## §1 Anneaux de Polynômes. (R. CHIBLOUN F.S. Mékès)

### 1. Transfert de la factorialité.

Dans toute la suite de ce n°, on suppose que A est factoriel.

#### 1.1. Définition.

Soit $P \in A[X] - (0)$, on note $c(P)$ un pgcd des coefficients non nuls de $P$ ($c(P)$ est défini à un facteur inversible près (ie $\forall a \in U(A)$ : $a.c(P)$ est un pgcd)), on l'appelle "contenu de $P$", $P$ est dit primitif lorsque $c(P) \in U(A)$.

#### 1.2. Remarques.

1°) Si $P \in A[X] - (0)$, alors $\exists P_1$ primitif tel que $P = c(P).P_1$.

2°) Si $P_1$ est primitif et $a \in A^*$ alors $c(a.P_1) = a$.

#### 1.3. Proposition.

1°) Si $P_1$ et $P_2$ sont primitifs alors $P_1.P_2$ est primitif.

2°) $\forall P, Q \in A[X] - (0)$, on a

$$c(PQ) = c(P).c(Q).$$

Preuve :

1°) Sinon, $\exists p$ irréductible de $A$ qui divise tous les coefficients de $P = P_1 . P_2$. Soit $f$ l'homomorphisme canonique $A \longmapsto \frac{A}{(p)}$, $f$ se prolonge d'une façon naturelle en un homomorphisme

$$\bar{f} : A[X] \longmapsto \frac{A}{(p)}[X]$$

$$a_0 + a_1 X + \dots + a_n X^n \longmapsto \bar{f}(a_0) + \bar{f}(a_1) X + \dots + \bar{f}(a_n) X^n,$$

$P_i$ étant primitif $(i = 1, 2)$ donc $\bar{f}(P_i) \neq 0$, or $(p)$ premier car $p$ irréductible, donc $\frac{A}{(p)}[X]$ intègre et $\bar{f}(P_1)\bar{f}(P_2) = \bar{f}(P_1 . P_2) \neq 0$ (i.e) il existe un coefficient de $P_1 P_2$ non divisible par $p$, ce qui est absurde; donc $P = P_1 P_2$ est primitif.

2°) $P = c(P) . P_1$ et $Q = c(Q) . Q_1$

$P . Q = c(P) . c(Q) (P_2 Q_1)$

$P_1 Q_1$ primitif d'après 1°), donc selon 2°) Rap

$$c(Q . P) = c(Q) . c(P).$$

C.Q.F.D.

1.4. Lemme.

Soit $K = Fr(A)$ " le corps des fractions de $A$ ".

1°) Soit $P \in A[X] - A$, s'il existe $Q_1, R_1$ dans $K[X] - K$ tels que $P = Q_1 . R_1$ alors $\exists\, Q, R \in A[X] - A$ tels que $P = Q.R$.

2°) i) Soit $P \in A$,

$P$ irréductible de $A[X] \iff P$ irréductible de $A$

ii) Soit $P \in A[X] - A$,

$P$ irréductible de $A[X] \iff \begin{cases} P \text{ primitif dans } A[X] \\ \text{et } P \text{ irréductible dans } K[X]. \end{cases}$

iii) Soit $Q \in K[X] - K$,

$Q$ irréductible dans $K[X] \iff \exists\, \lambda \in K^*$, $\exists\, q$ irréductible de $A[X]$ tels que $Q = \lambda q$.

Preuve :

1°) Soit $a$ un ~~coefficient~~ multiple commun des dénominateurs de tous les coefficients de $Q_1$ et $R_1$. On a $a.Q_1 = Q_2 \in A[X] - A$ et $aR_1 = R_2 \in A[X] - A$, donc $a^2 P = aQ_1 . aR_1 = Q_2 R_2$, or $P = c(P).P_1$ avec $P_1$ primitif, donc $a^2 c(P).P_1 = c(Q_2)c(R_2).Q_3.R_3$ ($P_1$, $Q_3$ et $R_3$ sont primitifs) donc $a^2 c(P) = c(Q_2)c(R_2)$

et $a^2 P = a^2 c(P).P_1 = c(Q_2)c(R_2)Q_3 R_3$

$= a^2 c(P) Q_3 R_3$

$a^2 \neq 0$, donc $P = c(P) Q_3 R_3$

On notera $Q = c(P) Q_3 \in A[X] - A$ et

$R = P_3 \in A[X] - A$, $P = Q.R$.

