème: *Soit K un corps commutatif, alors pour tout idéal I de $(K[X], +, .)$ il existe un polynôme B unitaire ou nul tel que $I = B.K[X]$*

Preuve:

1^{er} cas: Si $I = \{0\}$, alors $I = 0.K[X]$ et 0 est l'unique polynôme B vérifiant $B.K[X] = \{0\}$. Dans ce cas B est nul.

$2^{ème}$ cas: Si $I \neq \{0\}$, soit B un polynôme non nul de I de degré minimal. On choisit B unitaire (si B n'est pas unitaire, on le multiplie par l'inverse du coefficient

de son terme dominant, pour obtenir un polynôme de même degré dans I)

On a $B.K[X] \subset I$ (car I est un idéal).

Inversement; pour tout $P \in I$, il existe $(Q,R) \in K[X]^2$ tel que $R = P - QB$, avec $\deg R < \deg B$ (Voir **6.3.2**). Comme I est un idéal et $P \in I$, $QP \in I$, alors $R = P - QB \in I$ et le fait que $\deg R < \deg B$, implique $R = 0$ (car B est un polynôme non nul de I de degré minimal appartenant à I). Par conséquent $P = QB$ et $I \subset B.K[X]$

Les deux inclusions obtenues donnent l'égalité $I \subset B.K[X]$.

Si $B.K[X] = B'.K[X]$, alors $B = \lambda B'$ avec $\lambda \in K$ (voir **Propo.6.3.1.2**) et puisque B et B' sont unitaires ou nuls, alors $\lambda = 1$, d'où l'unicité de B.

6.3.4. Notion de pgcd et de ppcm.

Dans ce qui suit K est un corps commutatif.

6.3.4.1.Théorème et définition: *Soient $P_1, P_2, ..., P_s$ des polynômes de $K[X]$.*

1) Il existe un unique polynôme unitaire ou nul D vérifiant $\sum_{i=1}^{s} P_i.K[X] = D.K[X]$

2) Il existe un unique polynôme unitaire ou nul M vérifiant $\bigcap_{i=1}^{p} P_i.K[X] = M.K[X]$.

D s'appelle le plus grand commun diviseur de la fammille $P_1, P_2, ..., P_s$ et il est noté $pgcd(P_1, P_2, ..., P_s)$

M s'appelle le plus petit commun multiple de la fammille $P_1, P_2, ..., P_s$ et il est noté $ppcm(P_1, P_2, ..., P_s)$

Preuve: 1) Montrons que $\sum_{i=1}^{s} P_i.K[X]$ est un idéal de $(K[X], +, .)$. En effet:

1.1) $0 = P_1.0 + P_2.0 + ... + P_s.0$ donc $0 \in \sum_{i=1}^{s} P_i.K[X]$

1.2) Si $T \in \sum_{i=1}^{s} P_i.K[X]$ et $Q \in \sum_{i=1}^{s} P_i.K[X]$, alors $T = P_1.T_1 + P_2.T_2 + ... + P_s.T_s$ et $Q = P_1.Q_1 + P_2.Q_2 + ... + P_s.Q_s$ d'où $T - Q = P_1.(T_1 - Q_1) + P_2.(T_2 - Q_2) + ... + P_s.(T_s - Q_s) \in \sum_{i=1}^{s} P_i.K[X]$

1.3) Si $Q \in K[X]$ et $T \in \sum_{i=1}^{s} P_i.K[X]$, alors $T = P_1.T_1 + P_2.T_2 + ... + P_s.T_s$ d'où $Q.T = P_1.(Q.T_1) + P_2.(Q.T_2) + ... + P_s.(Q.T_s) \in \sum_{i=1}^{s} P_i.K[X]$

Donc, d'après **cours 4, Prop 4.2.6.1,** $\sum_{i=1}^{s} P_i.K[X]$ est un idéal de $(K[X], +, .)$

et par application du **th 6.3.3.1**, on conclut l'existence et l'unicité du polynôme D vérifiant $\sum_{i=1}^{s} P_i.K[X] = D.K[X]$.

2) Montrons que $\bigcap_{i=1}^{s} P_i.K[X]$ est un idéal de $(K[X], +, .)$. En effet:

2.1) $\forall i \in \{1, 2, ..., s\}$ on a $0 = P_i.0 \in P_i.K[X]$, alors $0 \in \bigcap_{i=1}^{s} P_i.K[X]$

2.2) Si $T \in \bigcap_{i=1}^{s} P_i.K[X]$ et $Q \in \bigcap_{i=1}^{s} P_i.K[X]$, alors $\forall i \in \{1, 2, ..., s\}$ on a $T \in P_i.K[X]$, et $Q \in P_i.K[X]$ donc $T - Q = P_i.(T_i - Q_i) \in P_i.K[X]$, et $(T - Q) \in \bigcap_{i=1}^{s} P_i.K[X]$

2.3) Si $Q \in K[X]$ et $T \in \bigcap_{i=1}^{s} P_i.K[X]$, alors $\forall i \in \{1, 2, ..., s\}$ on a $T \in P_i.K[X]$, et donc $Q.T = P_i.(Q.T_i) \in P_i.K[X]$, et $Q.T \in \bigcap_{i=1}^{s} P_i.K[X]$

