Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Eugène Malek

Matrices de compagnon généralisées

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 5 (1963-1964), exp. n° 17, p. 1-11

<http://www.numdam.org/item?id=SDPP_1963-1964__5__A11_0>

Séminaire DELANGE-PISOT
(Théorie des Nombres)
5e année, 1963/64, n° 17

27 avril 1964

MATRICES DE COMPAGNON GÉNÉRALISÉES

par Eugène MALEK

1. Notations utilisées et rappel de quelques résultats connus.

Soit K un corps quelconque dont on précisera la nature par la suite. On désignera par $K[x]$ l'anneau des polynômes à coefficients dans K.

Soit $P(x) \in K[x]$, $P(x) = x^n - a_{n-1} x^{n-1} - \dots - a_1 x - a_0$ un polynôme de degré n sur K ($a_i \in K$). On désignera par $(P(x))$ l'idéal principal de polynômes dans $K[x]$ engendré par $P(x)$.

Considérons l'anneau quotient $\overline{K}[x] = K[x]/(P(x))$. Les remarques suivantes sont immédiates.

1.1. - $\overline{K}[x]$ est une algèbre linéaire de degré n sur K avec pour base l'ensemble $\{1 , x , x^2 , \dots , x^{n-1}\}$. Autrement dit

$$\overline{K}[x] = \{ \sum_0^{n-1} b_i x^i \mid b_i \in K \} .$$

1.2. - K commutatif $\iff$ $\overline{K}[x]$ commutatif.

1.3. - $\overline{K}[x]$ intègre $\iff$ $P(x)$ est irréductible sur K. Si de plus K est commutatif, alors $\overline{K}[x]$ est isomorphe à un corps de rupture de $P(x)$ sur K.

Soit E un espace vectoriel de dimension n sur K, on désignera par $\mathfrak{L}(E , E)$ l'ensemble des transformations linéaires de E dans E.

Soit $\tau \in \mathfrak{L}(E , E)$ et $u \in E$; on désignera par $\{u\}$ le plus petit sous-espace vectoriel invariant par τ,

$$\{u\} = [u , \tau u , \tau^2 u , \dots , \tau^i u , \dots]$$

engendré par u et τ. $\{u\}$ sera l'espace cyclique (relatif à τ) engendré par u.

L'espace E est cyclique (relatif à τ), et τ sera cyclique s'il existe un vecteur $v \in E$ qui engendre E, c'est-à-dire $\{v\} = E$. Dans ce cas, le polynôme minimal de τ est égal au polynôme minimal de τ relatif à v.

1.4. - On démontre que " $\tau \in \mathfrak{L}(E , E)$ est cyclique $\iff$ son polynôme minimal $P(x)$ est de degré n sur K ", donc s'écrit :

$$P(x) = x^n - a_{n-1}\, x^{n-1} - \cdots - a_1\, x - a_0 \,.$$

1.5. - De 1.4, on déduit facilement que

$$\tau \in \mathfrak{L}(E\ ,\ E) \text{ est cyclique } \Longleftrightarrow \{\tau^0\ ,\ \tau^1\ ,\ \cdots\ ,\ \tau^{n-1}\}$$

est un ensemble linéairement indépendant sur K , où τ^0 est la transformation neutre.

Dans $\mathfrak{L}(E\ ,\ E)$, qui est un espace vectoriel de dimension n^2 sur K , on désignera par $K[\tau]$ l'anneau des expressions polynomiales en τ sur K , et par $K_0[\tau]$ l'ensemble des expressions polynomiales en τ qui sont égales à $0 \in \mathfrak{L}(E\ ,\ E)$.

1.6.- Dans $K[\tau]$, l'ensemble $K_0[\tau]$ est un idéal principal engendré par l'expression polynomiale $P(\tau)$, où $P(x)$ est le polynôme minimal de τ . On en déduit que l'anneau quotient

$$K[\tau]/(P(\tau)) = K[\tau]/K_0[\tau] = \overline{K}[\tau]$$

est une algèbre sur K avec multiplication modulo $P(\tau)$. Le degré de $\overline{K}[\tau]$ sur K est égal au degré du polynôme $P(x)$ sur K .