c.q.f.d.

ii) $\Rightarrow$

On a $U(A[X]) = U(A)$, donc $P$ est non nul et non inversible, et si $P = P_1 P_2$ alors $P_1 \in U(A[X]) = U(A)$ ou $P_2 \in U(A[X]) = U(A)$.

$\Leftarrow$

On a $P$ est non nul et non inversible de $A[X]$, et si $P = P_1.P_2$ avec $P_1$ et $P_2$ dans $A[X]$, alors $\deg P = \deg P_1 + \deg P_2 = 0$, d'où $P_1$ et $P_2$ sont dans $A$ et par suite $P_1 \in U(A) = U(A[X])$ ou $P_2 \in U(A) = U(A[X])$ donc $P$ irréductible de $A[X]$.

C.Q.F.D.

ii) $\Rightarrow$

Evidement $P$ primitif dans $A[X]$, montrons que $P$ irréductible dans $K[X]$, sinon $P = P_1.P_2$ avec

$P_1$ et $P_2$ dans $K[X]-K$, d'après 1°) il existe $Q_1, Q_2 \in A[X]-A$ tels que $P = Q_1 Q_2$, comme $Q_i \notin A$ alors $Q_i \notin U(A[X])$, d'où $P$ non inductible de $A[X]$, absurde.

$\Leftarrow$

Si $P = P_1 P_2$ avec $P_i \in A[X] \subset K[X]$, donc $P_i \in K[X]$, or $U(K[X]) = K^*$ et alors $P_1 \in K^*$ ou $P_2 \in K^*$, or $K^* \cap A[X] = A^*$, d'où $P_1 \in A$ ou $P_2 \in A$, si par exemple $P_1 \in A$, $c(P) = P_1 \cdot c(P_2) = 1$ (car $P$ primitif) d'où $P_1 \in U(A) = U(A[X])$ et par suite $P$ inductible dans $A[X]$.

C.Q.F.D

iii) $Q \in K[X]-K$

$\Rightarrow$

$$Q = \sum_{i=0}^{n} \frac{a_i}{b_i} X^i, \text{ soit } b = \prod_{i=0}^{n} b_i \in A^*,$$

$bQ = Q_2 \in A[X]-A$, $Q_2 = c(Q_2) \cdot q$ avec $q$ primitif dans $A[X]$, donc $bQ = c(Q_2) \cdot q$ et alors $Q = \frac{c(Q_2)}{b} \cdot q$, on pose $\lambda = \frac{c(Q_2)}{b} \in K^*$,

montrons que $q$ est inductible dans $A[X]$, sinon,

$q$ étant primitif, $\exists R_1, R_2 \in A[X] - A$ tels que $q = R_1 . R_2$, donc $Q = \lambda q = \lambda R_1 . R_2$, or $\lambda R_1$ et $R_2$ sont dans $K[X] - K$ (ie) $Q$ non irréductible dans $K[X]$, absurde.

($\Leftarrow$) Sinon, $\exists R_1$ et $R_2$ dans $K[X] - K$ tels que $Q = R_1 . R_2$, $\lambda \in K^*$ donc $\exists (\alpha, \beta) \in (A^*)^2$ avec $\lambda = \frac{\alpha}{\beta}$, $Q = \lambda . q = \left(\frac{\alpha}{\beta}\right) q$ ,

$\beta Q = \alpha q = \beta . R_1 R_2$, mais $\beta R_1$ et $R_2$ sont dans $K[X] - K$, donc $\alpha q$ non irréductible dans $K[X]$, $q = \frac{\beta}{\alpha} . R_1 . R_2$, d'après 2) il existe $H_1$ et $H_2$ dans $A[X] - A$ tels que $q = H_1 H_2$ (ie) $q$ non irréductible dans $A[X]$, ce qui est absurde.