Donc, d'après **cours 4, Prop 4.2.6.1,** $\bigcap_{i=1}^{s} P_i.K[X]$ est un idéal de $(K[X], +, .)$ et par application du **th 6.3.3.1**, on conclut l'existence et l'unicité du polynôme M vérifiant $\bigcap_{i=1}^{s} P_i.K[X] = M.K[X]$. ■

Exemple: $(2X^2 - 2).K[X] = \{(X^2 - 1).Q \ / \ Q \in K[X]\}$ et $(X + 1).K[X] = \{(X + 1).Q \ / \ Q \in K[X]\}$ et $(X^2 - 1).K[X] \cap (X + 1).K[X] = (2X^2 - 2).K[X]$ donc $ppcm(2X^2 - 2, X + 1) = X^2 - 1$

6.3.4.2 Remarque: Le $pgcd(P_1, P_2, ..., P_s)$ et le $ppcm(P_1, P_2, ..., P_s)$ son parfois notés respectivement $P_1 \wedge P_2 \wedge ... \wedge P_s$ et $P_1 \vee P_2 \vee ... \vee P_s$

6.3.4.3 Théorème (Caractérisation du *pgcd* et du *ppcm*): *Soient $P_1, P_2, ..., P_s$ des polynômes de $K[X]$.*

1) Le polynôme D est le $pgcd(P_1, P_2, ..., P_s)$, si et seulement, si D est unitaire ou nul et $\begin{cases} i)\ \forall i \in \{1, 2, ..., s\} \ : D \text{ divise } P_i \\ ii)\ (\forall i \in \{1, 2, ..., s\} \ : D' \text{ divise } P_i) \Longrightarrow D' \text{ divise } D \end{cases}$

2) Le polynôme M est le $ppcm(P_1, P_2, ..., P_s)$, si et seulement, si M est unitaire ou nul et $\begin{cases} i)\ \forall i \in \{1, 2, ..., s\} \ : P_i \text{ divise } M \\ ii)\ (\forall i \in \{1, 2, ..., s\} \ : P_i \text{ divise } M') \Longrightarrow M \text{ divise } M' \end{cases}$

Preuve:1) i) Si $D = pgcd(P_1, P_2, ..., P_s)$, alors D est unitaire ou nul et pour tout i on a $P_i.K[X] \subset \sum_{i=1}^{s} P_i.K[X] = D.K[X]$ donc d'après **Prop.6.3.1.2** D divise P_i, pour tout i

ii) Si D' divise tous les P_i, alors d'après la **Prop.6.3.1.2** $P_i.K[X] \subset D'.K[X]$ pour tout i , d'où $D'.K[X] \supset \sum_{i=1}^{s} P_i.K[X] = D.K[X]$ et toujours d'après la

Prop.6.3.1.2, D' divise D.

Inversement, soit D un polynôme unitaire ou nul vérifiant i) et ii). D'après i), D divise tous les P_i donc $P_i.K[X] \subset D.K[X]$ et $\sum_{i=1}^{s} P_i.K[X] \subset D.K[X]$, d'où D divise $pgcd(P_1, P_2, ..., P_s)$. En utilisant ii) et le fait que, $\forall i \in \{1, 2, ..., s\}$: $pgcd(P_1, P_2, ..., P_s)$ divise P_i, on conclut qe $pgcd(P_1, P_2, ..., P_s)$ divise D , d'où l'égalité $pgcd(P_1, P_2, ..., P_s) = \lambda.D$, avec $\lambda \in K$ (voir **Propo.6.3.1.2**) et puisque $pgcd(P_1, P_2, ..., P_s)$ et D sont unitaires ou nuls, alors $\lambda = 1$, d'où l'égalité

$pgcd(P_1, P_2, ..., P_s) = D$.

L'assertion 2) se démotre de la même façon que 1)

.

6.3.4.4 Propriétés du *pgcd* **et du** *ppcm***:** *Soient* $P_1, P_2, ..., P_s$ *des polynômes* $K[X]$.

1) Le pgcd et le ppcm ne changent pas en permuttant les P_i

2) $pgcd(\lambda_1 P_1, \lambda_2 P_2, ..., \lambda_s P_s) = pgcd(P_1, P_2, ..., P_s)$ *et* $ppcm(\lambda_1 P_1, \lambda_2 P_2, ..., \lambda_s P_s) = ppcm(P_1, P_2, ..., P_s)$ *pour* $\lambda_1, \lambda_2, ..., \lambda_s \in K$

3) Pour tout $C \in K[X]$ *on a* $pgcd(C.P_1, C.P_2, ..., C.P_s) = \widehat{C}.pgcd(P_1, P_2, ..., P_s)$ *et* $ppcm(C.P_1, C.P_2, ..., C.P_s) = \widehat{C}.ppcm(P_1, P_2, ..., P_s)$ où $\widehat{C}$ *est le polynôme unitaire ou nul associé à* C

4) Pour tout $q \in \{1, 2, ..., s\}$ *, on :*

$pgcd(P_1, P_2, ..., P_s) = pgcd(pgcd(P_1, P_2, ..., P_q), pgcd(P_{q+1}, P_{q+2}, ..., P_s))$ *et*

$ppcm(P_1, P_2, ..., P_s) = ppcm(ppcm(P_1, P_2, ..., P_q), ppcm(P_{q+1}, P_{q+2}, ..., P_s))$

(C.à. d pgcd et ppcm sont associatifs)

Preuve:1) $\sum_{i=1}^{s} P_i.K[X]$ ne change pas en permuttant les P_i d'où le résultat.

