



**HAL**  
open science

## Linear Algebra over a division ring

Cédric Milliet

► **To cite this version:**

| Cédric Milliet. Linear Algebra over a division ring. 2016. hal-01283071v4

**HAL Id: hal-01283071**

**<https://hal.science/hal-01283071v4>**

Preprint submitted on 14 Aug 2016 (v4), last revised 2 Jun 2020 (v7)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# GÉOMÉTRIE ALGÈBRIQUE ÉLÉMENTAIRE AU-DESSUS D'UN CORPS NON COMMUTATIF

CÉDRIC MILLIET

RÉSUMÉ. On considère un analogue de la topologie de Zariski sur un corps non commutatif  $K$ . Un fermé de base est donné par les zéros d'un polynôme en la conjugaison par un élément de  $K$  fixé à coefficients à droite dans  $K$ . Cela nous permet de développer des notions de géométrie algébrique élémentaire : variété algébrique affine, morphisme, comorphisme, une dimension de Zariski, un théorème de Chevalley pour les ensembles constructibles et un Nullstellensatz. On applique ces résultats à la théorie des modèles des corps non commutatifs, en considérant un corps non commutatif  $K$  dont la théorie dans le langage  $(+, \times, 0, 1)$  n'a pas la propriété d'indépendance de Shelah. Si  $K$  est de caractéristique  $p$ , on montre qu'il est de dimension finie sur son centre.

L'histoire des corps non commutatifs commence en 1843 avec la découverte du corps des quaternions (voir [Ham50]). Le premier exemple de corps non commutatif de dimension infinie sur son centre est donné en 1903 : le corps des séries de Laurent  $F((x, \sigma))$  à coefficients dans  $F = \mathbf{R}(t)$ , muni de la multiplication « tordue » par la règle  $ax = x\sigma(a)$ , où  $\sigma$  est l'automorphisme  $t \mapsto 2t$  (voir [Hil03]).

En géométrie algébrique classique, on étudie les solutions d'un système  $\mathcal{S}$  d'équations polynomiales en  $n$  variables  $x_1, \dots, x_n$  à coefficients dans un corps commutatif  $k$ . On recherche les solutions de  $\mathcal{S}$  dans  $k^n$ , ou plus souvent dans  $\mathbf{k}^n$ , pour une clôture algébrique  $\mathbf{k}$ . Si l'on autorise le corps  $k$  à être non commutatif, des problèmes élémentaires surgissent, à commencer par savoir ce que l'on entend par *polynôme en  $n$  variables*. Dans un tel corps, le nombre de racines d'un polynôme

$$p(x) = a_d + a_{d-1}x + \dots + a_0x^d$$

de degré  $d$  en une variable à coefficients à gauche dans  $k$  est soit inférieur ou égal à  $d$  soit infini (voir [Her56]). Les racines de  $p$  se répartissent en  $d$  classes de conjugaison, au plus (voir [GM65]). Le corps  $k$  est *algébriquement clos (à droite)* si chaque polynôme  $p$  non constant a une racine dans  $k$ . Les corps algébriquement clos non commutatifs de dimension finie sur leur centre sont les corps de quaternions dont le centre est un corps réel clos (voir [Niv41] et [NE44]). Chaque corps se plonge dans un corps algébriquement clos de même centre (voir [Coh95, Theorem 8.5.1]). Si l'on veut considérer des polynômes en deux variables et évaluer chaque variable, il faut bien s'autoriser à considérer des monômes en une variable de la forme  $axb$ , et plus généralement de la forme  $a_0xa_1 \dots xa_d$ . Dans ce cas, l'équation linéaire la plus

---

2010 *Mathematics Subject Classification*. 14R99, 14A22, 12E15, 03C45, 03C60.

*Key words and phrases*. Corps non commutatifs, géométrie algébrique, théorie des modèles, propriété d'indépendance.

Un grand merci à Franziska Jahnke, ainsi qu'à la communauté Mathoverflow <http://mathoverflow.net/> pour un riche échange d'idées, de questions et de réponses.

simple

$$ax - xb = c$$

peut n'avoir de solutions dans aucune extension de  $k$  (voir [Coh95, Theorem 8.1.3]). À l'autre extrême, il existe un corps non commutatif  $k$  tel que toute équation polynomiale en une variable à coefficients dans  $k$

$$a_0 + (a_{101}xa_{111} + \cdots + a_{10n}xa_{11n}) + \cdots + (a_{d01}x \dots xa_{dd1} + \cdots + a_{d0n}x \dots xa_{ddn}) = 0$$

ait une solution dans  $k$  (voir [ML85]). Plus généralement, on peut considérer un *polynôme en  $n$  variables* à coefficients dans  $k$  comme étant une somme finie de produits finis de constantes de  $k$  et de variables  $x_1, \dots, x_n$  ne commutant qu'avec les éléments du centre. On peut définir que  $k$  est *existentiellement clos* si pour tout système  $\mathcal{S}$  d'équations à coefficients dans  $k$  possédant une solution dans une quelconque des extensions de  $k$ ,  $\mathcal{S}$  possède une solution dans  $k$ ; on peut montrer que tout corps  $k$  se plonge dans une clôture existentielle  $\mathbf{k}$  de même centre et de même cardinal que  $k$  si  $k$  est infini (voir [Coh95, Theorem 6.5.3]). Cette notion de polynôme ne semble pourtant pas propice à définir une notion d'indépendance algébrique satisfaisant l'axiome de transitivité (voir [Coh95, p. 406]). Pas de dimension donc.

Motivé par une question de théorie des modèles, nous proposons une approche différente réduisant autant que faire se peut le rôle de la multiplication.

## 1. DISTORSIONS LINÉAIRES

1.1. **L'algèbre des distorsions linéaires**  $K_\sigma^1[x]$ . Soit  $K$  un corps, commutatif ou non, et soit  $\sigma$  un symbole de fonction unaire. On considère l'ensemble des polynômes *formels* en  $\sigma$  à coefficients à droite dans  $K$ , sans terme constant, qu'on appelle espace des *distorsions linéaires* de  $K$ .

$$K_\sigma^1[x] = \left\{ \sum_{i=0}^n x^{\sigma^i} k_i : (k_0, \dots, k_n) \in K^{n+1}, n \in \mathbf{N} \right\}.$$

L'ensemble  $K_\sigma^1[x]$  est un  $K$ -espace vectoriel à droite engendré par  $x, x^\sigma, x^{\sigma^2}$ , etc. Le  $\sigma$ -degré d'une distorsion  $\delta$  est la plus grande puissance de  $\sigma$  apparaissant avec un coefficient non nul dans l'écriture de  $\delta$ . On le note  $\deg_\sigma \delta$ , et on convient que le  $\sigma$ -degré de la distorsion nulle est égal à  $-\infty$ . Par définition, une distorsion est nulle si tous ses coefficients sont nuls.

On suppose que  $\sigma : K \rightarrow K$  est aussi un morphisme additif de  $K$ , vérifiant la propriété multiplicative suivante : il existe un morphisme injectif de corps  $\tau_\sigma : K \rightarrow K$  telle que pour tout  $(a, b) \in K^2$ , on ait

$$\sigma(ab) = \sigma(a)\tau_\sigma(b).$$

On appelle  $\sigma$  un  $\tau$ -*morphisme*. On considèrera par exemple les cas où  $\sigma$  est un morphisme de corps, avec  $\tau_\sigma = \sigma$ , ou encore la multiplication à gauche par un élément de  $K$ , auquel cas  $\tau_\sigma$  est l'identité. Dans tous les cas, la somme

$$\sum_{i=0}^n x^{\sigma^i} k_i + \sum_{j=0}^n x^{\sigma^j} h_j = \sum_{i=0}^n x^{\sigma^i} (k_i + h_i)$$

et la composée

$$\left( \sum_{i=0}^n x^{\sigma^i} k_i \right) \left( \sum_{j=0}^n x^{\sigma^j} h_j \right) = \sum_{i=0}^n \left( \sum_{j=0}^n x^{\sigma^{i+j}} \tau_{\sigma^i}(h_j) k_i \right)$$

munissent  $K_{\sigma}^1[x]$  d'une structure d'anneau associatif unitaire, intègre. Les seuls éléments inversibles sont les homothéties. Si  $\delta$  et  $\gamma$  sont deux distorsions linéaires, on a également

$$\deg_{\sigma}(\delta\gamma) = \deg_{\sigma} \delta + \deg_{\sigma} \gamma, \text{ et}$$

$$\deg_{\sigma}(\delta + \gamma) \leq \max(\deg_{\sigma} \delta, \deg_{\sigma} \gamma).$$

**Lemme 1.1** (Division euclidienne à droite dans  $K_{\sigma}^1[x]$ ). *Pour tout  $\delta$  et  $\gamma \neq 0$  dans  $K_{\sigma}^1[x]$ , il existe un unique couple  $q$  et  $r$  dans  $K_{\sigma}^1[x]$  tel que*

$$\delta = q(\gamma) + r \quad \text{et} \quad \deg_{\sigma} r < \deg_{\sigma} \gamma.$$

*Démonstration.* Par récurrence sur  $\deg_{\sigma} \delta$ . Si  $\deg_{\sigma} \delta = -\infty$ , on pose  $q = 0$  et  $r = 0$ . Si  $\deg_{\sigma} \delta = n + 1$  et  $\deg_{\sigma} \gamma = d$ , soient  $x^{\sigma^{n+1}} k_{n+1}$  et  $x^{\sigma^d} k_d$  les termes dominants de  $\delta$  et  $\gamma$ . Si  $d > n + 1$ , on pose  $q = 0$  et  $r = \delta$ . Si  $d \leq n + 1$ . On a

$$\deg_{\sigma} \left( \delta - (\gamma k_d^{-1})^{\sigma^{n+1-d}} k_{n+1} \right) < n + 1.$$

En posant  $q_1(x) = (x k_d^{-1})^{\sigma^{n+1-d}} k_{n+1}$ , on applique l'hypothèse de récurrence à  $\delta - q_1(\gamma)$  : il existe  $q_2$  et  $r$  tels que  $\deg_{\sigma} r < d$  et

$$\delta - q_1(\gamma) = q_2(\gamma) + r.$$

On pose alors  $q = q_1 + q_2$ . □

**Corollaire 1.2.**  *$K_{\sigma}^1[x]$  est un anneau principal à gauche et noethérien à gauche.*

*Démonstration.* Soit  $I$  un idéal à gauche non nul, et  $\gamma \in I \setminus \{0\}$  de degré minimal. Si  $\delta \in I$ , on a  $\delta = q(\gamma) + r$  avec  $\deg_{\sigma} r < \deg_{\sigma} \gamma$ . Mais  $q(\gamma) \in I$ , donc  $r = 0$  et  $I = \langle \gamma \rangle$ . □

**Corollaire 1.3** (Identité de Bézout). *Soient  $\delta$  et  $\gamma$  deux distorsions et  $\alpha$  leur plus grand facteur commun à droite. Il existe deux distorsions  $u$  et  $v$  telles que*

$$u\gamma + v\delta = \alpha.$$

*Démonstration.* L'idéal à gauche  $K_{\sigma}^1[x]\gamma + K_{\sigma}^1[x]\delta$  étant principal, il est égal à  $K_{\sigma}^1[x]\pi$  pour une distorsion  $\pi$ , et  $\pi$  divise  $\gamma$  et  $\delta$  à droite. On a donc l'égalité  $K_{\sigma}^1[x]\pi = K_{\sigma}^1[x]\alpha$ . □

**1.2. Évaluation dans  $K$ , racines et factorisation.** À une distorsion  $\delta = \sum_{i=1}^n x^{\sigma^i} k_i$ , on associe l'application évaluation  $\delta_K : K \rightarrow K$  définie par

$$\delta_K : g \mapsto \sum_{i=1}^n \sigma^i(g) k_i.$$

Pour toutes distorsions  $\delta$  et  $\gamma$ , on a

$$(\delta + \gamma)_K = \delta_K + \gamma_K, \text{ et}$$

$$(\delta\gamma)_K = \delta_K \circ \gamma_K$$

de sorte que l'opérateur évaluation  $eval : \delta \mapsto \delta_K$  est un morphisme d'anneaux.

**Lemme 1.4** (Factorisation à l'aide d'une racine non nulle). *Soit  $\delta$  une distorsion de  $\sigma$ -degré  $n + 1$ . Si  $a$  est une racine non nulle de  $\delta_K$ , il existe une distorsion  $\gamma$  de  $\sigma$ -degré  $n$  telle que*

$$\delta = \gamma(x^\sigma - xa^{-1}a^\sigma).$$

*Démonstration.* On divise  $\delta$  à droite par  $x^\sigma - xa^{-1}a^\sigma$  : il existe  $q \in K_\sigma^1[x]$  et  $r \in K$  tels que

$$\delta = \gamma(x^\sigma - xa^{-1}a^\sigma) + xr.$$

Puisque  $\delta_K$  et  $x^\sigma - xa^{-1}a^\sigma$  s'annulent en  $a$ , et du fait que  $\delta \mapsto \delta_K$  est un morphisme d'anneaux, on déduit que  $r$  est nul.  $\square$

Le lemme précédent est inutile pour factoriser une distorsion qui ne s'annule qu'en zéro. Lorsque  $\sigma$  est la conjugaison par un élément  $a \in K$ , on donne une condition suffisante (et nécessaire lorsque  $a$  est transcendant sur  $k$ ) pour factoriser une distorsion de degré  $n$ .

**Lemme 1.5.** *Soit  $\sigma$  la conjugaison par  $a$ . Une distorsion de degré  $n$  se factorise en produit de distorsions de degré un dès que tout polynôme  $a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$  de degré au plus  $n$  à coefficients dans  $K$  a une racine à droite dans  $K$ .*

*Démonstration.* Soit  $a^2x - ax\alpha + x\beta$  une distorsion de degré 2. Pour tout  $b$  et  $c$  dans  $K$ , on a

$$(ax - xc)(ax - xb) = a^2x - ax(b + c) + xbc.$$

On choisit pour  $c$  une solution de l'équation  $x^2 - \alpha x + \beta = 0$ , et l'on pose  $b = \alpha - c$ , de sorte que l'on a

$$b + c = \alpha \quad \text{et} \quad bc = \alpha c - c^2 = \beta.$$

Soit  $a^3x - a^2x\alpha + ax\beta - x\gamma$  une distorsion de degré 3. Pour tout  $b$ ,  $c$  et  $d$  dans  $K$ , on a

$$(ax - xd)(ax - xc)(ax - xb) = a^3x - a^2x(b + c + d) + ax(bc + bd + cd) - xbcd.$$

On choisit pour  $d$  une solution de l'équation  $x^3 - \alpha x^2 + \beta x - \gamma = 0$ , pour  $c$  une solution de l'équation  $x^2 - (\alpha - d)x + \beta + \alpha d - d^2 = 0$  et on pose  $b = \alpha - c - d$ , de sorte que l'on a

$$0 = (c^2 - (\alpha - d)c + \beta + \alpha d - d^2) \times d = c^2d - (\alpha - d)cd + \gamma = \gamma - bcd, \text{ et}$$

$$bc + bd + cd = (b + c)d + bc = (\alpha - d)d + bc = \alpha d - d^2 + \gamma d^{-1} = \beta.$$

Le cas des degrés supérieurs est similaire.  $\square$

**Lemme 1.6** (Structure de l'ensemble des racines). *Soit  $\sigma$  un morphisme de corps, et  $\delta$  une distorsion de degré  $n$ . L'ensemble des racines de  $\delta_K$  dans  $K$  est un  $\text{Fix}(\sigma)$ -espace vectoriel à gauche de dimension au plus  $n$ .*

*Démonstration.* Si  $n = 1$ , et si  $\delta$  est unitaire,  $\delta(x) = x^\sigma + xk_0$ . D'après le lemme 1.4, si  $a$  et  $b$  sont deux racines non nulles de  $\delta_K$ , on a nécessairement

$$(1) \quad a^{-1}a^\sigma = b^{-1}b^\sigma.$$

Ceci se traduit par  $ab^{-1} \in \text{Fix}(\sigma)$ , donc  $a$  et  $b$  sont liées à gauche. On conclut immédiatement par récurrence avec le lemme 1.4 sachant que  $\delta_K$  étant  $\text{Fix}(\sigma)$ -linéaire à gauche, si  $\delta = \delta_1\delta_2$ , la dimension du noyau de  $\delta_K$  ne peut excéder la somme des dimensions des noyaux de ses facteurs.  $\square$

*Exemples 1.7.* (1) Si  $K$  est commutatif de caractéristique  $p > 0$  et si  $\sigma$  est l'application de Froebenius,  $x \mapsto x^p$ , on retrouve qu'un polynôme en  $x^p$  de degré  $p^n$  n'a pas plus de  $p^n$  racines.

(2) Si  $K$  est un corps non commutatif, et  $\sigma$  la conjugaison par un élément  $a \in K$  hors du centre (ou la multiplication à gauche par  $a$ ), on obtient que les racines dans  $K$  d'une distorsion de degré  $n$  forment un  $C(a)$ -espace vectoriel à gauche de dimension au plus  $n$ .

