Q648 (119 3)

Soient $K \subset L$ *deux corps commutatifs,* $A_\ell, B_\ell \in M_n(K)$ *des matrices carrées à* n *lignes et* n *colonnes pour* $1 \leq \ell \leq k$. *On suppose qu'il existe* $P \in G\ell_n(L)$ *tel que* $PA_\ell P^{-1} = B_\ell$ *pour* $1 \leq \ell \leq k$.
Alors il existe $Q \in G\ell_n(K)$ *tel que* $QA_\ell Q^{-1} = B_\ell$ *pour* $1 \leq \ell \leq k$.

Démonstration (Jean Fresnel et Michel Matignon)

1) *On suppose que* K *est infini.*
Alors l'ensemble des coefficients de P engendre un sous-K-espace vectoriel de L qui est de dimension finie. Soient $(e_1, e_2, \ldots, e_m)$ une base sur K de ce sous-espace vectoriel. On a donc $\lambda_1, \lambda_2, \ldots, \lambda_m \in K$ avec
$P = P_1 e_1 + P_2 e_2 + \ldots + P_m e_m$ où $P_i \in M_n(K)$ pour $1 \leq i \leq m$.
De la relation $PA_\ell = B_\ell P$, il suit que $P_i A_\ell = B_\ell P_i$ pour $1 \leq i \leq m$ et $1 \leq \ell \leq k$.
On considère le polynôme de $K[X_1, X_2, \ldots, X_m]$ défini par
$S(X_1, X_2, \ldots, X_m) := \det(P_1 X_1 + P_2 X_2 + \ldots + P_m X_m)$. On a
$S(e_1, e_2, \ldots, e_m) = \det(P_1 e_1 + P_2 e_2 + \ldots + P_m e_m) = \det P \neq 0$; cela montre que $S(X_1, X_2, \ldots, X_m) \neq 0$. Sachant que K est un corps infini, il existe $\mu_1, \mu_2, \ldots, \mu_m \in K$ avec $S(\mu_1, \mu_2, \ldots, \mu_m) \neq 0$ ([Fr] corollaire 2.5.13, p. 103).
Soit $Q := P_1 \mu_1 + P_2 \mu_2 + \ldots + P_m \mu_m$, il suit de ce qui précède que $\det Q \neq 0$, que $Q \in G\ell_k(K)$ et que $QA_\ell Q^{-1} = B_\ell$ pour $1 \leq \ell \leq k$.

2) *On suppose que* K *est le corps fini* $\mathbb{F}_q$ *à* q *éléments* (*avec* $q = p^a$ *où* $p := \mathrm{car}(K)$).
Soit $K_1 := (\mathbb{F}_q)^{alg}$ une clôture algébrique de $\mathbb{F}_q$. Montrons qu'il existe
$P_1 \in G\ell_n(K_1)$ tel que $P_1 A_\ell {P_1}^{-1} = B_\ell$ pour $1 \leq \ell \leq k$.
En effet, soit $L_1 := L K_1$ le compositum de L et de K_1 . On a donc $P \in G\ell_n(L_1)$ tel que $PA_\ell P^{-1} = B_\ell$ pour $1 \leq \ell \leq k$. Sachant que K_1 est infini, la démonstration utilisée en 1) montre qu'il existe qu'il existe $Q \in G\ell_n(K_1)$ tel que $QA_\ell Q^{-1} = B_\ell$ pour $1 \leq \ell \leq k$.

3) *Il nous reste donc à considérer le cas suivant avec* $K = \mathbb{F}_q$, $L = (\mathbb{F}_q)^{alg}$,
$A_\ell, B_\ell \in M_n(K)$ *pour* $1 \leq \ell \leq k$ *avec* $P \in G\ell_n(L)$ *tel que* $PA_\ell P^{-1} = B_\ell$ *pour* $1 \leq \ell \leq k$.

Soit F l'automorphisme de L défini par $F(x) := x^q$; en particulier, on a $F(x) = x$ si et seulement si $x \in \mathbb{F}_q$. On note aussi $F : M_n(L) \to M_n(L)$ l'automorphisme d'anneau défini par $F([x_{i,j}]_{i,j}) := [F(x_{i,j})]_{i,j}$; bien entendu F induit un automorphisme de $G\ell_n(L)$ toujours noté F . En particulier $F([x_{i,j}]_{i,j}) = [x_{i,j}]_{i,j}$ si et seulement si $[x_{i,j}]_{i,j} \in M_n(K)$.
Par hypothèse, on a $P \in G\ell_n(L)$ tel que $PA_\ell = B_\ell P$ pour $1 \le \ell \le k$. On a donc aussi $A_\ell P^{-1} = P^{-1} B_\ell$ et $F(P) A_\ell = B_\ell F(P)$.
Soient $G(L) := \{ U \in G\ell_n(L) \mid UA_\ell = A_\ell U$ pour $1 \le \ell \le k \}$, c'est un sous-groupe de $G\ell_n(L)$ et on a $P^{-1} F(P) \in G(L)$.
Soit $f : G(L) \to G(L)$ l'application définie par $f(U) := U^{-1} F(U)$.
On suppose provisoirement que f est surjective . Ainsi il existe $U \in G(L)$ tel que $f(U) = P^{-1} F(P)$, il suit que $UP^{-1} = F(UP^{-1})$, ce qui veut dire que $Q := UP^{-1} \in G\ell_n(K)$. Ensuite pour $1 \le \ell \le k$ on a

$$QB_\ell = UP^{-1} B_\ell = UA_\ell P^{-1} = A_\ell U P^{-1} = A_\ell Q .$$

Il suit que $QA_\ell Q^{-1} = B_\ell$ pour $1 \le \ell \le k$ et $Q \in G\ell_n(K)$.
Ainsi l'énoncé est satisfait, sous la condition que l'application f est surjective. C'est l'objet de ce qui suit.