2) Pour tout i , ona $\lambda_i P_i.K[X] = P_i.K[X]$, donc $\sum_{i=1}^{s} P_i.K[X]$ ne change pas en remplaçant les P_i par $\lambda_i P_i$, d'où le résultat.

3) Pour tout i , ona $C.P_i.K[X] = \widehat{C}.P_i.K[X]$, donc $\sum_{i=1}^{s} C.P_i.K[X] = \widehat{C}.\sum_{i=1}^{s} P_i.K[X]$,d'où le résultat.

4) $\sum_{i=1}^{s} P_i.K[X] = \sum_{i=1}^{q} P_i.K[X] + \sum_{i=q+1}^{s} P_i.K[X]$, donc le *pgcd* est associatif.

La preuve est analogue pour le *ppcm*. ■

6.3.5. Algorithme d'Euclide

L'algorithme d'Euclide est un procédé itératif permettant le calcul du $pgcd\,(A,B)$, en se basant sur l'idée suivante: $pgcd\,(A,B) = pgcd\,(B,R)$ où R est le reste de la division euclidienne de A par B.

Exemple: Calculons $pgcd\,(X^4-1, X^3-1)$.

$$\begin{array}{r|l} 2X^4-2 & X^3-1 \\ \hline 2X-2 & 2X \end{array} \text{ et } \begin{array}{r|l} X^3-1 & 2X-2 \\ \hline X^2-1 & \frac{1}{2}X^2+\frac{1}{2}X+\frac{1}{2} \\ X-1 & \\ 0 & \end{array}$$

Alors $\begin{aligned} pgcd\,(2X^4-2, X^3-1) &= pgcd\,(X^3-1, 2X-2) = pgcd\,(2X-2, 0) \\ &= \tfrac{1}{2}(2X-2) = X-1 \end{aligned}$

On multiplie par $\frac{1}{2}$ pour obtenir un polynôme unitaire.

6.3.6. Polynômes premiers entre eux

6.3.6.1 Définition: *Soit* $(P_1, P_2, ..., P_s) \in K[X]^s$
1) On dit que $P_1, P_2, ..., P_s$ *sont premiers entre eux si* $a_1 \wedge a_2 \wedge ... \wedge a_q = 1$.
2) On dit que $P_1, P_2, ..., P_s$ *sont deux à deux premiers entre eux si* $P_i \wedge P_j = 1$. *pour* $i \neq j$ *(* $i, j \in \{1, 2, ..., s\}$*)*

6.3.6.2 Théorème de Bezout: *Les polynômes* $P_1, P_2, ..., P_s$ *sont premiers entre eux si, et seulement, s'il existe* $(U_1, U_2, ..., U_s) \in K[X]^s$ *tel que* $\sum_{i=1}^{s} P_i.U_i = 1$

Preuve: On a $P_1 \wedge P_2 \wedge ... \wedge P_s = 1$ donc $\sum_{i=1}^{s} P_i.K[X] = 1.K[X]$, alors il existe $(U_1, U_2, ..., U_s) \in K[X]^s$ tel que $\sum_{i=1}^{s} P_i.U_i = 1$.

Inversement, si $\sum_{i=1}^{s} P_iU_i = 1$, alors tout diviseur commun des P_i divise 1, donc $P_1 \wedge P_2 \wedge ... \wedge P_s$ divise 1, alors $\deg(P_1 \wedge P_2 \wedge ... \wedge P_s) = 0$ et puisqu'il est unitaire, il est égal à 1 ■

Exemple: Si α_1,$\alpha_2 \in K$, alors les polynômes $X-\alpha_1$ et $X-\alpha_2$ sont premiers enter eux si $\alpha_1 \neq \alpha_2$. En effet: $(\alpha_1-\alpha_2)^{-1}(X-\alpha_1) - (\alpha_1-\alpha_2)^{-1}(X-\alpha_2) = 1$.
.

6.3.6.3 Théorème de Gauss: *Soient* A, B, C *des polynômes de* $K[X]$
Si A *divise* $B.C$ *et* A *est premier avec* B *,* A *divise* C

Preuve: IL existe U et V tels que $AU + BV = 1$ en multipliant par $C = A.U.C + B.V.C$ donc A divise C car A divise $A.U.C + B.V.C$ ■.

.

6.3.6.4 Propriétés des polynômes premiers entre eux: *Soient* $P_1, P_2, ..., P_s$, A, B, C *des polynômes de* $K[X]$ *et* m, n *des entiers naturels*

1)Si $\forall i \in \{1, 2, ..., s\} : P_i \wedge C = 1$, *alors* $\left(\prod_{i=1}^{s} P_i\right) \wedge C = 1$

2) Si $A \wedge B = 1$ *Alors* $A^n \wedge B^m = 1$

3) Si $P_1, P_2, ..., P_s$ *sont deux à deux premiers entre eux, alors* $P_1 \vee P_2 \vee ... \vee P_s = \lambda \prod_{i=1}^{s} P_i$, *pour un certain* $\lambda \in K$

4) $(A \wedge B).(A \vee B) = \lambda.A.B$, *pour un certain* $\lambda \in K$ *(cette propriété n'est toujours vraie que pour deux polynômes)*

5) Si $P_1, P_2, ..., P_s$ *sont deux à deux premiers entre eux et chaque* P_i *divise* B , *alors* $\prod_{i=1}^{s} a_i$ *divise* B

Preuve: 1) $P_i \wedge C = 1$, alors il existe des entires U_i et V_i tels que $P_i U_i + C V_i = 1$. En multipliant ces égalités, on obtient $1 = \prod_{i=1}^{s} (P_i U_i + C V_i) = \left(\prod_{i=1}^{s} P_i U_i\right) + R$ où R est la somme des termes qui restent , qui contiennent tous C comme facteur.