**1.3. L'algèbre des distorsions  $n$ -linéaires**  $K_\sigma^1[x_1, \dots, x_n]$ . On définit le  $K$ -espace vectoriel à droite  $K_\sigma^1[x_1, \dots, x_n]$  des distorsions  $n$ -linéaires de  $K^n$  en posant

$$K_\sigma^1[x_1, \dots, x_n] = K_\sigma^1[x_1] \oplus \dots \oplus K_\sigma^1[x_n].$$

On le munit d'une structure d'anneau associatif non-commutatif en posant

$$\left( \sum_{i=1}^n \gamma_i(x_i) \right) \left( \sum_{j=1}^n \delta_j(x_j) \right) = \sum_{i=1}^n \left( \sum_{j=1}^n \gamma_i \delta_j(x_j) \right).$$

Cet anneau est dépourvu d'unité si  $n > 1$ . Les éléments  $x_1, \dots, x_n$  sont des unités à gauche, mais pas à droite. On voit aisément qu'il ne possède pas de diviseurs de zéros. Son centre est réduit à  $\{0\}$ .

**Théorème 1.8** (de Hilbert, version faible).  $K_\sigma^1[x_1, \dots, x_n]$  est un anneau noethérien à gauche.

*Démonstration.* Par récurrence sur  $n$ . Si  $K_\sigma^1[x_1, \dots, x_n]$  n'est pas noethérien à gauche, il existe un idéal à gauche  $I \subset K_\sigma^1[x_1, \dots, x_n]$  qui n'est pas finiment engendré. On construit par induction une suite  $(\delta_0, \delta_1, \delta_2, \dots)$  d'éléments de  $K_\sigma^1[x_1, \dots, x_n]$  en posant  $I_\ell = \langle \delta_0, \dots, \delta_\ell \rangle$ , de telle sorte que pour tout entier  $\ell$ , l'élément  $\delta_{\ell+1}$  soit de  $\sigma$ -degré minimal en  $x_n$  vérifiant

$$\delta_{\ell+1} \in I \setminus I_\ell.$$

Posons

$$d_\ell = \deg_{\sigma, x_n} \delta_\ell.$$

La chaîne des degrés  $d_0, d_1, d_2 \dots$  est croissante. Puisque  $K_\sigma^1[x_1, \dots, x_{n-1}]$  est un sous-anneau noethérien à gauche par hypothèse de récurrence,  $d_\ell$  est positif à partir d'un certain rang  $N$ . Les termes de plus haut degré en  $x_n$  de  $\delta_{N+1}$  et  $\delta_N$  sont de la forme  $x_n^{\sigma^{d_{N+1}}} k_{N+1}$  et  $x_n^{\sigma^{d_N}} k_N$ .

On pose

$$g = (\delta_N k_N^{-1})^{\sigma^{d_{N+1} - d_N}} k_{N+1} \in I_N,$$

de sorte que  $\deg_{\sigma, x_n}(\delta_{N+1} - g) < d_{N+1}$ . Mais  $\delta_{N+1} - g \in I \setminus I_N$ , contredisant le caractère minimal de  $d_{N+1}$ .  $\square$

## 2. $\sigma$ -ESPACE ET ALGÈBRE LINÉAIRE TORDUE

On considère un corps  $K$  muni d'un  $\tau$ -morphisme  $\sigma : K \rightarrow K$ .

**Définition 2.1** ( $\sigma$ -Espace). On appelle  $\sigma$ -espace tout  $K$ -espace vectoriel à droite  $E$  muni d'un morphisme additif  $\sigma_E : E \rightarrow E$  vérifiant la propriété multiplicative suivante. Pour tout  $e \in E$  et  $k \in K$ , on a

$$\sigma_E(ek) = \sigma_E(e)\tau(k).$$

*Exemples 2.2.* (1)  $E = K$ , avec  $\sigma_E = \sigma$  est un  $\sigma$ -espace.

(2)  $E = K_\sigma^1[x]$ , avec pour  $\sigma_E$  la multiplication à gauche par  $x^\sigma$ , est un  $\sigma$ -espace.

On définit un morphisme de  $K$ -espaces vectoriels  $eval : K_\sigma^1[x] \rightarrow E^E$ ,  $\delta \mapsto \delta_E$ , en posant

$$(x^{\sigma^i})_E(e) = \sigma_E^i(e)$$

pour les éléments de la base canonique de  $K_\sigma^1[x]$  et en étendant  $eval$  à  $K_\sigma^1[x]$  par linéarité.

**Lemme 2.3.** *Si  $E$  est un  $\sigma$ -espace, l'opérateur  $\delta \mapsto \delta_E$  est multiplicatif.*

*Démonstration.* On a pour tout  $e \in E$ ,

$$\begin{aligned} ((x^{\sigma^i}k)(x^{\sigma^j}\ell))_E(e) &= (x^{\sigma^{i+j}}\tau^i(\ell)k)_E(e) \\ &= \sigma_E^{i+j}(e)\tau^i(\ell)k \\ &= \sigma_E^i(\sigma_E^j(e)\ell)k \\ &= (x^{\sigma^i}k)_E \circ (x^{\sigma^j}\ell)_E(e). \end{aligned}$$

L'opérateur  $\delta \mapsto \delta_E$  étant additif par définition, on en déduit l'égalité  $(\delta\gamma)_E = \delta_E \circ \gamma_E$ .  $\square$

**Lemme 2.4.** *Un ensemble  $E$  est un  $\sigma$ -espace si et seulement si c'est un  $K_\sigma^1[x]$ -module à gauche.*

*Démonstration.* Un  $\sigma$ -espace  $E$  a une structure naturelle de  $K_\sigma^1[x]$ -module à gauche obtenue en posant pour tout  $\delta \in K_\sigma^1[x]$  et  $e \in E$ ,

$$\delta \cdot e = \delta_E(e).$$

Réciproquement, tout  $K_\sigma^1[x]$ -module à gauche  $E$  a une structure de  $K$ -espace vectoriel à droite, en posant  $ek = (xk) \cdot e$ , et de  $\sigma$ -espace, ce que l'on voit en posant  $\sigma_E(e) = x^\sigma \cdot e$ , d'où

$$\sigma_E(ek) = x^\sigma \cdot ek = ((x^\sigma)(xk)) \cdot e = (x^\sigma\tau(k)) \cdot e = \sigma_E(e)\tau(k). \quad \square$$

**Lemme 2.5.** *Supposons que  $\sigma(x) = ax$  ou  $\sigma(x) = x^a$  pour un élément  $a \notin k$ . L'opérateur  $K_\sigma^1[x_1, \dots, x_n] \rightarrow K^{K^n}$ ,  $\delta \mapsto \delta_K$  est injectif si  $[K : C(a)]$  est infini.*

*Démonstration.* C'est une conséquence du lemme 1.6  $\square$

**2.1. Algèbre linéaire tordue, indépendance algébrique, algébricité.** Étant donné un  $\sigma$ -espace  $E$ , un  $\sigma$ -sous-espace de  $E$  est un sous espace vectoriel stable par  $\sigma_E$ . Pour toute partie  $A \subset E$ , on note  $\langle A \rangle_\sigma$  l'intersection de tous les  $\sigma$ -sous-espaces contenant  $A$ . Une famille  $(e_1, \dots, e_n)$  de  $E$  est  $\sigma$ -liée s'il existe une distorsion non nulle  $\delta \in K_\sigma^1[x_1, \dots, x_n]$  telle que

$$\delta_E(e_1, \dots, e_n) = 0.$$

Dans le cas contraire, elle est  $\sigma$ -libre. Elle est  $\sigma$ -génératrice si pour tout élément  $f$  de  $E$ , il existe  $\delta \in K_\sigma^1[x_1, \dots, x_n]$  telle que

$$f = \delta_E(e_1, \dots, e_n).$$

C'est une  $\sigma$ -base si elle est  $\sigma$ -libre et maximale ayant cette propriété.

**Lemme 2.6** ( $\sigma$ -Base incomplète). *Soit  $E$  un  $\sigma$ -espace non nul,  $G$  une partie  $\sigma$ -génératrice et  $L \subset G$  une partie  $\sigma$ -libre. Il existe une  $\sigma$ -base  $B$  de  $E$  telle que  $L \subset B \subset G$ .*

*Démonstration.* Si  $\mathfrak{B} = \{B_i : i \in I\}$  est une réunion croissante de familles  $\sigma$ -libres de  $E$ , leur réunion  $\bigcup \mathfrak{B}$  l'est également, ce qui permet d'appliquer le lemme de Zorn.  $\square$

**Corollaire 2.7.** *Tout  $\sigma$ -espace possède une  $\sigma$ -base.*

Si  $B$  est une  $\sigma$ -base de  $E$ , alors, pour tout élément  $e$  de  $E \setminus B$ , la famille  $B \cup \{e\}$  est  $\sigma$ -liée : il existe  $b_1, \dots, b_n$  dans  $B$ , un élément  $\delta \in K_\sigma^1[x_1, \dots, x_n]$  et  $h \in K_\sigma^1[x]$  non nul tels que

$$h_E(e) = \delta_E(b_1, \dots, b_n).$$

L'ensemble des  $h \in K_\sigma^1[x]$  tels que  $h_E(e) \in \langle B \rangle_\sigma$  est un idéal à gauche non nul de  $K_\sigma^1[x]$  engendré par une unique distorsion unitaire  $\delta_e$  de degré  $d$  que l'on appelle la *distorsion minimale de  $e$* . On dit que  $e$  est  $\sigma$ -algébrique de degré  $d$  sur  $B$ .

**Définition 2.8** (Algébricité). Soit  $E$  un  $\sigma$ -espace,  $B \subset E$  une partie, et  $b \in B$ . On dit que  $b$  est  $\sigma$ -algébrique sur  $B$  s'il existe une distorsion  $h \in K_\sigma^1[x]$  non nulle telle que

$$h_E(b) \in \langle B \rangle_\sigma.$$

Une partie  $A \subset E$  est  $\sigma$ -algébrique sur  $B$  si tout  $a \in A$  est  $\sigma$ -algébrique sur  $B$ .

**Lemme 2.9** (Transitivité du caractère algébrique). *Soient  $A, B, C$  trois parties de  $E$ . Si  $A$  est  $\sigma$ -algébrique sur  $B$  et si  $B$  est  $\sigma$ -algébrique sur  $C$ , alors  $A$  est  $\sigma$ -algébrique sur  $C$ .*

*Démonstration.* Soit  $a \in A$ . Il existe des éléments non nuls  $h, \gamma_1, \dots, \gamma_n$  dans  $K_\sigma^1[x]$  et deux familles  $\delta_1, \dots, \delta_n$  de  $K_\sigma^1[x]$  et  $\beta_1, \dots, \beta_n$  de  $K_\sigma^1[x_1, \dots, x_n]$ , des éléments  $b_1, \dots, b_n$  dans  $B$  et  $c_1, \dots, c_m$  de  $C$  tels que pour tout  $i \in \{1, \dots, n\}$ ,

$$h_E(a) = \delta_{1E}(b_1) + \dots + \delta_{nE}(b_n) \quad \text{et} \quad \gamma_{iE}(b_i) = \beta_{iE}(c_1, \dots, c_m),$$

En particulier, en posant  $\bar{c} = (c_1, \dots, c_m)$ , il y a une expression de la forme

$$\varepsilon_E(a) = \beta_E(\bar{c}) + \sum_{i \in I} \pi_{iE}(b_i),$$

avec  $\varepsilon \in K_\sigma^1[x]$  non nulle, et on en choisit une de telle sorte que l'ensemble  $I \subset \{1, \dots, n\}$  soit de cardinal minimal possible. Montrons que  $I$  est nécessairement vide. S'il contient 1 disons, alors  $\pi_1$  est non nul. On appelle  $\alpha$  le plus grand diviseur commun à droite de  $\pi_1$  et  $\gamma_1$ , et il existe deux distorsions  $u$  et  $v$  telles que  $u\pi_1 + v\gamma_1 = \alpha$ . Si  $u = 0$ , alors  $\gamma_1$  divise  $\alpha$  à droite, donc  $\gamma_1$  divise  $\pi_1$  à droite :  $\pi_1 = \pi'_1\gamma_1$ . En remplaçant dans l'égalité ci-dessus, cela contredit



le caractère minimal de  $I$ . On a donc  $u \neq 0$ . En posant  $\gamma_1 = \gamma'_1 \alpha$ , on a alors

$$\begin{aligned}
 (\gamma'_1 u \varepsilon)_E(a) &= (\gamma'_1 u \beta)_E(\bar{c}) + \gamma'_{1E} \left( u_E \left( \sum_{i \in I} \pi_{iE}(b_i) \right) \right) \\
 &= (\gamma'_1 u \beta)_E(\bar{c}) + \gamma'_{1E} \left( (u \pi_1)_E(b_1) + \sum_{i \in I \setminus \{1\}} (u \pi_i)_E(b_i) \right) \\
 &= (\gamma'_1 u \beta)_E(\bar{c}) + \gamma'_{1E} \left( \alpha_E(b_1) - (v \gamma_1)_E(b_1) + \sum_{i \in I \setminus \{1\}} (u \pi_i)_E(b_i) \right) \\
 &= (\gamma'_1 u \beta)_E(\bar{c}) + \beta_{1E}(\bar{c}) - (\gamma'_1 v \beta_1)_E(\bar{c}) + \sum_{i \in I \setminus \{1\}} (\gamma'_1 u \pi_i)_E(b_i)
 \end{aligned}$$

avec  $\gamma'_1 u \varepsilon$  non nulle puisque  $\gamma'_1$ ,  $u$  et  $\varepsilon$  sont non nulles, une contradiction avec le caractère minimal de  $I$ .  $\square$

## 2.2. $\sigma$ -Dimension.

**Théorème 2.10** (de Steinitz,  $\sigma$ -dimension). *Soit  $E$  un  $\sigma$ -espace. Toutes les  $\sigma$ -bases de  $E$  ont même cardinal, que l'on appelle  $\sigma$ -dimension de  $E$ .*

*Démonstration.* On traite le cas particulier où  $E$  possède une  $\sigma$ -base finie  $(b_1, \dots, b_n)$ . Soit  $(c_1, \dots, c_m)$  une famille  $\sigma$ -libre de  $E$ . Par maximalité de la famille  $B = (b_1, \dots, b_n)$ , on peut écrire  $\gamma_E(c_1) = \delta_E(\bar{b})$  pour une certaine distorsion  $\gamma$  non nulle. En particulier,  $\delta$  est non nulle, donc  $x_1$  par exemple y apparaît. Dans ce cas,  $b_1$  est algébrique sur  $(c_1, b_2, \dots, b_n)$ , mais puisque  $E$  est algébrique sur  $B$ , d'après le lemme précédent,  $E$  est algébrique sur  $(c_1, b_2, \dots, b_n)$ , donc  $(c_1, b_2, \dots, b_n)$  est bien une  $\sigma$ -base. On conclut de la même façon que  $(c_1, c_2, b_3, \dots, b_n)$  est une  $\sigma$ -base, et de proche en proche, on peut rajouter tous les  $c_i$ . Si  $m < n$ , on arrive à la conclusion que  $c_m$  est algébrique sur ses prédécesseurs, une contradiction, d'où  $m \leq n$ . On conclut par symétrie que  $n = m$ .  $\square$

On note  $\dim_\sigma E$  la  $\sigma$ -dimension d'un  $\sigma$ -espace  $E$ . Le corps  $K$  est de  $\sigma$ -dimension nulle : si  $a \in K$  est un élément non nul,  $x^\sigma - x a^{-1} a^\sigma$  est non nul, et annule  $a$ . L'algèbre  $K_\sigma^1[x]$  est engendrée par  $x$  ; sa  $\sigma$ -dimension est égale à 1.

**Lemme 2.11** (Somme). *Soient  $E$  et  $F$  deux  $\sigma$ -espaces, alors la somme  $E \oplus F$  est naturellement munie d'une structure de  $\sigma$ -espace en posant  $\sigma_{E \oplus F}(e + f) = \sigma_E(e) + \sigma_F(f)$ , et*

$$\dim_\sigma E \oplus F = \dim_\sigma E + \dim_\sigma F.$$

*Démonstration.*  $\sigma_{E \oplus F}$  est additive, et pour tout  $e + f$  dans  $E \oplus F$  et tout  $k$  dans  $K$ , on a

$$\sigma_{E \oplus F}((e + f)k) = \sigma_E(ek) + \sigma_F(fk) = \sigma_E(e)\tau(k) + \sigma_F(f)\tau(k) = \sigma_{E \oplus F}(e + f)\tau(k),$$

ce qui montre que  $E \oplus F$  est un  $\sigma$ -espace. Si  $B$  et  $C$  sont deux bases respectives de  $E$  et  $F$ , on montre sans peine que  $B \cup C$  est une famille  $\sigma$ -libre maximale de  $E \oplus F$ .  $\square$

En particulier,  $K_\sigma^1[x_1, \dots, x_n]$  est un  $\sigma$ -espace. Les vecteurs  $(x_1, \dots, x_n)$  en forment une  $\sigma$ -base, et sa  $\sigma$ -dimension est égale à  $n$ .