Remarques Avant de démontrer que l'application f est surjective, nous devons faire quelques remarques.
1. Le cas où $k = 1$ peut se traiter avec la théorie des invariants de similitude. Rappelons ce que c'est ([F.M.] p. 15-18).
Si $A_1 \in M_n(K)$, on peut lui associer une suite $(P_1, P_2, \dots, P_n)$ de polynômes unitaires de $K[X]$ avec les propriétés qui suivent : $P_1 \mid P_2 \mid \dots \mid P_n$, $P_n = m_{A_1}$, le polynôme minimal de A_1 , $P_1 P_2 \dots P_n = \chi_{A_1}$, le polynôme caractéristique de A_1 et si $P_1 = P_2 = \dots = P_{s-1} = 1$ et $P_s \neq 1$, en notant $C(P_i)$ la matrice compagnon du polynôme P_i pour $i \ge s$, alors A_1 est semblable modulo $G\ell_n(K)$ à la matrice qui est le tableau diagonal
$(C(P_s), C(P_{s+1}), \dots, C(P_n))$. Et enfin $(P_1, P_2, \dots, P_n)$ est la seule suite qui possède les propriétés précédentes.
Il suit donc facilement de cette dernière propriété que s'il existe $S \in G\ell_n(L)$ avec $SA_1 S^{-1} = B_1$, alors il existe $T \in G\ell_n(K)$ avec $TA_1 T^{-1} = B_1$.
On peut aussi interpréter la théorie des invariants de similitude comme il suit.

Le groupe $G\ell_n(K)$ opère sur $M_n(K)$ par $(S,M)\mapsto SMS^{-1}$. Il suit alors que les orbites sont exactement caractérisées par les suites $(P_1,P_2,\dots,P_n)$ de polynômes unitaires de $K[X]$ telles que $\deg P_1P_2\dots P_n=n$ et $P_1|P_2|\dots|P_n$. A noter qu'il existe un algorithme pour calculer la suite $(P_1,P_2,\dots,P_n)$.

2. Pour $k\geq 2$, on serait tenté de faire opérer $G\ell_n(K)$ sur $M_n(K)^k$ par

$$(S,(M_1,M_2,\dots,M_k))\mapsto (SM_1S^{-1},SM_2S^{-1},\dots,SM_kS^{-1}).$$

Malheureusement, à notre connaissance, on ne sait pas encore caractériser de façon simple les orbites de $M_n(K)^k$ sous cette action, comme dans le cas $k=1$ ([L.B.]).

3. On pourrait espérer que le polynôme $S(X_1,X_2,\dots,X_m)$ construit en 1) à partir de la matrice P définit une fonction polynomiale sur K^m qui est non nulle. En fait, il n'en est rien.

On considère l'exemple qui suit. Soient $K:=\mathbb{F}_2$,

$A_1=\begin{bmatrix}0&1&0\\0&1&0\\1&1&1\end{bmatrix}$, $B_1=\begin{bmatrix}1&0&0\\0&0&0\\0&1&1\end{bmatrix}$, $A_2=\begin{bmatrix}0&0&1\\1&1&1\\0&0&1\end{bmatrix}$, $B_2=\begin{bmatrix}0&0&0\\0&1&0\\1&0&1\end{bmatrix}$. Soit $P:=\begin{bmatrix}1&0&1\\a&a&0\\0&1&a\end{bmatrix}$ avec $a\in\mathbb{F}_4-\mathbb{F}_2$. On a bien $P\in G\ell_2(\mathbb{F}_4)$, $PA_i=B_iP$ pour $i=1,2$. Ensuite la fonction polynomiale définie par le polynôme

$S(X_1,X_2)=\text{dét}\begin{bmatrix}X_2&0&X_2\\X_1&X_1&0\\0&X_2&X_1\end{bmatrix}=X_1X_2(X_1+X_2)$ s'annule sur $(\mathbb{F}_2)^2$. Toutefois on peut remarquer que $Q=\begin{bmatrix}1&0&1\\1&1&0\\1&0&0\end{bmatrix}\in G\ell_3(\mathbb{F}_2)$ satisfait $QA_iQ^{-1}=B_i$ pour $i=1,2$.

4. En 2010 de Seguins Pazzis avait déjà répondu à la question [S]. Sa méthode utilise essentiellement une description des orbites d'un groupe opérant simultanémant sur deux matrices. De façon plus précise, il considère $M_{n,p}(K)$, l'ensemble des matrices à n lignes et p colonnes à coefficients dans un corps commutatif K, alors le groupe $G\ell_n(K)\times G\ell_p(K)$ opère sur $M_{n,p}(K)^2$ de la façon qui suit : $((P,Q),(A,B))\mapsto(PAQ^{-1},PBQ^{-1})$. C'est la description d'un système de représentants des orbites qui est le point clé de sa démonstration.