Alors $1 = \left(\prod_{i=1}^{s} P_i\right).U + CV$; où $U = \prod_{i=1}^{s} U_i$ et $CV = R$, donc $\left(\prod_{i=1}^{s} P_i\right) \wedge C = 1$ (d'après le théorème de Bezout: **Th.6.3.6.2**)

2) Si $n = 0$ où $m = 0$, il est clair que $A^n \wedge B^m = 1$.

Et si $n \neq 0$ et $m \neq 0$, alors d'après 1), on a $A^n \wedge B = 1$ en choisissant $P_1 = P_2 = ... = P_n = A$ et $C = B$, en suite $A^n \wedge B^m = 1$ toujours d'après 1), en choisissant $P_1 = P_2 = ... = P_n = B$ et $C = A^n$.

3) Commençons par le cas $p = 2$, et soit $M = P_1 \vee P_2$. On $P_1 \wedge P_2 = 1$, alors il existe U_1, $U_2 \in K[X]$ tels que $P_1 U_1 + P_2 U_2 = 1$, donc $M = P_1 U_1 M + P_2 U_2 M$, or $M = P_1 M_1$ et $M = P_2 M_2$ d'où $M = P_1 P_2 (U_1 M_2 + U_2 M_1)$, et $P_1 P_2$ divise M, mais M divise $P_1 P_2$ (car $P_1 P_2$ est un multiple commun de P_1 et P_2), alors on a l'égalité $P_1 P_2 = \lambda M = \lambda (P_1 \vee P_2)$, pour un certain $\lambda \in K$ (Voir **Prop.6.3.1.2**)

Pour le cas p quelconque , on procède par récurrence en supposant la propriété vraie à l'ordre q et en la montant à l'ordre $q + 1$.

On a d'après 1) $\left(\prod_{i=1}^{q} P_i\right) \wedge P_{q+1} = 1$ et d'après le cas $p = 2$, ona $\left(\prod_{i=1}^{q} P_i\right) \vee P_{q+1} = \lambda' \prod_{i=1}^{q+1} P_i$. En utilisant l'hypothèse de récurrence et **Prop.6.3.4.4** 2) et 4) , on conclut que: $\lambda' \prod_{i=1}^{q+1} P_i = \lambda'' (a_1 \vee a_2 \vee ... \vee a_q) \vee a_{q+1} = a_1 \vee a_2 \vee ... \vee a_q \vee a_{q+1}$

4) Si $A = 0$ ou $B = 0$ l'égalité est triviale.

Et si $A \neq 0$ et $B \neq 0$, alors en posant $A = (A \wedge B).A'$ et $B = (A \wedge B).B'$, les polynômes A' et B' deviennent premiers entre eux, alors d'après 3) $A' \vee B' = \lambda A'B'$ et en utilisant **Pté 6.3.4.4,** on conclut que

$$\begin{aligned} \lambda AB &= (A \wedge B)^2 \lambda A'B' = (A \wedge B)^2 (A' \vee B') \\ &= (A \wedge B)((A \wedge B) A' \vee (A \wedge B) B') = (A \wedge B)(A \vee B) \end{aligned}$$

5) B est un multiple commun des P_i, donc c'est un multiple de leur *ppcm* qui est égal, d'après 3), à $\lambda \prod_{i=1}^{s} P_i$, donc $\prod_{i=1}^{s} P_i$ divise B. ■

6.3.7. Polynomes irréductibles

6.3.7.1 Définition: *On appelle polynôme irréductible ou premier dans* $K[X]$ *tout polynôme* P *tel que* $\deg P \geq 1$ *dont les seuls diviseurs sont les polynomes* λ *et* $\lambda.P$, où $\lambda \in K^* = K - \{0\}$.

Exemple 1: $X - a$ est un polynôme irréductible dans $K[X]$ et d'une façon générale tout polynôme P de degré 1 est irréductible dans $K[X]$.

En effet: Si B divise P, alors $\deg B \leq \deg P = 1$ et comme B ne peut pas être nul, on conclut que $\deg B \in \{0, 1\}$ donc $B \in \{\lambda, \lambda.P\}$ où $\lambda \in K^*$.

Exemple 2: $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ car on ne peut pas l'écrire comme produit de deux polynômes de degré 1 à coefficients dans $\mathbb{R}$.

Le même polynome X^2+1 est réductible dans $\mathbb{C}[X]$, car $X^2+1 = (X + i)(X - i)$

Exemple 3: X^4+4 est réductible $\mathbb{Q}[X]$, car $X^4+4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$

.

6.3.7.2 Proposition: *Soient* P *un polynôme irréductible et* $A, A_1, A_2, ..., A_s$ *des des polynômes de* $K[X]$*, alors:*

1) Ou bien P *est premier avec* A *ou bien* P *divise* A.

2) Si P *divise* $\prod_{i=1}^{s} A_i$ *, alors* P *divise au moins l'un des* A_i.