**Lemme 2.12** (Quotient). *Soit  $E$  un  $\sigma$ -espace et  $F \subset E$  un  $\sigma$ -sous-espace. Le quotient  $E/F$  est muni d'une structure de  $\sigma$ -espace en posant  $\sigma_{E/F}(e + F) = \sigma_E(e) + F$ , et l'on a*

$$\dim_{\sigma} E/F = \dim_{\sigma} E - \dim_{\sigma} F.$$

*Démonstration.*  $\sigma_{E/F}$  est bien définie, additive (et injective si  $F$  est  $\sigma$ -algébriquement clos). D'autre part, on a pour tout  $e \in E$  et  $k \in K$ ,

$$\sigma_{E/F}((e + F)k) = \sigma_{E/F}(ek + F) = \sigma_E(e)\tau(k) + F = \sigma_{E/F}(e + F)\tau(k),$$

donc  $E/F$  est bien un  $\sigma$ -espace. Soit  $(b_1 + F, \dots, b_n + F)$  une  $\sigma$ -base de  $E/F$  et  $(c_1, \dots, c_m)$  une  $\sigma$ -base de  $F$ . Montrons que  $A = (b_1, \dots, b_n, c_1, \dots, c_m)$  est une  $\sigma$ -base de  $E$ . S'il existe une distorsion  $\pi(\bar{x}, \bar{y})$  qui annule  $A$ , alors il existe deux distorsions  $\delta(\bar{x})$  et  $\gamma(\bar{y})$  telles que  $\pi(\bar{x}, \bar{y}) = \delta(\bar{x}) - \gamma(\bar{y})$  et

$$\delta_E(b_1, \dots, b_n) = \gamma_F(c_1, \dots, c_m) \in F.$$

En particulier, on a

$$\delta_{E/F}(b_1 + F, \dots, b_n + F) = 0,$$

donc  $\delta = 0$ , et  $\gamma_F(c_1, \dots, c_m) = 0$ , d'où  $\gamma = 0$ , et  $\pi = 0$ . La famille  $A$  est donc  $\sigma$ -libre. Montrons que  $E$  est algébrique sur  $A$ . Si  $e \in E \setminus A$ , alors par maximalité de  $(b_1 + F, \dots, b_n + F)$ , il existe une distorsion  $\delta$  non nulle, et une autres  $h$  telle que

$$\delta_E(e) - h_E(\bar{b}) \in F.$$

Mais par maximalité de  $(c_1, \dots, c_m)$ , l'élément  $\delta_E(e) - h_E(\bar{b})$  est algébrique sur  $(c_1, \dots, c_m)$  : il existe une distorsion non nulle  $\gamma$  telle que

$$\gamma_E(\delta_E(e) - h_E(\bar{b})) \in \langle c_1, \dots, c_m \rangle_{\sigma}.$$

Puisque  $\gamma\delta$  est non nulle,  $e$  est algébrique sur  $A$ . □

**Lemme 2.13** (Clôture algébrique). *Pour toute partie  $A \subset E$ , l'ensemble  $cl(A)$  des éléments de  $E$  qui sont  $\sigma$ -algébriques sur  $A$  est un  $\sigma$ -sous espace de  $E$ , et*

$$\dim_{\sigma} cl(A) = \dim_{\sigma} \langle A \rangle.$$

*Démonstration.* Soient  $a$  et  $b$  deux éléments  $\sigma$ -algébriques sur  $A$ . Alors, pour tout  $k \in K$ , les éléments  $a + b$ ,  $ak$  et  $a^{\sigma}$  sont  $\sigma$ -algébrique sur  $\{a, b\}$ , lesquels sont algébriques sur  $A$ , donc  $a + b$ ,  $ak$  et  $a^{\sigma}$  sont algébriques sur  $A$  d'après le lemme 2.9. Puisque  $\langle A \rangle \subset cl(A)$ , on a  $\dim_{\sigma} \langle A \rangle \leq \dim_{\sigma} cl(A)$ . Réciproquement, il suffit de montrer d'après le lemme précédent que l'on a  $\dim_{\sigma} E/cl(A) \geq \dim_{\sigma} E/\langle A \rangle$ , et même que pour tout  $a \in cl(A)$ , on a  $\dim_{\sigma} E/\langle A, a \rangle \geq \dim_{\sigma} E/\langle A \rangle$ . Supposons que  $a$  est dans la clôture de  $A$ . Soient  $b_1 + A, \dots, b_d + A$   $\sigma$ -libres. Montrons que  $b_1 + \langle A, a \rangle_{\sigma}, \dots, b_d + \langle A, a \rangle_{\sigma}$  sont  $\sigma$ -libres. Soit  $h(x_1, \dots, x_d)$  une distorsion linéaire telle que  $h_E(b_1, \dots, b_d) \in \langle A, a \rangle_{\sigma}$ . Il existe donc une distorsion  $g \in K^1[x]$  telle que

$$h_E(b_1, \dots, b_d) + g_E(a) \in A.$$

La clôture de  $A$  étant un module, elle contient  $g_E(a)$  : soit  $g_E(a) = 0$ , auquel cas  $h = 0$  par liberté de la famille  $b_1 + A, \dots, b_d + A$ , soit il existe une distorsion non nulle  $\gamma$  telle que  $\gamma g_E(a) \in A$ , d'où  $\gamma h_E(b_1, \dots, b_d) \in A$ , ce qui implique  $\gamma h = 0$ , et donc  $h = 0$ . □

**2.3. Morphismes de  $\sigma$ -espaces.** Soient deux  $\sigma$ -espaces  $E$  et  $F$ . Une application  $\alpha : E \rightarrow F$  est un *morphisme de  $\sigma$ -espaces* si  $\alpha \circ \delta_E = \delta_F \circ \alpha$  pour tout  $\delta$  dans  $K_\sigma^1[x_1, \dots, x_n]$ .

**Lemme 2.14.** *Soit  $\alpha : E \rightarrow F$  un morphisme de  $\sigma$ -espaces.*

- (1) *Si  $\alpha$  est injectif, on a  $\dim_\sigma E \leq \dim_\sigma F$ .*
- (2) *Si  $\alpha$  est surjectif, on a  $\dim_\sigma F \leq \dim_\sigma E$ .*
- (3) *Si  $\dim_\sigma E$  est fini, on a  $\dim_\sigma \text{Ker}\alpha + \dim_\sigma \text{Im}\alpha = \dim_\sigma E$ .*

*Démonstration.* (1) Si la famille  $(e_1, \dots, e_n)$  est  $\sigma$ -libre dans  $E$ , et s'il existe une distorsion  $\delta$  telle que  $\delta_F(\alpha e_1, \dots, \alpha e_n) = 0$ , alors

$$\delta_F(\alpha(e_1, \dots, e_n)) = \delta_F \circ \alpha(e_1, \dots, e_n) = \alpha \circ \delta_E(e_1, \dots, e_n) = 0.$$

$\alpha$  étant injective, on a  $\delta_E(e_1, \dots, e_n) = 0$ , ce qui implique  $\delta = 0$  par liberté de la famille  $e_i$ . La famille  $(\alpha e_1, \dots, \alpha e_n)$  est donc  $\sigma$ -libre.

(2) Si la famille  $(f_1, \dots, f_n)$  est  $\sigma$ -libre dans  $F$ , et si  $(e_1, \dots, e_n)$  en sont des antécédents par  $\alpha$  dans  $E$ , on montre que  $(e_1, \dots, e_n)$  est  $\sigma$ -libre : si on a  $\delta_E(e_1, \dots, e_n) = 0$ , en composant par  $\alpha$ , on déduit que  $\delta_F(f_1, \dots, f_n) = 0$ , d'où  $\delta = 0$  par liberté de la famille  $(f_1, \dots, f_n)$ .

(3)  $\text{Ker}\alpha$  et  $\text{Im}\alpha$  sont des  $\sigma$ -espaces. L'application induite  $E/\text{Ker}\alpha \rightarrow \text{Im}\alpha$  définit un morphisme de  $\sigma$ -espaces bijectif. On conclut avec (1), (2) et le lemme 2.12.  $\square$

### 3. CORPS $\sigma$ -ALGÈBRIQUEMENT CLOS ET THÉORÈME DE CHEVALLEY-COHN

Soit  $K$  un corps non commutatif de centre  $k$ , soit  $a \in K$  un élément hors du centre fixé, et  $\sigma : K \rightarrow K$  la multiplication à gauche par  $a$ .

**Lemme 3.1** (de Brauer). *L'extension de corps commutatifs  $k(a)/k$  est algébrique de degré  $n$  si et seulement si  $[K : C(a)]_{\text{gauche}}$  est égal à  $n$ . En particulier, on a*

$$[K : C(a)]_{\text{gauche}} = [K : C(a)]_{\text{droite}}.$$

*Démonstration.* On a  $[k(a) : k] = [K : C(a)]_{\text{gauche}}$  d'après un résultat de Brauer (voir [Coh95, Corollary 3.3.9]). Remarquer que si  $a$  satisfait l'équation  $a^n + \dots + ak_1 + k_0 = 0$ , alors  $C(a^n + \dots + ak_1) = K$ , mais appartenir à  $C(a^n + \dots + ak_1)$  est équivalent à être racine d'une certaine distorsion de degré  $n$ , donc  $[K : C(a)]_{\text{gauche}} \leq n$  d'après le lemme 1.6.  $\square$

Géométriquement, la situation où  $k(a)/k$  est algébrique est étrange puisque les ensembles de dimension 0 et 1 sont très similaires. Nous supposons donc  $a$  transcendant sur le centre  $k$ .

**Définition 3.2** (corps  $\sigma$ -algébriquement clos).  *$K$  est  $\sigma$ -algébriquement clos si pour tout  $(b, c)$  dans  $K^2$ , l'équation  $ax - xb = c$  a une solution dans  $K$ , et si toute distorsion de  $K_\sigma^1[x]$  se factorise en produit de distorsions de degré 1.*

**Théorème 3.3** (de Cohn).  *$K$  a une extension  $\sigma$ -algébriquement close  $\mathbf{K}/K$  de centre  $k$ .*

*Démonstration.* Le corps  $K$  se plonge dans une clôture existentielle  $\mathbf{K}$  de centre  $k$  d'après [Coh95, Theorem 6.5.3] et [Coh95, Corollary 6.5.6] (voir aussi et [HW75]). D'après [Coh73, Theorem 2], cela suffit pour que pour chaque  $(b, c)$  dans  $\mathbf{K}^2$ , l'équation  $ax - xb = c$  ait une solution dans  $\mathbf{K}$ . D'après [Coh95, Theorem 8.5.1], cela suffit également pour que tout

polynôme à coefficients dans  $\mathbf{K}$  ait une racine à droite dans  $\mathbf{K}$ . On conclut avec le lemme 1.5.  $\square$

Étant fixé un langage du premier ordre, et une théorie  $T$  dans ce langage, on dit que  $T$  *élimine les quantificateurs* si toute formule  $\varphi(x_1, \dots, x_n)$  de  $L$  est logiquement équivalente modulo  $T$  à une formule  $\psi(x_1, \dots, x_n)$  sans quantificateurs, i.e. si pour tout modèle  $M$  de  $T$ , et tout uplet  $(a_1, \dots, a_n)$  extrait de  $M$ , on a

$$\varphi(a_1, \dots, a_n) \models T \iff \psi(a_1, \dots, a_n) \models T$$

**Théorème 3.4** (de Tarski, élimination des quantificateurs). *Si  $\mathbf{K}$  est  $\sigma$ -algébriquement clos, la théorie de  $\mathbf{K}$ , exprimée dans le langage  $(+, \{\alpha_k\}_{k \in \mathbf{K}}, \sigma, 0)$  où chaque  $\alpha_k$  est un prédicat de fonction unaire interprété par la multiplication à droite par  $k$ , élimine les quantificateurs.*

*Démonstration.* Soit  $T$  la théorie de  $\mathbf{K}$  dans ce langage, et  $A$  et  $B$  deux modèles suffisamment saturés de  $T$ . Soient  $a_1, \dots, a_n$  des éléments de  $A$ , et  $b_1, \dots, b_n$  des éléments de  $B$  tels qu'il existe un *isomorphisme local*  $\pi$  entre  $a_1, \dots, a_n$  et  $b_1, \dots, b_n$ , c'est-à-dire que  $\pi$  est une bijection entre  $(a_1, \dots, a_n)$  et  $(b_1, \dots, b_n)$  telle que pour toute formule sans quantificateurs  $\varphi(x_1, \dots, x_n)$  en  $n$ -variables,  $\varphi(a_1, \dots, a_n)$  soit satisfaite dans  $A$  si et seulement si  $\varphi(b_1, \dots, b_n)$  est satisfaite dans  $B$ . Soit  $a_{n+1}$  un élément de  $A$ . Montrons que l'on peut prolonger  $\pi$  en un isomorphisme local de domaine de définition  $\{a_1, \dots, a_{n+1}\}$ . C'est suffisant d'après [Poi85, théorème 2.02]. Remarquons que  $A$  et  $B$  sont des  $\mathbf{K}$ -espaces vectoriels à droite, et des  $\sigma$ -espaces, puisque ces propriétés sont exprimables par des formules du premier ordre.

Si  $a_{n+1}$  est  $\sigma$ -transcendant sur  $(a_1, \dots, a_n)$ , on choisit pour  $b_{n+1}$  un élément transcendant sur  $(b_1, \dots, b_n)$ , ce qui est possible par hypothèse de saturation.

Si  $a_{n+1}$  est  $\sigma$ -algébrique sur  $(a_1, \dots, a_n)$ , alors il existe une unique distorsion minimale unitaire  $\delta$  et une autre distorsion  $\gamma$ , telle que

$$\delta_A(a_{n+1}) = \gamma_A(a_1, \dots, a_n).$$

On choisit alors pour  $b_{n+1}$  une solution dans  $B$  de l'équation  $\delta(x) = \gamma_B(b_1, \dots, b_n)$ , ce qui est possible puisque  $B$  satisfait la théorie de  $\mathbf{K}$ , et en particulier la formule  $\forall y \exists x (\delta(x) = y)$ .

Reste à vérifier que  $(a_1, \dots, a_{n+1})$  et  $(b_1, \dots, b_{n+1})$  satisfont les mêmes formules sans quantificateurs, c'est-à-dire combinaisons booléennes de formules de la forme

$$\delta(x_1, \dots, x_{n+1}) = 0.$$

Il suffit de le faire pour la formule ci-dessus, que l'on peut mettre sous la forme

$$\alpha(x_{n+1}) = \beta(x_1, \dots, x_n).$$

Si  $\alpha$  est la fonction nulle, alors il n'y a rien à démontrer. Si  $\alpha$  est non nulle, et si  $\alpha_A(a_{n+1}) = \beta_A(a_1, \dots, a_n)$ , alors  $a_{n+1}$  est  $\sigma$ -algébrique sur  $(a_1, \dots, a_n)$ , et l'on sait que  $\alpha = \alpha' \delta$  où  $\delta$  est la distorsion minimale de  $a_{n+1}$  et que  $\delta_A(a_{n+1}) = \gamma_A(a_1, \dots, a_n)$  pour une certaine distorsion  $\gamma$ . On a donc par construction de  $b_{n+1}$ , et d'après le lemme 2.3,

$$\alpha_B(b_{n+1}) = (\alpha' \delta)_B(b_{n+1}) = \alpha'_B(\gamma_B(b_1, \dots, b_n)).$$

Mais on a également  $(\alpha'\gamma)_A(a_1, \dots, a_n) = \beta_A(a_1, \dots, a_n)$ , qui est exprimable par une formule sans quanteur, donc par hypothèse, on a également  $(\alpha'\gamma)_B(b_1, \dots, b_n) = \beta_B(b_1, \dots, b_n)$ , d'où  $\alpha_B(b_{n+1}) = \beta_B(b_1, \dots, b_n)$ . La réciproque est symétrique.  $\square$

**Corollaire 3.5.** *Soit  $\mathcal{S}$  un système fini de  $\sigma$ -équations et de  $\sigma$ -inéquations à coefficients dans un corps  $\sigma$ -algébriquement clos  $\mathbf{K}$ . Si  $\mathcal{S}$  a une solution dans une extension  $\mathbf{L}/\mathbf{K}$  de centre  $k$ , il a une solution dans  $\mathbf{K}$ .*

*Démonstration.* Soit  $\mathbf{M}$  une extension  $\sigma$ -algébriquement close de  $\mathbf{L}$ . Par élimination des quanteurs, toute formule à paramètres dans  $K$  qui est vraie dans  $\mathbf{M}$  l'est aussi dans  $\mathbf{K}$ , donc  $\mathbf{K}$  possède une solution de  $\mathcal{S}$ .  $\square$

On définit sur  $K^n$  une topologie dont les fermés de bases sont de la forme  $\{\bar{x} \in K^n : \delta_K(\bar{x}) = 0\}$  pour une distortion affine  $\delta$ . Un sous ensemble  $C \subset K^n$  est *constructible* si  $C$  est une combinaison booléenne finie de fermés et d'ouverts de  $K^n$ . Une application  $f : K^n \rightarrow K^m$  est un  $\sigma$ -morphisme si ses applications coordonnées sont des distortions affines.

