Théorie des Modèles des Corps : La Propriété d'Indépendance

Christian d'Elbée

16 juillet 2015

Que ton vers soit la bonne aventure
Éparse au vent crispé du matin
Qui va fleurant la menthe et le thym. . .
Et tout le reste est littérature.
V.

Table des matières

Introduction

L'étude des corps dépendants entre dans le cadre d'une conjecture concernant la classification des corps stables. On sait en effet que les corps séparablement clos sont stables et non superstables ([13]). À ce titre la communauté des théoriciens des modèles ([2]) conjecture que ces corps sont les seuls qui soient stables. On commence donc par s'intéresser à certaines extensions séparables : les extensions d'Artin-Schreier. Un premier pas vers cette conjecture a été que les corps stables de caractéristique positive n'ont pas d'extensions d'Artin-Schreier ([14]). Mais quid des extensions séparables de degré premier avec la caractéristique ? et quid de la caractéristique 0 ? Une théorie est stable si et seulement si elle est simple et dépendante. Cela offre un nouvel angle d'attaque pour la conjecture : étudier les corps simples d'une part et les corps dépendants d'autre part. Ce sont ces derniers qui font l'objet principal de ce mémoire. Suivant [8], on y montre que tout comme les corps stables, les corps dépendants de caractéristique $p > 0$ n'ont pas d'extensions séparables finies de degré divisible par p (4.1).

La conjecture sus-citée n'a pas eu beaucoup d'avancée notable depuis l'article [14], et c'est d'autant plus vrai en ce qui concerne les corps type-définissables dans les théories stables. Néanmoins, on montre dans 4.2 que les corps type-définissables dépendants ont soit une infinité d'extensions d'Artin-Schreier, soit n'en ont aucune. Coinjointement à un résultat de [8] –non démontré dans ce mémoire– stipulant que les corps type-définissables dans une théorie simple n'ont qu'un nombre fini d'extensions d'Artin-Schreier, cela montre que les corps type-définissables dans une théorie stable sont Artin-Schreier clos.

Oubliant un peu la conjecture initiale, l'étude en soi des corps dépendants est un sujet à part entière. Ainsi on connait un certain nombre de corps dépendants, à commencer par tous les corps stables (corps algébriquement clos, différentiellement clos, séparablement clos), les corps réels clos ([17]) ainsi que certains corps valués (dont nous ne parlerons pas ici). Pour espérer comprendre ce que sont les corps NIP il est bon de savoir quels corps ne le sont pas, on s'est donc intéressé aux corps pseudo-algébriquement clos (5). En plus d'être un exemple de corps ayant la propriété d'indépendance, l'étude des corps pseudo-algébriquement clos fournit un corollaire bien senti donnant une propriété intéressante des corps dépendants (corollaire 5.2.5).

Ce mémoire s'organise en cinq sections. Les deux premières sont purement algébriques. Elles servent de rappels concernant la théorie de Galois et la géométrie algébrique en même temps qu'elles établissent des lemmes algébriques pour les preuves des principaux résultats de ce rapport. On se sera efforcé au moins de mentionner les résultats avant toute utilisation, le lecteur comprendra que toutes les preuves ne peuvent pas être données, tant pour des questions de temps que pour des questions de concision. La troisième partie établit le contexte modèle-théorique de notre étude. On y expose les notions de groupes et de corps dépendants ainsi que celles de groupes et de corps dépendants type-définissables. La quatrième partie est la plus importante, on utilise les trois sections précédentes pour montrer que les corps dépendants définissables sont Artin-Schreier clos, ainsi qu'une condition pour qu'un corps type-définissable dépendant soit Artin-Schreier clos. Enfin la cinquième et dernière partie est l'étude d'une classe de corps ayant

la propriété d'indépendance : les corps pseudo-algébriquement clos.
Ce mémoire a été pour moi l'occasion de me familiariser avec l'attirail algébrique nécessaire à l'étude des corps en théorie des modèles, en particulier avec la théorie de Galois et la géométrie algébrique. Ces deux domaines se sont imposés à moi autant pour la preuve des résultats sur les corps dépendants que pour l'étude elle-même des corps pseudo-algébriquement clos.

Enfin il est à noter que les deux principaux résultats exposés dans ce mémoire ont tous deux été récemment généralisés dans le contexte plus large des théories NIP_n [1]. En effet, Nadja Hempel montre [2] que tout corps NIP_n est Artin-Schreier clos, et que tout corps PAC non séparablement clos a IP_n.

1. Une théorie complète T est dite NIP_n si aucune formule n'a la propriété IP_n. Une formule $\phi(x_1, \ldots, x_n; y)$ est IP_n si il existe $(a_i^j \ ; \ 1 \leq j \leq n; i < \omega)$ et $(b_J)_{J \subseteq \omega^n}$ tels que

$$\models \phi(a^1_{i_1}, \ldots, a^n_{i_n}; b_J) \iff (i_1, \ldots, i_n) \in J$$

Une théorie est NIP_1 si et seulement si elle est NIP, et toute théorie NIP_n est NIP_{n+1}.

2. arXiv :1401.4880v2

Remerciements

Je tiens tout d'abord à remercier ma directrice de mémoire Zoé Chatzidakis, pour son suivit durant ce travaille, sa patience et la liberté qu'elle m'a accordée tant sur le sujet de ce mémoire que sur sa réalisation. Je remercie également Pierre Simon pour son aide sur certains points techniques ainsi que pour son livre. Je tiens à remercier Amador Martin-Pizarro pour son cours passionnant sur la stabilité, ainsi que Françoise Point pour son cours d'une part et pour ces discussions toujours intéressantes à Sophie Germain. Je remercie Martin Hils pour son cours, ses conseils avisés ainsi que sa dévotion à l'ensemble du LMFI. Je remercie sincèrement Partick Simonetta pour avoir accepté de faire partie du jury. Je remercie mon très cher Alex, co-apprenti théoricien des modèles de qui j'ai beaucoup appris et qui a toujours été de bon conseil. Je remercie mon cher ami Paulel' pour m'avoir soutenu et supporté tout au long de cette année. Je remercie bien sur mon cher Antoine dont l'incroyable faculté à rendre intéressant, voir passionnant des sujets aussi divers qu'hétérodoxes n'a d'égale que la sincérité de son amitié. Je remercie enfin mon très cher Jules pour m'avoir fait découvrir un Paris que je ne m'attendais pas à rencontrer, ainsi qu'une classe de « gars du sud-est »(dont il est sûrement le seul représentant) dont j'ignorais totalement l'existence et pour qui les plaisirs simples de la vie ne sont pas étranger. Qu'il recoive en gage de sa précieuse amitiée toute mon affection.
Enfin je remercie tous mes camarades du LMFI, en particulier Clément, Paulo, Simon (pour sa bière maison), et bien sûr Viri pour sa voix de pearl.
Mes pensées les plus affectueuses se dirigent bien sur vers ma famille, qui m'a toujours soutenue, et en particulier ma filleule Lucille.