C.Q.F.D

## 1.5. Théorème.

$A[X]$ est factoriel. $A$

Preuve :

Soit $P$ un élément non nul et non inversible de $A[X]$, si $P \in A$, $A$ étant factoriel, $P$ admet une décomposition unique en éléments irréductibles

de A, donc P admet une décomposition unique en éléments irréductibles de A[X] (d'après 1.6.2°) i)).

• Si P ∈ A[X] \ A, soit K = Frac(A), K[X] est principal donc factoriel, P admet donc une décomposition unique en éléments irréductibles de K[X], soit $P = a \prod Q^{n(Q)}$ avec les Q irréductibles de K[X] et $n(Q) \in \mathbb{N}$, $a \in A^*$, or le lemme 1.4 (2°) iii) implique, ∀Q, ∃ q dans A[X] et ∃ $\beta_Q \in A^*$ tels que $\beta_Q . Q = q$ irréductible dans A[X], soit $\beta = \prod_{n(Q)\neq 0} \beta_Q$ et $q = c(q).q'$, alors $\beta . P =$

$$= a\left(\prod (c(q))\right)\left(\prod q'^{n(q')}\right)$$

or $P = c(P).P'$, donc

$$\beta . c(P).P' = \left(a \prod (c(q))\right)\left(\prod q'^{n(q')}\right)$$

(ic) $\beta . c(P) = a \prod (c(q))$,

et

$$\beta P = a\left(\prod (c(q))\right)\left(\prod \left(q'^{n(q')}\right)\right)$$

$$= \beta c(P) \prod \left(q'^{n(q')}\right)$$

(ic) $P = c(P) \prod \left(q'^{n(q')}\right)$, comme A factoriel, $c(P) = u \prod \left(p^{n(p)}\right)$ où les p irréductibles et $u \in U(A)$, d'où $P = u \prod p^{n(p)} \prod q'^{n(q')}$

avec les $p$ irréductibles dans $A[X]$, de même pour les $q^i$.
Ainsi on a prouvé l'existence d'une décomposition de $P$ en éléments irréductibles de $A[X]$.
Quand à l'unicité, elle résulte de l'unicité des entiers $n(p)$ et $n(Q)$, qui résulte de la factorialité des anneaux $A$ et $K[X]$.

C.Q.F.D.

**1.6. Proposition (Critère d'Eisenstein)**

Soit $P = X^m + a_{m-1}X^{m-1} + \dots + a_0 \in A[X]$, si $p$ est un élément irréductible de $A$ tel que $\forall\, 0 \leqslant i \leqslant m-1$ : $p$ divise $a_i$ et $p^2$ ne divise pas $a_0$, alors $P$ est irréductible dans $A[X]$.

Preuve :
Sinon (i.e) si $P$ réductible dans $A[X]$, alors il existe $Q, R$ tous les deux non inversibles de $A[X]$ tels que $P = Q \cdot R$, si par exemple $Q \in A$, comme $P$ est unitaire alors $Q \in U(A) = U(A[X])$, donc on peut supposer $Q$ et $R$ tous les deux unitaires non constants. Soit $f$ l'homomorphisme canonique

$$A[X] \longrightarrow \frac{A}{(p)}[X]$$ qui prolonge

la surjection canonique $A \longrightarrow \frac{A}{(p)}$. Puisque

$\forall i$ : $p$ divise $a_i$ alors $f(P) = X^n$, et
$\forall B$ anneau commutatif unitaire : $\frac{B[X]}{(X)} \simeq B$,

on a $\frac{A_{(p)}[X]}{(X)} \simeq \frac{A}{(p)}$ intègre et

par suite $(X)$ idéal premier de $\frac{A}{(p)}[X]$.

