Chapitre 6 : Les polynômes formels à une indéterminée à coefficients dans un corps $\mathbb{K}$.

Dans ce chapitre, $(\mathbb{K},+,\times)$ désigne un corps (commutatif) quelconque.

I La construction

A) Etape 1

- Soit $P_{\mathbb{K}}$ l'ensemble des suites d'éléments de $\mathbb{K}$, indexées pas $\mathbb{N}$ et nulles à partir d'un certain rang.

C'est-à-dire que $P_{\mathbb{K}}$ est l'ensemble des $a \in \mathbb{K}^{\mathbb{N}}$ telles que $\exists N \in \mathbb{N}, \forall n > N, a_k = 0_{\mathbb{K}}$

- On peut définir deux lois + et $\times$ de la manière suivante :

Pour tous $P=(a_i)_{i\in\mathbb{N}}, Q=(b_i)_{i\in\mathbb{N}} \in P_{\mathbb{K}}$, on pose :

$P+Q=(a_i+b_i)_{i\in\mathbb{N}}$

et $P\times Q=(p_k)_{k\in\mathbb{N}}$ où $\forall k \in \mathbb{N}, p_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}$

Alors :

+ et $\times$ constituent des lois de composition internes sur $P_{\mathbb{K}}$, et $(P_{\mathbb{K}},+,\times)$ est un anneau commutatif.

- Déjà, + est bien une loi de composition interne sur $P_{\mathbb{K}}$.

En effet, si $P=(a_i)_{i\in\mathbb{N}}$ et $Q=(b_i)_{i\in\mathbb{N}} \in P_{\mathbb{K}}$, alors il existe $n \in \mathbb{N}$ tel que $\forall i > n, a_i = 0_{\mathbb{K}}$ et $m \in \mathbb{N}$ tel que $\forall i > m, b_i = 0_{\mathbb{K}}$. Donc $\forall i > \max(n,m), a_i + b_i = 0_{\mathbb{K}}$. Donc $P+Q$ est nulle à partir d'un certain rang, donc $P+Q \in P_{\mathbb{K}}$.

- Montrons que $\times$ est une loi de composition interne sur $P_{\mathbb{K}}$.

Soient $P=(a_i)_{i\in\mathbb{N}}, Q=(b_i)_{i\in\mathbb{N}} \in P_{\mathbb{K}}$, $n \in \mathbb{N}$ tel que $\forall i > n, a_i = 0_{\mathbb{K}}$ et $m \in \mathbb{N}$ tel que $\forall i > m, b_i = 0_{\mathbb{K}}$. Notons enfin $P\times Q=(p_k)_{k\in\mathbb{N}}$

Alors $\forall k > n+m$, $p_k = 0_{\mathbb{K}}$. En effet :

Soit $k > n+m$. Alors pour tout $(i,j) \in \mathbb{N}^2$:

Si $i+j=k$, alors $i > m$ ou $j > n$

(car sinon $j \le n$ et $i \le m$, et alors $i+j \le m+n < k$)

Donc $a_i = 0_{\mathbb{K}}$ ou $b_j = 0_{\mathbb{K}}$, soit $a_i b_j = 0_{\mathbb{K}}$

Donc $p_k = \sum_{i+j=k} a_i b_j = 0_{\mathbb{K}}$.

Donc $P\times Q \in P_{\mathbb{K}}$.

- + n'est autre que la restriction à $P_{\mathbb{K}}$ de la loi + sur $\mathbb{K}^{\mathbb{N}}$.

Donc + est associative et commutative.

De plus, la suite $(0_{\mathbb{K}})_{k\in\mathbb{N}}$ est évidemment neutre pour + et appartient à $P_{\mathbb{K}}$.

Et enfin, si $P=(a_i)_{i\in\mathbb{N}} \in P_{\mathbb{K}}$, alors $Q=(-a_i)_{i\in\mathbb{N}} \in P_{\mathbb{K}}$ et $P+Q=(0_{\mathbb{K}})_{k\in\mathbb{N}}$.

- Pour $\times$:

$\times$ est évidemment commutative (car $\times$ est commutative sur le corps $\mathbb{K}$)

Il existe un neutre pour $\times$, c'est $U=(1_{\mathbb{K}},0_{\mathbb{K}},0_{\mathbb{K}}...)$

En effet : notons $U=(u_i)_{i\in\mathbb{N}}$ avec $u_0=1_{\mathbb{K}}$ et $\forall i\geq 1, u_i=0_{\mathbb{K}}$.