**Théorème 3.6** (de Chevalley-Cohn). *Si  $\mathbf{K}$  est  $\sigma$ -algébriquement clos,  $f : \mathbf{K}^n \rightarrow \mathbf{K}^m$  un  $\sigma$ -morphisme et  $C \subset \mathbf{K}^n$  une partie constructible,  $f(C)$  est une partie constructible de  $\mathbf{K}^m$ .*

*Démonstration.* On a  $f(C) = \{\bar{y} \in \mathbf{K}^m : (\exists \bar{x} \in \mathbf{K}^n) f(\bar{x}) = \bar{y}\}$ , un sous-ensemble de  $\mathbf{K}^m$  définissable dans le langage étudié précédemment. D'après le théorème 3.4, il existe une formule  $\varphi(\bar{y})$  sans quantificateurs telle que  $f(C) = \{\bar{y} \in \mathbf{K}^m : \varphi(\bar{y})\}$ .  $\square$

**Corollaire 3.7.** *Soit  $\mathbf{K}$  un corps  $\sigma$ -algébriquement clos,  $F \subset \mathbf{K}^n$  un fermé et  $f : G \rightarrow \mathbf{K}^m$  un  $\sigma$ -morphisme. L'image  $f(F)$  est un fermé de  $\mathbf{K}^m$ .*

*Démonstration.* On peut se restreindre au cas où  $F$  est un ensemble  $\sigma$ -algébrique, et même un groupe, quitte à translater  $G$  et à composer  $f$  par une translation. On peut également supposer que  $f(0) = 0$  quitte à retrancher à  $f$  une translation et à translater  $f(F)$ . L'image  $f(F)$  est constructible d'après le théorème de Chevalley-Cohn. Elle contient donc un ouvert dense de son adhérence  $\overline{f(F)}$  (voir [TY05, Proposition 1.4.6]). Le groupe  $f(F)$  est donc fermé (voir [TY05, Proposition 21.2.2]).  $\square$

#### 4. GÉOMÉTRIE ALGÈBRIQUE ÉLÉMENTAIRE SUR $K^n$

On considère un corps non commutatif  $K$  muni de l'application  $\sigma : K \rightarrow K$  qui est soit la multiplication à gauche par un élément  $a \in K$ , soit la conjugaison par  $a$ . On note  $K_\sigma^1[x_1, \dots, x_n, K]$  l'ensemble des *distorsions affines*, que l'on considère comme un  $K_\sigma^1[x]$ -module à gauche.

**4.1. Ensemble algébrique, module d'un ensemble.** On appelle *ensemble  $\sigma$ -algébrique* l'ensemble des racines dans  $K^n$  d'une famille  $S \subset K_\sigma^1[x_1, \dots, x_n, K]$  de distorsions affines. On le note

$$V(S) = \{\bar{x} \in K^n : \delta_K(\bar{x}) = 0 \text{ pour tout } \delta \in S\}.$$

L'application  $V$  est décroissante, et l'on a  $V(0) = K^n$  et  $V(1) = \emptyset$ .

Réciproquement, étant donné un sous-ensemble  $V \subset K^n$ , on appelle *module de  $V$*  et l'on note  $I(V)$  l'ensemble des distorsions affines qui s'annulent sur  $V$ ,

$$I(V) = \{ \delta \in K_\sigma^1[x_1, \dots, x_n, K] : \delta_K(\bar{x}) = 0 \text{ pour tout } x \in V \}.$$

L'ensemble  $I(V)$  est un  $K_\sigma^1[x]$ -sous module à gauche de  $K_\sigma^1[x_1, \dots, x_n, K]$ . L'application  $I$  est décroissante. On a  $I(\emptyset) = K_\sigma^1[x_1, \dots, x_n, K]$ , ainsi que  $I(K^n) = 0$  dès que  $[K : k]$  est infini d'après le résultat d'Amitsur, et

$$V(I(V(S))) = V(S).$$

Remarquer que 1 appartient à  $I(V)$  si et seulement si  $V$  est vide, si et seulement si  $I(V)$  est égal à  $K_\sigma^1[x_1, \dots, x_n, K]$ .

**4.2. Irréductibilité.** Un espace topologique est *irréductible* s'il n'est pas la réunion de deux fermés propres.

**Lemme 4.1.** *Les fermés irréductibles sont précisément les ensembles  $\sigma$ -algébriques.*

*Démonstration.* Soit  $V(S)$  un ensemble  $\sigma$ -algébrique. Si  $V(S) = V(S_1) \cup \dots \cup V(S_m)$ , l'espace affine à gauche  $V(S)$  sur le corps  $C(a)$  est recouvert par une réunion finie de sous-espaces affines. Puisque  $C(a)$  est infini d'après [Lam91, Theorem 13.10], on en déduit que  $V(S)$  est inclus dans l'un des  $V(S_i)$ , donc  $V(S)$  est irréductible. Réciproquement, un fermé irréductible est un ensemble  $\sigma$ -algébrique.  $\square$

**Corollaire 4.2** (Densité). *Si  $\delta \in K_\sigma^1[x_1, \dots, x_n, K]$  s'annule en dehors d'un ensemble  $\sigma$ -algébrique  $V(S)$  propre de  $K^n$ , alors  $\delta$  est nulle.*

**4.3. Nullstellensatz.**

**Théorème 4.3** (Nullstellensatz faible). *Si  $\mathbf{K}$  est  $\sigma$ -algébriquement clos, un module maximal de  $\mathbf{K}_\sigma^1[x_1, \dots, x_n, \mathbf{K}]$  qui ne contient pas 1 est de la forme  $\langle x_1 - a_1, x_2 - a_2, \dots, x_n - a_n \rangle_\sigma$  pour un point  $(a_1, \dots, a_n) \in \mathbf{K}^n$ .*

*Démonstration.* On s'inspire de [Art10] et [Per01]. Si  $n = 1$ , et si  $I$  est un module maximal ne contenant pas 1, alors il existe une unique distorsion affine unitaire de degré minimal appartenant à  $I$ , qui s'écrit  $\delta - b_1$  où  $\delta$  est une distorsion linéaire unitaire et  $b_1 \in \mathbf{K}$ . Montrons que  $I$  est engendré par cet élément. Soit  $\gamma + b_2$  un autre élément de  $I$ , on a  $\gamma = q\delta + r$  avec  $\deg_\sigma(r) < \deg_\sigma(\delta)$ , puis  $\gamma + b_2 = q(\delta - b_1) + r + b_2 + q(b_1)$ , donc  $r + b_2 + q(b_1) \in I$  et  $r = 0$  par minimalité de  $\delta$ . On a donc  $b_2 + q(b_1) = 0$  puisque  $1 \notin I$ , et  $I = \langle \delta - b_1 \rangle$ . Mais puisque  $\mathbf{K}$  est  $\sigma$ -algébriquement clos,  $b_1 = \delta(a_1)$ . Par maximalité de  $I$ , on a  $I = \langle x - a_1 \rangle$ .

Si  $n > 1$ , et si  $x_1, \dots, x_n$  sont tous  $\sigma$ -algébriques sur  $I \cup \mathbf{K}$ , alors pour tout  $i$ , on a  $\delta_i(x_i - a_i) \in I$  pour un certain  $\delta_i$  de degré minimal et  $a_i \in \mathbf{K}$ , et  $I$  est donc contenu dans le module de la forme voulue, auquel il doit être égal par maximalité. Supposons au contraire que  $x_1$  par exemple soit  $\sigma$ -transcendant sur  $I \cup \mathbf{K}$ . On fixe un  $b \in \mathbf{K}$ , et on a  $1 \in \langle x_1 - b, I \rangle$  par maximalité de  $I$  : il existe  $h_b \in \mathbf{K}_\sigma^1[x]$  non nul tel que

$$h(x_1 - b) - 1 \in I,$$

i.e.  $x_1 - b$  est « inversible à gauche » dans  $\mathbf{K}_\sigma^1[x_1, \dots, x_n]/I$ . On peut supposer  $h_b$  de degré  $m$  constant indépendant de  $b$  (sans quoi l'on peut trouver  $b$  et  $c$  tels que  $h_c(x_1 - c) - h_b(x_1 - b)$  est non nul et appartient à  $I$ ). Posons

$$h_b(x) = \sum_{i=0}^m x^{\sigma^i} k_i,$$

d'où

$$h_b(x_1 - b) = \sum_{i=0}^m (x_1 - b)^{\sigma^i} k_i = \sum_{i=0}^m x_1^{\sigma^i} k_i - \sum_{i=0}^m b^{\sigma^i} k_i.$$

Si tous les coefficients sont constants en  $b$ , on a nécessairement pour tout  $b \in \mathbf{K}$ ,

$$\sum_{i=0}^m b^{\sigma^i} k_i = 0,$$

ce qui est impossible si  $a$  est transcendant sur  $k$ .  $\square$

**Corollaire 4.4.** *Supposons  $\mathbf{K}$   $\sigma$ -algébriquement clos et soit  $I$  un module ne contenant pas 1. Alors  $V(I)$  n'est pas vide.*

*Démonstration.* (1) D'après le lemme de Zorn,  $I$  est contenu dans un module maximal  $M$  qui ne contient pas 1, et  $V(M) \subset V(I)$  contient un point d'après le Nullstellensatz.  $\square$

**4.4. Clôture d'un module, composante radicale d'un ensemble algébrique.** Pour tout module  $I$  de  $K_\sigma^1[x_1, \dots, x_n, K]$ , on définit la *clôture de  $I$*  par :

$$\text{cl}(I) = \left\{ f \in K_\sigma^1[x_1, \dots, x_n, K] : \text{il existe } g \in K_\sigma^1[x] \text{ non nulle telle que } g(f) \in I \right\}.$$

On a l'inclusion  $I \subset \text{cl}(I)$ , et  $\text{cl}\{0\} = K$ . On dit que  $I$  est *clos* si  $I + K = \text{cl}(I)$ , et que  $V(I)$  est *radical* si  $I$  est clos.

**Lemme 4.5.**  *$\text{cl}(I)$  est un module de  $K_\sigma^1[x_1, \dots, x_n, K]$  et  $\text{cl}(\text{cl}(I)) = \text{cl}(I)$ .*

*Démonstration.* C'est une conséquence immédiate du corollaire 2.13 puisque  $\text{cl}(I)$  est précisément l'ensemble des éléments de  $K_\sigma^1[x_1, \dots, x_n, K]$  qui sont  $\sigma$ -algébriques sur  $I$ .  $\square$

Si  $I$  est un module de  $K_\sigma^1[x_1, \dots, x_n]$ , le quotient  $K_\sigma^1[x_1, \dots, x_n, K]/I$  est naturellement muni d'une structure de  $K_\sigma^1[x_1, \dots, x_n]$ -module à gauche. On dit que le quotient est *simple* si ses seuls sous-modules sont  $\{0\}$  et  $K_\sigma^1[x_1, \dots, x_n]/I$ .

**Lemme 4.6.** *Soit  $I$  un module de  $K_\sigma^1[x_1, \dots, x_n, K]$ .*

- (1)  *$I$  est maximal si et seulement si  $K_\sigma^1[x_1, \dots, x_n, K]/I$  est simple.*
- (2)  *$I$  est clos si et seulement si pour tout  $\bar{\delta} \in K_\sigma^1[x_1, \dots, x_n]/I$  non nul et  $\gamma \in K_\sigma^1[x]$  non nul,  $\gamma(\bar{\delta})$  est non nul.*

*Démonstration.* (1) Si  $I$  est maximal, soit  $\pi : K_\sigma^1[x_1, \dots, x_n] \rightarrow K_\sigma^1[x_1, \dots, x_n]/I$  la projection canonique, et  $M$  un  $K_\sigma^1[x_1, \dots, x_n]$ -sous-module de  $K_\sigma^1[x_1, \dots, x_n]/I$  non nul. Alors  $\pi^{-1}(M)$  est un idéal à gauche de  $K_\sigma^1[x_1, \dots, x_n]$  contenant  $I$  proprement, donc  $\pi^{-1}(M) = K_\sigma^1[x_1, \dots, x_n]$ , d'où  $M = K_\sigma^1[x_1, \dots, x_n]/I$ . Réciproquement, si  $I$  n'est pas maximal, soit  $J$  un idéal à gauche proprement compris entre  $I$  et  $K_\sigma^1[x_1, \dots, x_n]$ . Dans ce cas,  $J/I$  est un sous-module de  $K_\sigma^1[x_1, \dots, x_n]/I$  non trivial.  $\square$

**Théorème 4.7** (Nullstellensatz). *Si  $\mathbf{K}$  est  $\sigma$ -algébriquement clos, on a pour tout module  $J$  qui ne contient pas 1, on a*

$$I(V(J)) \subset \text{cl}(J).$$

*Si  $I \subset J$  est une inclusion propre de modules clos ne contenant pas 1, l'inclusion  $V(J) \subset V(I)$  est propre.*

*Démonstration.*  $\mathbf{K}_\sigma^1[x_1, \dots, x_n, \mathbf{K}]$  est un module à gauche de type fini sur l'anneau noethérien à gauche  $\mathbf{K}_\sigma^1[x]$ , donc  $J$  est finiment engendré. Soit  $\delta_1, \dots, \delta_r$  une famille génératrice finie de  $J$ . Soit  $\delta \in I(V(J))$ . On pose  $L = \langle \delta_1, \dots, \delta_r, \delta + 1 \rangle_\sigma$ . Si  $x \in V(L)$ , alors  $x \in V(J)$ , donc  $\delta(x) = 0$ . Mais on a aussi  $\delta(x) + 1 = 0$ , une contradiction, donc l'ensemble  $V(L)$  est vide. D'après le corollaire 4.4,  $L$  contient 1 et il existe  $h_1, \dots, h_r$  et  $h$  tels que

$$1 = h(\delta + 1) + h_1\delta_1 + \dots + h_r\delta_r.$$

$h$  est non nul puisque  $J$  ne contient pas 1. En appliquant l'égalité à un point de  $V(J)$ , qui est non vide puisque  $J$  est propre et d'après le corollaire 4.4, on a nécessairement  $h(1) = 1$ , d'où  $h\delta \in J$ , c'est-à-dire  $\delta \in \text{cl}(J)$ .

Si  $J$  est un module clos ne contenant pas 1, on en déduit  $I(V(J)) \subset J + K$  et donc  $I(V(J)) = J$ .  $\square$

**4.5. Morphismes, comorphismes.** Étant donné un ensemble  $\sigma$ -algébrique  $V \subset K^n$ , on définit

$$\Gamma_\sigma[V] = K_\sigma^1[x_1, \dots, x_n, K]/I(V)$$

le  $K_\sigma^1[x]$ -module quotient.

**Définition 4.8** ( $\sigma$ -Morphisme,  $\sigma$ -comorphisme). Soient  $U \subset K^n$  et  $V \subset K^m$  deux ensembles algébriques. On appelle  $\sigma$ -morphisme toute application  $f : U \rightarrow V$  dont les applications coordonnées  $f_1, \dots, f_m$  sont des distortions affines. On appelle  $\sigma$ -comorphisme de  $f$  le morphisme de  $K_\sigma^1[x]$ -modules

$$f^* : \Gamma_\sigma[V] \longrightarrow \Gamma_\sigma[U], \quad \delta + I(V) \mapsto \delta \circ f + I(U)$$

*Remarque 4.9.* Un  $\sigma$ -comorphisme  $f^* : \Gamma_\sigma[V] \rightarrow \Gamma_\sigma[U]$  est un morphisme de  $\sigma$ -espaces au sens de 6.5 : pour toute distortion  $\delta$  de  $K_\sigma^1[x_1, \dots, x_n]$  et  $e_1, \dots, e_n$  de  $K_\sigma^1[x_1, \dots, x_n, K]$ , on a  $f^* \circ \delta_{\Gamma[V]}(e_1 + I(V), \dots, e_n + I(V)) = f^*(\delta(e_1, \dots, e_n) + I(V)) = \delta(e_1, \dots, e_n) \circ f + I(U)$ , et

$$\delta_{\Gamma[U]} \circ f^*(e_1 + I(V), \dots, e_n + I(V)) = \delta_{\Gamma[U]}(e_1 \circ f + I(U), \dots, e_n \circ f + I(U))$$

**Définition 4.10** ( $\sigma$ -Morphisme dominant). Un  $\sigma$ -morphisme est *dominant* si son image  $f(U) \subset V$  est dense dans  $V$  pour la topologie de Zariski. C'est un  $\sigma$ -isomorphisme s'il est bijectif et si son inverse est un  $\sigma$ -morphisme.

**Lemme 4.11.** *Un morphisme  $f : U \rightarrow V$  est dominant si et seulement si son comorphisme  $f^* : \Gamma_\sigma[V] \rightarrow \Gamma_\sigma[U]$  est injectif.*

*Démonstration.* On a

$$I(f(U)) = \left\{ \gamma \in \Gamma_\sigma[K^m] : \gamma_K(f(U)) = 0 \right\} = \left\{ \gamma : f^*(\gamma)(U) = 0 \right\} = \left\{ \gamma : f^*(\gamma) \in I(U) \right\},$$



donc  $I(f(U))/I(V)$  est égal à  $\text{Ker } f^*$ . Donc  $f^*$  est injective si et seulement si  $I(f(U)) \subset I(V)$ , c'est-à-dire si et seulement si  $V(I(f(U))) = \overline{f(U)} = V$ .  $\square$

## 5. TOPOLOGIE TORDUE DE ZARISKI SUR $K^n$

Soit  $K$  un corps non commutatif de centre  $k$  tel que  $[K : k]$  soit infini, soit  $a$  un élément hors du centre, et  $\sigma$  la conjugaison par  $a$ . On appelle *fermé de base de  $K^n$*  un sous-ensemble

$$V(\delta) = \{(x_1, \dots, x_n) \in K^n : \delta_K(x_1, \dots, x_n) = 0\}$$

où  $\delta \in K_\sigma^1[x_1, \dots, x_n, K]$  est une distorsion affine de  $K^n$ . On considère sur  $K^n$  la topologie  $\tau_\sigma$ , dont les fermés de base constituent une base de fermés. Nous l'appellerons *topologie tordue de Zariski*. Dans le cas particulier où  $K$  est commutatif et algébriquement clos,  $\tau_\sigma$  correspond à la topologie de Zariski sur  $K^1$ , mais par sur  $K^n$  pour  $n \geq 2$ , puisque l'on ne considère pas les variétés définies par des polynômes irréductibles non linéaires. Cette topologie est en ce sens assez grossière. Une distorsion étant  $C(a)$ -linéaire à gauche, un fermé de base non vide a une structure de  $C(a)$ -espace affine à gauche.