$f(P) = f(Q).\ f(R) = X^n \quad (= f(Q.R))$

$\in (X)$, donc nécessairement $f(Q) = X^s$ et
$f(R) = X^{n-s}$ où $s \in \{0, \dots, n\}$.
Si $0 < s < n$ (ie) $f(Q) \neq 1$ et $f(R) \neq 1$ alors $p$ divise le terme constant $b_0$ de $Q$ et le terme constant $c_0$ de $R$, donc $p^2$ divise $a_0 = b_0.c_0$, ce qui est absurde. Donc $s = 0$ ou $s = n$ (ie) $f(Q) = 1$ ou $f(R) = 1$, or $Q$ et $R$ sont supposés unitaires, donc $Q = 1$ ou $R = 1$, absurde.
Donc $P$ irréductible.

C.Q.F.D.

1.7 Exemple :

$X^2 - 15X + 6$ et $X^3 + 18X^2 - 6X + 3$ sont irréductibles dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$ (prendre $p = 3$).

## 2. Anneaux de Polynômes.

### 2.1. Définition

À tout anneau commutatif unitaire $A$ on associe son anneau de polynôme $A[X]$, à l'anneau $A[X]$ on associe l'anneau de polynômes $A[X][Y]$ qu'on note $A[X,Y]$, et à l'anneau $A[X,Y]$ on associe l'anneau de polynômes $(A[X,Y])[Z]$ qu'on note $A[X,Y,Z]$ etc.... À l'anneau $A[X_1,\dots,X_{n-1}]$ on associe l'anneau de polynômes $A[X_1,\dots,X_{n-1}][X_n] = A[X_1,\dots,X_n]$, qu'on appelle anneau de polynômes à $n$ indéterminées sur $A$. On a $\forall i \leq n$:

$$A[X_1,\dots,X_n] \simeq A[X_1,\dots,X_{i-1},X_{i+1},\dots,X_n][X_i],$$

la forme générale d'un élément $P$ de $A[X_1,\dots,X_n]$ est

$$P = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1 i_2 \dots i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$$

où les coefficients $a_{i_1 i_2 \dots i_n}$ sont nuls sauf un nombre fini d'entre eux.

### 2.2. Remarques.

1°) $\forall \sigma \in S_n$ : $A[X_1,\dots,X_n] = A[X_{\sigma(1)},\dots,X_{\sigma(n)}]$

2°) Si $n=2$, on remplace $X_1, X_2$ par $X$ et $Y$, un polynôme à 2 indéterminées sur $A$ s'écrit

$P = \sum a_{ij} X^i Y^j$, les $a_{ij}$ sont presque tous nuls, en groupant les termes pour lesquels $(i+j)$ a une valeur donnée, on a:

$$P = a_{00} + (a_{10}X + a_{01}Y) + (a_{20}X^2 + a_{11}XY + a_{02}Y^2) + (a_{30}X^3 + a_{21}X^2Y + a_{12}XY^2 + a_{03}Y^3) + \cdots$$

3°) $\forall i = (i_1, i_2, \cdots, i_n) \in \mathbb{N}^n$, on notera $X^i = X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ et $|i| = i_1 + i_2 + \cdots + i_n$, donc un élément $P$ de $A[X_1, \cdots, X_n]$ s'écrit:

$$P = \sum_{i \in \mathbb{N}^n} a_i X^i$$, avec les $a_i$ sont presque tous nuls.

## 2.3 Définitions.

Soit $P = \sum_{i \in \mathbb{N}^n} a_i X^i \in A[X_1, \cdots, X_n]$, avec $P$ non nul.

L'entier $d = \sup\{|i| / a_i \neq 0\}$ s'appelle le degré total du polynôme $P$ et se note $\deg P$, On prolonge cette définition au polynôme nul en posant $\deg(0) = -\infty$ avec $-\infty < n$, $-\infty + n = -\infty$ et $(-\infty) + (-\infty) = -\infty$, $\forall n \in \mathbb{N}$.

Soit $j \in \{1, 2, \cdots, n\}$, en écrivant

$$A[X_1, \cdots, X_n] \simeq A[X_1, \cdots, X_{j-1}, X_{j+1}, \cdots, X_n][X_j]$$

le polynôme $P$ est donc un polynôme à une

indéterminée sur l'anneau de base $A[X_1, \dots, X_{j-1}, X_{j+1}, \dots, X_m]$, en tant que tel son degré s'appelle le degré partiel en $X_j$ qu'on note $\deg_{X_j} P$.