Soit alors $P=(a_i)_{i\in\mathbb{N}}\in P_{\mathbb{K}}$.

Alors $PU=(p_k)_{k\in\mathbb{N}}$, où $p_k=\sum_{i+j=k}a_iu_j=a_ku_0=a_k\times 1_{\mathbb{K}}=a_k$

Donc $PU=P$, et par commutativité $UP=P$, donc U est bien neutre pour $\times$.

Distributivité de $\times$ sur $+$:

Soient $P=(a_i)_{i\in\mathbb{N}},Q=(b_i)_{i\in\mathbb{N}},R=(c_i)_{i\in\mathbb{N}}\in P_{\mathbb{K}}$. Alors :

$P\times(Q+R)=(p_k)_{k\in\mathbb{N}}$, où, pour tout $k\in\mathbb{N}$:

$$p_k=\sum_{i+j=k}a_i(b_j+c_j)\underset{\substack{\uparrow\\ \text{distributivité dans le corps } \mathbb{K}}}{=}\sum_{i+j=k}a_ib_j+a_ic_j\underset{\substack{\uparrow\\ \text{associativité, commutativité de } + \text{ dans } \mathbb{K}}}{=}\sum_{i+j=k}a_ib_j+\sum_{i+j=k}a_ic_j$$

Et $P\times Q+P\times R=(q_k)_{k\in\mathbb{N}}$, où, pour tout $k\in\mathbb{N}$:

$q_k=\sum_{i+j=k}a_ib_j+\sum_{i+j=k}a_ic_j$.

Donc $P\times(Q+R)=P\times Q+P\times R$

Et $(Q+R)\times P=P\times(Q+R)=P\times Q+P\times R=Q\times P+R\times P$

Associativité de $\times$:

Soient $P=(a_i)_{i\in\mathbb{N}},Q=(b_i)_{i\in\mathbb{N}},R=(c_i)_{i\in\mathbb{N}}\in P_{\mathbb{K}}$.

Alors $P\times Q=(p_k)_{k\in\mathbb{N}}$, où, pour tout $k\in\mathbb{N}$, $p_k=\sum_{i+j=k}a_ib_j$.

Et $(P\times Q)\times R=(q_l)_{l\in\mathbb{N}}$, où, pour tout $l\in\mathbb{N}$, $q_l=\sum_{k+s=l}p_kc_s$

Donc $$q_l=\sum_{k+s=l}\left(\left(\sum_{i+j=k}a_ib_j\right)c_s\right)\underset{\substack{\uparrow\\ \text{distributivité dans } \mathbb{K}}}{=}\sum_{k+s=l}\left(\sum_{i+j=k}a_ib_jc_s\right)\underset{\substack{\uparrow\\ \text{associativité et commutativité de } + \text{ dans } \mathbb{K}}}{=}\sum_{i+j+s=l}a_ib_jc_s$$

Par ailleurs, on a de même $P\times(Q\times R)=(r_l)_{l\in\mathbb{N}}$, où, pour tout $l\in\mathbb{N}$:

$r_l=\sum_{i+j+s=l}a_ib_jc_s$.

D'où $P\times(Q\times R)=(P\times Q)\times R$, et le résultat comme $\times$ est commutative.

Donc $(P_{\mathbb{K}},+,\times)$ est bien un anneau commutatif.

B) Etape 2 : plongement de $\mathbb{K}$ dans $P_{\mathbb{K}}$.

Soit $\phi:\ \mathbb{K}\to P_{\mathbb{K}}$
$\lambda\mapsto\phi(\lambda)=(\lambda,0_{\mathbb{K}},0_{\mathbb{K}},...)$ noté $\hat{\lambda}$.

Alors ϕ est un morphisme injectif d'anneaux :

- $\phi(\lambda+\mu)=(\lambda+\mu,0_{\mathbb{K}},0_{\mathbb{K}}...)=(\lambda,0_{\mathbb{K}},0_{\mathbb{K}}...)+(\mu,0_{\mathbb{K}},0_{\mathbb{K}}...)=\phi(\lambda)+\phi(\mu)$
- $\phi(\lambda\mu)=(\lambda\mu,0_{\mathbb{K}},0_{\mathbb{K}}...)=(\lambda,0_{\mathbb{K}},0_{\mathbb{K}}...)(\mu,0_{\mathbb{K}},0_{\mathbb{K}}...)=\phi(\lambda)\phi(\mu)$

Justification de la deuxième égalité :

$\underbrace{(\lambda,0_{\mathbb{K}},0_{\mathbb{K}}...)}_{(a_i)_{i\in\mathbb{N}}}\underbrace{(\mu,0_{\mathbb{K}},0_{\mathbb{K}}...)}_{(b_i)_{i\in\mathbb{N}}}=(c_k)_{k\in\mathbb{N}}$

avec $c_k=\sum_{i+j=k}a_ib_j$.