**5.1. Topologie sur la droite  $K^1$ .** Si  $K$  est commutatif, ses fermés sont les ensembles finis de points. Il en va différemment si  $K$  est non commutatif et  $a$  hors du centre. Les fermés propres irréductibles sont de deux types, donnés soit par

$$x = b,$$

qui correspond au singleton  $\{b\}$ , soit par une équation

$$xk_\ell + x^\sigma k_{\ell-1} + \dots + x^{\sigma^\ell} k_0 = b.$$

Un cas particulier, l'équation

$$(2) \quad xk_\ell + x^{\sigma^\ell} = b,$$

qui correspond à l'ensemble vide ou à l'espace affine  $\alpha + C(a^\ell)\beta$  de  $C(a)$ -dimension finie au plus  $\ell$ , le point  $\alpha$  étant une solution particulière de (2), et  $\beta$  une solution particulière non nulle de l'équation homogène associée  $xk_\ell + x^{\sigma^\ell} = 0$  (voir aussi [Coh95, p. 408]).

**Lemme 5.1** (Fermés de  $K$ ). *Un fermé propre de  $K$  est une réunion finie de  $C(a)$ -espaces affines à gauche de dimensions finies. Si  $\mathbf{K}$  est  $\sigma$ -algébriquement clos, les fermés propres de  $\mathbf{K}$  sont les réunions finies de  $C_{\mathbf{K}}(a)$ -espaces affines à gauche de dimension finie.*

*Démonstration.* La première assertion est une conséquence immédiate du lemme 1.6.(1). Réciproquement, pour tout  $k_0 \in K$ , l'ensemble  $C(a)k_0$  est l'ensemble des racines de  $x^a - xk_0^{-1}k_0^\sigma$ , donc c'est un fermé de  $K$ . L'application de  $\alpha_K : K^n \rightarrow K$  définie par

$$C(a)k_1 \times \dots \times C(a)k_n \rightarrow C(a)k_1 + \dots + C(a)k_n, (x_1, \dots, x_n) \mapsto x_1 + \dots + x_n$$

est un  $\sigma$ -morphisme de groupes, donc, si  $\mathbf{K}$  est  $\sigma$ -algébriquement clos, l'image de  $\alpha_{\mathbf{K}}$  est fermée d'après le corollaire 3.7, de même que chacun de ses translatés.  $\square$

**Corollaire 5.2.** *La topologie tordue de Zariski sur  $K$  est noethérienne.*

5.2. **Topologie sur  $K^n$ .** Au dessus d'un corps commutatif, un fermé de Zariski ne coupe une droite propre qu'en un nombre fini de points. Ici :

**Corollaire 5.3** (Intersection d'une droite et d'un fermé de  $K^n$ ). *Soit  $F$  un fermé de  $K^n$  et  $L$  une droite affine à gauche de  $K^n$ , propre dans  $F$ . Alors  $L$  coupe  $F$  en une réunion finie de  $C(a)$ -espaces affines de dimensions finies.*

*Démonstration.* Il suffit de montrer que pour un fermé de base  $V(\delta)$  défini par l'application

$$(3) \quad \delta(x_1, \dots, x_n) = \sum_{i=0}^{\ell} x_1^{\sigma^i} k_{1,i} + \dots + \sum_{i=0}^{\ell} x_n^{\sigma^i} k_{n,i} = \alpha,$$

soit l'espace vectoriel  $V(\delta) \cap L$  est de dimension finie sur  $C(a)$ , soit  $L \subset V(\delta)$ . Supposons  $V(\delta) \cap L$  non vide. La droite  $L$  est une intersection de  $n - 1$  hyperplans à gauche d'équation du type  $x_1 \alpha_1 + \dots + x_n \alpha_n = \alpha_{n+1}$  avec  $(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$  dans  $K^{n+1}$ , de sorte que l'on peut exprimer chaque coordonnée d'un point  $(x_1, \dots, x_n)$  de  $L$  comme  $x_i = x_1 \beta_i + \beta_{n+1}$ . En remplaçant dans (3), on obtient une équation de la forme

$$x c_{\ell} + x^{\sigma} c_{\ell-1} + \dots + x^{\sigma^{\ell}} c_0 = \beta,$$

et on conclut comme précédemment.  $\square$

**Lemme 5.4.** *Tout  $K$ -espace affine à gauche est fermé.*

**Lemme 5.5.** *L'espace topologique  $K^n$  est noethérien.*

*Démonstration.* À une suite décroissante d'ensembles  $\sigma$ -algébriques  $V(I_1) \supset V(I_2) \supset V(I_3) \dots$  correspond une suite croissante de modules  $I_1 \subset I_2 \subset I_3 \dots$  de  $K_{\sigma}^1[x_1, \dots, x_n, K]$ , qui est un module noethérien, donc les deux suites stationnent. Un fermé de Zariski étant une réunion finie d'ensembles  $\sigma$ -algébriques, on conclut facilement.  $\square$

## 6. DIMENSION DE ZARISKI

6.1. **Dimension et hypersurface.** On considère  $\mathbf{K}$  un corps  $\sigma$ -algébriquement clos.

**Définition 6.1** (Dimension de Zariski). On définit la *dimension de Zariski d'un ensemble algébrique*  $V \subset \mathbf{K}^n$  par  $\dim(V) = -1$  si  $V$  est vide, et sinon

$$\dim(V) = \begin{cases} -1 & \text{si } V \text{ est vide} \\ \dim_{\sigma} \Gamma_{\sigma}[V] = n - \dim_{\sigma} I(V) & \text{sinon.} \end{cases}$$

*Remarques 6.2.* (1)  $\mathbf{K}$  est de dimension 1. Si  $a$  n'est pas dans le centre,  $C_{\mathbf{K}}(a)$  ainsi que tous les fermés propres de  $\mathbf{K}$  considérés précédemment sont de dimension 0.

(2) L'espace  $\mathbf{K}^n$  est de dimension  $n$  et ses singletons de dimensions 0.

(3) La dimension est croissante : si  $F \subset G$  sont deux fermés irréductibles,  $\dim F \leq \dim G$ .

**Théorème 6.3** (Section par une hypersurface). *Soit  $V \subset \mathbf{K}^n$  un ensemble  $\sigma$ -algébrique, et  $\delta$  une distorsion de  $\mathbf{K}_{\sigma}^1[x_1, \dots, x_n, \mathbf{K}]$ .*

*Si  $\delta$  est dans la clôture de  $I(V)$ , et si  $V \cap V(\delta)$  n'est pas vide, alors*

$$\dim V \cap V(\delta) = \dim V.$$

Si  $\delta$  n'est pas dans la clôture de  $I(V)$ , et si  $V \cap V(\delta)$  n'est pas vide,

$$\dim V \cap V(\delta) = \dim V - 1.$$

En particulier, si  $\delta \notin \mathbf{K}$ ,

$$\dim V(\delta) = n - 1.$$

*Démonstration.* Si  $\delta \in \text{cl}(I(V))$ , et si  $V \cap V(\delta)$  n'est pas vide, 1 n'appartient pas à  $\langle I(V), \delta \rangle_\sigma$ . D'après le Nullstellensatz et le lemme 4.5, on a donc

$$I(V) \subset I(V \cap V(\delta)) = IV(I(V), \delta) \subset \text{cl}(I(V) \cup \{\delta\}) = \text{cl}(I(V)).$$

D'après le lemme 2.13, on a  $\dim_\sigma I(V) = \dim_\sigma \text{cl}(I(V))$ , d'où la première égalité.

Supposons  $\delta \notin \text{cl}(I(V))$  et posons  $\dim V = d$ . Supposons  $\dim V \cap V(\delta) \geq d$  et soient  $\delta_1, \dots, \delta_p$  dans  $\mathbf{K}_\sigma^1[x_1, \dots, x_n, \mathbf{K}]$  tels que  $\delta_1 + I(V \cap V(\delta)), \dots, \delta_d + I(V \cap V(\delta))$  soient  $\sigma$ -libres. La famille  $(\delta_1 + I(V), \dots, \delta_d + I(V), \delta + I(V))$  est  $\sigma$ -liée donc il existe une distorsion  $g \in \mathbf{K}^1[x_1, \dots, x_{d+1}]$  non nulle telle que  $g(\delta_1, \dots, \delta_d, \delta) \in I(V)$ . Si  $g$  ne met en jeu que la variable  $x_{d+1}$ , elle est du type  $h(x_{d+1})$  pour une certaine distorsion  $h \in \mathbf{K}^1[x_{d+1}]$  non nulle, et dans ce cas  $h(\delta) \in I(V)$  d'où  $\delta \in \text{cl}(I(V))$ , une contradiction. La distorsion  $g(x_1, \dots, x_d, 0)$  est donc non nulle, mais on a également

$$g(\delta_1, \dots, \delta_d, 0) \in -g(0, \dots, 0, \delta) + I(V) \subset I(V \cap V(\delta))$$

ce qui contredit la liberté de  $\delta_1 + I(V \cap V(\delta)), \dots, \delta_p + I(V \cap V(\delta))$ . On a donc montré

$$\dim V \cap V(\delta) \leq d - 1.$$

Réciproquement, si  $V \cap V(\delta)$  n'est pas vide (en particulier, 1 n'appartient pas à  $\langle I(V), \delta \rangle_\sigma$ ), on considère une famille  $\delta_1 + I(V), \dots, \delta_d + I(V)$   $\sigma$ -libre et on cherche à montrer qu'il existe un entier  $i \in \{1, \dots, d\}$  telle que la seule distorsion  $\gamma$  vérifiant

$$\gamma(\delta_1, \dots, \delta_{i-1}, \delta_{i+1}, \dots, \delta_d) \in I(V \cap V(\delta))$$

soit la distorsion nulle (on en déduit alors que  $\delta_1 + I(V \cap V(\delta)), \dots, \delta_{i-1} + I(V \cap V(\delta)), \delta_{i+1} + I(V \cap V(\delta)), \dots, \delta_d + I(V \cap V(\delta))$  est  $\sigma$ -libre d'où  $\dim V(I) \cap V(\delta) \geq d - 1$ ). Supposons au contraire que pour tout  $i \in \{1, \dots, d\}$ , il existe une distorsion non nulle  $\gamma_i$  telle que

$$\gamma_i(\delta_1, \dots, \delta_{i-1}, \delta_{i+1}, \dots, \delta_d) \in I(V \cap V(\delta)).$$

Étant non nulle,  $\gamma_1$  met en jeu au moins un  $\delta_i$ , disons  $\delta_2$ , qui est  $\sigma$ -algébrique sur  $\{\delta_3, \dots, \delta_d\} \cup IV(I(V), \delta)$ , donc sur  $\{\delta_3, \dots, \delta_d\} \cup \text{cl}(I(V) \cup \{\delta\})$  d'après le Nullstellensatz. Mais  $\gamma_2$  nous indique qu'il existe  $\gamma \neq 0$  telle que

$$\gamma\gamma_2(\delta_1, \delta_3, \dots, \delta_d) \in \langle I(V), \delta \rangle_\sigma$$

. On en déduit que  $\delta$  est algébrique sur  $\{\delta_1, \delta_3, \dots, \delta_d\} \cup I(V)$ . Par transitivité,  $\delta_2$  est algébrique sur  $\{\delta_1, \delta_3, \dots, \delta_d\} \cup I(V)$ , une contradiction, ce qui montre la deuxième égalité.

Si  $\delta \notin \mathbf{K}$ , alors  $\delta \notin \text{cl}\{0\}$ . D'autre part,  $V(\delta)$  n'est pas vide puisque  $\mathbf{K}$  est  $\sigma$ -algébriquement clos. On conclut avec l'égalité précédente appliquée à  $V = \mathbf{K}^n$  et  $I(V) = \{0\}$ .  $\square$

**Corollaire 6.4.** Soient  $V \subset W$  deux ensembles algébriques distincts de  $\mathbf{K}^n$ .

(1) Si  $W$  est radical et non vide, on a  $\dim V < \dim W$ .

(2) Si  $J$  est un module vérifiant  $I(V) \subset J \subset \text{cl}(I(V))$  et  $1 \notin J$ , on a  $\dim V(J) = \dim V$ .

**Théorème 6.5** (Définitions équivalentes de la dimension). *La dimension de Zariski d'un ensemble algébrique  $V \subset \mathbf{K}^n$  non vide est égale*

- (1) à la longueur maximale d'une chaîne  $I_0 \subset I_1 \subset \dots \subset I_d$  de modules de  $\mathbf{K}_\sigma^1[x_1, \dots, x_n, \mathbf{K}]$  ne contenant pas 1 qui soient clos et distincts, avec  $I(V) \subset I_0$ ,
- (2) à la longueur maximale d'une chaîne  $V_0 \subset V_1 \subset \dots \subset V_d$  d'ensembles algébriques radicaux distincts et non vides de  $\mathbf{K}^n$  avec  $V_d \subset V$ .
- (3) au nombre minimal de distorsions  $\delta_1, \dots, \delta_d$  de  $\mathbf{K}_\sigma^1[x_1, \dots, x_n, \mathbf{K}]$  nécessaires pour que  $V \cap V(\delta_0, \dots, \delta_d)$  soit de dimension 0.

*Démonstration.* (1) Montrons l'équivalence de (1) et (2). Si (2) nous donne une chaîne d'ensembles  $\sigma$ -algébriques radicaux  $V_0, \dots, V_d$ , alors les modules de la chaîne correspondante  $I(V_0), \dots, I(V_d)$  sont clos et distincts et ne contiennent pas 1. Réciproquement, si l'on a une chaîne  $I_0, \dots, I_d$  de modules clos donnée par (1), on considère la chaîne des variétés correspondante  $V(I_0), \dots, V(I_d)$ . Elle est constituée de variétés distinctes et radicale d'après le théorème 4.7, et non vide d'après le corollaire 4.4.

(2) Montrons que  $\dim V \leq d$  en construisant une chaîne comme en (2) de longueur  $m = \dim V$ . Si  $m = 0$ , on choisit un module  $J$  maximal ne contenant pas 1 et vérifiant  $I(V) \subset J \subset \text{cl}(I(V))$ .  $J$  est donc clos et la chaîne  $V(J)$  est maximale d'après le corollaire 6.4.1. Si  $m > 0$ , on choisit  $J$  comme ci-dessus et l'on pose  $V_m = V(J)$ . On a  $\dim V_m > 0$  et  $\dim_\sigma \text{cl}(I(V_m)) < n$  d'après le lemme 2.13. D'après le théorème 4.3, il existe  $\delta \in \mathbf{K}_\sigma^1[x_1, \dots, x_n, \mathbf{K}] \setminus \text{cl}(I(V_m))$  tel que  $\langle \delta, I(V_m) \rangle_\sigma$  ne contienne pas 1. L'ensemble  $V_{m-1} = V_m \cap V(\delta)$  n'est donc pas vide, et l'on a  $\dim V_{m-1} = m - 1$  d'après le théorème 6.3. On finit par récurrence.

Réciproquement, si (2) nous donne une chaîne d'ensembles algébriques radicaux de longueur  $d$ , montrons par induction sur  $i$  que pour tout  $i \leq d$ , on a  $\dim V_i = i$ . Pour  $i = 0$ , le module  $I(V_0)$  est maximal ne contenant pas 1 donc  $\dim V_0 = 0$  d'après le théorème 4.3. Si  $\dim V_i = i$ , soit  $\delta \in I(V_i) \setminus I(V_{i+1})$  et soit  $V' = V_{i+1} \cap V(\delta)$ . On a  $\dim V' = \dim V_{i+1} - 1$  d'après le théorème 6.3. Si  $V'$  est radical, il est égal à  $V_i$  par maximalité de la chaîne, et  $\dim V_{i+1} = i + 1$ . Si  $V'$  n'est pas radical, on peut choisir un module maximal  $J$  ne contenant pas 1 et vérifiant  $I(V') \subset J \subset \text{cl}(I(V'))$ , de sorte que  $V(J)$  est clos et vérifie  $V_i \subset V(J) \subset V' \subset V_{i+1}$ . On a  $V_i = V(J)$  par maximalité de la chaîne, et  $\dim V(J) = \dim V'$  d'après le corollaire 6.4.2, d'où  $\dim V_{i+1} = i + 1$ . Ceci montre que  $\dim V_d = d$ , et donc  $\dim V \geq d$ .