Comme on le verra ci-après, notre méthode utilise essentiellement un résultat de géométrie algébrique concernant les groupes algébriques sur les corps finis.

4. **Montrons que l'application $f: G(L) \to G(L)$ est surjective**

4.1. **Construction de l'idéal premier $\mathfrak{P}$.**
Soient K un corps commutatif, L une clôture algébrique de K.
La lecture des relations matricielles $[X_{i,j}]_{i,j} A_\ell - A_\ell [X_{i,j}]_{i,j} = 0$ pour $1 \le \ell \le k$, en chaque position (i,j) définissent $n^2 \times k$ polynômes $P_{i,j,\ell}$ qui sont homogènes de degré 1 ou nuls. On a donc la proposition qui suit.

Proposition 1 *Soit $M = [m_{i,j}]_{i,j} \in M_n(L)$, alors les propriétés suivantes sont équivalentes.*
i) On a $[m_{i,j}]_{i,j} A_\ell = A_\ell [m_{i,j}]_{i,j}$, $1 \le \ell \le k$,
ii) on a $P_{i,j,\ell}(\boldsymbol{m}) = 0$ pour $1 \le i,j \le n$ et $1 \le \ell \le k$ où $\boldsymbol{m}$ désigne le n^2-uple $(m_{r,s}) \in L^{n^2}$.

Il s'agit maintenant de montrer que l'idéal $\mathfrak{P}_1$ de $K[X_{i,j}, 1 \le i,j \le n]$ engendré par les $P_{i,j,\ell}$ est premier.
Soit E le sous-K–espace vectoriel de $H := \bigoplus_{1 \le i,j \le n} KX_{i,j}$ engendré par les $P_{i,j,\ell}$, soit s la dimension de E . On peut supposer $\{P_1, P_2, \dots, P_s\}$ est une base de E. Par ailleurs, on peut extraire de la famille $\{X_{i,j}\}_{1 \le i,j \le n}$ des éléments $\{Q_{s+1}, Q_{s+2}, \dots, Q_{n^2}\}$ de façon que $\{P_1, P_2, \dots, P_s, Q_{s+1}, Q_{s+2}, \dots, Q_{n^2}\}$ soit une base de H . Facilement $K[X_{i,j}, 1 \le i,j \le n] = K[P_1, P_2, \dots, P_s, Q_{s+1}, Q_{s+2}, \dots, Q_{n^2}]$, i.e. $\{P_1, P_2, \dots, P_s, Q_{s+1}, Q_{s+2}, \dots, Q_{n^2}\}$ sont n^2 variables sur K.
Clairement, on a $\mathfrak{P}_1 := \sum_{i=0}^{s} P_i K[X_{i,j}, 1 \le i,j \le n]$ et $\dfrac{K[X_{i,j}, 1 \le i,j \le n]}{\mathfrak{P}_1} \simeq K[Q_{s+1}, Q_{s+1}, \dots, Q_{n^2}]$. C'est un anneau de polynômes à $n^2 - s$ variables, il est donc intègre et $L \otimes_K K[Q_{s+1}, Q_{s+1}, \dots, Q_{n^2}] = L[Q_{s+1}, Q_{s+2}, \dots, Q_{n^2}]$ est aussi intègre.
Soit $u: K[X_{i,j}, 1 \le i,j \le n] \to \dfrac{K[X_{i,j}, 1 \le i,j \le n]}{\mathfrak{P}_1}$ la surjection canonique, $D(X_{i,j}) := \det [X_{i,j}]_{i,j} = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) X_{1,\sigma(1)} X_{2,\sigma(2)} \dots X_{n,\sigma(n)}$, on souhaite montrer que $u(D(X_{i,j})) \ne 0$, afin de prolonger u en un homomorphisme de

$A := K[X_{i,j}, 1 \le i,j \le n][D^{-1}]$ dans $\mathrm{Fr}(\frac{K[X_{i,j}, 1 \le i,j \le n]}{\mathfrak{P}_1})$.

Soit $e : K[X_{i,j}, 1 \le i,j \le n] \to K$ le K-homomorphisme défini par $e(X_{i,j}) = \delta_{i,j}$, le symbole de Kronecker. Sachant que $I_n A_\ell = A_\ell I_n$ pour $1 \le \ell \le k$, il suit de la proposition 1 que $P_1(\boldsymbol{\delta}) = 0$, $P_2(\boldsymbol{\delta}) = 0$, ... , $P_k(\boldsymbol{\delta}) = 0$ où $\boldsymbol{\delta}$ désigne le n^2-uple $(\delta_{i,j}) \in L^{n^2}$; il existe donc un K-homomorphisme $v : \frac{K[X_{i,j}, 1 \le i,j \le n]}{\mathfrak{P}_1} \to K$ tel que $v u = e$. Ainsi $v(u(D)) = \det I_n = 1$, ce qui montre que $u(D) \neq 0$.

Soit maintenant $\mathfrak{P} := P_1 A + P_2 A + \ldots, + P_r A$, on a donc $\frac{A}{\mathfrak{P}} \simeq K[Q_{s+1}, Q_{s+2}, \ldots, Q_{n^2}][u(D)^{-1}]$, cet anneau est intègre et on a $L \otimes_K \frac{A}{\mathfrak{P}} \simeq L[Q_{s+1}, Q_{s+2}, \ldots, Q_{n^2}][u(D)^{-1}]$ qui est aussi intègre.