Preuve: 1) Les seuls diviseurs de P sont λ et λP, ($\lambda \in K^*$)alors ou bien $pgcd(A, P) = \lambda^{-1}\lambda = 1$, donc P et premier avec A, ou bien $pgcd(A, P) = \widehat{P}$ (où est le polynôme unitaire associé à P) donc P divise A.

2) Supposons que P ne divise aucun A_i , alors d'après 1) , il est premier avec tous les A_i, et d'après **Ptè 6.3.6.4** , P est premier avec $\prod_{i=1}^{s} P_i$, ce qui est absurde. ■

.

6.3.7.3 Théorème: *Tout polynôme* P *de* $K[X]$ *tel que* $\deg P \geq 1$*, possède au moins un diviseur irréductible unitaire.*

Preuve: L'ensemble $Deg\mathcal{D}_P$ des degrés des polynômes non constants diviseurs de P, n'est pas vide (car $\deg P \in Deg\mathcal{D}_P$), alors il possède un plus petit élément $\deg Q$. Cet élément Q est irréductible. En effet: Soit D un diviseur de Q , alors ou bien D est constant ($D = \lambda \in K^*$), ou bien D est non constant donc $\deg D \in Deg\mathcal{D}_P$, alors $\deg Q \leq \deg D$, d'où $\deg Q = \deg D$ et $Q = \lambda D$, alors Q est irréductible.

En fin $\widehat{Q}$ le polynôme unitaire associé à Q est un diviseur de P. ■

6.3.7.4 Théorème: (Décomposition en facteurs irréductibles)

Pour tout polynôme P de $K[X]$ tel que $\deg P \geq 1$, *il existe, de façon unique (à une permutation près), des polynômes irréductibles $P_1, P_2, ..., P_r$ unitaires, deux à deux distincts de $K[X]$ et des nombres entiers naturels strictement positifs $\alpha_1, \alpha_2, ..., \alpha_r$ et il existe un élément unique $\lambda \in K^*$ tels que $P = \lambda \prod_{i=1}^{r} p_i^{\alpha_i}$.*

Preuve: 1) Montrons l'existance de la décomposition par récurrence sur $\deg P$

1.1) Si $\deg P = 1$, alors P est irréductible et $P = \lambda \widehat{P}$ où $\widehat{P}$ est le polynôme unitaire associé à P.

1.2) Supposons maintenant que la décomposition est valable pour tout polynôme non constant de degré inférieur à n et montrons qu'elle reste valable pour un polynôme P de degré n.

Si P est irréductible alors $P = \lambda \widehat{P}$ où $\widehat{P}$ est le polynôme unitaire associé à P.

Sinon $P = AB$ où A et B sont des polynômes non constants de degrés inférieurs à n, alors en appliquant l'hypothèse de récurrence à A et B, on obtient une décomposition de leur produit P.

2) Pour l'unicité, supposons $P = \lambda \prod_{i=1}^{r} P_i^{\alpha_i} = \gamma \prod_{j=1}^{s} Q_j^{\beta_j}$.

2.1) Comme $\prod_{i=1}^{r} P_i^{\alpha_i}$ et $\prod_{j=1}^{s} Q_j^{\beta_j}$ sont unitaires, alors $\lambda = \gamma$ et $\prod_{i=1}^{r} P_i^{\alpha_i} = \prod_{j=1}^{s} Q_j^{\beta_j}$

2.2) On a chaque P_i divise $\prod_{j=1}^{s} Q_j^{\beta_j}$, alors d'après **Prop 6.3.7.2**, P_i divise au moins l'un des Q_j , et puisque Q_j et P_i sont unitaires et irréductibles alors $P_i = Q_j$. Par cconséquent $\{P_1, P_2, ..., P_r\} \subset \{Q_1, Q_2, ..., Q_s\}$. De la même façon, on montre l'autre inclusion, d'où l'égalité $\{P_1, P_2, ..., P_r\} = \{Q_1, Q_2, ..., Q_s\}$

Ainsi $r = s$ et à une permutation près on peut écrire $P_i = Q_i$.

Pour montrer que $\alpha_i = \beta_i$, supposons $\alpha_i < \beta_i$

Or $0=\prod_{i=1}^{r}P_i^{\alpha_i}-\prod_{i=1}^{r}Q_i^{\beta_i}=P_i^{\alpha_i}\left(\prod_{\substack{k=1\\k\neq i}}^{r}P_k^{\alpha_k}-Q_i^{\beta_i-\alpha_i}\prod_{\substack{k=1\\k\neq i}}^{r}Q_k^{\beta_k}\right)$ et comme $K[X]$ est intègre et $P_i^{\alpha_i}\neq 0$, alors $\prod_{\substack{k=1\\k\neq i}}^{r}P_k^{\alpha_k}=Q_i^{\beta_i-\alpha_i}\prod_{\substack{k=1\\k\neq i}}^{r}Q_k^{\beta_k}$ et Q_i divise le deuxième membre sans diviser le premier, ce qui est impossible. De la même façon, on montre qu'il est impossible d'avoir $\alpha_i>\beta_i$, d'où l'égalité $\alpha_i=\beta_i$ ■

.