Soit $k$ un entier $\leq \deg P$. On note $P_k$ la somme $P_k = \sum_{|i|=k} a_i X^i$ qu'on appelle la composante homogène de degré $k$ de $P$ et on a:

$$P = P_0 + P_1 + P_2 + \dots + P_{\deg P},$$

donc $\deg P = d \iff d$ le plus grand entier tel que $P_d \neq 0$.

On dira que le polynôme $P$ est homogène de degré $d$ si $P = P_d$ (ie) pour tout coefficient non nul $a_i$ de $P$, on a: $|i| = d$.

## 2.4. Exemples

1°) $P = X_1 - X_1^2 X_2 \in A[X_1, X_2]$

$P = a_{10} X_1 + a_{21} X_1^2 X_2$ avec $a_{10} = 1$ et $a_{21} = -1$

donc $\deg P = 3$, $\deg_{X_1} P = 2$ et $\deg_{X_2} P = 1$

on a $P_1 = X_1$, $P_2 = 0$ et $P_3 = a_{21} X_1^2 X_2 = -X_1^2 X_2$, ainsi la composante homogène de degré 1 est $X_1$, de degré 2 est 0 et de degré 3 est $-X_1^2 X_2$.

2°) $P = X_1^3 + X_1 X_2^2 - 2X_2^3$

est un polynôme homogène de degré 3.

## 2.5. Proposition.

1°) $A$ intègre $\Longleftrightarrow$ $A[X_1, \dots, X_n]$ intègre.

2°) $A$ factoriel $\Longleftrightarrow$ $A[X_1, \dots, X_n]$ factoriel.

3°) $\forall P, Q$ dans $A[X_1, \dots, X_n]$ :

i) $\deg(P.Q) \leq \deg(P) + \deg(Q)$

( et on a l'égalité si $A$ est intègre )

ii) $\deg(P+Q) \leq \sup(\deg P, \deg Q)$

( on a l'égalité si $\deg P \neq \deg Q$ ).

Preuve :

1°) et 2°) Vues.

3°) Par récurrence sur $n$.

## 2.6 Soit $P = \sum_{i \in \mathbb{N}^n} a_i X^i \in A[X_1, \dots, X_m]$,

on lui associe la fonction polynôme

$$\tilde{P} : A^n \longrightarrow A$$

$$(a_1, \dots, a_m) \longmapsto \tilde{P}(b_1, \dots, b_m)$$

avec $\widetilde{P}(b_1, \dots, b_m)$ est obtenu en remplaçant $X_j$ par $b_j$ ($\forall j \in \{1, \dots, n\}$) dans l'expression de $P$.

En notant $\mathcal{F}(A^n, A)$ l'anneau des applications de $A^n \longrightarrow A$, l'application

$$\phi : A[X_1, \dots, X_n] \longrightarrow \mathcal{F}(A^n, A)$$
$$P \longmapsto \phi(P) = \widetilde{P}$$

est un homomorphisme d'anneaux.

**Théorème :**

Si $A$ est intègre infini, $\phi$ est alors injectif.

**Preuve :**

Par recurrence sur $n$.

- Si $n = 1$, $\widetilde{P} = \widetilde{Q} \Longrightarrow \forall x \in A : \widetilde{P}(x) - \widetilde{Q}(x) = 0$ (ie) si $T = P - Q$, on a $\widetilde{T}(x) = 0 \ \forall x \in A$, or $T \in A[X] \subset K[X]$ avec $K$ corps des fractions de $A$, donc $T$ a une infinité de racines, d'où $T = 0$ (ie) $P = Q$.
- Supposons le théorème vrai pour $n - 1$.