Proposition 2.

Soient K un corps commutatif, L une clôture algébrique de K et A et $\mathfrak{P}$ comme ils ont été définis précédemment. Soit $s : A \to \frac{A}{\mathfrak{P}}$ la surjection canonique.

1. *Soient $\rho \in \mathrm{Hom}_K(A, L)$, $\theta(\rho) := [\rho(X_{i,j})]_{i,j}$* i.e. *l'élément de $M_n(L)$ dont le terme en position (i,j) est $\rho(X_{i,j})$. Alors $\theta(\rho) \in G\ell_n(L)$ et l'application $\theta : \mathrm{Hom}_K(A, L) \to G\ell_n(L)$ est bijective.*

2. *Soient $\mu \in \mathrm{Hom}_K(\frac{A}{\mathfrak{P}}, L)$, $\theta(\mu) := [\mu\, s(X_{i,j})]_{i,j}$* i.e. *l'élément de $M_n(L)$ dont le terme en position (i,j) est $\mu\, s(X_{i,j})$. Alors $\theta(\mu) \in G(L)$ (défini en 3)) et l'application $\theta : \mathrm{Hom}_K(\frac{A}{\mathfrak{P}}, L) \to G(L)$ est bijective.*

3. *L'application $\mu \mapsto \mu\, s$ est une injection de $\mathrm{Hom}_K(\frac{A}{\mathfrak{P}}, L)$ dans $\mathrm{Hom}_K(A, L)$.*

Démonstration

La partie 1. est immédiate. La partie 2. résulte de la proposition 1. La partie 3. est aussi immédiate

4.2. **Définition d'un groupe algébrique affine sur un corps commutatif K.**
Soient K un corps commutatif, L une clôture algébrique de K. Un groupe algébrique affine sur K est d'abord la donnée d'une K-algèbre B de type fini, géométriquement intègre ; cela veut dire que $L\otimes_K B$ est intègre.
Ensuite, c'est la donnée d'un K-homomorphisme $m^\sharp: B\to B\otimes_K B$, (resp. $i^\sharp: B\to B$, $e: B\to K$).
On demande en plus que les propriétés suivantes soient vérifiées.
Soit $G:=\mathrm{Hom}_K(B,L)$, on définit sur G une multiplication comme il suit. Soient $\rho_1,\rho_2\in G$ et $\rho_{1,2}: B\otimes_K B\to L$ défini par $\rho_{1,2}(a\otimes b):=\rho_1(a)\,\rho_2(b)$ et $\rho_1.\rho_2:=m^\sharp\rho_{1,2}$. Ensuite si $\rho\in G$, on définit l'inverse de ρ, que l'on note ρ^{-1} par $i^\sharp\rho$. On demande donc que G muni de la multiplication "$.$" soit un groupe dans lequel ρ^{-1} est l'inverse de ρ et e est l'élément neutre.
On peut aussi dire que si $\rho,\rho_1,\rho_2,\rho_3\in G$, on a $\rho_1.(\rho_2.\rho_3)=(\rho_1.\rho_2).\rho_3$, $\rho.\rho^{-1}=\rho^{-1}.\rho=e$ et $\rho.e=e.\rho$.

4.3. **Définition du groupe algébrique affine $G\ell_n$ sur un corps commutatif**
Soient K un corps commutatif $K[X_{i,j},1\le i,j\le n]$ l'anneau des polynômes en les n^2 variables $X_{i,j}$, $D:=D(X_{i,j}):=\det([X_{i,j}]_{i,j})$ comme il est défini en 4.1. et $A:=K[X_{i,j},1\le i,j\le n][D^{-1}]$. On sait par 4.1. que A est intègre et que $L\otimes_K A=L[X_{i,j},1\le i,j\le n][D^{-1}]$ est aussi intègre.
On définit $m^\sharp: A\to A\otimes_K A$ par $m^\sharp(X_{i,j})=\sum_{k=1}^{n} X_{i,k}\otimes X_{k,j}$. Ensuite, on définit $i^\sharp(X_{i,j}):=D^{-1}M_{i,j}$ où $M_{i,j}$ est l'élément en position (i,j) de la transposée de la comatrice de $[X_{i,j}]_{i,j}$. Enfin $e: A\to K$ est défini par $e(X_{i,j})=\delta_{i,j}$, le symbole de Kronecker.
Soit $G:=\mathrm{Hom}_K(A,L)$, nous allons montrer que l'application $\theta: G\to G\ell_n(L)$ définie à la proposition 2 partie 1. est un isomorphisme de groupe.
Soient $\rho_1,\rho_2\in G$, et soit $\rho_{1,2}: A\otimes_K A\to K$ défini par $\rho_{1,2}(a\otimes b):=\rho_1(a)\,\rho_2(b)$ et $\rho_1.\rho_2:=m^\sharp\rho_{1,2}$. Il s'agit de montrer que $\theta(\rho_1.\rho_2)=\theta(\rho_1)\theta(\rho_1)$. *On a* $\theta(\rho_1)=[a_{i,j}]_{i,j}$ avec $a_{i,j}=\rho_1(X_{i,j})$, $\theta(\rho_2)=[b_{i,j}]_{i,j}$ avec $b_{i,j}=\rho_2(X_{i,j})$, enfin $\theta(m^\sharp\rho_{1,2})=[c_{i,j}]_{i,j}$ avec