6.3.7.4 Calcul du *pgcd* et du *ppcm* à l'aide de la décomposition en facteurs irréductibles:

Soit $A\in K[X]^*=K[X]-\{0\}$, Pour tout polynôme irréductible unitaire P, on note par $v_P(A)$, l'exposant de P dans la décomposition en facteurs irréductibles de A. Alors:

$v_P(A)=0$, si P ne divise pas A

$v_P(A)\neq 0$, si P divise A

Donc la décomposition donnée par le théorème **Th 6.3.7.3** , peut être écrite $A=\lambda\prod_{P\in\mathcal{P}}P^{v_p(A)}$, où $\mathcal{P}$ est l'ensemble de tous les polynômes irréductibles unitaires de $K[X]$.

Exemple: Dans $\mathbb{C}[X]$, on a: $v_{X+i}(X^2+1)=1$, $v_{X+1}(X^2+1)=0$

6.3.7.4.1 Théorème: *Soient $A_1,A_2,...A_s$ des polynômes de $K[X]^*$.*

On a, alors
$$\begin{cases} pgcd(A_1,A_2,...A_s)=\prod_{P\in\mathcal{P}}P^{\min(v_P(A_1),v_p(A_2),...,v_p(A_s))}\\ ppcm(A_1,A_2,...A_s)=\prod_{P\in\mathcal{P}}P^{\max(v_P(A_1),v_p(A_2),...,v_p(A_s))}\end{cases}$$

Preuve: 1) Soit $D=pgcd(A_1,A_2,...A_s)$ et $\Gamma=\prod_{P\in\mathcal{P}}P^{\min(v_P(A_1),v_p(A_2),...,v_p(A_s))}$.

Pour tout i ; $P^{\min(v_P(A_1),v_p(A_2),...,v_p(A_s))}$ divise les $P^{v_p(A_i)}$, d'où

$\Gamma=\prod_{P\in\mathcal{P}}P^{\min(v_P(A_1),v_p(A_2),...,v_p(A_s))}$ divise les $\prod_{P\in\mathcal{P}}P^{v_p(A_i)}=A_i$ et d'après le **Th 6.3.4.3** on conclut que Γ divise D.

Inversement, $D=pgcd(A_1,A_2,...A_s)$ et comme D divise les A_i, alors $v_P(D)\leq v_P(A_i)$, pour tout $i\in\{1,2,...,s\}$, donc $v_P(D)\leq\min(v_P(A_1),v_P(A_2),...,v_P(A_s))$ et $P^{v_P(D)}$ divise $P^{\min(v_P(A_1),v_p(A_2),...,v_p(A_s))}$, et par passage aux produits, on aura D divise Γ , d'où l'égalité $D=\Gamma$.

2) La preuve est analogue pour le *ppcm* ■

6.4. Fonctions polynômes d'une variable, polynôme dérivé et racine d'un polynôme

6.4.1 Définitions: *Soit* $P = a_0 + a_1X^1 + ... + a_{n-1}X^{n-1} + a_nX^n$ *un polynôme de* $K[X]$.

1) On appelle fonction polynôme d'une variable x *associée à* P*, la fonction* $\widetilde{P}$ *de* K *dans* K *définie par:* $\widetilde{P}(x) = a_0 + a_1x^1 + ... + a_{n-1}x^{n-1} + a_nx^n$

2) On dit qu'un élément α *est une racine ou zéro de* P*, si* $\widetilde{P}(\alpha) = 0$.

3) On appelle polynôme dérivé du polynôme P *le polynôme noté* P' *défini par:* $P' = a_1 + 2a_2X^1 + ... + (n-1)a_{n-1}X^{n-2} + na_nX^{n-1}$

Exemple 1: La fonction polynôme associée au polynôme $P = X^2 + 2X - 3$ de $\mathbb{R}[X]$ est la fonction $\widetilde{P} : \mathbb{R} \to \mathbb{R}$ telle que $\widetilde{P}(x) = x^2 + 2x - 3$ et les seules racines de P sont -3 et 1 car $\widetilde{P}(-3) = \widetilde{P}(1) = 0$

Le polynôme dérivé de P est $P' = 2X + 2$

Exemple 2: La fonction polynôme associée au polynôme $P = X^2 - 2$ de $\mathbb{Q}[X]$ est la fonction $\widetilde{P} : \mathbb{Q} \to \mathbb{Q}$ telle que $\widetilde{P}(x) = x^2 - 2$ et P n'a pas de racine car $\widetilde{P}(x) \neq 0$ pour tout $x \in \mathbb{Q}$.

Le polynôme dérivé de P est $P' = 2X$

6.4.2 Remarque: 1) On dit que $\widetilde{P}(x)$ est obtenu par substitution de x à X dans P.

2) On vérifie facilement que $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$, $\widetilde{P.Q} = \widetilde{P}.\widetilde{Q}$, $\widetilde{P'} = \widetilde{P'}$, $(P+Q)' = P' + Q'$ et $(P.Q)' = P'.Q + P.Q'$

3) Si $\deg P \geq 1$, alors $\deg P' = \deg P - 1$ et $\deg P < 1$, alors $\deg P' = -\infty$

6.4.3 Théorème: *Soit* $P \in K[X]$ *et* $\alpha \in K$*, alors:*

1) Le reste de la division euclidienne de P *par* $X - \alpha$ *est* $\widetilde{P}(\alpha)$.