1 Théorie de Galois

1.1 Extensions d'Artin-Schreier

Les notations employées ici seront les suivantes, on dénotera par F, k, K, l, L, $\Bbbk$, $\mathbb{K}$ des corps et extensions de corps ($\mathbb{K}$ sera souvent supposé algébriquement clos). On s'intéressera uniquement à des corps de caractéristique p strictement positive, et p désignera toujours la caractéristique du corps ambiant. Pour un corps K on notera K^+ et $K^\times$ respectivement les groupes additif et multiplicatif associés. Pour une extension galoisienne L/K on notera $Gal(L/K)$ son groupe de Galois. $\mathbb{F}_p$ désigne le corps premier. On considèrera souvent ici l'application $\wp : K \to K$ définie par $\wp(x) = x^p - x$. C'est un homomorphisme pour le groupe additif K^+. On notera respectivement K^{ins}, K^{sep}, K^{gal} et K^{alg}, les clôtures inséparable, séparable, galoisienne et algébrique du corps K (éventuellement dans une extension, ce sera précisé le cas échéant).

Definition 1.1.1. *Une extension non triviale L/K est dite d'*Artin-Schreier *si il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $\wp(\alpha) = \alpha^p - \alpha \in K$.*

La première caractérisation des extensions d'Artin-Schreier est la suivante :

Théorème 1.1.2. *Une extension L/K est d'Artin-Schreier si et seulement si c'est une extension de Galois de degrée p.*

Preuve : On suppose que $L = K(\alpha)$ avec $\alpha^p - \alpha = a \in K$. On remarque que le polynôme $X^p - X - a$ s'annule non seulement en α mais aussi en $\alpha + n$ pour tout $n \in \mathbb{F}_p$ on a donc que $X^p - X - a = (X-\alpha)(X-\alpha-1)\dots(X-\alpha-p+1)$, en particulier si le polynôme est irréductible, l'extension est normale et séparable. Le polynôme est irréductible car le degré de l'extension est premier : si Q est un facteur irréductible, alors l'extension qu'engendre une de ses racines est de degré divisant p donc égal à p et donc Q est un facteur trivial car le polynôme est séparable.

Réciproquement on suppose que L/K est cyclique de degrée p et on prend σ un générateur du groupe de Galois. On commence par montrer l'existence d'un $\alpha \in L$ tel que $\sigma\alpha = \alpha + 1$. Pour cela on considère l'opérateur $T = \sigma - Id$ qui est une application K-linéaire de L, de noyau K puisque σ engendre le groupe de Galois. On a $T^p = \sigma^p - Id = 0$ (car Id commute avec σ) et donc $T(T^{p-1}(L)) = 0$ autrement dit $ImT^{p-1} \subseteq \ker T = K$ de plus comme ImT^{p-1} est un K-espace vectoriel, on a $ImT^{p-1} = K$ et donc il existe un $c \in L$ tel que $T^{p-1}(c) = 1$ et soit enfin $\alpha = T^{p-2}(c)$. À présent comme $T(\alpha) = 1$ on a $\sigma\alpha = \alpha + 1$ ainsi $\sigma^i(\alpha) = \alpha + i$ pour $i \in \mathbb{F}_p$. On peut maintenant conclure. Comme $\sigma\alpha \neq \alpha$ on a $\alpha \in L \setminus K$ et comme $[L : K]$ est premier $L = K(\alpha)$, et on a de plus $\sigma(\alpha^p - \alpha) = \alpha^p + 1 - (\alpha + 1) = \alpha^p - \alpha$ et donc $\alpha^p - \alpha \in K$ et on conclut. □

Remarquons que la preuve montre que le polynôme $X^p - X - a$ est irreductible sur K si et seulement si il n'a pas de racines dans K.

Remarque 1.1.3 (Théorie de Galois infinie et le nombre d'extensions d'Artin-Schreier)**.** *On s'intéresse à présent au nombre d'extensions d'Artin-Schreier du corps K. On cherche donc le*

nombre d'extensions galoisiennes de degrée p de K. Par théorie de Galois infini, en posant $G = Gal(K^{sep}/K)$ *on sait que les extensions galoisienne de degrée p sont en bijection avec les sous-groupes fermés (pour la topologie des espaces profinis) distingués d'indice p de G. On considère à présent un homomorphisme* $\phi : G \to \mathbb{F}_p^+$ *non nul, donc surjectif puisque* $\mathbb{F}_p^+$ *est cyclique d'ordre p. On a alors que* $\ker\phi$ *est un sous groupe de G qui est d'indice p et distingué dans G (et même caractéristique). Les sous-groupes distingués de G sont des voisinages ouverts de* 1 *et si l'indice est fini alors son complémentaire est une union finie de ses translatés qui sont encore des ouverts et donc les sous-groupes distingués de G d'indice finis sont fermés. Donc* $\ker\phi$ *est un sous groupe fermé de G d'indice p ; notez qu'on a de plus que* ϕ *est continue*[1]*. Réciproquement si H est un sous groupe fermé distingué d'indice p de G alors il existe* $\bar{\phi} : G/H \cong \mathbb{F}_p^+$ *et* $\phi : G \to \mathbb{F}_p$ *défini par* $\phi(x) = \bar{\phi}(x + H)$ *est alors telle que* $\ker\phi = H$*. On conclut donc que le nombre d'extensions d'Artin-Schreier est égal au cardinal de l'ensemble*

$$\mathcal{N} = \left\{\ker\phi \mid \phi \in hom(G, \mathbb{F}_p^+)\right\}$$

où $hom(G, \mathbb{F}_p^+)$ *est l'ensemble des homomorphismes continus entre G et* $\mathbb{F}_p^+$*.*