$c_{i,j}=\sum_{k=1}^{n} a_{i,k}\otimes b_{k,j}$ ce qui montre que $[c_{i,j}]_{i,j}=[a_{i,j}]_{i,j}[b_{i,j}]_{i,j}$, i.e. $\theta(\rho_1.\rho_2)=\theta(\rho_1)\theta(\rho_2)$. On montrerait de même que $\theta(\rho^{-1})=\theta(\rho)^{-1}$, et $\theta(e)=I_n$.
Ainsi l'anneau A avec $m^\sharp$, $i^\sharp$ et e définit un groupe algébrique que l'on note $G\ell_n$ et souvent appelé le *groupe algébrique linéaire*.

4.4. **Définition d'un sous-groupe algébrique irréductible de** $G\ell_n$
Soit toujours $G\ell_n$ défini par $A:=K[X_{i,j},1\le i,j\le n][D^{-1}]$, $m^\sharp$, $i^\sharp$ et e (selon 4.3.). Un sous-groupe algébrique irréductible $\mathcal{G}$ de $G\ell_n$ est défini par la donnée d'un idéal premier $\mathfrak{P}$ de A avec les propriétés qui suivent. Soit $s:A\to\frac{A}{\mathfrak{P}}$ la surjection canonique, on demande que $(s\otimes s)m^\sharp=m_1^\sharp s$, $s\ i^\sharp=i_1^\sharp s$, $e=s\,e_1$ et enfin que $L\otimes_K\frac{A}{\mathfrak{P}}$ soit intègre.
On dit alors que $\mathcal{G}$ est le *sous-groupe algébrique de* $G\ell_n$ *associé à l'idéal premier* $\mathfrak{P}$ *de* A .
Dans cette situation l'homomorphisme canonique de $\mathrm{Hom}_K(\frac{A}{\mathfrak{P}},L)$ dans $\mathrm{Hom}_K(A,L)=G\ell_n(L)$ défini par $\rho\mapsto\rho s$ est un homomorphisme injectif de groupes.

Proposition 3 *Soient* K *un corps commutatif,* L *une clôture algébrique de* K , $G\ell_n$ *le groupe algébrique linéaire associé à l'anneau* $A:=K[X_{i,j},1\le i,j\le n][D^{-1}]$ *avec* $D:=D(X_{i,j}):=\mathrm{dét}([X_{i,j}]_{i,j})$ *comme il est défini en* 4.3. *Soit* $\mathfrak{P}$ *un idéal premier de* A *tel que* $L\otimes_K\frac{A}{\mathfrak{P}}$ *soit intègre.*

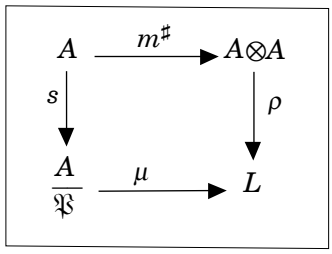
Alors les propriétés suivantes sont équivalentes.
i) Il existe un sous-groupe algébrique $\mathcal{G}$ *de* $G\ell_n$ *associé à l'idéal premier* $\mathfrak{P}$,
ii) l'image de $\mathrm{Hom}_K(\frac{A}{\mathfrak{P}},L)$ *dans* $\mathrm{Hom}_K(A,L)=G\ell_n(L)$ *est un sous-groupe de* $G\ell_n(L)$.

Démonstration
L'implication *i)* donne *ii)* est une conséquence immédiate de la définition de sous-groupe de sous-groupe algébrique de $G\ell_n$.

Montrons que ii) implique i).

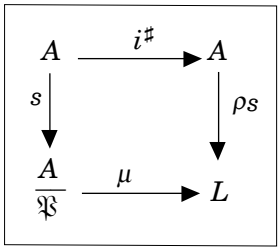
1) Soient $s : A \to \frac{A}{\mathfrak{P}}$ la surjection canonique, $\rho : \frac{A}{\mathfrak{P}} \to L$ un K-homomorphisme, alors l'application $\rho \mapsto \rho s$ est une injection de $\mathrm{Hom}_K(\frac{A}{\mathfrak{P}}, L)$ dans $\mathrm{Hom}_K(A, L) = G\ell_n(L)$.

(1) Soient $\rho_1, \rho_2 \in \mathrm{Hom}_K(\frac{A}{\mathfrak{P}}, L)$,

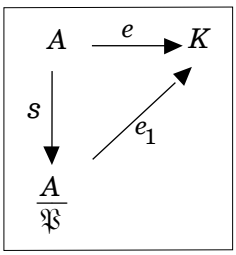


$\rho_{1,2} \in \mathrm{Hom}_K(A \otimes_K A, L)$ défini par $\rho_{1,2}(a \otimes b) := \rho_1 s(a)\, \rho_2 s(b)$. Alors le fait que le produit de $\rho_1 s$ et $\rho_2 s$ est dans l'image de $\mathrm{Hom}_K(\frac{A}{\mathfrak{P}}, L)$ dans $\mathrm{Hom}_K(A, L) = G\ell_n(L)$ se traduit par le fait qu'il existe $\mu : \frac{A}{\mathfrak{P}} \to L$ tel que $\rho_{1,2}\, m^\sharp = \mu s$