(3) Si  $V = V(S)$  est de dimension  $d$  (avec  $S$  une base de  $I(V)$ ), d'après le théorème 6.3, il faut exactement  $d$  distorsions  $\delta_1, \dots, \delta_d$  pour que  $V \cap V(\delta_1, \dots, \delta_d)$  soit de dimension 0. On peut effectivement trouver de telles distorsions en procédant comme ci-dessus.  $\square$

**Lemme 6.6** (Dimension d'un produit). *Soient  $V \subset \mathbf{K}^n$  et  $W \subset \mathbf{K}^m$  deux ensembles  $\sigma$ -algébriques non vides. Alors  $V \times W \subset \mathbf{K}^{n+m}$  est un ensemble  $\sigma$ -algébrique, et*

$$\dim V \times W = \dim V + \dim W.$$

*Démonstration.* Si  $V = V(\delta_1(\bar{x}), \dots, \delta_n(\bar{x}))$  et  $W = V(\gamma_1(\bar{y}), \dots, \gamma_m(\bar{y}))$ , alors

$$V \times W = V(\delta_1(\bar{x}), \dots, \delta_n(\bar{x}), \gamma_1(\bar{y}), \dots, \gamma_m(\bar{y})),$$

et l'on a  $I(V \times W) = I(V) \oplus I(W)$  dès que  $I(V)$  et  $I(W)$  ne contiennent pas 1, donc  $\dim_\sigma I(V \times W) = \dim_\sigma I(V) + \dim_\sigma I(W)$  d'après le lemme 2.11, c'est-à-dire

$$n + m - \dim(V \times W) = n - \dim V + m - \dim W. \quad \square$$

**6.2. Groupes  $\sigma$ -algébriques.** On note  $\mathbf{G}_{\mathbf{a},\sigma}^n$  le groupe additif de  $\mathbf{K}^n$ . On appelle *groupe  $\sigma$ -algébrique* tout ensemble  $\sigma$ -algébrique de la forme  $V(S)$  où  $S$  est un ensemble fini de distortions linéaires. On note  $\text{cl}(S)$  la clôture de  $S$  dans  $\mathbf{K}_\sigma^1[x_1, \dots, x_n]$ . Étant donné  $G \subset \mathbf{G}_{\mathbf{a},\sigma}^n$  un groupe algébrique, on note

$$G^0 = V(\text{cl}(S)),$$

que l'on appelle *composante radicale* de  $G$ . Le groupe  $G^0$  est bien défini, indépendamment de  $S$  puisque l'on a  $S \subset I(V)$ , et  $\text{cl}(S) \subset \text{cl}(I(V))$  d'où  $V(\text{cl}(I(V))) \subset V(\text{cl}(S))$ . Ces deux groupes étant radicaux et de même dimension  $\dim V$  d'après le théorème 6.3, ils sont égaux d'après le corollaire 6.4.1.

**Lemme 6.7** (Composante radicale). *Le groupe  $G^0$  est l'intersection de tous les sous-groupes algébriques de  $G$  de dimension  $\dim G$ , et on a*

$$\dim G^0 = \dim G,$$

et  $G/G^0$  est un  $C_{\mathbf{K}}(a)$ -espace vectoriel à gauche de dimension finie.

*Démonstration.*  $G^0$  est un groupe algébrique puisque  $\mathbf{K}^n$  est noethérien. Les deux premières assertions résultent du théorème 6.3. Pour la dernière assertion, il suffit de montrer que s'il existe une distortion  $n$ -linéaire  $\delta \in \text{cl}(I(G))$ , alors  $G/G \cap V(\delta)$  est un  $C_{\mathbf{K}}(a)$ -espace vectoriel à gauche de dimension finie. Soit donc  $\gamma \in \mathbf{K}_\sigma^1[x]$  non nulle de degré  $m$  telle que  $\gamma\delta \in I(G)$ . Soient  $g_0, \dots, g_m$  dans  $G$ . On a donc  $\gamma_{\mathbf{K}}(\delta_{\mathbf{K}}(g_i)) = 0$  pour tout  $i$ . D'après le lemme 1.6, il existe une combinaison  $C(a)$ -linéaire non triviale  $\lambda_0\delta_{\mathbf{K}}(g_0) + \dots + \lambda_n\delta_{\mathbf{K}}(g_m) = 0$ , donc  $\lambda_0g_0 + \dots + \lambda_n g_n \in G \cap V(\delta)$ . On en déduit que  $\dim_{C_{\mathbf{K}}(a)} G/G \cap V(\delta)$  vaut au plus  $m$ .  $\square$

### 6.3. Morphismes et dimension.

**Théorème 6.8.** *Soit  $V \subset \mathbf{K}^n$  un ensemble  $\sigma$ -algébrique et  $f : V \rightarrow \mathbf{K}^m$  un  $\sigma$ -morphisme.*

- (1) *Alors  $f(V)$  est un ensemble  $\sigma$ -algébrique, et  $\dim V \geq \dim f(V)$ .*
- (2) *Si  $f : V \rightarrow f(V)$  est un  $\sigma$ -isomorphisme, alors  $\dim V = \dim f(V)$ .*
- (3) *Si les fibres de  $f$  sont de dimension au plus  $r$ ,  $\dim f(V) \geq \dim V - r$ .*

*Démonstration.* (1)  $f(V)$  est fermé d'après le théorème de Chevalley-Cohn. L'image d'un irréductible par une application continue étant irréductible, l'ensemble  $f(V)$  est un fermé irréductible d'après le lemme 4.1, donc un ensemble  $\sigma$ -algébrique. Considérons la restriction  $f : V \rightarrow f(V)$ . C'est un  $\sigma$ -morphisme dominant, donc son  $\sigma$ -comorphisme  $f^* : \Gamma_\sigma[f(V)] \rightarrow \Gamma_\sigma[V]$  est injectif d'après le lemme 4.11, ce qui implique  $\dim f(V) \leq \dim V$  d'après le lemme 2.14.

(2) Procède de (1).

(3) D'après le théorème 6.5.3, il existe  $\delta_1, \dots, \delta_s$  dans  $\mathbf{K}_\sigma^1[x_1, \dots, x_m, \mathbf{K}]$  telles que

$$\dim(V(\delta_1, \dots, \delta_s) \cap f(V)) = 0,$$

avec  $s = \dim f(V)$ . Le module engendré par  $\delta_1, \dots, \delta_s$  et  $I(f(V))$  ne contient pas 1. Il est contenu dans un module maximal  $J$  ne contenant pas 1. D'après le théorème 4.3, il existe un point  $y \in f(V)$  tel que

$$\{y\} = V(J).$$

Puisque  $J$  est finiment engendré, il existe  $\alpha_1, \dots, \alpha_p$  dans  $\text{cl}(\delta_1, \dots, \delta_s, I(f(V)))$  tels que

$$J = \langle \delta_1, \dots, \delta_s, I(f(V)), \alpha_1, \dots, \alpha_p \rangle_\sigma.$$

Soit  $X$  le fermé  $f^{-1}(y)$ , soit  $\delta_i^* = \delta_i \circ f$  et  $\alpha_i^* = \alpha_i \circ f$ . On a

$$X = V(\delta_1^*, \dots, \delta_s^*, \alpha_1^*, \dots, \alpha_p^*) \cap V,$$

et  $\{\alpha_1^*, \dots, \alpha_p^*\} \subset \text{cl}(\delta_1^*, \dots, \delta_s^*, I(V))$ . On déduit du théorème 6.3 que

$$\dim X \geq \dim V - s.$$

D'autre part, on a  $\dim X \leq r$  par hypothèse, d'où  $\dim f(V) \geq \dim V - r$ .  $\square$

**Théorème 6.9** (de Ax-Grothendieck). *Soit  $f : \mathbf{K}^n \rightarrow \mathbf{K}^n$  un  $\sigma$ -morphisme. Si les fibres de  $f$  sont de dimension zéro,  $f$  est surjectif.*

*Première démonstration.* L'image  $f(G)$  est un ensemble algébrique de  $\mathbf{K}^n$  d'après le théorème 6.8.1. Il est de dimension  $n$  d'après le théorème 6.8.(3). Puisque  $\mathbf{K}^n$  est radical,  $f(\mathbf{K}^n) = \mathbf{K}^n$  d'après le corollaire 6.4.1.  $\square$

## 7. SOUS-GROUPES FERMÉS IRRÉDUCTIBLES DE $\mathbf{G}_{\mathbf{a},\sigma}^n$

$K$  est toujours un corps non-commutatif, et  $\sigma$  la conjugaison par un élément hors du centre. On considère  $\mathbf{K}/K$  une extension  $\sigma$ -algébriquement close de centre  $k$ . On note  $\mathbf{G}_{\mathbf{a},\sigma}^n$  le groupe additif de  $\mathbf{K}^n$ . On cherche à classer les sous-groupe  $\sigma$ -algébriques de  $\mathbf{G}_{\mathbf{a},\sigma}^n$ , à  $\sigma$ -isomorphisme près. On s'inspire de [Hum75, Theorem 20.5].

**Lemme 7.1.** *Soit un entier  $n \geq 1$ , un sous-groupe  $G \subset \mathbf{G}_{\mathbf{a},\sigma}^{n+1}$ . Si  $G = V(\delta)$  pour une distorsion non nulle à coefficients dans  $K$ , il existe un  $\sigma$ -automorphisme  $\alpha_{\mathbf{K}}$  de  $\mathbf{G}_{\mathbf{a},\sigma}^{n+1}$  à coefficients dans  $K$  tel que  $\delta_{\mathbf{K}} \circ \alpha_{\mathbf{K}}$  s'annule sur  $\{0\} \times \mathbf{G}_{\mathbf{a},\sigma}^n$ . De plus, si  $\mathbf{d} = (0, \dots, 0, \mathbf{d}_{n+1})$  est un point de  $G$ , on peut choisir  $\alpha$  tel que  $\alpha_{\mathbf{K}}(\mathbf{d}) = \mathbf{d}$ .*

*Démonstration.* On traite le cas  $n = 1$ , le cas général étant similaire. Soit

$$\delta(x, y) = \sum_{i=1}^m x^{\sigma^i} k_i + \sum_{j=1}^{\ell} y^{\sigma^j} h_j.$$

On appelle *partie principale* de  $\delta$  le polynôme  $x^{\sigma^m} k_m + y^{\sigma^\ell} h_\ell$ . On montre le résultat par induction sur  $m + \ell$ . Si  $m + \ell = 0$ , alors  $\delta(x, y) = xa + yb$ . Si  $a = 0$ , on pose  $\alpha = id$ ; si  $b = 0$  (auquel cas le point  $\mathbf{d}$  est nul), on pose  $\alpha(x, y) = (y, x)$ . Si  $ab \neq 0$ , en posant

$$(x, y) = (ua^{-1} - vba^{-1}, v) = \alpha(u, v),$$

on a

$$\delta \circ \alpha(u, v) = \delta(x, y) = u,$$

donc  $\delta_{\mathbf{K}} \circ \alpha_{\mathbf{K}}$  s'annule sur  $\{0\} \times \mathbf{G}_{\mathbf{a},\sigma}^1$ , et  $\alpha_{\mathbf{K}}(\mathbf{d}) = \mathbf{d}$ .

Cas général, si  $m + \ell > 0$ , on ne perd rien à supposer  $m \geq \ell$  d'où  $m > 0$ . On peut trouver  $(a, b) \in K^2$  non nul annulant la partie principale de  $\delta$ . On peut supposer  $a \neq 0$  par exemple. On pose

$$(x, y) = (ua, v + u^{\sigma^{m-\ell}}b) = \alpha(u, v).$$

On a bien  $\alpha_K(\mathbf{d}) = \mathbf{d}$ , et

$$\begin{aligned} \delta(x, y) &= x^{\sigma^m}k_m + y^{\sigma^\ell}h_\ell + (\text{termes de degré} < m). \\ &= (ua)^{\sigma^m}k_m + (v + u^{\sigma^{m-\ell}}b)^{\sigma^\ell}h_\ell + (\text{termes de degré} < m). \\ &= u^{\sigma^m}a^{\sigma^m}k_m + v^{\sigma^\ell}h_\ell + u^{\sigma^m}b^{\sigma^\ell}h_\ell + (\text{termes de degré} < m). \\ &= v^{\sigma^\ell}h_\ell + (\text{termes de degré} < m). \end{aligned}$$

On applique l'hypothèse d'induction à  $\delta \circ \alpha$ . □

**Théorème 7.2** (Sous-groupes algébriques radicaux). *Soit  $G \subset \mathbf{G}_{\mathbf{a},\sigma}^n$  un sous-groupe algébrique radical de dimension  $\ell \geq 1$  tel que  $G = V(\delta_1, \dots, \delta_{n-\ell})$  et tel que  $V(\delta_1, \dots, \delta_i)$  soit radical pour tout  $i \in \{1, \dots, n - \ell\}$ . Alors  $G$  est  $\sigma$ -isomorphe à  $\mathbf{G}_{\mathbf{a},\sigma}^\ell$ . De plus, si  $\mathbf{d} = (0, \dots, 0, \mathbf{d}_n)$  est un point de  $G$ , on peut choisir un  $\sigma$ -isomorphisme  $\alpha_K : G \rightarrow \mathbf{G}_{\mathbf{a},\sigma}^\ell$  tel que  $\alpha_K(\mathbf{d}) = (0, \dots, 0, \mathbf{d}_n)$ .*

*Démonstration.* On traite seulement le cas  $\ell = 1$ . On procède par récurrence sur  $n$ . Si  $n = 1$ , le groupe  $G$  est égal à  $\mathbf{G}_{\mathbf{a},\sigma}^1$  d'après le corollaire 6.4.1. Si  $n = 2$ , on a  $G = V(\delta)$ . D'après le lemme précédent, il existe un  $\sigma$ -automorphisme  $\alpha_K$  de  $\mathbf{G}_{\mathbf{a},\sigma}^2$  (fixant  $\mathbf{d}$ ) tel que  $\delta_K \circ \alpha_K$  s'annule sur  $\{0\} \times \mathbf{G}_{\mathbf{a},\sigma}^1$ . On a donc

$$\alpha_K^{-1} : V(\delta) \subset \mathbf{G}_{\mathbf{a},\sigma}^2 \longrightarrow V(\delta \circ \alpha) \supset \{0\} \times \mathbf{G}_{\mathbf{a},\sigma}^1,$$

qui est un  $\sigma$ -isomorphisme. Mais  $V(\delta \circ A)$  est aussi radical, et de dimension 1 d'après le théorème 6.3, donc on a nécessairement

$$V(\delta \circ A) = \{0\} \times \mathbf{G}_{\mathbf{a},\sigma}^1,$$

donc  $\alpha_K^{-1} : G \rightarrow \{0\} \times \mathbf{G}_{\mathbf{a},\sigma}^1$  est surjectif.

Si  $G \subset \mathbf{G}_{\mathbf{a},\sigma}^{n+1}$ , on a  $G \subset V(\delta_1)$ . D'après le lemme précédent, il existe un automorphisme  $\alpha$  de  $\mathbf{G}_{\mathbf{a},\sigma}^{n+1}$  tel que  $\delta_1 \circ \alpha$  s'annule sur  $\{0\} \times \mathbf{G}_{\mathbf{a},\sigma}^n$  (et fixe  $\mathbf{d}$ ). On a donc

$$\alpha^{-1} : V(\delta_1) \subset \mathbf{G}_{\mathbf{a},\sigma}^{n+1} \longrightarrow V(\delta_1 \circ \alpha) \supset \{0\} \times \mathbf{G}_{\mathbf{a},\sigma}^n,$$

qui est un  $\sigma$ -automorphisme. Mais  $V(\delta \circ A)$  est aussi radical, et de dimension  $n$ , donc

$$V(\delta_1 \circ \alpha) = \{0\} \times \mathbf{G}_{\mathbf{a},\sigma}^n.$$

$V(\delta_1 \circ \alpha, \dots, \delta_{n-1} \circ \alpha)$  est radical et de dimension 1. Par hypothèse de récurrence, il existe un  $\sigma$ -isomorphisme  $\beta$  entre  $V(\delta_1 \circ \alpha, \dots, \delta_{n-1} \circ \alpha)$  et  $\mathbf{G}_{\mathbf{a},\sigma}^1$  (tel que  $\beta_K(\mathbf{d}) = \mathbf{d}_n$ ). On a donc en particulier la restriction

$$\beta \circ \alpha^{-1} : G \longrightarrow V(\delta_1 \circ \alpha \circ \beta^{-1}, \dots, \delta_{n-1} \circ \alpha \circ \beta^{-1}) \subset \mathbf{G}_{\mathbf{a},\sigma}^1.$$

Mais l'image de  $\beta \circ \alpha^{-1}$  est radicale et de dimension 1, donc égale à  $\mathbf{G}_{\mathbf{a},\sigma}^1$ . □

*Remarque 7.3.* Si les coefficients définissant les équations de  $G$  sont dans le corps  $K$ , le  $\sigma$ -isomorphisme  $\alpha$  est à coefficients dans  $K$ .

## 8. RETOUR SUR TERRE

On considère un corps *non commutatif*  $K$  dont la caractéristique est un entier premier  $p$  ou 0, et on s'intéresse à sa théorie du premier ordre  $\text{Th}(K)$  exprimée dans le langage des corps  $(+, \times, 0, 1)$ . Puisque  $K$  n'est pas commutatif, d'après Wedderburn, il est infini. La théorie de  $K$  n'est pas superstable (voir [Che78]). Si  $K$  est de caractéristique  $p$ , sa théorie n'est pas non plus menue (voir [Mil07]). La question de savoir si  $\text{Th}(K)$  peut être stable est encore ouverte, mais si  $\text{Th}(K)$  est stable et de caractéristique  $p$ , le corps  $K$  n'est pas loin d'être commutatif puisque c'est un espace vectoriel de dimension finie sur son centre (voir [Mil11]).