Donc $c_k=a_0b_0=\lambda\mu$ si $k=0$ et $c_k=0_{\mathbb{K}}$ sinon.

- $\phi(1_{\mathbb{K}})=(1_{\mathbb{K}},0_{\mathbb{K}},0_{\mathbb{K}},...)=1_{P_{\mathbb{K}}}$
- Enfin, si $(\lambda,0_{\mathbb{K}},0_{\mathbb{K}}...)=(\mu,0_{\mathbb{K}},0_{\mathbb{K}}...)$, alors évidemment $\lambda=\mu$

Par conséquent, $\phi(\mathbb{K})$ est un sous anneau de $P_{\mathbb{K}}$, isomorphe à l'anneau $(\mathbb{K},+,\times)$.

(On dit qu'« il y a une copie de $\mathbb{K}$ dans $P_{\mathbb{K}}$ ») On va identifier cette copie à $\mathbb{K}$, c'est-à-dire identifier, pour chaque $\lambda\in\mathbb{K}$, λ et $\hat{\lambda}$.

Ainsi, pour $\lambda,\mu\in\mathbb{K}$ et $P,Q\in P_{\mathbb{K}}$ (avec $\hat{\lambda}=(u_i)_{i\in\mathbb{N}}$, $P=(a_i)_{i\in\mathbb{N}}$) :

- $\lambda P=\hat{\lambda}P=(\lambda,0_{\mathbb{K}},0_{\mathbb{K}},...)P=(c_k)_{k\in\mathbb{N}}$ où $c_k=\sum_{i+j=k}u_ia_j=\lambda a_k$

Donc $\lambda P=(\lambda a_0,\lambda a_1,\lambda a_2,...)=(\lambda a_i)_{i\in\mathbb{N}}$

- $(\lambda+\mu)P=\lambda P+\mu P$
- $\lambda(P+Q)=\lambda P+\lambda Q$
- $(\lambda\mu)P=\lambda(\mu P)$
- $1_{\mathbb{K}}\times P=\hat{1}_{\mathbb{K}}\times P=1_{P_{\mathbb{K}}}\times P=P$

Les éléments de $\mathbb{K}$ seront appelés des scalaires.

C) Etape 3 : introduction de l'indéterminée

Soit X l'élément de $P_{\mathbb{K}}$ défini par :

$X=(0_{\mathbb{K}},1_{\mathbb{K}},0_{\mathbb{K}},0_{\mathbb{K}},...)$

C'est-à-dire $X=(\delta_i)_{i\in\mathbb{N}}$ où $\delta_1=1_{\mathbb{K}}$ et $\forall k\in\mathbb{N}\setminus\{1\},\delta_k=0_{\mathbb{K}}$

Alors $\forall k\in\mathbb{N},X^k=(u_i^{(k)})_{i\in\mathbb{N}}$ où $u_k^{(k)}=1_{\mathbb{K}}$ et $\forall i\in\mathbb{N}\setminus\{k\},u_i^{(k)}=0_{\mathbb{K}}$

Démonstration : par récurrence sur *k*.

Pour $k=0$: $X^0=1_{P_{\mathbb{K}}}=(1_{\mathbb{K}},0_{\mathbb{K}},0_{\mathbb{K}}...)$

Soit $k\in\mathbb{N}$, supposons que $X^k=(u_i^{(k)})_{i\in\mathbb{N}}$ où $u_k^{(k)}=1_{\mathbb{K}}$ et $\forall i\in\mathbb{N}\setminus\{k\},u_i^{(k)}=0_{\mathbb{K}}$

Alors $X^{k+1}=X^kX=(c_i)_{i\in\mathbb{N}}$

Où $\forall i\in\mathbb{N},c_i=\sum_{\alpha+\beta=i}u_\alpha^{(k)}\delta_\beta=\begin{cases}u_{i-1}^{(k)}\delta_1 \text{ si } i\neq 0\\ u_0^{(k)}\delta_0=0 \text{ si } i=0\end{cases}$

Soit, pour $i\neq 0$, $c_i=u_{i-1}^{(k)}=\begin{cases}0 \text{ si } i\neq k+1\\ 1 \text{ si } i=k+1\end{cases}$

Donc $X^{k+1}=(u_i^{(k+1)})_{i\in\mathbb{N}}$

Théorème fondamental :

Soit $P\in P_{\mathbb{K}}$. Alors P s'écrit de manière unique sous la forme :

$P=\sum_{k\in\mathbb{N}}a_kX^k$ où les a_k sont des scalaires, nuls à partir d'un certain rang.