Dans tout ce qui suit on supposera que K est commutatif. On désignera par K_n l'espace des n-uples sur K , par $\{\varepsilon_1\ ,\ \varepsilon_2\ ,\ \cdots\ ,\ \varepsilon_n\}$ la base orthonormale de K_n ,

$$\varepsilon_1 = (1\ ,\ 0\ ,\ \ldots,\ 0)\ ,\ \cdots\ ,\ \varepsilon_i = (0\ ,\ 0\ ,\ \ldots,\ 1\ ,\ 0\ ,\ \ldots,\ 0)\ ,\ \ldots\ ,\ \varepsilon_n = (0\ ,\ \ldots,1)$$

et par $\mathfrak{L}(K_n\ ,\ K_n)$ l'espace de transformations linéaires de K_n dans K_n . On désignera par $M(K_n\ ,\ K_n)$ l'espace des matrices carrées d'ordre n sur K . On a donc

$$\mathfrak{L}(K_n\ ,\ K_n) \overset{\varphi_1}{\sim} M(K_n\ ,\ K_n)\ ,$$

c'est-à-dire les deux algèbres sont isomorphes par un isomorphisme φ_1 .

Pour une matrice carrée $A \in M(K_n\ ,\ K_n)$ on désignera par $K[A]$ l'anneau des expressions polynomiales en A sur K , et par $K_0[A]$ l'ensemble des expressions polynomiales qui sont égales à la matrice nulle.

Dans $K[A]$ l'ensemble $K_0[A]$ est un idéal principal engendré par l'expression polynomiale $P(A)$, où $P(x)$ est le polynôme minimal de A . On en déduit que l'anneau quotient

$$K[A]/(P(A)) = K[A]/K_0[A] = \overline{K}[A]$$

est une algèbre commutative sur K , avec multiplication modulo $P(A)$. Pour

$\tau = \varphi_1(A)$, on a

$$K[\tau] \underset{\sim}{\overset{\varphi_1}{}} K[A] \quad \text{et} \quad \overline{K}[\tau] \underset{\sim}{\overset{\varphi_1}{}} \overline{K}[A] .$$

1.8. - A chaque polynôme unitaire $P(x) = x^n - a_{n-1} x^{n-1} - \dots - a_1 x - a_0$ de degré n sur K , on peut **associer** une matrice carrée d'ordre n dont le polynôme minimal est $P(x)$, et dont le polynôme caractéristique est $(-1)^n P(x)$. Cette matrice, qu'on appelle "matrice compagnon" de $P(x)$, est de la forme

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ & & & 1 & \\ 0 & & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & & a_{n-1} \end{pmatrix}$$

2. La matrice de compagnon généralisée.

2.1. - Soient $\tau \in \mathcal{L}(K_n , K_n)$ une transformation linéaire cyclique quelconque, et $P(x)$ son polynôme minimal ; alors l'algèbre commutative

$$K[\tau]/(P(\tau)) = K[\tau]/(0) = \overline{K}[\tau] = \{\Phi \mid \Phi = \sum_0^{n-1} b_i \tau^i , \ b_i \in K\}$$

est **isomorphe** à $\overline{K}[x]$ par l'isomorphisme

$$\Phi = \sum_0^{n-1} b_i \tau^i \overset{\varphi_2}{\longleftrightarrow} \sum_0^{n-1} b_i x^i \in \overline{K}[x] ,$$

où la multiplication s'effectue modulo $P(\tau)$ et $P(x)$ respectivement.

En effet " τ cyclique $\Longrightarrow \{1 , \tau , \dots , \tau^{n-1}\}$ " est un ensemble linéairement indépendant sur K . Donc $K[\tau]$ est un espace vectoriel de dimension n sur K . D'où l'isomorphisme naturel des deux espaces vectoriels $K[\tau]$ et $K[x]$.