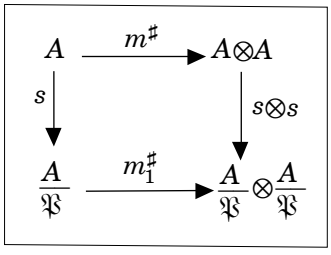
(2) Soient $\rho \in \mathrm{Hom}_K(\frac{A}{\mathfrak{P}}, L)$, alors le fait que l'inverse de ρs est dans l'image de $\mathrm{Hom}_K(\frac{A}{\mathfrak{P}}, L)$ dans $\mathrm{Hom}_K(A, L) = G\ell_n(L)$ se traduit par le fait qu'il existe $\mu : \frac{A}{\mathfrak{P}} \to L$ avec $\mu s = \rho s\, i^\sharp$.



(3) Le fait que l'élément neutre e de $\mathrm{Hom}_K(A, L) = G\ell_n(L)$ est dans l'image de $\mathrm{Hom}_K(\frac{A}{\mathfrak{P}}, L)$ dans $\mathrm{Hom}_K(A, L) = G\ell_n(L)$ se traduit par le fait qu'il existe $e_1 : \frac{A}{\mathfrak{P}} \to L$ avec $e_1 s = e$; on rappelle que e est défini par $e(X_{i,j}) := \delta_{i,j}$.



2) *Il nous faut d'abord montrer qu'il existe un homomorphisme* $m_1^\sharp : \frac{A}{\mathfrak{P}} \to \frac{A}{\mathfrak{P}} \otimes_K \frac{A}{\mathfrak{P}}$, *tel que* $(s \otimes s) m^\sharp = m_1^\sharp s$.



Pour cela le pas essentiel est l'égalité qui suit. Soit $u := (s \otimes s) m^\sharp$, montrons que

(4) $\{u^{-1}(\mathfrak{M}) \mid \mathfrak{M}$ est un idéal maximal de $\frac{A}{\mathfrak{P}}\otimes_K\frac{A}{\mathfrak{P}}\} =$

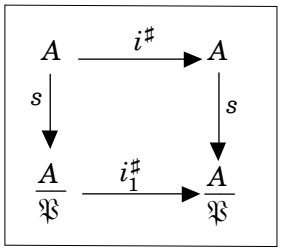
$\{\mathfrak{M}' \mid \mathfrak{M}'$ est un idéal maximal de A avec $\mathfrak{M}'\supset\mathfrak{P}\}$.

Soit $\mathfrak{M}$ un idéal maximal de $\frac{A}{\mathfrak{P}}\otimes_K\frac{A}{\mathfrak{P}}$, il existe donc un K-homomorphisme $\rho_1:\frac{A}{\mathfrak{P}}\otimes_K\frac{A}{\mathfrak{P}}\to L$ avec $\ker\rho_1=\mathfrak{M}$. Soit $\rho:=\rho_1(s\otimes s)$ et $a_{i,j}:=\rho(X_{i,j}\otimes 1)$, $b_{i,j}:=\rho(1\otimes X_{i,j})$. On a donc $\rho\, m^\sharp(X_{i,j})=c_{i,j}$ avec $c_{i,j}=\sum_{k=1}^{n}a_{i,k}\otimes b_{k,j}$ ce qui veut dire que $[c_{i,j}]_{i,j}=[a_{i,j}]_{i,j}[b_{i,j}]_{i,j}$. Il suit de (1) qu'il existe $\mu:\frac{A}{\mathfrak{P}}\to L$ tel que $\rho\, m^\sharp=\mu\, s$. Comme $\mu\, s(\mathfrak{P})=0$, on a $\rho\, m^\sharp(\mathfrak{P})=0$ et donc $\rho_1(s\otimes s)\, m^\sharp(\mathfrak{P})=0$, i.e. $\rho_1(u(\mathfrak{P}))=0$, ainsi $u(\mathfrak{P})\subset\mathfrak{M}$. Cela veut bien dire que $u^{-1}(\mathfrak{M})$ est un idéal maximal de A avec $u^{-1}(\mathfrak{M})\supset\mathfrak{P}$.