2) α *est une racine de* P *si, et seulement, si* $X - \alpha$ *divise* P

Preuve: 1) On a $P = (X - \alpha)Q + R$ où R et Q sont respectivement le reste et le quotient de la division euclidienne de P par $X - \alpha$. Alors $\widetilde{P} = \widetilde{(X - \alpha)}\widetilde{Q} + \widetilde{R}$,ainsi $\widetilde{P}(\alpha) = \widetilde{R}(\alpha)$.

Or $\deg R < 1$ donc R et constant, d'où $\widetilde{R} = R$ et $\widetilde{R}(\alpha) = R$. Par conséquent $\widetilde{P}(\alpha) = R$.

2) est une conséquence directe de 1). ■

Exemple: -3 est une racine du polynôme $P = X^3 + 5X^2 + 3X - 9$ de $\mathbb{R}[X]$, alors $P = (X + 3)Q$ avec $Q = 2X + X^2 - 3$

6.4.4 Ordre de multiplicité d'une racine: *Soit* $P \in K[X]^*$ *et* α *une racine de* P*. On appelle ordre de multiplicité de la racine* α *de* P*, le plus grand* $m \in \mathbb{N}$

tel que $(X-\alpha)^m$ *divise* P.

* *Si* $m=1$, *on dit que* α *une racine simple de* P

* *Si* $m=2$, *on dit que* α *une racine double de* P.

* *Si* $m=3$, *on dit que* α *une racine triple de* P. *...etc*

Exemple: -3 est une racine double du polynôme $P=X^3+5X^2+3X-9$ de $\mathbb{R}[X]$, car $P=(X+3)^2(X-1)$

6.4.5 Théorème: *Soient* $P\in K[X]^*$ *et* $\alpha\in K$. α *est une racine simple de* P *si, et seulement, si* $\widetilde{P}(\alpha)=0$ *et* $\widetilde{P}'(\alpha)\neq 0$ *(où* $\widetilde{P}'$ *est la dérivée de* $\widetilde{P}$*)*

Preuve: α est une racine simple de P si, et seulement, s'il existe $Q\in K[X]$ tel que $P=(X-\alpha)Q$ et $Q(\alpha)\neq 0$.

Or $\widetilde{P}'=\widetilde{Q}+(x-\alpha)\widetilde{Q}'$ donc $\widetilde{P}'(\alpha)=Q(\alpha)$, d'où l'équivalence voulue. ■

Exemple: Soit le polynôme $P=X^3+5X^2+3X-9$ de $\mathbb{R}[X]$,

On a $\widetilde{P}(1)=0$ et $\widetilde{P}'(1)\neq 0$ $(\widetilde{P}'(x)=3X^2+10X+3)$

6.4.6 Proposition: *Si* $\alpha_1,\alpha_2,...,\alpha_r$ *sont des racines deux à deux distinctes de* P, *d'ordres de multiplicité respectifs* $m_1,m_2,...,m_r$, *alors* $\prod_{i=1}^{r}(X-\alpha_i)^{m_i}$ *divise* P.

Preuve: Les α_i sont deux à deux distinctes, alors les polynomes $X-\alpha_i$ sont premiers entre eux et par suite $(X-\alpha_i)^{m_i}$sont premiers entre eux

Or $(X-\alpha_i)^{m_i}$ divise P donc $\prod_{i=1}^{r}(X-\alpha_i)^{m_i}$ divise P. (voir **Ptés 6.3.6.4**). ■

6.4.6.1 Corollaire: *1) Un polynôme de degré* $n\in\mathbb{N}$ *admet au plus* n *racines distinctes.*

2) *Si* P *possède une infinité de racines, alors* P *est le polynome nul.*

Preuve: 1) Supposons $\alpha_1,\alpha_2,...,\alpha_{n+1}$ des racines distinctes de P, alors d'après la proposition précédente, $\prod_{i=1}^{n+1}(X-\alpha_i)$ divise P, donc $n+1=\deg\left(\prod_{i=1}^{n+1}(X-\alpha_i)\right)\leq \deg P=n$ ce qui est absurde.

2) L'assertion 1) montre que si P admet une infinité de racine, alors $\deg P\notin\mathbb{N}$, donc P est nul. ■

6.4.7 Théorème:(Théorème fondamental de l'algèbre): *Tout polynôme non constant de* $\mathbb{C}[X]$ *admet au moins une racine dans* $\mathbb{C}$.
Autrement dit: Les polynômes irréductibles de $\mathbb{C}[X]$ *sont les polynômes de degré* 1

(La preuve de ce théorème dépasse le cadre du cours d'algèbre de $1^{ère}$ année LMD)

6.4.7.1 Remarque: Il existe des formules donnant les racines d'un polynôme de degré $1,2,3$ et 4 de $\mathbb{C}[X]$. De telles formules n'existent pas pour un polynôme

de degré $n \geq 5$, alors on ne peut décomposer un polynôme de $\mathbb{C}[X]$ que dans des cas particuliers.

Exemple: Soit $P = X^7 - 8X$

$$\begin{aligned} P &= X^7 - 8X = X\left(X^6 - 8\right) = X\left(\left(X^2\right)^3 - 2^3\right) = X\left(X^2 - 2\right)\left(X^4 + 2X^2 + 4\right) \\ &= X\left(X^2 - 2\right)\left(X^2 + 1 - i\sqrt{3}\right)\left(X^2 + 1 + i\sqrt{3}\right) \\ &= X\left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)\left(X - \tfrac{1+i\sqrt{3}}{\sqrt{2}}\right)\left(X + \tfrac{1+i\sqrt{3}}{\sqrt{2}}\right)\left(X - \tfrac{1-i\sqrt{3}}{\sqrt{2}}\right)\left(X + \tfrac{1-i\sqrt{3}}{\sqrt{2}}\right) \end{aligned}$$

cette écriture est une décomposition de P en facteurs irréductibles dans $\mathbb{C}[X]$.