D'autre part, pour $\Phi_1 , \Phi_2 \in K[\tau]$, le produit $\Phi_1 . \Phi_2$ se ramène à $\Phi_3 \pmod{P(\tau)} \in K[\tau]$, en utilisant la formule $\tau^n = \sum_0^{n-1} a_i \tau^i$. De même, pour $\Phi_1(x) , \Phi_2(x) \in \overline{K}[x]$, $\Phi_1(x).\Phi_2(x)$ se ramène à $\Phi_3(x) \pmod{P(x)} \in \overline{K}[x]$. D'où l'isomorphisme

$$\Phi_1(\tau).\Phi_2(\tau) \pmod{P(\tau)} \overset{\varphi_2}{\longleftrightarrow} \Phi_1(x).\Phi_2(x) \pmod{P(x)} .$$

Donc si τ correspond à une certaine matrice $A \in M(K_n , K_n)$, on a

$$K[A] \underset{\sim}{\overset{\varphi_1}{}} K[\tau] \underset{\sim}{\overset{\varphi_2}{}} \overline{K}[x] .$$

D'où l'isomorphisme $K[A] \underset{\sim}{\overset{\varphi}{}} \overline{K}[x]$, où $\varphi = \varphi_2 \circ \varphi_1$.

2.2. - La "matrice compagnon"

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & & & & 1 \\ a_0 & a_1 & \cdots & & a_{n-1} \end{pmatrix}$$

associée au polynôme $P(x) = x^n - a_{n-1} x^{n-1} - \ldots - a_1 x - a_0$ est cyclique.

Puisque $\mathfrak{L}(K_n , K_n) \underset{\sim}{\overset{\varphi_1}{}} M(K_n , K_n)$, il suffit de démontrer que la transformation linéaire T , correspondant à A , est cyclique. Or les lignes de A sont les coordonnées de transformés de vecteurs $\varepsilon_1 , \varepsilon_2 , \ldots , \varepsilon_n \in K_n$ par T . En effet on a

$$T\varepsilon_1 = \varepsilon_2 = (0 , 1 , 0 , \ldots , 0)$$

$$T\varepsilon_2 = \varepsilon_3 = (0 , 0 , 1 , 0 , \ldots , 0)$$

$$\ldots$$

$$T\varepsilon_n = a_0 \varepsilon_1 + a_1 \varepsilon_2 + \ldots + a_{n-1} \varepsilon_n = (a_0 , a_1 , \ldots , a_{n-1}) .$$

Ceci entraîne que $[\varepsilon_1 , T\varepsilon_1 , \ldots , T^{n-1} \varepsilon_1] = \{\varepsilon_1\} = K_n$. D'où, d'après la définition, T est cyclique, et par conséquent A aussi.

Donc d'après 2.1.,

$$K[A] \underset{\sim}{\overset{\varphi}{}} \overline{K}[x] ,$$

où

$$K[A] = \{B \; ; \; B = \sum_0^{n-1} b_i A^i , \; b_i \in K\} .$$

2.3. - $B \in K[A] \implies B$ est engendré par récurrence de la manière suivante

$$B = \sum_0^{n-1} b_i A^i =$$

$$= \begin{pmatrix} b_0 & b_1 & \cdots & b_i & \cdots & b_{n-1} \\ b_{n-1}a_0 & b_{n-1}a_1 + b_0 & \cdots & b_{n-1}a_i + b_{i-1} & \cdots & b_{n-1}a_{n-1} + b_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ b_{i1} & b_{i2} & \cdots & b_{ii} & \cdots & b_{in} \\ b_{in}a_0 & b_{in}a_1 + b_{i1} & \cdots & b_{in}a_{i-1} + b_{i(i-1)} & \cdots & b_{in}a_{n-1} + b_{i(n-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

c'est-à-dire dans la $(i+1)$-ième ligne, on a

$$b_{(i+1)j} = b_{in}\, a_{j-1} + b_{i(j-1)} \text{ , où } b_{i0} = 0 \quad (j = 1 , 2 , \dots , n) .$$