Remarque 1.1.4 (Un isomorphisme)**.** *Considérons* $G = Gal(K^{sep}/K)$ *et* $hom(G, \mathbb{F}_p^+)$ *le groupe des homomorphismes additifs continus. Soit* $a \in K$*, on constate premièrement que si* $x \in K^{sep}$ *avec* $\wp x = a$ *alors le nombre* $\sigma x - x$ *ne dépend pas du x choisi, pour chaque* $\sigma \in G$*. On définit alors une application*

$$\begin{array}{rccc} \Phi : K^+ & \longrightarrow & hom(G, \mathbb{F}_p^+) \\ a & \longmapsto & \varphi_a \end{array}$$

telle que $\varphi_a(\sigma) = \sigma x - x$ *pour un* $x \in \wp^{-1}(a)$*. On vérifie d'abord que* φ_a *est un homomorphisme de groupe :* $\varphi(\sigma\circ\tau) = \sigma(\tau x) - \sigma x + \sigma x - x = \sigma(\varphi_a(\tau)) + \varphi_a(\sigma) = \varphi_a(\sigma) + \varphi_a(\tau)$ *(car* $\tau x - x \in \mathbb{F}_p$*). On vérifie alors que* Φ *est un homomorphisme. En effet le choix de* $\wp^{-1}(a+b)$ *n'importe peu et donc on prend* $(x+y)^p - (x+y) = a + b$ *et on a* $\varphi_{a+b}(\sigma) = \sigma x - x + \sigma y - y = \varphi_a(\sigma) + \varphi_b(\sigma)$*. Enfin si* $\varphi_a = 1_{hom(G,\mathbb{F}_p^+)}$ *cela signifie que* $\wp^{-1}(a) \subseteq K$*, on conclut que* $\ker\Phi = \wp K$*. On a donc établit l'isomorphisme suivant :*

$$K^+/\wp K \cong hom(G, \mathbb{F}_p^+)$$

Remarque 1.1.5 (Action par multiplication)**.** *Il est clair que l'on dispose d'une action de* $\mathbb{F}_p^\times$ *sur le groupe additif de tout corps de caractéristique p, c'est exactement celle de* $\mathbb{Z}$ *qu'on a rendu fidèle. Plus généralement,* $\mathbb{F}_p^\times$ *agit sur tout groupe d'exposant p fidèlement par translation.*

Théorème 1.1.6. *Le nombre d'extensions d'Artin-Schreier du corps K est égal au nombre d'orbites non-triviales dans l'action de* $\mathbb{F}_p^\times$ *sur le groupe* $K^+/\wp K$*.*

PREUVE : Par la remarque 1.1.3 il faut montrer que $\mathcal{N}$ est en bijection avec les orbites non triviales de l'action de $\mathbb{F}_p^\times$ sur $K^+/\wp K$. On commence par considérer l'action de $\mathbb{F}_p^\times$ sur $hom(G, \mathbb{F}_p^+)$. Dans cette action il n'y a qu'une orbite réduite à un point, c'est celle de l'homomorphisme trivial $x \mapsto 0$. En considérant $\varphi \in hom(G, \mathbb{F}_p^+)\setminus\{0\}$, l'orbite est notée $\mathbb{F}_p^\times\varphi$ et soit $(\varphi_i)_{i\in I}$ un système de représentant des orbites non triviales. On a que pour tout $\psi \in hom(G, \mathbb{F}_p^+)$, soit $\psi = 0$ soit il existe $i \in I$ et $a \in \mathbb{F}_p^\times$ tels que $\psi = a\varphi_i$. À présent on vérifie que $\psi \in \mathbb{F}_p^\times\varphi_i$ si et seulement si $\ker\psi = \ker\varphi_i$, le sens direct est immédiat et le sens réciproque suit du fait que $\varphi \circ \psi^{-1} : \mathbb{F}_p^+ \to G/\ker\psi = G/\ker\varphi \to \mathbb{F}_p^+$ est $\mathbb{F}_p$-linéaire, donc de la forme $x \mapsto ax$ et on conclut. L'application qui a φ_i associe $\ker\varphi_i$ est donc une bijection de l'ensemble des orbites

1. En effet la préimage d'un voisinage de $0_{\mathbb{F}_p}$ est une union finie de translatés de $\ker\phi$ qui est un ouvert.

non triviales pour l'action de $\mathbb{F}_p^\times$ sur $hom(G, \mathbb{F}_p^+)$ à l'ensemble $\mathcal{N}$. Enfin on a un isomorphisme entre $K^+/\wp K$ et $hom(G, \mathbb{F}_p^+)$ par la remarque 1.1.4, on conclut donc le théorème. □

Remarque 1.1.7. *Remarquons que si $[K^+ : \wp K]$ est infini, comme le cardinal de chaque orbite sous l'action de $\mathbb{F}_p$ est fini alors le nombre d'extensions d'Artin-Schreier est infini.*

Definition 1.1.8. *On dit qu'un corps K est* Artin-Schreier clos *si il n'admet pas d'extension d'Artin-Schreier.*

Remarque 1.1.9. *Il est immédiat qu'un corps est Artin-Schreier clos si et seulement si $\wp : K \to K$ est une surjection. Ainsi cela signifie que « K est Artin-Schreier clos »est une propriété élémentaire de K : cela se traduit par*

$$K \models \forall x \exists y y^p - y = x$$

Exemple 1.1.10.

- *Le polynôme $X^p - X - a$ étant séparable, on a que tout corps séparablement clos est Artin-Schreier clos.*
- *Un corps fini $\mathbb{F}_q$ n'est pas Artin-Schreier clos, puisque $\wp : \mathbb{F}_q \to \mathbb{F}_q$ n'est pas injective car son noyau est $\mathbb{F}_p$. On en déduit qu'un ultraproduit non-principal de corps finis de la famille $(\mathbb{F}_{p^n})_{n<\omega}$ n'est pas Artin-Schreier clos non plus par la remarque précédente.*

Remarque 1.1.11 (Extensions cycliques de degré premier)**.** *Rappelons quelques faits classiques sur les extensions cycliques. Ce qui marche dans les résultats d'Artin-Schreier est que le polynôme $X^p - X - a$ est séparable et que ses racines sont obtenues à partir d'une seule et $\mathbb{F}_p$. On aimerait pouvoir étudier de même le cas où l'extension est cyclique de degré un nombre différent de la caractéristique. En considérant une extension L/K* radicielle [2] *de degré $l \neq p$ (l premier), alors on constate que l'application $x \mapsto x^l$ joue le même rôle*[3] *que l'application $\wp$ dans les extensions d'Artin-Schreier. Une telle extension est alors engendrée par une racine du polynôme $X^l - a$ pour un $a \in K$. On appelle une extension radicielle de degrée premier $l \neq p = carK$ une* extension de Kummer*. En récapitulant ce que l'on sait sur une extension cyclique radicielle L/K donnée de degré l premier. Soit l est égal à la caractéristique de K, dans ce cas l'extension est d'Artin-Schreier et il existe $a \in K$ tel que $L = K(\wp^{-1}a)$. Soit on a $l \neq p$, l'extension est donc de Kummer et il existe un $a \in K$ tel que $L = K(\sqrt[l]{a})$.*