Nous nous intéressons ici au cas où  $\text{Th}(K)$  n'a pas la *propriété d'indépendance* au sens de Shelah. En caractéristique zéro, un exemple est donné par le corps des quaternions sur  $\mathbf{R}$ , interprétable dans le corps des réels. Voici un exemple de caractéristique  $p$ .

Soit  $\Gamma_p = \langle \frac{1}{p^i} : i \in \mathbf{N} \rangle$  le sous-groupe ordonné de  $\mathbf{R}^+$ . On considère le corps *commutatif*  $H = \mathbf{F}_p^{\text{alg}}((\Gamma_p))$  des séries formelles de Hahn

$$a = \sum_{g \in \Gamma_p} a_g t^g$$

ayant un support  $S(a) \subset \Gamma_p$  bien ordonné et des coefficients  $a_g$  dans  $\mathbf{F}_p^{\text{alg}}$ . Muni de sa valuation naturelle  $v$  associant à une série le minimum de son support, le corps valué  $(H, v)$  est maximal, *i.e.* n'a pas d'extension de corps valué ayant à la fois le même corps résiduel et le même groupe de valuation (voir [Kru32] ou [EP05, Exercice 3.5.6]). Son corps résiduel est infini, parfait et n'a pas la propriété d'indépendance. Son groupe de valuation est  $p$ -divisible, donc  $H$  n'a pas la propriété d'indépendance d'après [KSW11, Theorem 5.9]. Si la caractéristique  $p$  est un entier impair, l'extension  $H(\sqrt{t})/H$  est galoisienne et cyclique de groupe de Galois engendré par l'automorphisme  $\sigma \in \text{Aut}(H(\sqrt{t})/H)$  échangeant  $\sqrt{t}$  et  $-\sqrt{t}$ . On considère le  $H(\sqrt{t})$ -espace vectoriel de dimension 2 à gauche

$$K = H(\sqrt{t}) \oplus H(\sqrt{t}) \cdot x$$

muni de la multiplication interne définie par les deux règles

$$x^2 = t^{1/p} \quad \text{et} \quad x \cdot k = \sigma(k)x \quad \text{pour tout } k \in H(\sqrt{t}).$$

$K$  est une  $H$ -algèbre non commutative de centre  $H$  et de dimension 4, interprétable dans  $H$ , donc  $K$  n'a pas la propriété d'indépendance. Puisque la norme  $N_{H(\sqrt{t})/H}$  de l'extension  $H(\sqrt{t})/H$  est définie par

$$N_{H(\sqrt{t})/H}(a + b\sqrt{t}) = a^2 + b^2t,$$

il n'est pas difficile de vérifier que l'on a

$$t^{1/p} \notin N_{H(\sqrt{t})/H}(H(\sqrt{t})),$$

donc  $K$  est un corps d'après [Lam91, Corollary 14.8]. En caractéristique 2, on peut réitérer une construction similaire à partir de l'extension cyclique galoisienne  $H(\sqrt[3]{t})/H$ .

Remarquons que le corps  $K$  ci-dessus n'est pas stable, puisque son centre ne l'est pas :  $H$  est Hensélien (voir [Efr06, Corollary 18.4.2]), et possède une valuation non-triviale définissable dans le langage des corps (voir [KJ15b, Theorem 5.2] ou [KJ15a, Theorem 3.10]).



**Définition 8.1** (Corps sans propriété d'indépendance). Un corps gauche  $K$  n'a pas la propriété d'indépendance si chaque formule  $\varphi(x, \bar{y})$  dans le langage des corps a une dimension de Vapnis-Chervonenkis finie, c'est-à-dire s'il existe un entier naturel maximal  $n$  dépendant de  $\varphi$  et des éléments  $(a_1, \dots, a_n)$  et  $(\bar{b}_J)_{J \subset \{1, \dots, n\}}$  dans  $K$  tels que que

$$(K \models \varphi(a_i, \bar{b}_J)) \iff i \in J.$$

Les groupes définissables dans un corps sans propriété d'indépendance satisfont la condition noethérienne suivante (voir [Poi87]).

**Condition de chaîne de Baldwin-Saxl 8.2** ([BS76]). Soit  $G$  un groupe, et  $\mathfrak{H}$  une famille de sous-groupes de  $G$  uniformément définissable par une formule  $\varphi(x, \bar{y})$ . Si  $\varphi(x, \bar{y})$  a pour dimension de Vapnis-Chervonenkis  $n$ , alors pour toute famille finie  $\mathfrak{K} \subset \mathfrak{H}$ , il existe une famille  $\mathfrak{K}_n \subset \mathfrak{K}$  de taille au plus  $n$  telle que

$$\bigcap \mathfrak{K} = \bigcap \mathfrak{K}_n.$$

On peut étendre cette conditions à certaines parties d'un groupe uniformément définissables qui ne sont pas nécessairement stables par multiplications (voir [Mil16]).

**8.1. Préliminaire sur les corps commutatifs sans propriété d'indépendance.** Si  $K$  est un corps commutatif de caractéristique  $p$ , une extension commutative  $K(a)/K$  est de type Artin-Schreier si  $a$  est racine de l'équation

$$X^p - X = b$$

pour un certain élément  $b$  de  $K$ . On sait peu de choses sur les corps commutatifs pour lesquels  $\text{Th}(K)$  n'a pas la propriété d'indépendance. Nous utiliserons principalement le résultat suivant (voir [KSW11, Theorem 4.3]), dont la démonstration repose sur la classification des sous-groupes fermés irréductibles de  $\mathbf{G}_a^n$  de dimension 1 :

**Théorème 8.3** (de Kaplan et Scanlon). *Un corps commutatif infini de caractéristique  $p$  sans propriété d'indépendance n'a pas d'extension propre de type Artin-Schreier.*

Avec comme conséquence immédiate utilisant le résultat de Duret sur les corps faiblement algébriquement clos non séparablement clos (voir [Dur79, Théorème 6.4] et [KSW11, Corollary 4.5]) :

**Corollaire 8.4** (de Kaplan et Scanlon). *Un corps commutatif infini de caractéristique  $p$  sans propriété d'indépendance contient le corps  $\mathbf{F}^{alg}$ .*

**8.2. Préliminaires sur les corps non commutatifs de caractéristique  $p > 0$  sans propriété d'indépendance.** On renvoie à [Her96, Lemma 3.1.1 p.70], [Lam03, Exercice 13.8 p. 205] et [Lam03, Exercice 16.11 p. 239] pour les résultats suivants.

**Lemme 8.5** (de Herstein). *Soit  $K$  un corps non commutatif de caractéristique  $p$ . Soit  $a$  un élément de  $K^\times$  d'ordre fini et hors du centre de  $K$ . Il existe un élément  $b$  de  $K$  et un entier  $i > 0$  tels que*

$$bab^{-1} = a^i \neq a.$$

**Lemme 8.6** (de Lam). *Soit  $K$  un corps non commutatif de caractéristique  $p$ . Soit  $a$  un élément de  $K^\times$  hors du centre de  $K$  tel que  $a^{p^n}$  soit dans le centre de  $K$ . Il existe un élément  $b$  de  $K$  tel que*

$$bab^{-1} = b + 1.$$

**Lemme 8.7** (de Lam). *Soit  $K$  un corps non commutatif de centre  $Z(K)$ , et  $a \in K$  un élément algébrique sur  $Z(K)$ . L'équation  $ax - xa = 1$  a une solution  $x$  dans  $D$  si et seulement si  $a$  n'est pas séparable sur  $Z(K)$ .*

On considère un corps non commutatif  $K$  de caractéristique  $p$  tel que  $\text{Th}(K)$  n'a pas la propriété d'indépendance.

**Théorème 8.8.** *Le centre de  $K$  est infini, et contient  $\mathbf{F}_p^{\text{alg}}$ .*

*Démonstration.* Si tous les éléments de  $K$  sont d'ordre fini, on montre que  $K$  est commutatif : s'il existe un élément  $a$  hors du centre, d'après le lemme de Herstein il existe un élément  $b$  de  $D$  et un entier  $i > 0$  tels que  $bab^{-1} = a^i \neq a$ . Puisque l'on a supposé que  $b$  aussi est d'ordre fini, il s'en suit que le corps engendré par  $a$  et  $b$  est fini, ce qui contredit le théorème de Wedderburn. Supposons donc qu'il existe un élément  $c$  d'ordre infini. Le corps  $Z(C(c))$  est infini et commutatif. Il contient une copie de  $\mathbf{F}_p^{\text{alg}}$  d'après le corollaire 8.4. Il suffit de montrer que le centre de  $K$  contient toute racine  $p^n$ -ième de l'unité. Supposons au contraire qu'il existe un élément  $a \in K \setminus Z(K)$  tel que  $a^{p^n} = 1$ . D'après le lemme de Lam, il existe un élément  $b \in K$  tel que

$$(4) \quad b^a = b + 1.$$

En élevant à la puissance  $p$ , on en déduit  $(b^p)^a = b^p + 1$ , puis

$$(5) \quad (b^p - b)^a = b^p - b.$$

Si  $(b^p - b)$  est d'ordre fini, disons  $(b^p - b)^{p^m} = b^p - b$ , on a pour tout entier  $q$ ,

$$(b^p - b)^{p^{qm}} = b^p - b, \quad \text{et}$$

$$\left( (b^{p^{qm}})^p - b^{p^{qm}} \right) = b^p - b.$$

Dans le corps commutatif engendré par  $b$ , le polynôme  $X^p - X - (b^p - b)$  n'a qu'un nombre fini de racines, donc il existe deux entiers  $q_1 \neq q_2$  tels que  $b^{p^{q_1 m}} = b^{p^{q_2 m}}$ , et l'ordre de  $b$  est fini. D'après (4),  $a$  et  $b$  engendrent un corps fini, une contradiction avec le théorème de Wedderburn. L'ordre de  $(b^p - b)$  est donc infini, et le corps commutatif  $Z(C(b^p - b))$  est infini. L'élément  $b$  commute avec  $Z(C(b^p - b))$  donc  $Z(C(b^p - b))(b)/Z(C(b^p - b))$  est une extension de type Artin-Schreier. D'après le théorème 8.3, l'élément  $b$  appartient à  $Z(C(b^p - b))$ , donc  $b$  et  $a$  commutent d'après (5), une contradiction avec (4).  $\square$

*Remarque 8.9.* Les corps non commutatifs ayant un centre fini existent. Considérons l'automorphisme de Froebenius  $\sigma : x \mapsto x^p$  sur le corps  $\mathbf{F}_p^{\text{alg}}$ , et le corps  $K = \mathbf{F}_p^{\text{alg}}((x, \sigma))$  des séries de Laurent

$$\sum_{i=m}^{+\infty} a_i x^i$$

où les  $a_i$  sont des éléments de  $\mathbf{F}_p^{alg}$ , et  $m \in \mathbf{Z}$ . La multiplication sur  $K$  est définie en posant

$$x \cdot a = \sigma(a) \cdot x \quad \text{pour tout } a \in \mathbf{F}_p^{alg}.$$

Ceci définit bien une structure de corps non commutatif sur  $K$  (voir par exemple [Lam91, Exemple 1.8]). On peut vérifier que le centre de  $K$  est  $\mathbf{F}_p$  (voir [Lam91, Proposition 14.2]).

**Lemme 8.10.** *Pour tout élément  $a$  de  $K$ , on a*

$$C(a^p - a) = C(a).$$

*Démonstration.* Puisque  $a$  commute avec  $Z(C(a^p - a))$ , le corps  $Z(C(a^p - a))(a)$  est commutatif, et l'extension  $Z(C(a^p - a))(a)/Z(C(a^p - a))$  est de type Artin-Schreier. Le corps  $Z(C(a^p - a))$  est infini d'après le lemme précédent. D'après le théorème 8.3, l'élément  $a$  appartient à  $Z(C(a^p - a))$ , donc  $a$  commute avec  $C(a^p - a)$ , et  $C(a^p - a) \subset C(a)$ .  $\square$

**Lemme 8.11** (Équation du métré). *Pour tout élément  $a$  de  $K$ , l'équation  $ax - xa = 1$  n'a pas de solution dans  $K$ .*

*Démonstration.* Sinon, il existe un  $y$  tel que  $y^a = y + 1$ . On en déduit  $(y^p)^a = y^p + 1$ . En retranchant ces deux identités, on obtient

$$(y^p - y)^a = y^p - y.$$

L'élément  $a$  commute avec  $y^p - y$ , mais ne commute pas avec  $y$ , une contradiction avec le lemme précédent.  $\square$

*Remarque 8.12.* Les corps non commutatifs qui pour chaque élément  $a$  hors du centre possèdent une solution à l'équation  $ax - xa = 1$  sont nombreux. On sait que pour tout corps non commutatif  $K$  de centre  $k$ , il existe une extension  $L$  de  $K$  gardant pour centre  $k$  et telle que l'équation  $ax - xa = 1$  ait une solution dans  $L$  pour tout  $a \in L$  transcendant sur  $k$  (voir [Coh73]).

**Corollaire 8.13.** *Pour tout élément  $a$  de  $K$ , on a*

$$C(a^p) = C(a).$$

*Démonstration.* L'élément  $a$  est algébrique sur  $ZC(a^p)$ . Puisque l'équation  $ax - xa = 1$  n'a pas de solution dans  $K$  d'après le lemme précédent,  $a$  est séparable sur  $ZC(a^p)$  d'après le lemme de Lam, et  $a \in ZC(a^p)$ , donc  $a$  commute avec  $C(a^p)$ , et  $C(a^p) \subset C(a)$ .  $\square$

### 8.3. Résultat général.

**Théorème 8.14.** *Un corps gauche sans propriété d'indépendance de caractéristique  $p > 0$  est de dimension finie sur son centre.*

*Démonstration.* Supposons que  $K$  contienne un élément  $a$  transcendant sur son centre  $k$ . Puisque  $k(a)/k$  est transcendant, en posant  $\sigma_K(x) = a^{-1}xa$ , on peut choisir une extension  $\sigma$ -algébriquement close  $\mathbf{K}/K$  de  $K$  d'après le théorème 3.3. Soit  $\gamma_K : x \mapsto x^\sigma - x$ . On cherche à montrer que  $\gamma_K$  est surjective, une contradiction avec le lemme 8.11 : dans ce cas,  $K$  est algébrique sur son centre, et par un argument de compacité, il est de dimension finie sur  $k$ .

Pour tout entier  $m \geq 1$ , on munit  $\mathbf{K}^m$  de la topologie de Zariski tordue associée à  $\sigma$ . On emprunte une idée de [Sca99, KSW11] : pour tout uplet  $\bar{b} = (b_0, \dots, b_m)$  d'éléments non nuls de  $K^{m+1}$ , on considère le sous-groupe algébrique  $G_{\bar{b}}^{m+1}(\mathbf{K}) \subset \mathbf{G}_{\mathbf{a},\sigma}^{m+1}$  défini par

$$G_{\bar{b}}^{m+1} = \left\{ (x_0, x_1, \dots, x_m) \in \mathbf{K}^{m+1} : \gamma_{\mathbf{K}}(x_0)b_0 = \gamma_{\mathbf{K}}(x_i)b_i \text{ pour tout } 1 \leq i \leq m \right\}.$$

Il s'agit d'une intersection non vide de  $m$  hypersurfaces, donc  $\dim G_{\bar{b}}^{m+1} \geq 1$  d'après le théorème 6.3. Le noyau de la première projection

$$\pi_1 : G_{\bar{b}}^{m+1} \longrightarrow \mathbf{G}_{\mathbf{a},\sigma}^1$$

est de dimension 0, donc  $\dim G_{\bar{b}}^{m+1} \leq 1$  d'après le théorème 6.8.3. D'après la condition de chaîne 8.2, il existe un entier  $n$  tel que pour tout  $\bar{b} = (b_1, \dots, b_{n+1})$  dans  $K^{n+1}$ , il existe un  $b_i$ , disons par exemple  $b_{n+1}$  tel que

$$\bigcap_{i=0}^{n+1} \gamma_{\mathbf{K}}(K)b_i = \bigcap_{i=0}^n \gamma_{\mathbf{K}}(K)b_i,$$

donc la projection

$$\pi_K : G_{\bar{b}}^{m+1}(K) \longrightarrow G_{\bar{b}}^m(K), (x_0, x_1, \dots, x_n) \mapsto (x_0, x_1, \dots, x_{n-1})$$

est surjective. Enfin,

**Lemme 8.15** (de Hempel). *Le groupe  $G_{\bar{b}}^m(\mathbf{K})$  est radical si et seulement si la famille  $(b_0^{-1}, \dots, b_m^{-1})$  est  $C_{\mathbf{K}}(a)$ -libre à droite.*

*Démonstration du lemme.* On s'inspire de [Hem15, Lemme 5.3]. On traite le cas  $m = 2$ , le cas général étant similaire. Si  $b_0^{-1}, b_1^{-1}$  et  $b_2^{-1}$  sont  $C_{\mathbf{K}}(a)$ -liés à droite, alors il existe  $k_0, k_1$  et  $k_2$  non tous nuls dans  $C_{\mathbf{K}}(a)$  tels que

$$b_0^{-1} \cdot k_0 + b_1^{-1} \cdot k_1 + b_2^{-1} \cdot k_2 = 0.$$

Soit  $(x_0, x_1)$  un élément fixé de  $G_{\bar{b}}^2$ . On a

$$\begin{aligned} (x_0, x_1, x_2) \in G_{\bar{b}}^3 &\iff (x_0^\sigma - x_0)b_0 = (x_2^\sigma - x_2)b_2 \\ &\iff (x_0^\sigma - x_0)b_0b_2^{-1}k_2 = (x_2^\sigma - x_2)k_2 \\ &\iff -(x_0^\sigma - x_0)k_0 - (x_0^\sigma - x_0)b_0b_1^{-1}k_1 = (x_2^\sigma - x_2)k_2 \\ &\iff -(x_0^\sigma - x_0)k_0 - (x_1^\sigma - x_1)k_1 = (x_2^\sigma - x_2)k_2 \\ &\iff (x_0k_0 + x_1k_1 + x_2k_2)^\sigma - (x_0k_0 + x_1k_1 + x_2k_2) = 0, \end{aligned}$$

On en déduit  $x_0k_0 + x_1k_1 + x_2k_2 \in \text{cl}(I(G_{\bar{b}}^3))$ . Si  $k_3 \neq 0$  par exemple, le point  $(0, 0, a) \in G_{\bar{b}}^3$  n'annule pas  $x_0k_0 + x_1k_1 + x_2k_2$ , donc  $x_0k_0 + x_1k_1 + x_2k_2 \notin I(G_{\bar{b}}^3)$ . Ceci montre que  $G_{\bar{b}}^3$  n'est pas radical.

