19/03/2021 Jean Fresnel et Michel Matignon

Similitude simultanée et extensions de corps avec un théorème de Lang sur les groupes algébriques sur les corps finis

0 Introduction

Le problème de la similitude simultanée et de l'extension de corps peut s'exprimer comme il suit.
Soient $K \subset L$ *deux corps commutatifs,* $M_n(K)$ *la* K*-algèbre des matrices à* n *lignes et* n *colonnes à coefficients dans* K*. Soient* $(A_1, A_2, \dots, A_s) \in M_n(K)^s$, $(B_1, B_2, \dots, B_s) \in M_n(K)^s$*. On suppose qu'il existe* $P \in G\ell_n(L)$, i.e. *une matrice inversible à* n *lignes et* n *colonnes à coefficients dans* L*, telle que* $PA_\ell P^{-1} = B_\ell$ *pour* $1 \leq \ell \leq s$.
Existe-t-il $Q \in G\ell_n(K)$*, tel que* $QA_\ell Q^{-1} = B_\ell$ *pour* $1 \leq \ell \leq s$?

C'est la question posée par de Seguin Pazzis en 2009 (Q 648, RMS 119-3).
La réponse positive admet une démonstration élémentaire si le corps K est infini, ou tout au moins s'il possède assez d'éléments.

La réponse à la question est toujours oui. En 2010 [Se1] de Seguin Pazzis a publié une démonstration de cela qui est valable pour tous les corps commutatifs, en particulier pour les corps finis. Il utilise essentiellement un résultat de Kronecker-Weierstrass qui caractérise un système de représentants des couples de matrices $(A, B) \in M_{n,m}(K)^2$ sous l'action de l'équivalence simultanée ; de façon simple (A', B') est équivalent à (A, B) s'il existe $P \in G\ell_n(K)$, $Q \in G\ell_m(K)$ et $A' = PAQ^{-1}$, $B' = PBQ^{-1}$.
Toutefois la démonstration de Kronecker-Weierstrass concernait la situation où $K = \mathbb{R}, \mathbb{C}$. Dans son article, de Seguin Pazzis donne brièvement une démonstration de la réduction de Kronecker-Weierstrass qui fonctionne pour tous les corps commutatifs.

Curieusement, la RMS a continué à éditer cette même question. C'est encore de Seguin Pazzis qui y a répondu en 2020 en disant que le problème de la similitude simultanée et de l'extension de corps n'est autre chose qu'un lemme de Noether-Deuring. Ce lemme a l'énoncé suivant.

Soient $K \subset L$ deux corps commutatifs, $\mathcal{A}$ (resp. $\mathcal{B}$) *une sous-K-algèbre unitaire de $M_n(K)$. On suppose qu'il existe $P \in G\ell_n(L)$ tel que $A \mapsto PAP^{-1}$ soit un isomorphisme de $\mathcal{A}$ sur $\mathcal{B}$.*
Alors il existe $Q \in G\ell_n(K)$ tel que $A \mapsto QAQ^{-1}$ soit un isomorphisme de $\mathcal{A}$ sur $\mathcal{B}$.

A cette même époque, on avait suggéré une solution utilisant un théorème de Lang sur les groupes algébriques sur les corps finis [La1] .
Ici, on reprend cette idée sachant que l'on démontre de façon presque élémentaire le théorème de Lang adapté à cette situation.

1. Similitude simultanée et extensions de corps

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 $1 \leq \ell \leq s$. On suppose qu'il existe $P \in G\ell_n(L)$ tel que $PA_\ell P^{-1} = B_\ell$ pour $1 \leq \ell \leq s$.
Alors il existe $Q \in G\ell_n(K)$ tel que $QA_\ell Q^{-1} = B_\ell$ pour $1 \leq \ell \leq s$.

Démonstration

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 $P_1, P_2, \ldots, P_m \in M_n(K)$ avec
$P = P_1 e_1 + P_2 e_2 + \ldots + P_m e_m$.
De la relation $PA_\ell = B_\ell P$, il suit que $P_i A_\ell = B_\ell P_i$ pour $1 \leq \ell \leq s$ et $1 \leq i \leq m$.
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 $S(\mu_1, \mu_2, \ldots, \mu_m) \neq 0$ ([Fre] 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 $1 \leq \ell \leq s$.