En effet nous avons vu plus haut que, à T considéré comme transformation linéaire par rapport à la base $\{\varepsilon_1 , \varepsilon_2 , \dots , \varepsilon_n\}$, correspond A .Donc, à T^2 correspond A^2 , et en général à T^i correspond A^i $(i = 1 , 2 , \dots , n-1)$. Considérons donc la transformation linéaire $\sum_0^{n-1} b_i T^i$ par rapport à la base $\{\varepsilon_1 , \varepsilon_2 , \dots , \varepsilon_n\}$.

$$(\sum_0^{n-1} b_i T^i).\varepsilon_1 = \sum_0^{n-1} b_i \varepsilon_{i+1}$$

$$(\sum_0^{n-1} b_i T^i).\varepsilon_2 = (\sum_0^{n-1} b_i T^i).T.\varepsilon_1 = \sum_0^{n-1} (b_{n-1}\, a_i + b_{i-1}).\varepsilon_{i+1} ,$$

où $b_{-1} = 0$.

Soit $(\sum_0^{n-1} b_i T^i)\varepsilon_k = \sum_{k=1}^{n} b_{ik} \varepsilon_k$, alors

$$(\sum_0^{n-1} b_i T^i).\varepsilon_{k+1} = (\sum_0^{n-1} b_i T^i).T.\varepsilon_k = T(\sum_{k=1}^{n} b_{ik} \varepsilon_k) = \sum_{k=1}^{n} (b_{in}\, a_{k-1} + b_{i(k-1)}).\varepsilon_k ,$$

où $b_{i0} = 0$.

Ce système équivaut à

$$\sum_0^{n-1} b_i T^i \begin{Bmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \cdot \\ \cdot \\ \cdot \\ \varepsilon_n \end{Bmatrix} = \sum_0^{n-1} b_i A^i$$

et on constate que les coefficients sont ceux précédemment indiqués.

2.4. - Soient B , $C \in K[A]$, $B = (b_{ij})$, $C = (c_{ij})$, alors la multiplication $B.C$ s'effectue de la manière suivante :

Soit $(b_{11} , \dots , b_{1n})$ la première ligne de B , et soit

$$(b_{11} , \dots , b_{1n}).C = (d_{11} , \dots , d_{1n})$$

la première ligne de $D = B.C$.

D est engendré par récurrence à partir de $(d_{11} , \dots , d_{1n})$ de la manière indiquée dans 2.3.

En effet

$$B\ ,\ C \in K[A] \implies B = \sum_1^n b_{1i}\ A^{i-1} \quad \text{et} \quad C = \sum_1^n c_{1i}\ A^{i-1}\ .$$

Or A correspond à T par rapport à la base $\{\varepsilon_1\ ,\ \varepsilon_2\ ,\ \ldots\ ,\ \varepsilon_n\}$. Donc B correspond à $\sum_1^n b_{1i}\ T^{i-1}$ et C correspond à $\sum_0^{n-1} c_{1i}\ T^{i-1}$ par rapport à la même base $\{\varepsilon_1\ ,\ \varepsilon_2\ ,\ \ldots\ ,\ \varepsilon_n\}$. D'où, puisque $K[T] \underset{\sim}{\varphi_1^0} K[A]$, D correspond à

$$(\sum_1^n b_{1j}\ T^{j-1})(\sum_1^n c_{1j}\ T^{j-1})$$

par rapport à la base $\{\varepsilon_1\ ,\ \varepsilon_2\ ,\ \ldots\ ,\ \varepsilon_n\}$.