Réciproquement, supposons  $G_{\bar{b}}^2$  radical et  $b_0^{-1}, b_1^{-1}, b_2^{-1}$  libres à droite sur  $C_{\mathbf{K}}(a)$ , et montrons que  $G_{\bar{b}}^3$  est radical. La projection  $\pi : G_{\bar{b}}^3 \rightarrow G_{\bar{b}}^2$  est surjective, et son noyau est de dimension 0, donc

$$\pi((G_{\bar{b}}^3)^0) = G_{\bar{b}}^2$$

puisque  $G_b^2$  est radical, d'après le théorème 6.8.3 et le corollaire 6.4.1. Supposons par l'absurde que  $G_b^3$  ne soit pas radical. On prétend la chose suivante.

Pour tout  $(x_0, x_1) \in G_b^2$ , il existe un unique  $x_2 \in \mathbf{K}$  tel que  $(x_0, x_1, x_2) \in (G_b^3)^0$ .

En effet, s'il existe deux éléments distincts  $x_2$  et  $y_2$  tels que  $(x_0, x_1, x_2)$  et  $(x_0, x_1, y_2)$  soient dans  $(G_b^3)^0$ , alors leur différence  $(0, 0, x_2 - y_2)$  est également dans  $(G_b^3)^0$ , et donc  $x_2 - y_2 \in \text{Ker}_{\mathbf{K}}\gamma$ , et  $\{0\} \times \{0\} \times \text{Ker}_{\mathbf{K}}\gamma$  est un sous-groupe non trivial de  $(G_b^3)^0$ . Pour chaque élément  $(x_0, y_1, z_2) \in G_{b_1, b_2}^3$ , puisque  $\pi((G_b^3)^0) = G_b^2$ , il existe  $u_2 \in \mathbf{K}$  tel que  $(x_0, y_1, u_2) \in (G_b^3)^0$ . De même, la différence  $u_2 - z_2$  appartient à  $\text{Ker}_{\mathbf{K}}\gamma$ , et

$$(x_0, y_1, z_2) = (x_0, y_1, u_2) + (0, 0, z_2 - u_2) \in (G_b^3)^0,$$

ce qui contredit le fait que l'inclusion  $(G_b^3)^0 \subset G_b^3$  soit propre.

On peut donc définir  $f : G_b^2 \rightarrow \mathbf{K}$  une fonction  $C(a)$ -linéaire et définissable qui à  $(x_0, x_1)$  associe cet unique élément  $x_2$ . Son graphe est le groupe algébrique  $G_b^2 \cap (G_b^3)^0$ , défini par  $V(S)$  pour un ensemble  $S \subset \mathbf{K}_\sigma^1[x_0, x_1, x_2]$ . L'ensemble  $S$  contient l'équation  $\gamma(x_2) = \gamma(x_0)b_0b_2^{-1}$ , et puisque cette dernière définit à  $(x_0, x_1)$  fixé une  $C_{\mathbf{K}}(a)$ -droite affine,  $S$  contient au moins une autre équation de la forme  $\delta(x_2) = \alpha(x_0) + \beta(x_1)$  avec  $\delta$  non nulle, unitaire et distincte de  $\gamma$ . On suppose  $\delta$  de degré minimal, donc  $\delta(x) = x$  (sinon on remplace  $x_2^\sigma$  par  $x_2 - \gamma(x_0)b_0b_2^{-1}$ , ce qui contredit la minimalité de  $\delta$ ). On a donc

$$x_2 = \alpha(x_0) + \beta(x_1),$$

et en remplaçant  $x_1^\sigma$  par  $x_1 - \gamma(x_0)b_0b_1^{-1}$ , et quitte à modifier  $\alpha$ , on peut supposer que  $\beta(x_1) = x_1k_1$  pour un  $k_1 \in \mathbf{K}$ . On a aussi  $k_1 = f(0, 1) \in C_{\mathbf{K}}(a)$ . En remplaçant  $x_2$  dans  $\gamma(x_2)b_2 = \gamma(x_0)b_0$ , on obtient

$$(\alpha(x_0)^\sigma - \alpha(x_0) + (x_1^\sigma - x_1)k_1)b_2 - \gamma(x_0)b_0 = 0,$$

puis

$$(\alpha(x_0)^\sigma - \alpha(x_0) + \gamma(x_0)b_0b_1^{-1}k_1)b_2 - \gamma(x_0)b_0 = 0.$$

Comme cette dernière équation est valable pour tout  $x_0 \in \mathbf{K}$ , la distortion considérée est nulle, et pour des raisons de degré, on a  $\alpha(x_0) = x_0k_0$  avec  $k_0 = f(1, 0) \in C_{\mathbf{K}}(a)$ . On en déduit pour tout  $x_0 \in \mathbf{K}$ ,

$$\gamma(x_0)k_0 + \gamma(x_0)b_0b_1^{-1}k_1 - \gamma(x_0)b_0b_2^{-1} = 0,$$

et

$$b_0^{-1}k_0 + b_1^{-1}k_1 + b_2^{-1} = 0,$$

donc  $(b_0^{-1}, b_1^{-1}, b_2^{-1})$  est  $C_{\mathbf{K}}(a)$ -liée à droite. Puisque  $\bar{b}$  est un uplet d'éléments de  $K$ , la famille  $(b_0^{-1}, b_1^{-1}, b_2^{-1})$  est également  $C_K(a)$ -liée, une contradiction avec l'hypothèse.  $\square$

**Lemme 8.16.** *Il existe un uplet  $\bar{b} \in K^m$  qui soit  $C_{\mathbf{K}}(a)$ -libre à droite.*

*Démonstration.* Sinon, il existe un uplet  $\bar{b} \in K^m$  tel que  $K \subset b_1C_{\mathbf{K}}(a) + \dots + b_mC_{\mathbf{K}}(a)$ . D'après le lemme 5.1, ce dernier ensemble est fermé pour la topologie duale, et même un ensemble algébrique puisqu'irréductible. Il existe donc un entier  $\ell$  et  $\mathbf{a}_1, \dots, \mathbf{a}_\ell \in \mathbf{K}$  tel que pour tout  $x \in K$ , on ait

$$\mathbf{a}_0x + \mathbf{a}_1xa + \dots + \mathbf{a}_\ell xa^\ell + xa^{\ell+1} = 0.$$

On montre par récurrence sur  $i$  que  $\mathbf{a}_i \in K + \mathbf{a}_{i+1}K + \cdots + \mathbf{a}_\ell K$ . Pour  $i = 0$ , il suffit de prendre  $x = 1$  dans l'équation. Si c'est vrai jusqu'au rang  $i$ , alors pour tout  $j \leq i$ , on a  $\mathbf{a}_j \in K + \mathbf{a}_{j+1}K + \cdots + \mathbf{a}_\ell K$ . En remplaçant ces expressions dans l'égalité ci-dessus, on en déduit qu'il existe des distortions  $\delta_q(x) = xa^q + \lambda_{q-1}xa^{q-1} + \cdots + \lambda_0x$  de degré  $q$  et à coefficients à gauche dans  $K$  pour  $q \in \{i+1, \dots, \ell\}$  telles que pour tout  $x \in K$ , on ait,

$$\mathbf{a}_{i+1}\delta_{i+1}(x) + \cdots + \mathbf{a}_\ell\delta_\ell(x) + xa^{\ell+1} = 0.$$

Les racines de  $\delta_{i+1}$  dans  $K$  formant un  $C_K(a)$ -espace vectoriel de dimension finie, il existe  $c \in K$  tel que  $\delta_{i+1}(c) \neq 0$ , d'où  $a_{i+1} \in K + \mathbf{a}_{i+2}K + \cdots + \mathbf{a}_\ell K$ , ce qui achève la récurrence. Pour  $i = \ell$  on en déduit en particulier que  $\mathbf{a}_\ell \in K$ , et par ricochet que  $\mathbf{a}_i \in K$  pour tout  $i$ . On déduit de la première équation que  $K$  est de dimension finie sur  $C_K(a)$ , une contradiction.  $\square$

D'après les deux lemmes précédents, on peut choisir un uplet  $\bar{b}$  de sorte que les groupes  $G_{\bar{b}}^{m+1}$  et  $G_{\bar{b}}^n$  soient radicaux. D'après le théorème 7.2, il existe deux  $\sigma$ -isomorphismes  $\delta_K : G_{\bar{b}}^{m+1} \rightarrow \mathbf{G}_{\mathbf{a},\sigma}^1$  et  $\varepsilon_K : G_{\bar{b}}^n \rightarrow \mathbf{G}_{\mathbf{a},\sigma}^1$  à coefficients dans  $K$ , et l'on peut choisir  $\delta$  tel que  $\delta_K(d) = d$  avec  $d = (0, \dots, 0, 1)$ . Le  $\sigma$ -morphisme  $\rho_K = \varepsilon_K \circ \pi_K \circ \delta_K^{-1}$  fait donc commuter le diagramme

$$\begin{array}{ccc} G_{\bar{b}}^{m+1} & \xrightarrow{\pi_K} & G_{\bar{b}}^n \\ \delta_K \downarrow & & \downarrow \varepsilon_K \\ \mathbf{G}_{\mathbf{a},\sigma}^1 & \xrightarrow{\rho_K} & \mathbf{G}_{\mathbf{a},\sigma}^1 \end{array}$$

Le noyau de  $\pi_K$  est égal à  $C(a)d$ , qui est de dimension 0, donc son image est de dimension 1 d'après le théorème 6.8.2. Mais  $G_{\bar{b}}^n(\mathbf{K})$  est radical, de sorte que  $\pi_K$  est surjective. Donc  $\rho_K$  l'est aussi. Puisque  $\delta_K(d) = d$ , le noyau de  $\rho_K$  est égal à  $C_K(a)$ . D'après le lemme 1.4,  $\rho_K$  se factorise dans  $\mathbf{K}_\sigma^1[x]$  en  $\rho_K = \beta_K \circ \gamma_K$  avec

$$\gamma_K(x) = x^\sigma - x.$$

Puisque  $\gamma$  et  $\rho$  sont à coefficients dans  $K$ ,  $\beta$  est également à coefficients dans  $K$ . La fonction  $\beta_K$  est nécessairement injective, ainsi que sa restriction  $\beta_K$ . Mais, d'après la condition de chaîne,  $\pi_K$  est surjective, donc  $\rho_K$  et  $\beta_K$  aussi. On en déduit que  $\gamma_K : K \rightarrow K$  est surjective.  $\square$

### RÉFÉRENCES

- [Art10] Michael Artin, *Algebra*, Pearson, Second Edition, 2010.
- [BS76] John Baldwin and Jan Saxl, *Logical stability in group theory*, J. Austral. Math. Soc. Ser. A **21** (1976), no. 3, 267–276.
- [Che78] Gregory Cherlin, *Superstable division rings*, Logic Colloquium 1977, 1978, pp. 99–111.
- [Coh73] Paul Moritz Cohn, *The range of derivations on a skew field and the equation  $ax - xb = c$* , Journal of the Indian Mathematical Society **37** (1973), 61–69.
- [Coh95] ———, *Skew fields, theory of general division rings*, Encyclopedia of Mathematics and its Applications, vol. 57, Cambridge University Press, Cambridge, 1995.

- [Dur79] Jean-Louis Duret, *Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendance*, Model Theory of Algebra and Arithmetic (proc. Karpacz), Lecture Notes in Mathematics, vol. 834, Springer-Verlag, Berlin, 1979, pp. 13–162.
- [Efr06] Ido Efrat, *Valuations, orderings, and milnor k-theory*, Mathematical Surveys and Monographs, vol. 124, American Mathematical Society, Providence, RI, 2006.
- [EP05] Antonio Engler and Alexander Prestel, *Valued fields*, Springer Monographs in Mathematics, 2005.
- [GM65] Basil Gordon and Theodore Motzkin, *On the zeros of polynomials in division rings*, Transactions of the American Mathematical Society **116** (1965), 218–226.
- [Ham50] William Hamilton, *On quaternions, or on a new system of imaginaries in algebra*, The London, Edinburgh and Dublin Philosophical Magazine and Journal of Science (1844-1850).
- [Hem15] Nadja Hempel, *On  $n$ -dependent groups and fields*, to appear in Mathematical Logic Quarterly (2015).
- [Her56] Israel Herstein, *Conjugates in division rings*, Proceedings of the American Mathematical Society **7** (1956), 1021–1022.
- [Her96] ———, *Noncommutative rings*, The Mathematical Association of America, fourth edition, 1996.
- [Hil03] David Hilbert, *Grundlagen der geometrie*, 2nd Edition, Leipzig (1903).
- [Hum75] James Humphreys, *Linear algebraic groups*, Graduate texts in mathematics, Springer-verlag, 1975.
- [HW75] Joram Hirschfeld and William Wheeler, *Forcing, arithmetic, division rings*, Springer-verlag, 1975.
- [KJ15a] Jochen Koenigsmann and Franziska Jahnke, *Definable henselian valuations*, The Journal of Symbolic Logic **80** (2015), 85–99.
- [KJ15b] ———, *Uniformly defining  $p$ -henselian valuations*, Annals of Pure and Applied Logic **166** (2015), 741–754.
- [Kru32] Wolfgang Krull, *Allgemeine bewertungstheorie*, Journal für Mathematik **167** (1932), 160–196.
- [KSW11] Itay Kaplan, Thomas Scanlon, and Frank O. Wagner, *Artin-Schreier extensions in NIP and simple fields*, Israel J. Math. **185** (2011), 141–153.
- [Lam91] Tsit Yuen Lam, *A first course in noncommutative rings*, Graduate Texts in Mathematics, vol. 131, Springer-Verlag, Berlin/Heidelberg, 1991.
- [Lam03] ———, *Exercises in classical ring theory*, Problem books in Mathematics, Springer-Verlag, New York, 2003, Second Edition.
- [Mil07] Cédric Milliet, *Small skew fields*, Mathematical Logic Quarterly **53** (2007), 86–90.
- [Mil11] ———, *Stable division rings*, Journal of Symbolic Logic **76** (2011), 348–352.
- [Mil16] ———, *Variations sur un thème de Aldama et Shelah*, The Journal of Symbolic Logic (2016), 1–31.
- [ML85] Leonid Makar-Limanov, *Algebraically closed skew fields*, Journal of Algebra **93** (1985), 117–135.
- [NE44] Ivan Niven and Samuel Eilenberg, *The 'fundamental theorem of algebra' for quaternions*, Bulletin of the American Mathematical Society **50** (1944), 246–248.
- [Niv41] Ivan Niven, *Equations in quaternions*, The American Mathematical Monthly **48** (1941), 654–661.
- [Per01] Daniel Perrin, *Géométrie algébrique, une introduction*, EDP Sciences, CNRS Éditions, 2001.
- [Poi85] Bruno Poizat, *Cours de théorie des modèles*, Bruno Poizat, Lyon, 1985, Une introduction à la logique mathématique contemporaine. [An introduction to contemporary mathematical logic].
- [Poi87] ———, *Groupes stables*, Nur al-Mantiq wal-Ma'rifah [Light of Logic and Knowledge], 2, Bruno Poizat, Lyon, 1987, Une tentative de conciliation entre la géométrie algébrique et la logique mathématique. [An attempt at reconciling algebraic geometry and mathematical logic].
- [Sca99] Thomas Scanlon, *Infinite stable fields are Artin-Schreier closed*, unpublished (1999).
- [TY05] Patrice Tauvel and Rupert Yu, *Lie algebras and algebraic groups*, Springer Monographs in Mathematics, 2005.

5, RUE ORNANO,  
69001 LYON, FRANCE

*E-mail address:* `cedric.milliet@gmail.com`