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 $P_1A_\ell P_1{}^{-1}=B_\ell$ pour $1\le\ell\le s$.
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 $1\le\ell\le s$. Sachant que K_1 est infini, la démonstration utilisée en 1) montre qu'il existe $Q\in G\ell_n(K_1)$ tel que $QA_\ell Q^{-1}=B_\ell$ pour $1\le\ell\le s$.

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* $1\le\ell\le s$ *avec* $P\in G\ell_n(L)$ *tel que* $PA_\ell P^{-1}=B_\ell$ *pour* $1\le\ell\le s$.

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 $1\le\ell\le s$. 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 $1\le\ell\le s\}$, 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 sait par le théorème de Lang ci-après 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 $1\le\ell\le s$ on a

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

Il suit que $QA_\ell Q^{-1}=B_\ell$ pour $1\le\ell\le s$ et $Q\in G\ell_n(K)$.

3. Un cas particulier du théorème de Lang sur les groupes algébriques

Théorème de Lang (cas particulier, [La1], [Bor] p. 211, [Ser] p. 118)
Soient p un nombre premier $q=p^\alpha$ avec $\alpha\geq 1$, $\mathbb{F}_q$ le corps à q éléments, L une clôture algébrique de $\mathbb{F}_q$ et $A_\ell\in M_n(\mathbb{F}_q)$ pour $1\leq\ell\leq k$.
Soit F l'automorphisme de L défini par $F(x):=x^q$. On note aussi $F:M_n(L)\to M_n(L)$ l'automorphisme d'anneau défini par $F([m_{i,j}]):=[F(m_{i,j})]$.
Soient $G(L):=\{\,U\in G\ell_n(L)\mid UA_\ell=A_\ell U \text{ pour } 1\leq\ell\leq s\,\}$, c'est un sous-groupe de $G\ell_n(L)$. Soit $f:G(L)\to G(L)$ l'application définie par $f(U):=U^{-1}F(U)$.
Alors l'application f est surjective.

Démonstration

3.1) **Construction de l'idéal premier $\mathfrak{P}$.**
Soient $X_0, X_{i,j}$ pour $1\leq i,j\leq n$, $1+n^2$ variables sur L et notons $L[X_0, X_{i,j}\mid 1\leq i,j\leq n]$ l'anneau des polynômes sur L en ces variables.
La lecture des relations matricielles $[X_{i,j}]_{i,j}A_\ell - A_\ell[X_{i,j}]_{i,j}=0$ pour $1\leq\ell\leq s$, en chaque position (i,j) définissent $n^2\times s$ polynômes $P_{i,j,\ell}$ qui sont homogènes de degré 1 ou nuls.
Soit $\mathfrak{P}$ l'idéal de $L[X_0, X_{i,j}\mid 1\leq i,j\leq n]$ engendré par $X_0\,\text{dét}([X_{i,j}]_{i,j})-1$ et les $n^2\times s$ polynômes $P_{i,j,\ell}$. Assez facilement $\mathfrak{P}$ est un idéal premier.
Soient $A:=\dfrac{L[X_0, X_{i,j}\mid 1\leq i,j\leq n]}{\mathfrak{P}}$ et x_0 (resp. $x_{i,j}$) l'image de X_0 (resp. $X_{i,j}$) dans l'anneau intègre A.

3.2) **La construction de $g_Y:A\to A$**
Soient $Y\in G\ell_n(L)$, $\text{Fr}(A)$ le corps des fractions de A et
(1) $\quad [x'_{i,j}]:=[x_{i,j}]^{-1}Y[F(x_{i,j})]\in M_n(\text{Fr}(A))$.
Montrons que $[x'_{i,j}]\in M_n(A)$. En effet, on a $x_0\,\text{dét}[x_{i,j}]=1$ et donc
(2) $\quad [x_{i,j}]^{-1}=x_0[\Delta(x_{i,j})]$
où $\Delta(x_{i,j})$ est le coefficient en position (i,j) de la transposée de la comatrice de $[x_{i,j}]_{i,j}$, ainsi $[x'_{i,j}]\in M_n(A)$.
(3) Soit $x'_0:=F(x_0)\dfrac{1}{\text{dét}\,Y}\,\text{dét}[x_{i,j}]\in A^\times$,
Ensuite il suit de (1), de $x_0\,\text{dét}[x_{i,j}]=1$ et de $\text{dét}\,Y\in L^\times$ que