Pour simplifier l'écriture, posons

$$\sum_1^n b_{1j}\ T^{j-1} = b(T) \quad \text{et} \quad \sum_1^n c_{1j}\ T^{j-1} = c(T)\ .$$

On aura donc

$$b(T)\ c(T) = b_{11}\ c(T) + b_{12}\ c(T).T + \ldots + b_{1n}\ c(T).T^{n-1}\ .$$

La première ligne de D sera

$$\begin{aligned} b(T)\ c(T).\varepsilon_1 &= b_{11}\ c(T).\varepsilon_1 + b_{12}\ c(T).T.\varepsilon_1 + \ldots + b_{1n}\ c(T).T^{n-1}.\varepsilon_1 \\ &= b_{11}\ c(T).\varepsilon_1 + b_{12}\ c(T).\varepsilon_2 + \ldots + b_{1n}\ c(T).\varepsilon_n \\ &= b_{11} \sum_1^n c_{1j}\ \varepsilon_j + b_{12} \sum_1^n c_{2j}\ \varepsilon_j + \ldots + b_{1n} \sum_1^n c_{nj}\ \varepsilon_j \\ &= \sum_{j=1}^n b_{1j}(\sum_{k=1}^n c_{jk}\ \varepsilon_k) = (b_{11}\ ,\ \ldots\ ,\ b_{1n}).C = (d_{11}\ ,\ \ldots\ ,\ d_{1n}) \\ &= \sum_1^n d_{1j}\ \varepsilon_j = (\sum_1^n d_{1j}\ T^{j-1}).\varepsilon_1\ . \end{aligned}$$

La deuxième ligne de D sera

$$\begin{aligned} b(T)\ c(T).\varepsilon_2 &= b_{11}\ c(T).\varepsilon_2 + b_{12}\ c(T).T.\varepsilon_2 + \ldots + b_{1n}\ c(T).T^{n-1}.\varepsilon_2 \\ &= b_{11}\ c(T).T.\varepsilon_1 + b_{12}\ c(T).T.\varepsilon_2 + \ldots + b_{1n}\ c(T).T.\varepsilon_n \\ &= (\sum_{j=1}^n d_{1j}\ T^{j-1}).T.\varepsilon_1 = \sum_{j=1}^n (d_{1j}\ T^{j-1}).\varepsilon_2\ . \end{aligned}$$

De même la m-ième ligne sera

$$(\sum_1^n d_{1j}\ T^{j-1}).T^{m-1}.\varepsilon_1 = (\sum_1^n d_{1j}\ T^{j-1}).\varepsilon_m\ .$$

On voit donc que ce système donne lieu au même type de récurrence que celui précisé en 2.3. Autrement dit, D est engendré par récurrence à partir de sa première ligne $(b_{11}, \dots, b_{1n})C = (d_{11}, \dots, d_{1n})$.

On voit facilement que la multiplication de deux telles matrices ne nécessite qu'au plus $2n^2 - n$ multiplications et $2n^2 - 3n + 1$ additions.

2.5. - L'inverse d'une matrice $B \in K[A]$, s'il existe, peut se déterminer de la manière suivante :

Soit $C = B^{-1} = (c_{ij})$, C est engendré par récurrence à partir de sa première ligne $(c_{11}, \dots, c_{1n})$. Pour déterminer $(c_{11}, \dots, c_{1n})$ il suffit de résoudre le système d'équations linéaires

$$B^* \begin{pmatrix} c_{11} \\ \vdots \\ c_{1n} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

où B^* est la transposée de B.

En effet soit $f(x)$ le polynôme minimal de B,

$$f(x) = x^m - a_{m-1} x^{m-1} - \dots - a_1 x - a_0 , \qquad a_i \in K .$$

Donc

$$B^m - a_{m-1} B^{m-1} - \dots - a_1 B - a_0 I = 0 = \text{matrice nulle.}$$

Si B est inversible, alors

$$B^{-1} = 1/a_0[B^{m-1} - a_{m-1} B^{m-2} - \dots - a_1 I] .$$

D'où $B^{-1} \in K[A]$, et, d'après 2.3, est engendré par récurrence à partir de sa première ligne de la manière qui y est indiquée.