Soit maintenant $\mathfrak{M}'$ un idéal maximal de A avec $\mathfrak{M}'\supset\mathfrak{P}$, il faut montrer qu'il existe un idéal maximal $\mathfrak{M}$ de $\frac{A}{\mathfrak{P}}\otimes_K\frac{A}{\mathfrak{P}}$ tel que $u^{-1}(\mathfrak{M})=\mathfrak{M}'$. On a donc $s(\mathfrak{M}')$ qui est un idéal maximal de $\frac{A}{\mathfrak{P}}$, ainsi il existe $\rho_1:\frac{A}{\mathfrak{P}}\to L$ tel que $\ker\rho_1=s(\mathfrak{M}')$. Soit $e:A\to L$ défini par $e(X_{i,j}):=\delta_{i,j}$, il suit de (3) qu'il existe $e_1:\frac{A}{\mathfrak{P}}\to L$ avec $e_1 s=e$. Soit $\psi:\frac{A}{\mathfrak{P}}\otimes_K\frac{A}{\mathfrak{P}}\to L$ défini par $\psi(a\otimes b)=\rho_1(a)\, e_1(b)$. On a donc $\psi(s\otimes s)(X_{i,j}\otimes 1)=\rho_1 s(X_{i,j})=:a_{i,j}$, $\psi(s\otimes s)(1\otimes X_{i,j})=\delta_{i,j}$. Par ailleurs $\psi(s\otimes s)m^\sharp(X_{i,j})=:c_{i,j}$ avec $[c_{i,j}]_{i,j}=[a_{i,j}]_{i,j}[\delta_{i,j}]_{i,j}=[a_{i,j}]_{i,j}I_n=[a_{i,j}]_{i,j}$. En conséquence $\psi(s\otimes s)m^\sharp(X_{i,j})=\rho_1 s(X_{i,j})$, i.e. $\psi u=\rho_1 s$. Soit $\mathfrak{M}:=\ker\psi$, on a donc $u^{-1}(\mathfrak{M})=\mathfrak{M}'$.
Il suit que (4) est vérifié.
Comme A est une K-algèbre de type fini, comme $\mathfrak{P}$ est un idéal premier, on sait que $\mathfrak{P}$ est l'intersection de tous les idéaux maximaux de A qui contiennent $\mathfrak{P}$ ([F] corollaire 6.5.3.2, p. 236) . Comme $L\otimes_K\frac{A}{\mathfrak{P}}$ est intègre, on sait que $\frac{A}{\mathfrak{P}}\otimes_K\frac{A}{\mathfrak{P}}$ est intègre ([Bki] corollaire 3, AV.137) , ainsi $\{0\}$ est l'intersection de tous les idéaux maximaux de $\frac{A}{\mathfrak{P}}\otimes_K\frac{A}{\mathfrak{P}}$ ([F] corollaire

6.5.3.2, p. 236). Il suit alors de (4) que $u(\mathfrak{P})=\{0\}$, ce qui montre l'existence de $m_1^\sharp:\frac{A}{\mathfrak{P}}\to\frac{A}{\mathfrak{P}}\otimes_K\frac{A}{\mathfrak{P}}$, avec $(s\otimes s)m^\sharp=m_1^\sharp s$.

3) *Il faut montrer qu'il existe un K-homomorphisme* $i_1^\sharp:\frac{A}{\mathfrak{P}}\to\frac{A}{\mathfrak{P}}$ *tel que* $s\ i^\sharp=i_1^\sharp s$.

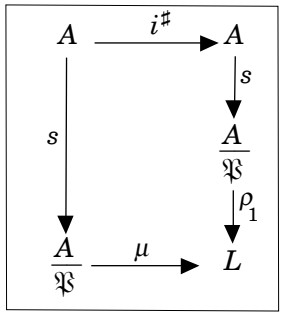


Pour cela, le pas essentiel est l'égalité qui suit. Soit $u:=s\ i^\sharp$, montrons que

(5) $\{u^{-1}(\mathfrak{M})\mid \mathfrak{M}$ est un idéal maximal de $\frac{A}{\mathfrak{P}}\}=$

$\{\mathfrak{M}'\mid \mathfrak{M}'$ est un idéal maximal de A avec $\mathfrak{M}'\supset\mathfrak{P}\}$.

Soient $\mathfrak{M}$ est un idéal maximal de $\frac{A}{\mathfrak{P}}$, $\rho_1:\frac{A}{\mathfrak{P}}\to L$ tel que $\rho_1(\mathfrak{M})=\{0\}$. Soit $\rho:=\rho_1 s$, alors il suit de (2) qu'il existe $\mu:\frac{A}{\mathfrak{P}}\to L$ tel que $\mu\ s=\rho_1(s\ i^\sharp)=\rho_1 u$. Comme $\mu\ s(\mathfrak{P})=\{0\}$, on a $\rho_1 u(\mathfrak{P})=\{0\}$, i.e. $u(\mathfrak{P})\subset\mathfrak{M}$, ainsi $u^{-1}(\mathfrak{M})\supset\mathfrak{P}$.



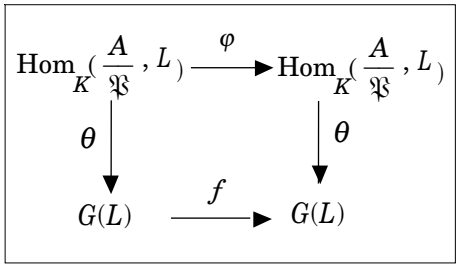
Soit $\mathfrak{M}'$ un idéal maximal de A avec $\mathfrak{M}'\supset\mathfrak{P}$, ainsi $s(\mathfrak{M}')$ est un idéal maximal de $\frac{A}{\mathfrak{P}}$. Soit $\rho_1:\frac{A}{\mathfrak{P}}\to L$ tel que $\rho_1(s(\mathfrak{M}'))=\{0\}$. Alors par (2) il existe $\mu:\frac{A}{\mathfrak{P}}\to L$ tel que $\mu\ s=\rho_1(s\ i^\sharp)=\rho_1 u$. Comme $\mu\ s(\mathfrak{P})=\{0\}$, on a $\rho_1 u(\mathfrak{P})=\{0\}$ et donc $u(\mathfrak{P})\subset s(\mathfrak{M}')$, soit $s\ i^\sharp(\mathfrak{P})\subset s(\mathfrak{M}')$ et donc $i^\sharp(\mathfrak{P})\subset\mathfrak{M}'$, sachant que $\mathfrak{P}\subset\mathfrak{M}'$. Comme l'intersection de tous les idéaux maximaux contenant $\mathfrak{P}$ est égal à $\mathfrak{P}$ ([F] corollaire 6.5.3.2, p. 236) , il suit que $i^\sharp(\mathfrak{P})\subset\mathfrak{P}$. Et comme $(i^\sharp)^2=\mathrm{Id}$, on a $i^\sharp(\mathfrak{P})=\mathfrak{P}$. Il suit facilement de cela que $u^{-1}(u(\mathfrak{M}'))=\mathfrak{M}'$. Cela montre (5) .