(4) $\qquad x'_0 \det[x'_{i,j}] - 1 = 0$

Par ailleurs, sachant que $[x_{i,j}]A_\ell - A_\ell[x_{i,j}] = 0$, que $F(A_\ell) = A_\ell$ pour $1 \le \ell \le s$, il suit que

(5) $\qquad [x'_{i,j}]A_\ell - A_\ell[x'_{i,j}] = 0$ pour $1 \le \ell \le s$.

Soit $\theta : L[X_0, X_{i,j} \mid 1 \le i,j \le n] \to A$ défini par $\theta(X_0) := x'_0$ et $\theta(X_{i,j}) := x'_{i,j}$.

Il suit facilement de (4) et (5) que $\mathfrak{P} \subset \ker\theta$, ainsi θ induit un homomorphisme $g_Y : A \to A$ et comme $g_Y(A)$ est intègre, il suit que $\ker g_Y$ est un idéal premier de A .

3.3) **Montrons que** $\ker g_Y = \{0\}$

Soient $G := \mathrm{Frac}(g_Y(A))$ et $E := \mathrm{Frac(A)}$, montrons que $E^q G = E$.

On a $E = \mathrm{Frac(A)} = L(x_{i,j} \mid 1 \le i,j \le n)$ parce que $x_0 = \dfrac{1}{\det[x_{i,j}]}$,

$G = \mathrm{Frac}(g_Y(A)) = L(x'_{i,j} \mid 1 \le i,j \le n)$ parce que $x'_0 = \dfrac{1}{\det[x'_{i,j}]}$.

On a $E^q = L((x_{i,j})^q \mid 1 \le i,j \le n)$, alors $E^q G = L((x_{i,j})^q,\ x'_{i,j} \mid 1 \le i,j \le n)$.

Comme $[x'_{i,j}] := [x_{i,j}]^{-1} Y[(x_{i,j})^q]$, on a $E^q G = E$.

Il suit alors du corollaire de la proposition 1 ci-après que E est algébrique fini sur G . Cela montre que $\dim A = \dim g_Y(A)$ (la dimension de Krull) ; ainsi $\ker g_Y = \{0\}$.

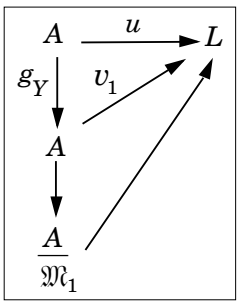
3.4) **Montrons que** $f_Y(\mathrm{Spm}(A)) \cap f_{I_n}(\mathrm{Spm}(A)) \neq \emptyset$

En effet $\mathrm{Spm}(A)$ désigne l'espace topologique constitué des idéaux maximaux de A et $f_Y(\mathfrak{M}) := {g_Y}^{-1}(\mathfrak{M}) \in \mathrm{Spm}(A)$. Il suit de la proposition 2, ci-après qu'il existe $a \in A - \{0\}$ tel que $f_Y(\mathrm{Spm}(A)) \supset D(a)$ où $D(a) := \{\mathfrak{M} \in \mathrm{Spm}(A) \mid a \notin \mathfrak{M}\}$ et que $D(a) \neq \emptyset$.

Si on remplace Y par I_n , et donc g_Y (resp. f_Y) par g_{I_n} (resp. f_{I_n}) on montre aussi qu'il existe $b \in A - \{0\}$ tel que $f_{I_n}(\mathrm{Spm}(A)) \supset D(b)$ où $D(b) := \{\mathfrak{M} \in \mathrm{Spm}(A) \mid b \notin \mathfrak{M}\}$.