Or $B^{-1} = C = (c_{ij}) \implies (c_{11}, \dots, c_{1n})B = (1, 0, \dots, 0)$. Ceci équivant à $B^* \begin{pmatrix} c_{11} \\ \vdots \\ c_{1n} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, où B^* est la transposée de B. D'où le résultat cherché.

2.6. - La matrice $B = \sum_0^{n-1} b_i A^i \in K[A]$ est régulière si et seulement si $(\sum_0^{n-1} b_i x^i , P(x)) = 1$. Ceci permet donc de déterminer par isomorphisme le groupe G_0 des unités de $\overline{K[A]}$.

En effet, soient $\{\alpha_1 , \dots , \alpha_n\}$ les racines de $(-1)^n P(x)$, alors

$$\{\sum_0^{n-1} b_i \alpha^i , \dots , \sum_0^{n-1} b_i \alpha_n^i\}$$

seront les valeurs propres de B et $\det(B) = (-1)^n \prod_{j=1}^{n} (\sum_{i=0}^{n-1} b_i \alpha_j^i)$. Or $(\sum_0^{n-1} b_i x^i , P(x)) = d(x)$ de degré $> 0 \implies$ il existe un α_j $(j = 1 , 2 , \dots , n)$ tel que $d(\alpha_j) = 0$. D'où, puisque $d(x) \mid \sum_0^{n-1} b_i x^i$,

$$\det(B) = (-1)^n \prod_{j=1}^{n} (\sum_{i=0}^{n} b_i \alpha_j^i) = 0$$

et B n'est pas régulière.

D'autre part

$$(\sum_0^{n-1} b_i x^i , P(x)) = 1 \implies \forall \alpha_j \quad (j = 1 , 2 , \dots , n) \quad \sum_{i=0}^{n-1} b_i \alpha_j^i \neq 0 ,$$

car

$$\sum_{i=0}^{n-1} b_i \alpha_j^i = 0 \implies (\sum_0^{n-1} b_i x^i , P(x)) \neq 1 .$$

D'où $\det(B) \neq 0$ et B est régulière.

Remarquons qu'on pourra déduire le même résultat à partir de l'identité de Bezout.

2.7. - Remarque. Nous avons récemment démontré le résultat suivant : Pour une matrice carrée quelconque M d'ordre n , il existe $n + 1$ matrices A_i d'ordre n du type défini dans 2.3, telles que $M = \sum_{i=1}^{n+1} A_i$.

3. Applications.

3.1. - A chaque élément $b(x) = \sum_0^{n-1} b_i x^i \in \overline{K}[x]$ correspond un polynôme (qu'on appellera polynôme normal de $b(x)$) qui est le polynôme caractéristique de $\sum_0^{n-1} b_i A^i = B \in K[A]$, où A est la "matrice compagnon" de $P(x)$.

Puisque les puissances de B s'obtiennent par récurrence, la méthode de Le Verrier permet, dans ce cas, de calculer rapidement le polynôme normal de $b(x)$ (à partir de la formule de Newton pour les traces

$$kc_k = s_k - c_1 s_{k-1} - \dots - c_{k-1} s_1 \quad (k = 1 , 2 , \dots , n) ,$$

où s_k est la trace de B^k). En particulier ceci donne une méthode efficace pour calculer le polynôme normal d'un nombre algébrique quelconque.

3.2. - Considérons $y = \sum y_i A^i \in K[A] = Q[A]$, K étant dans ce cas le corps des rationnels , A la "matrice compagnon" de $P(x) \in Q[x]$.

$\det(y)$ est une forme homogène de degré n en y_i $(i = 0 , 1 , 2 , \dots , n-1)$ à coefficients dans Q .

D'après 2.6, $\det(y) = 0$ si et seulement si $(\sum_0^{n-1} y_i x^i , P(x)) \neq 1$. On en déduit que si P(x) est irréductible alors la forme homogène $\det(y) = 0$ n'aura pas de solution rationnelle autre que zéro.