Démonstration :

Soit $P \in P_{\mathbb{K}}$.

- P s'écrit $P = (a_k)_{k\in\mathbb{N}}$, suit d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang, disons à partir du rang $n+1$.

On a aussi :

$$\begin{aligned} P &= (a_0, a_1, ...a_n, 0_{\mathbb{K}}, 0_{\mathbb{K}}...) \\ &= (a_0, 0_{\mathbb{K}}, 0_{\mathbb{K}}...) + (0_{\mathbb{K}}, a_1, 0_{\mathbb{K}}, 0_{\mathbb{K}}...) + ... + (0_{\mathbb{K}}, 0_{\mathbb{K}}, ...0_{\mathbb{K}}, a_n, 0_{\mathbb{K}}, 0_{\mathbb{K}}...) \\ &= a_0(1_{\mathbb{K}}, 0_{\mathbb{K}}, 0_{\mathbb{K}}...) + a_1(0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, 0_{\mathbb{K}}...) + ... + a_n(0_{\mathbb{K}}, 0_{\mathbb{K}}, ...0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, 0_{\mathbb{K}}...) \\ &= a_0X^0 + a_1X^1 + ... + a_nX^n \end{aligned}$$

D'où l'existence de P sous la forme $\sum_{k\in\mathbb{N}} a_kX^k$ où les a_k sont nuls à partir d'un certain rang.

- Unicité de l'écriture :

Si $\sum_{k\in\mathbb{N}} a_kX^k = \sum_{k\in\mathbb{N}} b_kX^k$, où les a_k et les b_k sont nuls à partir d'un certain rang.

Alors $(a_k)_{k\in\mathbb{N}} = \sum_{k\in\mathbb{N}} a_kX^k = \sum_{k\in\mathbb{N}} b_kX^k = (b_k)_{k\in\mathbb{N}}$.

Vocabulaire :

- Les éléments de $P_{\mathbb{K}}$ seront toujours notés sous la forme $\sum_{k\in\mathbb{N}} a_kX^k$, où les a_k sont des éléments de $\mathbb{K}$ nuls à partir d'un certain rang (on oublie la forme $(a_k)_{k\in\mathbb{N}}$).

Ils sont appelés polynômes formels à une indéterminée à coefficients dans $\mathbb{K}$.

- Le polynôme X est appelé l'indéterminée.
- L'ensemble $P_{\mathbb{K}}$ des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

D) Etape 4 : conclusion, récapitulation

- Tout $P \in \mathbb{K}[X]$ s'écrit de manière unique sous la forme $P = \sum_{k\in\mathbb{N}} a_kX^k$ où les a_k sont des éléments de $\mathbb{K}$ nuls à partir d'un certain rang.

Ainsi, $\sum_{k\in\mathbb{N}} a_kX^k = \sum_{k\in\mathbb{N}} b_kX^k \Rightarrow \forall k \in \mathbb{N}, a_k = b_k$

- $(\mathbb{K}[X], +, \times)$ est un anneau, dont $\mathbb{K}$ est un sous anneau.
- Si $P = \sum_{i\in\mathbb{N}} a_iX^i$, et $Q = \sum_{i\in\mathbb{N}} b_iX^i$ où les a_i sont nuls à partir du rang $n+1$ et les b_i à partir du rang $m+1$, alors :

$$P = \sum_{i=0}^{n} a_iX^i,\ Q = \sum_{i=0}^{m} b_iX^i$$

$$P + Q = \sum_{i=0}^{n} a_iX^i + \sum_{i=0}^{m} b_iX^i = \sum_{i=0}^{N} a_iX^i + b_iX^i = \sum_{i=0}^{N} (a_i + b_i)X^i, \text{ où } N = \max(n, m)$$