En conséquence $u(\mathfrak{P})=\{0\}$, ainsi il existe $i_1^\sharp:\frac{A}{\mathfrak{P}}\to\frac{A}{\mathfrak{P}}$ tel que $s\ i^\sharp=i_1^\sharp s$.

4.5. **Théorème de Lang** (version sous-groupe algébrique affine de $G\ell_n$, [L] , [B] 16.4 Corollary p. 211, [Ser] proposition 3, p. 119)
Soient $K=\mathbb{F}_q$ *le corps à* $q=p^\alpha$ *éléments où* p *est un nombre premier,* L *une clôture algébrique de* $\mathbb{F}_q$.
Soient $A:=K[X_{i,j},1\le i,j\le n][D^{-1}]$ *et* $G\ell_n$ *le groupe algébrique linéaire associé à* $(A,m^\sharp,i^\sharp,e)$ *selon* 4.3.
Soient $\mathfrak{P}$ *un idéal premier de* A *tel que* $L\otimes_K\frac{A}{\mathfrak{P}}$ *soit intègre. On suppose qu'il existe un sous–groupe algébrique* $\mathcal{G}$ *de* $G\ell_n$ *associé à* $\mathfrak{P}$ *selon* 4.4.
Soit $F_1^\sharp:A\to A$ *le K-homomorphisme défini par* $F_1^\sharp(x):=x^q$; comme $F_1^\sharp(\mathfrak{P})\subset\mathfrak{P}$, *il induit un K-homomorphisme* $F^\sharp:\frac{A}{\mathfrak{P}}\to\frac{A}{\mathfrak{P}}$. *Par ailleurs* $F^\sharp$ *induit une application* $F:\mathrm{Hom}_K(\frac{A}{\mathfrak{P}},L)\to\mathrm{Hom}_K(\frac{A}{\mathfrak{P}},L)$ *définie par* $F(\rho):=\rho F^\sharp$.
Soit $\varphi:\mathrm{Hom}_K(\frac{A}{\mathfrak{P}},L)\to\mathrm{Hom}_K(\frac{A}{\mathfrak{P}},L)$ *l'application définie par*
$\varphi(\rho):=\rho^{-1}.F(\rho)$ *où* $"."$ *et* ρ^{-1} sont définis en 4.2.
Alors l'application φ *est surjective.*

La démonstration de ce théorème nécessite la connaissance des variétés algébriques avec des résultats élémentaires ou pas.

4.6. **Application du théorème de Lang.**
Soient toujours $K=\mathbb{F}_q$, le corps à $q=p^\alpha$ éléments où p est un nombre premier, L une clôture algébrique de $\mathbb{F}_q$. Soit $\mathfrak{P}$ l'idéal premier de A défini en 4.1. On sait que l'image injective de $\mathrm{Hom}_K(\frac{A}{\mathfrak{P}},L)$ dans $G\ell_n(L)$ est le sous-groupe $G(L)$ (proposition 2, partie 2), il suit alors de la proposition 3 qu'il existe un sous-groupe algébrique $\mathcal{G}$ de $G\ell_n$ associé à $\mathfrak{P}$ selon 4.4. On peut donc appliquer de théorème de Lang à $\mathcal{G}$. Ainsi la bijection $\theta:\mathrm{Hom}_K(\frac{A}{\mathfrak{P}},L)\to G(L)$



est un isomorphisme de groupe (4.4), on a facilement $f\theta=\theta\varphi$ et comme φ est surjectif, il suit que l'application f est surjective.

Bibliographie

[Bor] Borel A. *Linear Algebraic Groups* Graduate Texts in Mathematics 126, 1991 Springer
[Bou] Bourbaki N. *Algèbre* ch. 4 à 7, 1981 Masson
[F] Fresnel J. *Anneaux* Hermann 2001
[F.M.] Fresnel J & Matignon M. *Algèbre et Géométrie 81 thèmes pour l'Agrégation, 2017,* Ellipses
[La] Lang S. *Algebraic groups over finite fields* Amer. Jour. Math. 87 (1965) 555-563
[Le] Le Bruyn, Lieven (B-ANTW) *Orbits of matrix tuples. Algèbre non commutative, groupes quantiques* (Reims, 1995) 245-261 Sémin. Congr., 2 Soc. Math. France Paris 1997
[Seg] de Seguins Pazzis C. *Invariance of simultaneous similarity and equivalence of matrices under extension of ground field (en accès libre)* Linear Algebra Appl. 433-3 (2010) 618-624.
[Ser] Serre J.-P.. *Groupes algébriques et corps de classes* Hermann 1959 (2010) 618-624.