Par contre, si P(x) est réductible, il y aura une infinité de solutions rationnelles et même une infinité de solutions qui sont des entiers rationnels.

En effet, tout n-uple $(y_0 , y_1 , \dots , y_{n-1})$ à coordonnés entière sera une solution si $(\sum_0^{n-1} y_i x^i , P(x)) \neq 1$.

3.3. - Supposons que K est un champs de Galois, $K = C.G(p^h) = C.G(g)$ et A est la "matrice compagnon" de P(x) polynôme unitaire de degré n sur K , alors le nombre d'unités $B \in K[A]$ est égal à

$$U = g^n \prod_{i=1}^{m} (1 - (1/g^{\beta_i})) ,$$

où $P(x) = \prod_{i=1}^{m} P_i^{\alpha_i}(x)$ et $\partial^0 P_i(x) = \beta_i$, $P_i(x)$ $(i = 1 , 2 , \dots , m)$ irréductible sur K . D'où "l'ordre du groupe des unités $G \subset \overline{K}[x]$ = l'ordre du groupe des unités $G' \subset K[A]$ " est égal à U .

G' est un sous-groupe commutatif du groupe $\overline{G}$ d'automorphismes de l'espace vectoriel K^n , où l'ordre de $\overline{G}$ est $\prod_{i=0}^{n-1} (g^n - g^i)$.

En effet on a vu plus haut que $\overline{K}[x] \overset{\varphi}{\simeq} K[A]$. Or d'après 2.6, $B = \sum_{i=0}^{n-1} b_i A^i$ est régulière si et seulement si $(\sum_{i=0}^{n-1} b_i x^i , P(x)) = 1$. Il suffit donc de déterminer le nombre d'unités de $\overline{K}[x]$. Nous allons donc démontrer que le nombre d'unités de $\overline{K}[x]$ est $g^n \prod_{i=1}^{m} (1 - (1/g^{\beta_i}))$, ceci par récurrence sur le nombre m de facteurs distincts et irréductibles de P(x) .

$m = 1 \Longrightarrow P(x) = P_1^{\alpha_1}(x) \implies$ le nombre d'éléments non nuls divisibles par $P_1(x)$ est $(g^{n-\beta_1} - 1)$.

Donc le nombre d'éléments de $\overline{K}[x]$ divisibles par $P_1(x)$ est

$$(g^{n-\beta_1} - 1) + 1 = g^{n-\beta_1} .$$

D'où, le nombre d'éléments relativement premiers à P(x) est

$$g^n - g^{n-\beta_1} = g^n(1 - 1/g^{\beta_1}) = U .$$

$m = 2 \implies P(x) = P_1^{\alpha_1}(x)\, P_2^{\alpha_2}(x) \implies$ le nombre d'éléments non nuls divisibles par $P_1(x)$ est $g^{n-\beta_1} - 1$.

Le nombre d'éléments non nuls divisibles par $P_2(x)$ mais pas par $P_1(x)\, P_2(x)$ est est

$$(g^{n-\beta_2} - 1) - (g^{n-\beta_1-\beta_2} - 1) .$$

Donc le nombre d'éléments qui ne sont pas premiers à $P(x)$ est

$$(g^{n-\beta_1} - 1) + (g^{n-\beta_2} - 1) - (g^{n-\beta_1-\beta_2} - 1) + 1 .$$

D'où le nombre d'éléments relativement premiers à $P(x)$ est

$$g^n - (g^{n-\beta_1} + g^{n-\beta_2}) + g^{n-\beta_1-\beta_2}$$

$$= g^n(1 - g^{-\beta_1} - g^{-\beta_2} + g^{-\beta_1-\beta_2}) = g^n(1 - g^{-\beta_1})(1 - g^{-\beta_2}) = U .$$

$m = 3 \implies P(x) = P_1^{\alpha_1}(x).P_2^{\alpha_2}(x).P_3^{\alpha_3}(x) \implies$ le nombre d'éléments non nuls divisibles par $P_1(x)$ est $(g^{n-\beta_1} - 1)$.