Pour obtenir la décomposition en facteurs irréductibles dans $\mathbb{R}[X]$, il faut remplacer les facteurs dont les produits sont des polynômes irréductibles dans $\mathbb{R}[X]$ par leurs produits.

$$\begin{aligned} P &= X\left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)\left(X - \tfrac{1+i\sqrt{3}}{\sqrt{2}}\right)\left(X - \tfrac{1-i\sqrt{3}}{\sqrt{2}}\right)\left(X + \tfrac{1+i\sqrt{3}}{\sqrt{2}}\right)\left(X + \tfrac{1-i\sqrt{3}}{\sqrt{2}}\right) \\ &= X\left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)\left(X^2 - \sqrt{2}X + 2\right)\left(X^2 + \sqrt{2}X + 2\right) \end{aligned}$$

cette écriture est une décomposition de P en facteurs irréductibles dans $\mathbb{R}[X]$.

Pour obtenir la décomposition en facteurs irréductibles dans $\mathbb{Q}[X]$, il faut remplacer les facteurs dont les produits sont des polynômes irréductibles dans $\mathbb{Q}[X]$ par leurs produits.

$$\begin{aligned} P &= X\left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)\left(X^2 - \sqrt{2}X + 2\right)\left(X^2 + \sqrt{2}X + 2\right) \\ &= X\left(X^2 - 2\right)\left(X^4 + 2X^2 + 4\right) \end{aligned}$$

cette écriture est une décomposition de P en facteurs irréductibles dans $\mathbb{Q}[X]$.

Université Ibn Khaldoun de Tiaret.
Département d'Informatique.
Module:Algèbre 1 ($1^{ère}$ Année LMD)

Fiche de T.D N^0 6

Exercice 1: Montrer que dans $\mathbb{Z}[X]$ le polynôme Q divise le polynôme P dans les cas suivants: 1) $P = nX^{n+1} - (n+1)X^n + 1 \quad Q = (X-1)^2$
2) $P = 1 + X + X^2 + ... + X^{2n+1} \quad Q = 1 + X^{2n}$ (Calculer $(1-X)P$)

Exercice 2: Trouver dans $\mathbb{R}[X]$ les polynômes de degré $n \leq 6$, divisibles par X^2+1 et $X^2 - X + 1$

Exercice 3: Déterminer 1) $pgcd\,(X^5 + X^4 - X^3 + X^2 + X - 1, X^5 + X^4 + 2X^2 - 1)$
2) $ppcm\,(3X^5 + X^3 - 6X^2 - 2, 3X^4 - 2X^2 - 1)$
3) $pgcd\,(X^{3n} + 1, X^{2n} - 1)$

Exercice 4: Dans $\mathbb{R}[X]$, montrer que les polynômes $P = X^3 + 1$ et $Q = X^4 + 1$ sont premiers entre eux et déterminer deux polynômes U et V vérifiant $UP + VQ = 1$

Exercice 5: Donner une condition nécessaire et suffisante pour qu'un polynome de degré 2 soit irréductible dans $\mathbb{R}[X]$ (resp dans $\mathbb{Q}[X]$).
Application: $P_1 = \frac{1}{2}X^2 - 3$, $P_2 = X^2 - 2X - 3$, $P_1 = X^2 + X + 1$

Exercice 5: Dans $\mathbb{R}[X]$, décomposer $X^6 + 1$ et $X^4 + 2X^2 + 1$ en facteurs irréductibles puis calculer leur *pgcd*.

Exercice 6: Dans $\mathbb{R}[X]$, un polynôme P a pour restes respectifs $3, 7, 13$ dans les divisions euclidienne par $(X-1)$, $(X-2)$, $(X-3)$. Déterminer le reste de la division euclidienne de P par $(X-1)(X-2)(X-3)$.

Exercice 7: Soit $A = a_0 + a_1X + ...a_nX^n \in \mathbb{Z}[X]$, avec $a_n \neq 0$ et $n \geq 2$.
1) Soit $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $p \wedge q = 1$. Montrer que si $\frac{p}{q}$ est une racine de A alors p divise a_0 et p divise a_n.
2) Que peut-on dire des racines rationnelles de A si A est unitaire.
3) Déterminer les racines rationnelles des polynômes:
$X^4 - 10X^2 + 1$, $3X^3 + 23X^2 + 57X + 45$.

Exercice 8: Soit $\mathbb{R}_2[X]$ le sous ensemble de $\mathbb{R}[X]$, formé des polynômes de degré au plus 2.
1) Montrer que $(\mathbb{R}_2[X], +)$ est un sous groupe de $(\mathbb{R}[X], +)$.
2) Soit u l'application définie de $\mathbb{R}_2[X]$ dans $\mathbb{R}_2[X]$ définie par $u(P) = X^2P' - 2XP$.
Montrer que u est un endomorphisme de $(\mathbb{R}_2[X], +)$ et calculer son noyau et son image.