Soit $T \in A[X_1, \dots, X_n] \simeq A[X_1, \dots, X_{n-1}][X_n]$, ordonnons $T$ suivant les puissances croissantes de $X_n$, on a $T = \sum_{k=0}^{m} A_k \cdot X_n^k$ avec $A_k \in A[X_1, \dots, X_{n-1}]$,

si $T \neq 0$ donc $\exists k_0 \in \{1, \dots, m\}$ tel que $A_{k_0} \neq 0$. L'H.R montre qu'il existe $(b_1, \dots, b_{m-1}) \in A^{m-1}$ tel que $\phi(A_{k_0})(b_1, \dots, b_{m-1}) \neq 0$

donc le polynôme $Q \in A[X_m]$ défini par $Q(X_m) = \sum_{0 \leq k \leq m} \tilde{A}_k(b_1, \dots, b_{m-1}) X_m^k$ est non nul,

donc $\exists b_m \in A$ tel que $\tilde{Q}(b_m) \neq 0$ (i.e) $\tilde{T}(b_1, \dots, b_m) \neq 0$ et $\phi(T) = 0 \Rightarrow T = 0$

(i.e) $\phi$ injectif.

C.Q.F.D

Remarque

Si $A$ intègre infini et $B$ une partie infinie de $A$, soit $P \in A[X_1, \dots, X_n]$, si $\forall (b_1, \dots, b_n) \in B^n$ on a $\tilde{P}(b_1, \dots, b_n) = 0$ alors $P = 0$.

## I.7. Définitions.

Soit $A$ un anneau commutatif unitaire, $n \in \mathbb{N}^*$.

1°) Un polynôme $P \in A[X_1, \dots, X_n]$, est dit symétrique si $\forall \sigma \in S_n$ on a:

$$P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n).$$

2°) On appelle polynômes symétriques élémentaires de $X_1, X_2, \dots, X_n$, les polynômes symétriques :

$$\Delta_1 = X_1 + X_2 + \cdots + X_n = \sum_{i=1}^{n} X_i$$

$$\Delta_2 = X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n = \sum_{1\le i<j\le n} X_iX_j$$

$$\Delta_3 = X_1X_2X_3 + \cdots + = \sum_{1\le i<j<k\le n} X_iX_jX_k$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\Delta_k = \sum_{1\le i_1<i_2<\cdots<i_k\le n} X_{i_1}X_{i_2}\cdots X_{i_k}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\Delta_n = X_1X_2\cdots X_n.$$

## 2.8. Proposition :

Soit $f(X) = (X-a_1)(X-a_2)\cdots(X-a_n)$

$$= X^n + b_1X^{n-1} + \cdots + b_0$$

alors on a :

$$b_1 = -(a_1 + a_2 + \cdots + a_n) = -\left(\sum_{i=1}^{n} a_i\right)$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$b_k = (-1)^k \left(\sum_{1\le i_1<i_2<\cdots<i_k\le n} a_{i_1}a_{i_2}\cdots a_{i_k}\right)$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$b_n = (-1)^n a_1a_2\cdots a_n.$$

Preuve : facile par récurrence sur l'entier n.

## 2.9 Proposition.

K corps algébriquement clos de caractéristique 0.
Soient $F \in K[X_1, \dots, X_n]$ et $G \in K[X_1, \dots, X_n]$
tels que $G(X_1, \dots, X_n) = F(S_1, \dots, S_n)$.
Alors on a

$$G = 0 \iff F = 0.$$

Preuve:

Soit $x = (x_1, \dots, x_n) \in K^n$
On pose $\tilde{S}(x) = (\tilde{S}_1(x), \dots, \tilde{S}_n(x)) \in K^n$
l'application $\tilde{S} : K^n \longrightarrow K^n$ est surjective
car si $y = (y_1, \dots, y_n) \in K^n$, l'équation

$$X^n - y_1 X^{n-1} + y_2 X^{n-2} + \dots + (-1)^n y_n = 0$$

admet n racines $x_1, \dots, x_n$ (distinctes ou non, K étant algébriquement clos).
Soit $x = (x_1, \dots, x_n) \in K^n$, d'après la proposition précédente on a : $\forall i \leq n$ : $y_i = \tilde{S}_i(x)$
donc $\tilde{S}(x) = y$ (ie) $\tilde{S}$ surjective ; G étant supposé nul, $\forall y = (y_1, \dots, y_n) \in K^n$, il existe $x = (x_1, \dots, x_n) \in K^n$ tel que

$$\tilde{S}(x) = y \text{ (ie) } (\tilde{S}_1(x), \dots, \tilde{S}_n(x)) = (y_1, \dots, y_n)$$

donc $\widetilde{F}(y_1, \dots, y_n) = \widetilde{F}(\tilde{S}_1(x), \dots, \tilde{S}_n(x))$

$$= \tilde{G}(x_1, \dots, x_n) = 0, \text{ donc}$$

$\widetilde{F} = 0$, or caract $K = 0$ donc K infini et

d'après (2.6), $F = 0$.