En résumé $f_Y(\mathrm{Spm}(A)) \supset D(ab)$ et $f_{I_n}(\mathrm{Spm}(A)) \supset D(ab)$ et comme $ab \neq 0$, on a $D(ab) \neq \emptyset$ ([Fre] corollaire 6.5.3.2). Ce qui est 3.4).

3.5) **La conclusion**



Soit $\mathfrak{M}\in D(a\,b)$, on a donc $\mathfrak{M}=f_Y(\mathfrak{M}_1)$ avec $\mathfrak{M}_1\in \mathrm{Spm}(A)$, i.e. $\mathfrak{M}=g_Y^{-1}(\mathfrak{M}_1)$.
Soit $u:A\to L$ un L-homomorphisme avec $\ker u=\mathfrak{M}$, alors il existe un L-homomorphisme $v_1:A\to L$ tel que $\ker v_1=\mathfrak{M}_1$ et que $u=v_1 g_Y$.
Soient $U:=[u(x_{i,j})]$ et $V_1:=[v_1(x_{i,j})]$, alors $U,V_1\in G(L)$.
Par ailleurs, il suit de la relation $u=v_1 g_Y$ que $U=V_1^{-1}YF(V_1)$.
De la même façon, en remplaçant Y par I_n , on a donc $\mathfrak{M}=f_{I_n}(\mathfrak{M}_2)$ avec $\mathfrak{M}_2\in \mathrm{Spm}(A)$, i.e. $\mathfrak{M}=g_{I_n}^{-1}(\mathfrak{M}_2)$. On déduit donc qu'il existe $V_2\in G(L)$ avec $U=V_2^{-1}I_nF(V_2)$.
Il suit alors de l'égalité $V_1^{-1}YF(V_1)=V_2^{-1}I_nF(V_2)$ que $Y=(V_2V_1^{-1})^{-1}F(V_2V_1^{-1})$. Ainsi pour tout $Y\in G(L)$ il existe $Z\in G(L)$ avec $f(Z)=Y$. Ce qui est le théorème.

Proposition 1 *Soient $G\subset E$ deux corps commutatifs avec $\mathrm{car}\,E=p$ un nombre premier. On suppose que E est de type fini sur G ,* i.e. *$E=G(x_1,x_2,\dots,x_s)$ et qu'il existe un entier $m\geq 1$ avec $E^qG=E$ où $q:=p^m$.*
Alors E est algébrique fini sur G .

Démonstration
1) *Soient $G\subset F\subset E$ trois corps commutatifs, on suppose que E est de type fini sur G , que E est algébrique sur F , donc fini sur F et que $\mathrm{car}\,E=p$ un nombre premier. Soit $m\geq 0$ un entier. Alors on a $[E^qG:F^qG]\leq [E:F]$.*
Comme $x\mapsto x^q$ est un homomorphisme injectif de E dans E , il suit que $[E^q:F^q]=[E:F]$. On a donc
(1) $\quad E^q=F^qe_1\oplus F^qe_2\oplus\dots\oplus F^qe_r$ avec $r=[E:F]$.
Il suit facilement que
(2) $\quad E^qG=F^qGe_1+F^qGe_2+\dots+F^qGe_r$,
ainsi
(3) $\quad [E^qG:F^qG]\leq r=[E:F]$.

2) *Soient* G *et* E *qui satisfont les hypothèses de la proposition 1.*
On souhaite montrer que E est algébrique sur G.
Supposons le contraire, on a donc $\dim_{alg}(E/G)=s\geq 1$. On a donc une famille $(t_1,t_2,\dots,t_s)$ de E qui est algébriquement libre sur G , i.e. $G(t_1,t_2,\dots,t_s)$ s'identifie au corps des fractions rationnelles sur G à s variables et de plus E est fini sur $G(t_1,t_2,\dots,t_s)$.
Facilement