$$P\times Q=\left(\sum_{i=0}^{n}a_iX^i\right)\left(\sum_{i=0}^{m}b_iX^i\right)=\sum_{\substack{i\in[\![0,n]\!]\\ j\in[\![0,m]\!]}}(a_iX^i)(b_jX^j)=\sum_{\substack{i\in[\![0,n]\!]\\ j\in[\![0,m]\!]}}a_ib_jX^{i+j}$$

$$=\sum_{k=0}^{n+m}\sum_{\substack{i\in[\![0,n]\!],j\in[\![0,m]\!]\\ i+j=k}}a_ib_jX^{i+j}=\sum_{k=0}^{n+m}\sum_{\substack{i\in[\![0,n]\!],j\in[\![0,m]\!]\\ i+j=k}}a_ib_jX^{k}=\sum_{k=0}^{n+m}c_kX^k$$

Où $c_k=\sum_{i+j=k}a_ib_j$

II Degré

A) Définition

Soit $P\in\mathbb{K}[X]$, $P=\sum_{i\in\mathbb{N}}a_iX^i$ où les a_i sont des éléments de $\mathbb{K}$ nuls à partir d'un certain rang.

- Si $P=0_{\mathbb{K}[X]}$, c'est-à-dire $P=0_{\mathbb{K}}$ ou $P=0$. Alors $\forall i\in\mathbb{N},a_i=0_{\mathbb{K}}$. On dit alors que P est de degré $-\infty$
- Sinon, $P\neq 0_{\mathbb{K}[X]}$ et donc il existe $i\in\mathbb{N}$ tel que $a_i\neq 0_{\mathbb{K}}$. On peut alors introduire $n=\max\{i\in\mathbb{N},a_i\neq 0_{\mathbb{K}}\}$ (puisque l'ensemble est non vide, et majoré car les a_i sont nuls à partir d'un certain rang). n est appelé le degré de P.

Ainsi :

Pour tout $P\in\mathbb{K}[X]$, $\deg P\in\mathbb{N}\cup\{-\infty\}$, et on a l'équivalence :

$P\neq 0_{\mathbb{K}[X]}\Leftrightarrow\deg P\in\mathbb{N}$

Les polynômes de degré 0 sont exactement les $\lambda\in\mathbb{K}\setminus\{0_{\mathbb{K}}\}$

Les polynômes de degré 1 sont exactement les $aX+b$ avec $a\neq 0$

Les polynômes de degré n sont exactement les $\sum_{i=0}^{n}a_iX^i$ avec $a_n\neq 0$.

Les polynômes de degré $\leq n$ sont exactement les $\sum_{i=0}^{n}a_iX^i$

L'ensemble de ces derniers est noté $\mathbb{K}_n[X]$; en particulier, $\mathbb{K}_0[X]$ n'est autre que $\mathbb{K}$, ensemble des polynômes constants.

B) Propriétés

Soient $P,Q\in\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$. Alors :

- $\deg(P+Q)\leq\max(\deg P,\deg Q)$
- $\deg(P\times Q)=\deg P+\deg Q\quad(\forall n\in\mathbb{N},-\infty+n=-\infty,-\infty+(-\infty)=-\infty)$
- $\deg(\lambda P)=\begin{cases}\deg P\text{ si }\lambda\neq 0\\ -\infty\text{ sinon}\end{cases}$
- $\forall m\in\mathbb{N}^*,\deg(P^m)=m\deg P\quad(\forall n\in\mathbb{N}^*,n\times(-\infty)=-\infty)$

Démonstration :

- Cas $P=Q=0$ évident.

- Si $P=0$ et $Q\neq 0$ (ou $P\neq 0$ et $Q=0$), le résultat est immédiat aussi.
- Maintenant si $P\neq 0$ et $Q\neq 0$:

Notons $p=\deg P$ et $q=\deg Q$.

- On pose $n=\max(p,q)$.

On a $P=\sum_{i=0}^{n} a_i X^i$, et $Q=\sum_{i=0}^{n} b_i X^i$

Donc $P+Q=\sum_{i=0}^{n}(a_i+b_i)X^i$, donc $\deg(P+Q)\leq n$

- $P\times Q=\left(\sum_{i=0}^{p} a_i X^i\right)\left(\sum_{i=0}^{q} b_i X^i\right)$ où $a_p\neq 0_{\mathbb{K}}$ et $b_q\neq 0_{\mathbb{K}}$

Donc $P\times Q=\underbrace{a_p b_q}_{\neq 0} X^{p+q}+\ldots$

- $\lambda P=\sum_{i=0}^{p}\lambda a_i X^i$ avec $a_p\neq 0_{\mathbb{K}}$
- Résultat avec une récurrence immédiate sur *m*.