Le nombre d'éléments non nuls divisibles par $P_2(x)$, mais pas par $P_1(x)\, P_2(x)$ est

$$(g^{n-\beta_2} - 1) - (g^{n-\beta_1-\beta_2} - 1) .$$

Le nombre d'éléments non nuls divisibles par $P_3(x)$, mais par par $P_1\, P_3$, $P_2\, P_3$, $P_1\, P_2\, P_3$ est

$$(g^{n-\beta_3} - 1) - (g^{n-\beta_1-\beta_3} - 1) - (g^{n-\beta_2-\beta_3} - 1) + (g^{n-\beta_1-\beta_2-\beta_3} - 1) .$$

Donc le nombre d'éléments qui ne sont pas premiers à $P(x)$ est

$$g^{n-\beta_1} + g^{n-\beta_2} + g^{n-\beta_3} - g^{n-\beta_1-\beta_3} - g^{n-\beta_2-\beta_3} + g^{n-\beta_1-\beta_2-\beta_3} .$$

D'où le nombre d'éléments relativement premiers à $P(x)$ est

$$g^n - [g^{n-\beta_1} + g^{n-\beta_2} + g^{n-\beta_3} - g^{n-\beta_1-\beta_2} - g^{n-\beta_1-\beta_3} - g^{n-\beta_2-\beta_3} + g^{n-\beta_1-\beta_2-\beta_3}]$$

$$= g^n[1 - g^{-\beta_1} - g^{-\beta_2} - g^{-\beta_3} + g^{-\beta_1-\beta_2} + g^{-\beta_1-\beta_3} + g^{-\beta_2-\beta_3} - g^{-\beta_1-\beta_2-\beta_3}]$$

$$= g^n(1 - g^{-\beta_1})(1 - g^{-\beta_2})(1 - g^{-\beta_3}) = U .$$

Supposons que la formule soit vraie pour $P(x) = \prod_{i=1}^{m-1} P_i^{\alpha_i}(x)$ avec $\partial^0 P_i(x) = \beta_i$, et démontrons-la pour $P(x) = \prod_{i=1}^{m} P_i^{\alpha_i}(x)$ avec $\partial^0 P_i(x) = \beta_i$, $(i = 1 , 2, \ldots, m)$.

Le nombre d'éléments non nuls divisibles par $P_m(x)$, mais relativement premiers à $P_1(x)\ P_2(x)\ \ldots\ P_{m-1}(x)$ est égal à

$$(g^{n-\beta_m} - 1) - (\sum_{i=1}^{m-1} g^{n-\beta_m-\beta_i} - 1) + (\sum_{\substack{i,j=1 \\ i\neq j}}^{m-1} g^{n-\beta_m-\beta_i-\beta_j} - 1)$$

$$- \ldots + (-1)^{m-1}(g^{n-\sum_1^m \beta_i} - 1) = g^{n-\beta_m} \prod_{i=1}^{m-1} (1 - g^{-\beta_i}) .$$

Donc le nombre d'éléments qui ne sont pas relativement premiers à $P(x)$ est

$$g^n - g^n \prod_{i=1}^{m-1} (1 - g^{-\beta_i}) + g^{n-\beta_m} \prod_{i=1}^{m-1} (1 - g^{-\beta_i}) .$$

D'où le nombre d'éléments relativement premiers à $P(x)$ est

$$g^n - [g^n - g^n \prod_{i=1}^{m-1} (1 - g^{-\beta_i}) + g^{n-\beta_m} \prod_{i=1}^{m-1} (1 - g^{-\beta_i})]$$

$$= g^n \prod_{i=1}^{m-1} (1 - g^{-\beta_i})[1 - g^{-\beta_m}] = g^n \prod_{i=1}^{m} (1 - g^{-\beta_i}) = U .$$

D'où le résultat cherché.