(4) $$(G(t_1,t_2,\dots,t_s))^qG=G(t_1^q,\ t_2^q,\dots,t_s^q)$$

et

(5) $$[\ G(t_1,t_2,\dots,t_s):G(t_1^q,\ t_2^q,\dots,t_s^q)]=q^s\ .$$

Il suit de 1) avec $F:=G(t_1,t_2,\dots,t_s)$ que

(6) $$[E^qG:(G(t_1,t_2,\dots,t_s))^qG]\leq [E:G(t_1,t_2,\dots,t_s)]\ .$$

Compte tenu de $E^qG=E$, et de (4) , la formule (6) devient

(7) $$[E:G(t_1^q,\ t_2^q,\dots,t_s^q)]\leq [E:G(t_1,t_2,\dots,t_s)]\ .$$

Enfin

(8) $$[E:G(t_1^q,\ t_2^q,\dots,t_s^q)]=$$
$$[E:G(t_1,t_2,\dots,t_s)][G(t_1,t_2,\dots,t_s):G(t_1^q,\ t_2^q,\dots,t_s^q)].$$

Enfin compte tenu de (5) , (8) est en contradition avec (7).
Ce qui veut dire que seule l'hypothèse E est algébrique sur G est à retenir.

Remarque On pourrait ajouter que E est séparable sur G . La proposition 1 se trouve essentiellement dans [La2] proposition 4.9, p. 366.

Proposition 2 *Soient* K *un corps commutatif,* A *une* K*-algèbre de type fini qui est un anneau intègre,* $g:A\to A$ *un* K*-homomorphisme injectif. On suppose que* $\mathrm{Fr(A)}$ *est algébrique fini sur* $\mathrm{Fr(g(A))}$ *. Soient* $\mathrm{Spm}(A)$ *l'espace topologique constitué des idéaux maximaux de* A *,* $f:\mathrm{Spm}(A)\to \mathrm{Spm}(A)$ *l'application continue définie par* $f(\mathfrak{M}):=g^{-1}(\mathfrak{M})$ *. Alors il existe* $a\in A-\{0\}$ *tel que* $D(a)\subset f(\mathrm{Spm}(A))$ *où* $D(a):=\{\mathfrak{M}\in\mathrm{Spm}(A)\mid a\notin\mathfrak{M}\}$ *est l'ouvert principal associé à* a *et on a* $D(a)\neq\emptyset$ ([Fre] corollaire 6.5.3.2).

Démonstration
On a donc $A=K[t_1,t_2,\dots,t_r]=g(A)[t_1,t_2,\dots,t_r]$ et t_i est racine d'un polynôme de la forme $b_{0,i}+b_{1,i}X+\dots+b_{s_i,i}X^{s_i}$, avec $b_{k,i}\in g(A)$ et $b_{s_i,i}\neq 0$. Soit $b:=b_{s_1,1}b_{s_2,2}\dots b_{s_r,r}$, on a donc $b=g(a)$ avec $a\in A$. Il suit donc que $A[\frac{1}{a}]$ est entier sur $g(A[\frac{1}{a}])$. Si donc $\mathfrak{M}$ est un maximal de $A[\frac{1}{a}]$, i.e. un élément de $D(a)$, alors $g(\mathfrak{M})$ est un maximal de $g(A[\frac{1}{a}])$ et il existe un maximal $\mathfrak{M}_1$ de $A[\frac{1}{a}]$ avec $\mathfrak{M}_1\cap g(A[\frac{1}{a}])=g(\mathfrak{M})$ ([Fre] théorème 8.2.4). Cela montre bien que $D(a)\subset f(\mathrm{Spm}(A))$.

Remarque La proposition 2 est un cas particulièrement simple d'un théorème de Chevalley qui décrit l'image d'un morphisme de variétés algébriques ([Har] 3.19 p. 94)

Bibliographie

[Bor] Borel A. *Linear Algebraic Groups* Graduate Texts in Mathematics 126, 1991 Springer
[Fre] Fresnel J. *Anneaux* Hermann 2001
[Har] Hartshorne R. *Algebraic geometry* Springer Verlag 1977
[La 1] Lang S. *Algebraic groups over finite fields* Amer. Jour. Math. 87 (1965) 555-563
[La 2] Lang S. *Algebra* Addison-Wesley Publishing Company 1993
[Seg1] 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.
[Seg2] de Seguins Pazzis C. *R648 Similitude simultanée et extension de corps,* RMS n° 130-3 avril 2020, p. 198
[Ser] Serre J.-P. *Groupes algébriques et corps de classes* Hermann 1959.