Vocabulaire :

- Si P est un polynôme de degré n, le terme $a_n X^n$ s'appelle le terme dominant de P et a_n le coefficient dominant de P.
- Par convention, le coefficient dominant du polynôme nul est 0.
- a_k s'appelle le coefficient de X^k, et $a_k X^k$ s'appelle le monôme/terme de degré k.
- Un polynôme P non nul est dit unitaire lorsque son coefficient dominant est 1.

III Début d'arithmétique dans $(\mathbb{K}[X],+,\times)$.

Théorème :
$(\mathbb{K}[X],+,\times)$ est un anneau intègre.

Démonstration :

- Déjà, $(\mathbb{K}[X],+,\times)$ est commutatif et non réduit à $\{0_{\mathbb{K}}\}$.
- Soient maintenant $P,Q\in\mathbb{K}[X]$, supposons que $PQ=0_{\mathbb{K}}$

Montrons qu'alors $P=0_{\mathbb{K}}$ ou $Q=0_{\mathbb{K}}$.

Supposons que non, c'est-à-dire que $P\neq 0_{\mathbb{K}}$ et $Q\neq 0_{\mathbb{K}}$.

Soient alors $p=\deg P, q=\deg Q$. Ainsi, $p,q\in\mathbb{N}$.

Alors $P=\sum_{i=0}^{p} a_i X^i$ et $Q=\sum_{i=0}^{q} b_i X^i$, avec $a_p\neq 0_{\mathbb{K}}$ et $b_q\neq 0_{\mathbb{K}}$

Mais alors le coefficient de X^{p+q} est $a_p b_q\neq 0_{\mathbb{K}}$, donc $PQ\neq 0_{\mathbb{K}}$, ce qui est exclu.

Autre démonstration :

$\deg(PQ)=\deg P+\deg Q$, et si $\deg P+\deg Q=-\infty$, alors forcément soit $\deg Q=-\infty$, soit $\deg P=-\infty$.

Théorème :
Les éléments inversibles de $(\mathbb{K}[X],+,\times)$ sont exactement les éléments de $\mathbb{K}\setminus\{0_{\mathbb{K}}\}$.

Démonstration :

- Soit $P\in\mathbb{K}[X]$. Si P est inversible, alors il existe $Q\in\mathbb{K}[X]$ tel que $PQ=1_{\mathbb{K}}$.

Alors $\deg P+\deg Q=0$. Or, $\deg P,\deg Q\in\mathbb{N}\cup\{-\infty\}$.
Donc $\deg P=\deg Q=0$

- Réciproquement, si $P=\lambda\in\mathbb{K}\setminus\{0_{\mathbb{K}}\}$, alors λ admet un inverse λ^{-1}.

Donc $Q=\lambda^{-1}$ est inverse de P.

Définition :
Soient $P,Q\in\mathbb{K}[X]$. On dit que P est multiple de Q ou que Q est un diviseur de P lorsqu'il existe $S\in\mathbb{K}[X]$ tel que $P=QS$.

Définition :
Soient $P,Q\in\mathbb{K}[X]$. On dit que P et Q sont associés lorsque P divise Q et Q divise P (ce qui équivaut à dire qu'il existe $\lambda\in\mathbb{K}\setminus\{0_{\mathbb{K}}\}$ tel que $Q=\lambda P$)

Démonstration de la parenthèse :

- Si $Q=\lambda P$ avec $\lambda\in\mathbb{K}\setminus\{0_{\mathbb{K}}\}$ alors P divise Q et aussi $Q=\lambda^{-1}P$ donc Q divise P.
- Si P divise Q et Q divise P alors il existe $S,S'\in\mathbb{K}[X]$ tels que $Q=PS$ et $P=QS'$. Donc $Q=QSS'$. Donc $Q(1_{\mathbb{K}}-SS')=0_{\mathbb{K}}$, d'où, comme $\mathbb{K}[X]$ est intègre, soit $Q=0_{\mathbb{K}}$ soit $SS'=1_{\mathbb{K}}$.
  - Si $Q=0_{\mathbb{K}}$, alors $P=0_{\mathbb{K}}$ car Q divise P donc il existe $R\in\mathbb{K}[X]$ tel que $P=QS=0_{\mathbb{K}}$.
  - Si $SS'=1_{\mathbb{K}}$, alors S est inversible, donc $S=\lambda\in\mathbb{K}\setminus\{0_{\mathbb{K}}\}$, donc $Q=\lambda P$.