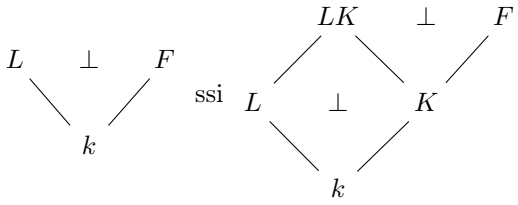
1.2 Extensions régulières

Cette sous-section n'est pas fondamentale pour comprendre la preuve du principal résultat de ce mémoire. Les notions de polynômes absolument irréductibles et d'extensions régulières interviendront dans l'étude des corps pseudo-algébriquement clos, dans la section 5. On rappelle que si l'on considère deux extensions L et K de k on dit que L et K sont *linéairement disjoints sur* k si toute famille finie k-linéairement indépendante de L est aussi K-linéairement indépendante dans le compositum LK ; ou de manière équivalente toute famille finie k-linéairement indépendante de K reste L-linéairement indépendante dans KL (on le notera $L \perp_k K$). On vérifie que

2. Une extension L/K est radicielle si K contient une racine primitive l-ième de 1.

3. La preuve est en fait légèrement différente, en effet on se donne L/K une extension cyclique radicielle de degrée l, σ un générateur du groupe de Galois et on cherche un α tel que $\sigma\alpha = \zeta\alpha$ avec ζ racine primitive l-ième de 1. L'argument simple de la preuve d'Artin-Schreier ne fonctionne plus ici à cause de la caractéristique, mais on voit que ce que l'on cherche est un vecteur propre de σ pour la valeur propre ζ. Pour montrer que σ admet ζ comme valeur propre, on utilise l'indépendance des caractères.

dans le cas où les extensions sont finies cela revient à demander à ce que $[L : k] = [LK : K]$, et dans le cas où L/k est galoisienne, il suffit juste que $L \cap K = k$. On a de plus que si $\bar{t}$ est algébriquement indépendant sur L, alors L et $k(\bar{t})$ sont linéairement disjoints sur k. Enfin la propriété de transitivité, si $k \subseteq K \subseteq F$ et $k \subseteq L$ alors $L \perp_k F$ ssi $L \perp_k K$ et $LK \perp_K F$, visuellement :



Enfin remarquons que cette définition est locale, donc pour montrer $L \perp_k K$ il suffit de montrer que $L_0 \perp_k K$ pour tout $L_0 \subseteq L$ finiment engendrée contenant k. Enfin, on montre que cette relation ternaire est en fait symmétrique, i.e. $L \perp_k K \iff K \perp_k L$.

Rappelons par exemple comment la notion d'extension séparable est définie grâce à la relation $\perp$ lorsque les extensions ne sont pas nécessairement algébriques : on dit que L/K est séparable si $L \perp_K K^{ins}$. On voit de par les propriétés de la relation $\perp$ que si L/K est séparable, alors il en est de même pour F/K pour tout F corps intermédiaire. On a aussi que si L/F et F/K sont séparables, alors L/K l'est aussi. Une propriété qui aide à comprendre ce qu'est une extension séparable est l'existence de *base de transcendance séparante*. Si L/K est une extension séparable alors pour tout $L_0 \subseteq L$ finiment engendré contenant K, on peut montrer qu'il existe $t_1, \dots, t_l \in L_0$ algébriquement indépendants sur K et tels que $L_0/K(t_1, \dots, t_l)$ soit finie et séparable. On décompose donc L_0/K en $L_0/K(t_1, \dots, t_l)$ séparable finie et $K(t_1, \dots, t_l)/K$ purement transcendante. On appelle $t_1, \dots, t_l$ une *base de transcendance séparante*. On peut montrer que l'existence d'une base de transcendance séparante pour toute sous-extension finiment engendrée est une condition nécessaire et suffisante pour être une extension séparable.

Une extension L/K est dite *régulière* si $L \perp_K K^{alg}$. On montre facilement que c'est équivalent à ce que l'on ait les deux points suivants :

— L/K est séparable

— K est algébriquement clos dans L

En utilisant les propriétés de $\perp$ on a de la même façon que précédemment que pour $K \subseteq F \subseteq L$ et L/K est régulière, alors F/K est régulière aussi. Si L/F et F/K sont régulières alors il en est de même pour L/K. On va mettre ici en bijection les extensions régulières d'un corps K avec le spectre des idéaux *absolument premiers* de $K[\bar{X}]$, i.e. les idéaux premiers P de $K[\bar{X}]$ qui engendrent dans $K^{alg}[\bar{X}]$ un idéal qui est encore premier. Un polynôme est *absolument irréductible* s'il engendre un idéal absolument premier.

Remarque 1.2.1 (Extensions régulières et produit tensoriel)**.** *La condition $L \perp_k K$ est équivalente à ce que l'application k-linéaire $L \otimes_k K \to LK$ définie par $u \otimes v \mapsto uv$ soit injective (ou de manière équivalente : définisse un isomorphisme avec $L[K]$). Cela utilise principalement qu'une fois qu'on a fixé une K-base de L disons l_i alors l'écriture des éléments de $L \otimes_k K$ comme $\sum l_i \otimes a_i$ est unique. On constate de plus que c'est équivalent à ce que $L \otimes_k K$ soit un anneau intègre. En particulier, une extension L/K est régulière si et seulement si $L \otimes_K K^{alg}$ est intègre.*

On considère à présent la bijection entre les extensions engendrées par n éléments de K et le spectre des idéaux premiers de $K[X_1, \dots, X_n]$, qui a $K(a_1, \dots, a_n)$ associe

$$I(a_1, \dots, a_n/K) = \{f \in K[X_1, \dots, X_n] \mid f(a_1, \dots, a_n) = 0\}$$

autrement dit en notant $\mathcal{F}_n$ la classe des extensions finiment engendrées par n éléments de K (représentées à isomorphisme près), on a

$$\begin{array}{rcl} I : \mathcal{F}_n & \longrightarrow & Spec_P(K[X_1, \ldots, X_n]) \\ K(a_1, \ldots, a_n) & \longmapsto & I(a_1, \ldots, a_n/K) \end{array}$$