C.Q.F.D.

## 2.10 Corollaire.

K alg. clos et caract. $k = 0$.
Soit $G \in K[X_1, \dots, X_n]$, si $F \in K[X_1, \dots, X_n]$ tel que $G(X_1, \dots, X_n) = F(S_1, \dots, S_n)$, alors F est unique.

Preuve:

$G_T(X_1, \dots, X_n) = F_1(S_1, \dots, S_n) = F_2(S_1, \dots, S_n)$
donc $(F_1 - F_2)(S_1, \dots, S_n) = 0$
d'où $F_1 = F_2$.

C.Q.F.D.

## 2.11 Proposition

Les composantes homogènes de tout polynôme symétrique sont symétriques.

Preuve:

Soit G symétrique, donc $G = G_0 + G_1 + \dots + G_q$, avec $q = \deg G$ et $\forall\, 0 \leq k \leq q$: $G_k$ la composante homogène de degré k, l'écriture est unique.
Soit $\sigma \in S_n$, on a

$$G(X_1, X_2, \dots, X_n) = G(X_{\sigma(1)}, \dots, X_{\sigma(1)})$$
$$= \sum_{k=0}^{q} G_k(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

Or si $P = \sum_{i \in \mathbb{N}^n} a_i X^i$ un polynôme homogène de degré $d$, on a $\forall i \in \mathbb{N}^n$ tel que $a_i \neq 0$

$|i| = i_1 + i_2 + \cdots + i_n = d$

donc $\forall \sigma \in S_n$, $\forall i \in \mathbb{N}^n$ tel que $a_i \neq 0$

$$\deg\left(a_i X_{\sigma(1)}^{i_1} X_{\sigma(2)}^{i_2} \cdots X_{\sigma(n)}^{i_n}\right) = |i| = d$$

donc $\deg\left(P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})\right) = \deg P = d$,

$\forall\, 0 \leq k \leq q$ : $\deg G_k(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = k$

l'unicité de l'écriture implique donc

$\forall\, 0 \leq k \leq q$ : $G_k(X_1, \ldots, X_n) = G_k(X_{\sigma(1)}, \ldots X_{\sigma(n)})$

d'où $G_k$ est symétrique.

C.Q.F.D

**2.12 Remarque.**

Soit $G$ un polynôme symétrique, $\forall k_1, k_2$ dans $\{1, \ldots, n\}$ :

$$\deg_{X_{k_1}} G = \deg_{X_{k_2}} G.$$

Preuve:

$$G = \sum_{i \in \mathbb{N}^n} a_i X_1^{i_1} \cdots X_n^{i_n}$$

Soit $M = \{ i \in \mathbb{N}^n / a_i \neq 0 \}$

on a $G = \sum_{i \in M} a_i X_1^{i_1} \cdots X_n^{i_n}$ , pour simplifier les notations, soit $k_1 = 1$ et $k_2 = n$,

$\deg_{X_1} G = \sup_{i \in M} \{ i_1 \}$ et $\deg_{X_n} G = \sup_{i \in M} \{ i_n \}$

or $G(X_1, \ldots, X_n) = G(X_n, X_2, \ldots, X_{n-1}, X_1)$

$$= \sum_{i \in M} a_i X_n^{i_1} \cdots X_1^{i_n} = F(X_1, \ldots, X_n)$$

donc $\deg_{X_1} F = \sup_{i \in M} \{ i_n \} = \deg_{X_1} G = \sup_{i \in M} \{ i_1 \}$

et par suite $\deg_{X_1} G_1 = \deg_{X_n} G$.