A) Division euclidienne dans $\mathbb{K}[X]$.

Théorème :
Soient $A,B\in\mathbb{K}[X]$, avec $B\neq 0_{\mathbb{K}}$.
Alors il existe un unique couple (Q,R) d'éléments de $\mathbb{K}[X]$ tels que $A=BQ+R$ et $\deg(R)<\deg(B)$.
On dit que Q est le quotient dans la division euclidienne de A par B et que R est le reste dans la division euclidienne de A par B.

Démonstration :

- Unicité :

Si $A=BQ+R$, avec $\deg(R)<\deg(B)$
Et $A=BQ'+R'$, avec $\deg(R')<\deg(B)$,
Alors $B(Q-Q')=R'-R$. Donc $\deg(B)+\deg(Q-Q')=\underbrace{\deg(R'-R)}_{\leq\max(\deg R,\deg R')}$
Ainsi, $\deg(B)+\deg(Q-Q')<\deg(B)$, donc $\deg(Q-Q')\notin\mathbb{N}$. Donc $Q-Q'=0$.
Donc $B\times 0_{\mathbb{K}}=R'-R$, soit $R'=R$.
D'où l'unicité.

- Existence :

Soit $B \in \mathbb{K}[X] \setminus \{0_{\mathbb{K}}\}$, de degré $p \in \mathbb{N}$ et de coefficient dominant b_p.

Montrons par récurrence que $\forall n \in \mathbb{N}, P(n)$, où :

$P(n) = \forall A \in \mathbb{K}_n[X], \exists (Q,R) \in \mathbb{K}[X]^2, A = BQ + R$ et $\deg R < p$

- Déjà, $P(0)$ est vrai, puisque si $\deg A \leq 0$, on a :
  - Soit $p \geq 1$, et alors $A = 0_{\mathbb{K}} \times B + A$, donc $(0_{\mathbb{K}}, A)$ convient.
  - Soit $p = 0$, et donc $B = b \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}$ et donc $A = b(b^{-1}A) + 0_{\mathbb{K}}$, donc le couple $(b^{-1}A, 0_{\mathbb{K}})$ convient.
- Soit $n \in \mathbb{N}$, supposons $P(n)$. Soit alors A de degré $\leq n+1$.

Alors A s'écrit $A = \underbrace{a_{n+1}}_{\in \mathbb{K}} X^{n+1} + \underbrace{a_n X^n + \ldots + a_0 X^0}_{A_1 \text{ où } \deg A_1 \leq n}$.

Supposons $p \leq n+1$ (dans le cas contraire, $A = 0_{\mathbb{K}} \times B + A$ et $(0_{\mathbb{K}}, A)$ convient)

On peut donc écrire :

$$A = \underbrace{a_{n+1} b_p^{-1} X^{n+1-p} \underbrace{(b_p X^p + B_1)}_{B} - a_{n+1} b_p^{-1} X^{n+1-p} \underbrace{B_1}_{\deg B_1 < p}}_{a_{n+1} X^{n+1}} + A_1$$

Donc $A = a_{n+1} b_p^{-1} X^{n+1-p} B + \underbrace{(A_1 - a_{n+1} b_p^{-1} X^{n+1-p} B_1)}_{A_2, \deg A_2 \leq n}$

Or, $\deg A_2 \leq n$. Donc $A_2 = BQ_1 + R_1$ avec $(Q_1, R_1) \in \mathbb{K}[X]^2$ et $\deg(R_1) < p$.

Donc $A = (a_{n+1} b_p^{-1} X^{n+1-p} + Q_1)B + R_1$.

Exemple :

$A = X^5 + 2X^3 - 2X - 2 \quad B = X^2 + 1$

$A = X^3(X^2+1) - X^3 + 2X^3 - 2X - 2 = X^3 B + X^3 - 2X - 2$

$= X^3 B + X(X^2+1) - X - 2X - 2 = (X^3 + X)B - 3X - 2$

IV Substitution d'un polynôme à l'indéterminée

A) Définition, propriétés

Soit $P \in \mathbb{K}[X]$. P s'écrit $P = \sum_{k \in \mathbb{N}} a_k X^k$ où les a_k sont nuls à partir d'un certain rang, disons $n+1$. Donc $P = \sum_{k=0}^{n} a_k X^k$

Soit $Q \in \mathbb{K}[X]$.