Étant donné P un idéal premier de $K[X_1, \ldots, X_n]$ on a que P est l'image de l'extension $K[X_1, \ldots, X_n]/P = K[X_1 + P, \ldots, X_n + P]$. À présent $K(a_1, \ldots, a_n)/K$ est une extension régulière si et seulement si $K(a_1, \ldots, a_n) \otimes_K K^{alg}$ est intègre, ce qui est équivalent à ce que $K[a_1, \ldots, a_n] \otimes_K K^{alg}$ soit intègre. À présent soit $J = K^{alg}[\bar{X}] \cdot I(a_1, \ldots, a_n/K)$. On vérifie qu'on a l'isomorphisme de K-algèbre entre $K[a_1, \ldots, a_n] \otimes K^{alg}$ et $K[X_1, \ldots, X_n]/J$ donné par $f(a_1, \ldots, a_n) \otimes l \mapsto l \cdot f(X_1, \ldots, X_n) + J$. On a alors que $K(a_1, \ldots, a_n)/K$ est régulière si et seulement si J est premier, si et seulement si I est absolument premier. On a donc montré :

Lemme 1.2.2. *L'extension $K(a_1, \ldots, a_n)/K$ est régulière si et seulement si $I(a_1, \ldots, a_n/K)$ est absolument premier.*

Remarque 1.2.3. *Avec les notations du lemme précédent, et si l'on rajoute de plus l'hypothèse que*

$$tr.deg(a_1, \ldots, a_n/K) = n - 1$$

alors disons que a_n est algébrique sur $a_1, \ldots, a_{n-1}$ de polynôme minimal $P(X_n) \in K(a_1, \ldots, a_{n-1})[X_n]$, soit $g(X_1, \ldots, X_{n-1})$ le ppcm des polynômes $g_k(X_1, \ldots, X_{n-1})$ ou $g_k(a_1, \ldots, a_{n-1})$ sont les dénominateurs des coefficients de P et soit $f(\bar{X}) = g(X_1, \ldots, X_{n-1}).P(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$. Alors ce polynôme est irréductible et engendre l'idéal annulateur $I(a_1, \ldots, a_n/K)$ qui est donc principal. En effet il suffit de considérer, étant donné $Q \in I(a_1, \ldots, a_n/K)$ la division euclidienne (dans $K(X_1, \ldots, X_{n-1})[X_n]$) de Q par P et on a alors une contradiction sur la minimalité de P. Dans le cas où l'extension est régulière, le polynôme f est absolument irréductible.

2 Géométrie algébrique élémentaire et théorie des modèles.

2.1 Rappels de base sur les groupes algébriques

Dans cette section il s'agit d'introduire les notions de géométrie algébrique que l'on va utiliser. On se place donc dans le contexte usuel de la géométrie algébrique, avec un univers ambiant $\mathbb{K} \models ACF_p$ (p un nombre premier ou 0) i.e. un corps algébriquement clos et un sous corps K. On suppose en général que $|\mathbb{K}| > |K|$ (en particulier, le degré de transcendance de $\mathbb{K}$ sur K est infini) ainsi que le corps K est parfait, on reviendra sur ces hypothèses un peu plus loin. Les groupes algébriques qui seront maniés ici seront des groupes algébriques dits *affine*. On commence par quelques rappels de base concernant la géométrie algébrique classique.

Étant donné un ensemble $S \subseteq \mathbb{K}[X_1, \ldots, X_n]$, une *variété affine* (ou *fermé de Zariski*) est donnée par $V(S) := \{(x_1, \ldots, x_n) \in \mathbb{K}^n \mid \forall P \in S \; P(\bar{x}) = 0\}$. On associe alors à une variété V un idéal $I(V)$ de $\mathbb{K}[\bar{X}]$ formé des polynômes qui s'annulent sur tout élément de V. De même on pourra associer $V(K)$ l'ensemble des points rationnels de V sur K, i.e. $V(K) = V \cap K^n$. On rappelle que sur $\mathbb{K}^n$, les variétés affines sont les fermés d'une topologie appelée *topologie de Zariski* qui est *noethérienne* (i.e. toute suite décroissante de fermés est finie), cette topologie se restreint sur K^n ainsi que sur toute variété affine et garde la noethérianité. Noter que l'on utilisera la dénomination de variété affine lorsque l'on parlera de l'espace topologique pour la topologie restreinte alors que l'on préfèrera le terme fermé de Zariski pour l'élément de la topologie de $\mathbb{K}^n$ (ou K^n). On définit le produit de deux variétés affines $V = V(f_1, \ldots, f_s) \subseteq \mathbb{K}^n$ et $W = V(g_1, \ldots, g_r) \subseteq \mathbb{K}^m$ en posant $V \times W := V(f_1(X_1, \ldots, X_n), \ldots, f_s(X_1, \ldots, X_n), g_1(Y_1, \ldots, Y_m), \ldots, g_r(Y_1, \ldots, Y_m)) \subseteq \mathbb{K}^{n+m}$, ainsi le produit de deux variétés affines est encore une variété affine dont la topologie est noetherienne [1]. Un élément d'une topologie est dit *irréductible* s'il n'est pas réunion de deux fermés distincts. Un ensemble topologique non nécessairement séparé quelconque se décompose toujours en composantes irréductibles maximales, si de plus la topologie est noethérienne ces composantes maximales sont en nombre fini (et la décomposition est unique à permutation près). On montre aisément que $I(V)$ est premier si et seulement si V est irréductible (dans $\mathbb{K}^n$). On a donc que toute variété affine se décompose en une union finie de variétés affines irréductibles. Notez que le produit de deux variétés irréductibles est encore une variété irréductible. Remarquons que si deux variétés affines distinctes ont des idéaux associés distincts, on peut tout à fait avoir deux idéaux distincts définissant la même variété affine. Le Nullstellensatz de Hilbert nous assure que si l'on se restreint aux idéaux *radicaux* on a une et une seule variété affine correspondante. Le

1. Il est à noter que la topologie du produit ainsi définie n'est pas du tout la topologie produit au sens topologique : pour s'en convaincre, remarquer que les fermés de $\mathbb{K}$ sont soit finis soit $\mathbb{K}$ et donc les fermés de la topologie produit sur $\mathbb{K}^2$ qui ne sont pas de la forme $C \times \mathbb{K}$ doivent aussi être finis ; or pour peu que le corps soit infini il existe une infinité de points dans le fermé de Zariski $V(XY - 1)$.

spectre radical de $\mathbb{K}[X]$ est donc en bijection avec l'ensemble des variétés affines de $\mathbb{K}^n$. De plus on a aussi que le spectre des idéaux premiers de $\mathbb{K}[X]$ lui est en bijection avec l'ensemble des variétés affines irréductibles [2] de $\mathbb{K}^n$.