C.Q.F.D.

## 2.13 Théorème (th fondamental).

Soit $K$ un corps algébriquement clos de caractéristique nulle. Soit $G \in K[X_1, \dots, X_n]$, symétrique et de degré $q$. Alors on a:

a) Il existe $P$ unique de $K[X_1, \dots, X_n]$ tel que $G(X_1, \dots, X_n) = P(S_1, \dots, S_n)$.

b) $\delta(P) = q$ (ie) tout monôme non nul $\lambda S_1^{\alpha_1} \cdots S_n^{\alpha_n}$ de $P(S_1, \dots, S_n)$ est tel que

$\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n \leq q$, et il existe au moins un monôme non nul $\beta S_1^{i_1} \cdots S_n^{i_n}$ de $P(S_1, \dots, S_n)$ tel que $i_1 + 2i_2 + \cdots + ni_n = q$.

Preuve:

* L'unicité découle de 2.10
* L'existence:

par double récurrence sur $n$ et $q$.

. Si $n = 1$, c'est évident.

. On suppose que $n > 1$, et comme H.R. la propriété à montrer est vraie pour tous les polynômes symétriques à $k$ indéterminées où $k \in \{1, 2, \dots, n-1\}$, sur

le corps K.

Soit donc $G \in K[X_1, \dots, X_n]$, symétrique et de degré $q$. On raisonne alors par récurrence sur l'entier $q$.

• Si $q = 0$, c'est évident.

• On suppose que $q > 0$, et comme H.R$_1$ c'est vraie pour tous les $G' \in K[X_1, \dots, X_n]$ tels que $G'$ symétrique et $\deg G' \leq q-1$. Soit $G_1(X_1, \dots, X_{n-1}) = G(X_1, \dots, X_{n-1}, 0)$, $G_1$ est symétrique de $K(X_1, \dots, X_{n-1})$, d'après H.R. il existe $P_1 \in K[X_1, \dots, X_{n-1}]$ tel que

$G_1(X_1, \dots, X_{n-1}) = P_1(S_1', \dots, S_{n-1}')$ où $\forall 1 \leq i \leq n-1$: $S_i' = S_i(X_1, \dots, X_{n-1}, 0)$, et $\delta(P_1) = \deg G_1$;

On a $\deg G_1 \leq \deg G = q$, soit $G_2(X_1, \dots, X_n) = G(X_1, \dots, X_n) - P_1(S_1, S_2, \dots, S_{n-1})$, on a $\deg G_2 \leq q$ et $G_2$ symétrique, $G_2(X_1, \dots, X_{n-1}, 0) = 0$, donc $\forall i \in \{1, \dots, n-1, n\}$ : $X_i$ divise $G_2$ donc $S_n = \prod_{i=1}^{n} X_i$ divise $G_2$ et $G_2(X_1, \dots, X_n) = S_n G_3(X_1, \dots, X_n)$, $G_3$ est symétrique et $\deg G_3 = \deg G_2 - n \leq q - n$, d'après l'H.R$_2$. il existe $P_2 \in K[X_1, \dots, X_n]$ tel que $G_3(X_1, \dots, X_n) = P_2(S_1, \dots, S_n)$ et $\delta(P_2) = \deg G_3 \leq q - n$,

Soit alors $\underline{P}(X_1,\dots,X_n) = X_n P_2(X_1,\dots,X_n) + P_1(X_1,\dots,X_{n-1})$, on a

$G_r(X_1,\dots,X_n) = \underline{P}(S_1,\dots,S_n)$.

Montrons que $\delta(P) = q$.

Comme $\delta(X_n P_2(X_1,\dots,X_n)) \leq n + (q-n) = q$ et $\delta(P_1) \leq q$ alors $\delta(P) \leq q$, et si pour tout monôme non nul $\lambda S_1^{\alpha_1} \cdots S_n^{\alpha_n}$ de $P(S_1,\dots,S_n)$, on a $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n \leq q-1$ alors tous les monômes de $G_r$ seront de degrés $\leq q-1$, ce qui est absurde, d'où $\delta(P) = q$.

C.Q.F.D.