On note $\hat{P}(Q) = \sum_{k \in \mathbb{N}} a_k Q^k$, soit $\hat{P}(Q) = \sum_{k=0}^{n} a_k Q^k$

Théorème :

Soient $P_1, P_2 \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}[X]$. Alors :

$(P_1 \hat{+} P_2)(Q) = \hat{P}_1(Q) + \hat{P}_2(Q)$

$(P_1 \hat{\times} P_2)(Q) = \hat{P}_1(Q) \times \hat{P}_2(Q)$

$\hat{\lambda}(Q) = \lambda$

Démonstration :

Soient $P_1 = \sum_{k\in\mathbb{N}} a_k X^k$, $P_2 = \sum_{k\in\mathbb{N}} b_k X^k$.

On introduit $n\in\mathbb{N}$ tel que $\deg P_1 \le n$ et $\deg P_2 \le n$. On a alors :

- $P_1 + P_2 = \sum_{k=0}^{n} (a_k + b_k) X^k$

Donc $\hat{P}_1(Q) + \hat{P}_2(Q) = \sum_{k=0}^{n} a_k Q^k + \sum_{k=0}^{n} b_k Q^k = \sum_{k=0}^{n} (a_k + b_k) Q^k = (P_1 \hat{+} P_2)(Q)$

- $P_1 \times P_2 = \sum_{k=0}^{2n} c_k X^k$ où $c_k = \sum_{i+j=k} a_i b_j$

et $\hat{P}_1(Q) \times \hat{P}_2(Q) = \left(\sum_{k=0}^{n} a_k Q^k\right)\left(\sum_{k=0}^{n} b_k Q^k\right) = \sum_{0\le i,j\le n} a_i b_j Q^{i+j} = \sum_{k=0}^{2n} \sum_{i+j=k} a_i b_j Q^k = \sum_{k=0}^{2n} c_k Q^k$

- $\hat{\lambda}(Q) = \hat{\lambda . X^0}(Q) = \lambda . Q^0 = \lambda$

Remarque :

Le théorème s'énonce aussi ainsi :

Pour tout $Q\in\mathbb{K}[X]$, l'application $\begin{array}{c}\mathbb{K}[X]\to\mathbb{K}[X] \\ P\mapsto\hat{P}(Q)\end{array}$ est un endomorphisme de l'anneau $(\mathbb{K}[X],+,\times)$ (mais ni injectif ni surjectif).

Remarque :

Pour $Q\notin\mathbb{K}_0[X]$ et si $\mathbb{K}$ est un sous corps de $\mathbb{C}$, $P\mapsto\hat{P}(Q)$ est injective.

B) Polynômes pairs, impairs

On suppose ici que $1_{\mathbb{K}} + 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ (c'est-à-dire que $1_{\mathbb{K}}$ n'est pas un élément d'ordre 2 du groupe $(\mathbb{K},+)$)

Définition :

Soit $P\in\mathbb{K}[X]$

On dit que P est pair lorsque $P(-X) = P(X)\ (= P)$

On dit que P est impair lorsque $P(-X) = -P(X)\ (= -P)$

Proposition :

P est pair si et seulement si $\forall k\in\mathbb{N}, a_{2k+1} = 0_{\mathbb{K}}$

P est impair si et seulement si $\forall k\in\mathbb{N}, a_{2k} = 0_{\mathbb{K}}$

Démonstration :

$P(-X) = \sum_{k\in\mathbb{N}} (-1)^k a_k X^k$.

Donc P est pair $\Leftrightarrow \forall k\in\mathbb{N}, (-1)^k a_k = a_k \Leftrightarrow \forall i\in\mathbb{N}, -a_{2i+1} = a_{2i+1}$

$\Leftrightarrow \forall i\in\mathbb{N}, 2.a_{2i+1} = 0_{\mathbb{K}}$

Or, $2.a_{2i+1} = a_{2i+1} + a_{2i+1} = (1_{\mathbb{K}} + 1_{\mathbb{K}}) a_{2i+1}$. On a supposé que $1_{\mathbb{K}} + 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$.

Donc $\forall i\in\mathbb{N}, 2.a_{2i+1} = 0_{\mathbb{K}} \Leftrightarrow \forall i\in\mathbb{N}, a_{2i+1} = 0_{\mathbb{K}}$

On fait de même pour impair.