Un variété V sera dite *définie sur* $K \subseteq \mathbb{K}$ si $I(V)$ est engendré (dans $\mathbb{K}[\bar{X}]$) par $I(V) \cap K[\bar{X}]$. Si $V = V(f_1, \ldots, f_n)$ il ne suffit pas que le corps K contienne les coefficients des f_i pour que V soit définie [3] sur K. On peut montrer que toute variété admet un plus petit corps de définition. En fait on montre que ce dernier est le corps engendré par les coefficients des monômes qui sont liés dans $\mathbb{K}[X]/I(V)$ lorsqu'on les exprimes dans la base monomiale de $\mathbb{K}[X]/I(V)$ et que ce corps est inclu dans la clôture inséparable d'un corps contenant les générateurs de $I(V)$.

On rappelle que ACF_p est complète et a l'élimination des quantificateurs. Par l'élimination des quantificateurs, si φ isole un type, comme elle est ACF_p-equivalente à une formule sans quanteurs, i.e. une combinaison booléenne d'équation polynomiales, elle contient nécessairement une équation polynomiale, car sinon la formule ne pourrait pas isoler le type. Les 1-types dans ACF_p sont donc de deux sortes : algébriques et donc isolés (par une formule contenant une et une seule équation polynomiale et ce polynôme est alors le polynôme minimal sur le corps engendré par les paramètres du type) et un unique type transcendant. On note respectivement $dcl(A)$ et $acl(A)$ les clôtures définissable et algébrique au sens de la théorie des modèles. On note $\Bbbk$ le sous-corps premier de $\mathbb{K}$. On fait ici la correspondance entre les notions d'algébricité et de définissabilité au sens de la géométrie algébrique et au sens de la théorie des modèles.

Lemme 2.1.1. *Avec les notations précédentes, si $A \subseteq \mathbb{K}$ alors $acl(A) = \Bbbk(A)^{alg}$ et $dcl(A) = \Bbbk(A)^{ins}$.*

PREUVE : Comme $\Bbbk = acl(\emptyset) = dcl(\emptyset)$ il est clair que si a est algébrique sur $\Bbbk(A)$ alors $a \in acl(A)$. Réciproquement si $a \in acl(A)$ alors $tp(a/A)$ est algébrique et donc la formule isolant le type contient une équation polynomiale à coefficient dans $\Bbbk(A)$ donc a est algébrique sur ce dernier. Soit à présent $a \in \Bbbk(A)^{ins}$, et soit donc $m(X)$ le polynôme minimal de a sur $\Bbbk(A)$. Comme a est purement inséparable, $m(X)$ n'a qu'une seule racine et donc la formule $m(x) = 0$ à paramètre dans $\Bbbk(A)$ définit a sur A. Réciproquement si $a \in dcl(A)$ il vient que $tp(a/A)$ est isolé disons par une formule contenant une (et une seule) équation polynomiale à coefficient dans $\Bbbk(A)$ et ce polynôme n'a par hypothèse qu'une seule racine : a ; qu'importe le degré du polynôme cela implique que $a \in \Bbbk(A)^{ins}$. □

Il vient alors de ce lemme que l'on va pouvoir parler sans ambiguité de la notion d'élément *algébrique* sur un certain ensemble. Si l'on considère une variété V définissable sur un corps K (au sens de la théorie des modèles i.e. $V = \phi(\mathbb{K})$ où ϕ est une conjonction d'égalités polynomiales à paramètres dans $A \subseteq \mathbb{K}$) alors les paramètres de ϕ sont dans $dcl(A)$ et donc par le lemme il est clair que V est définie sur $\Bbbk(A)^{ins}$. Réciproquement soit V une variété définie sur un corps K_0 (au sens de la géométrie algébrique). Alors si V est définissable sur K au sens de la théorie des modèles, il apparaît par le lemme que $K_0 \subseteq K^{ins}$ et donc V est définissable sur K^{ins}. On a donc que V est définissable sur le corps K (au sens de la théorie des modèles) si et seulement si V est définie sur K^{ins} (au sens de la géométrie algébrique). En particulier les deux notions coïncident lorsque K est parfait et dans ce cas précis on utilisera simplement le terme *définissable*.

Soit V une variété affine, on peut voir $\mathbb{K}[X]/I(V)$ comme un anneau de fonctions polynomiales $V \to \mathbb{K}$ car si $f - g \in I(V)$ $f = g + h$ avec $h \in I(V)$ et donc f et g coïncident sur

2. Remarquons qu'une conséquence de cela est que tout idéal premier est une intersection finie d'idéaux radicaux.

3. Le contre-exemple classique est pour un corps de caractéristique p, $a \in K$ tel que $X^p - a$ soit irréductible, et α l'unique racine de $X^p - a$. Alors si $V = V(X^p - a)$ on a que $I(V) = \mathbb{K}[X] \cdot (X - \alpha)$ et $I(V) \cap K[X]$ engendre dans $\mathbb{K}[X]$ l'idéal $\mathbb{K}[X] \cdot (X^p - a)$, ainsi on voit que V est définie sur $K(\alpha)$ mais pas sur K.

V. On appelle $K[V] := K[X]/I(V)$ l'*anneau des fonctions de* V. Dans le cas où V est irréductible cet anneau est intègre et on note $K(V)$ son corps de fractions, appelé *corps des fonctions de* V. On appelle *dimension* de la variété affine irréductible V le degré de transcendance de l'extension $\mathbb{K}(V)/\mathbb{K}$ qui est fini puisque $K[V]$ est finiment engendré. Dans le cas d'une variété affine quelconque, la dimension est le max des dimensions de chaque composante irréductible. Étant donné que l'on a supposé que $\mathbb{K}$ était de degré de transcendance infini sur K, si l'on considère une variété affine irréductible V définie sur K, on peut considérer un élément $\bar{\alpha} \in \mathbb{K}^n$ tel que $K(V)$ soit isomorphe à $K(\bar{\alpha})$. Un tel point est appelé un *générique de* V *sur* K, c'est un élément vérifiant les équations de V et n'en vérifiant aucune autre. Si un élément $\bar{a}$ et un corps K sont donnés, on peut aussi se demander quelles sont les équations que cet uplet vérifie sur K et de quelle variété cet uplet est-il un générique sur K : on considère pour cela $I(\bar{a}/K)$ l'idéal (premier) des polynômes de $K[\bar{X}]$ qui s'annulent en $\bar{a}$, et ensuite $V_{\bar{a}} := V(I(\bar{a}/K)) \subseteq \mathbb{K}^{|\bar{a}|}$. C'est une variété irréductible sur K définie sur K dont $\bar{a}$ est un générique. On l'appelle le *locus de* $\bar{a}$ *sur* K. Il peut tout à fait arriver que le locus de $\bar{a}$ sur K ne soit pas irréductible dans une extension de K, en revanche si l'idéal $I(\bar{a}/K)$ est absolument premier c'est le cas pour toute extension.

Noter qu'un élément de $K(V)$ est défini partout sauf sur un fermé de V (les zéros du dénominateur) et son domaine de définition est donc un ouvert de la variété affine irréductible V i.e. l'intersection d'un fermé de Zariski et d'un ouvert de Zariski. On appelle cela une *variété quasi-affine*. On peut remarquer qu'un tel ouvert d'une variété est l'intersection d'un fermé de Zariski (disons défini par $f_1, \ldots, f_s$) avec un ouvert (complémentaire du fermé défini par disons $g_1, \ldots, g_r$) il en résulte qu'il est définissable par la formule $\bigwedge_{i=1,\ldots,s} f_i(x) = 0 \wedge \bigvee_{i=1,\ldots,r} g_i(x) \neq 0$. Remarquons que si l'on parle du domaine d'un élément de $K(V)$, on a $r = 1$. Soit U un ouvert de Zariski. Une application $f : U \to \mathbb{K}$ sera dite *régulière* si elle est localement une fonction rationnelle définie, en d'autres termes si pour tout $a \in U$ il existe un voisinage de a $U_a \subset U$ ainsi que $P, Q \in \mathbb{K}[X]$ avec Q n'ayant pas de zéros dans U_a et tels que pour tout $b \in U_a$ $f(b) = \frac{P(b)}{Q(b)}$. Les éléments de $K(V)$ sont des fonctions régulières sur l'ouvert complémentaire des zéros du dénominateur. Ce sont clairement des fonctions à valeurs dans $\mathbb{K}$ qui sont continues pour la topologie de Zariski, et il en est de même pour les fonctions régulières qui sont continues sur tout voisinage, donc continues. Notez que la noetherianité de l'espace implique qu'une fonction régulière est en fait un recollement de fonctions rationnelles sur un nombre fini d'ouverts.

Si $V \subseteq \mathbb{K}^n$ et $W \subseteq \mathbb{K}^m$ sont deux variétés affines, une application $f : V \to W$ est un *morphisme* si $f = (f_1, \ldots, f_m)$ avec f_i régulières sur tout V. Les morphismes sont bien entendu les applications continues pour la topologie de Zariski. Un *isomorphisme* est un morphisme bijectif dont l'application réciproque est aussi un morphisme. Par exemple si K est un corps de caractéristique p positive, parfait, l'application $x \mapsto x^p$ est clairement un morphisme de K dans K mais la réciproque n'est pas continue, ce n'est pas un polynôme. Le graphe d'un morphisme est une variété affine et le *corps de définition de* f sera celui de son graphe. Encore une fois, lorsque le corps de définition est parfait il n'y aura pas d'ambiguité quant aux notions algébriques et modèle-théorique de la définissabilité. Noter que l'on a la formule $dim V = dim \ker f + dim \mathrm{im} f$. Remarquons enfin qu'une variété quasi-affine est toujours isomorphe à une variété affine, quitte à la regarder dans un espace plus grand. En effet considérons $V(f_i) \cap \{g \neq 0\}$, avec $f_i, g \in \mathbb{K}[X_1, \ldots, X_n]$, on pose $V' = V(f_i, Y.g(\bar{X}) - 1) \subseteq \mathbb{K}[X_1, \ldots, X_n, Y]$ et on considère le morphisme $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, \frac{1}{g(x_1,\ldots,x_n)})$ qui est bien un isomorphisme de $V(f_i) \cap \{g \neq 0\}$ dans V'.

Remarque 2.1.2. *Un morphisme* $f : \mathbb{K} \to V$ *défini sur* K *est nécessairement de la forme* $(f_1, \ldots, f_n)$ *avec* $f_i \in K[X]$*, puisque* f *est défini partout sur un corps qui est algébriquement clos, si il y avait des dénominateurs,* f *aurait des pôles.*

Remarque 2.1.3 (La descente de Weil)**.** *Considérons une variété affine irréductible V définie sur une extension séparable finie L de K. Alors il existe une variété W définie sur K appelée* réduction de Weil *de V sur K, telle que :*
• *W est isomorphe à $V^{[L:K]}$ sur L^{gal}*
• *Il existe une bijection entre les points rationnels de V sur L et les points rationnels de W sur K*
La méthode pour prouver ce théorème est ce que l'on appelle la descente de Weil. *La preuve de ce théorème est donnée en appendice.*

Un *groupe algébrique* est la donnée d'une variété affine G muni de deux morphismes $\mu : G \times G \to G$ et $\iota : G \to G$ qui en font un groupe. De manière plus pratique et équivalente, on se donne une variété quasi-affine sur laquelle on définit un structure de groupe avec des morphismes. L'exemple classique est $Gl_n(\mathbb{K})$, c'est l'ouvert de $\mathbb{K}^{n^2}$ complémentaire de $V(det(X_1, \ldots, X_{n^2}))$, la multiplication est donnée par un polynôme, c'est donc bien un morphisme et l'inverse est le produit de $\frac{1}{det}$ avec l'application qui associe la transposée de la comatrice, qui est polynomiale. Noter que si l'on se tient à la définition par variété affine, il faudrait considérer des couples $(M, det^{-1}M)$ et définir la multiplication et l'inverse en conséquence. Un autre exemple, plus trivial mais qui sera mentionné plus tard est celui du groupe $(\mathbb{K}^n, +)$.
Dans un groupe algébrique G, on vérifie la chose suivante : si e est l'unité alors une et une seule composante irréductible passe par e on l'appelle G^0. Comme $x \mapsto \mu(a, x)$ et ι sont des morphismes, G^0 est stable par multiplication et inverse et on en déduit que G^0 est un sous-groupe et que ses translatés sont les autres composantes irréductibles, qui sont en nombre fini et donc G^0 est d'indice fini dans G. Cela implique aussi que les composantes irréductibles sont disjointes, ce sont donc des composantes connexes de l'espace topologique G, en particulier on appelera G^0 la *composante connexe de G*. Comme c'est une composante irréductible, G^0 est un fermé de G (remarquons qu'il est aussi ouvert car son complémentaire est une union finie de classes à gauche). Enfin si H est un sous groupe fermé d'indice fini de G alors il existe des classes à gauche de H qui recouvrent G^0 qui s'écrit alors comme union de fermés disjoints et par connexité de G^0 cela force G^0 à être lui même dans une classe et donc dans celle de l'identité i.e. $G^0 \subseteq H$. On voit alors que G^0 est le plus petit sous groupe de G fermé d'indice fini dans G. Noter que les sous-groupes fermés de G sont encore des groupes algébriques et que les sous-groupes définissables de G sont fermés. On en déduit que G^0 est définissable sur le même ensemble sur lequel G est défini, puisque G^0 est l'intersection de tous les sous-groupes algébriques de G, or par noethériannité de G cette intersection doit être finie et donc G^0 est bien définissable, c'est bien un sous-groupe algébrique et les paramètres utilisés sont ceux de G. En utilisant l'ω-stabilité en théorie des modèles : G est un groupe définissable dans la théorie ACF_p qui est fortement minimale, donc de rang de Morley 1, cela force toute chaîne infinie décroissante d'ensembles définissables à être finie et donc l'intersection sur les formules définissant un sous-groupe de G d'indice fini dans G est donc une intersection finie, qui définit G^0 et on a utilisé pour cela uniquement les paramètres qui définissent G.

2.2 Groupes vectoriels

Definition 2.2.1. *On dit que G est un* groupe vectoriel *si G est un groupe algébrique isomorphe au groupe algébrique $(\mathbb{K}^n, +)$.*

Lemme 2.2.2. *Soit G un groupe vectoriel et H un sous groupe fermé et connexe de G alors H est un groupe vectoriel.*

PREUVE : La preuve de ce résultat n'est pas très compliquée mais ferait une trop grande

digression dans le corpus de ce mémoire, elle est donnée en appendice. □

Remarque 2.2.3 (Rappels de cohomologie Galoisienne élémentaire)**.** *On se donne un G-module abelien A, G est noté multiplicativement et A additivement. Un* 1-cocycle *est une application $f : G \to A$ tel que pour $\sigma, \tau \in G$ on ait $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$. Une application $f : G \to A$ sera appelée un* 1-cobord *si il existe $\beta \in A$ tel que $f(\sigma) = \sigma\beta - \beta$. Tout 1-cobord est un 1-cocycle. Un fait intéressant apparaît lorsque la réciproque est vraie, dans ce cas on traduit le résultat par $H^1(G, A) = 0$. Dans le cas d'une extension galoisienne finie K/k de groupe de Galois G, on a que $K^\times$ est un G-module et on peut montrer que l'on a toujours $H^1(G, K^\times) = 1$.*

Le théorème principal qui nous intéresse :

Théorème 2.2.4. *Soit G un groupe vectoriel connexe de dimension 1 défini (dans $\mathbb{K}$) sur le corps parfait K alors il existe un isomorphisme entre G et $\mathbb{K}^+$ défini sur K.*

Preuve : On a donc que G est isomorphe au groupe additif $\mathbb{K}^n$. Comme G est un groupe vectoriel connexe on peut parler de son corps de fonction qui est de degré de transcendance 1 et donc c'est $K(X)$ où X est une indéterminée. À présent l'idéal de $\mathbb{K}^n$ est $(0) \subsetneq K[X_1, \ldots, X_n]$ donc son corps de fonctions est $K[X_1, \ldots, X_n]$ ce dernier doit être isomorphe à $K[X]$ ce qui force $n = 1$.
À présent soit $\theta : G \to \mathbb{K}^+$ l'isomorphisme additif en question. Il est à paramètres dans $\mathbb{K}$ mais on va montrer qu'on peut le modifier de façon à ce que les paramètres soient dans K. On suppose donc que L est une extension galoisienne (finie) de K contenant les paramètres définissant [4] θ. On sait que $H^1(Gal(L/K), L^\times) = 1$, ce qui signifie que tout 1-cocycle de G dans $L^\times$ est un 1-cobord. On va associer à θ un 1-cocycle de G dans $L^\times$. Pour $\sigma \in Gal(L/K)$ on pose θ^σ l'application obtenue en appliquant σ aux coefficients. On a, puisque θ est une application rationnelle que $\theta^\sigma = \sigma \circ \theta \circ \sigma^{-1}$, en effet si $\theta(x) = \frac{P(x,\bar{a})}{Q(x,\bar{a})}$ où $\bar{a}$ est l'uplet de paramètres définissant θ alors

$$\theta^\sigma(x) = \frac{P(x, \sigma\bar{a})}{Q(x, \sigma\bar{a})} = \frac{\sigma(P(\sigma^{-1}x, \bar{a}))}{\sigma(Q(\sigma^{-1}x, \bar{a}))} = \sigma(\theta(\sigma^{-1}(x)))$$

On définit maintenant $f : Gal(L/K) \to L^\times$ par $f(\sigma) = \theta^\sigma(\theta^{-1}(1))$. Montrons que f est un 1-cocycle. On remarque déjà que pour tout σ, $\theta^\sigma \circ \theta^{-1}$ est un isomorphisme [5] additif (de variétés affines) de $\mathbb{K}$, c'est par conséquent une application $\mathbb{K}$-linéaire et on a donc $\theta^\sigma \circ \theta^{-1}(x) = f(\sigma) \cdot x$ (avec $f(\sigma) \in L^\times$). On calcule alors

$$\begin{aligned}
f(\sigma\tau) &= \theta^{\sigma\tau}(\theta^{-1}(1)) \\
&= \sigma(\theta^\tau(\sigma^{-1}(\theta^{-1}(1)))) \\
&= \sigma(\theta^\tau(\theta^{-1}[\theta(\sigma^{-1}(\theta^{-1}(1)))])) \\
&= \sigma(\theta^\tau(\theta^{-1}[\sigma^{-1}(f(\sigma))])) \\
&= \sigma(\sigma^{-1}(f(\sigma)) \cdot \theta^\tau(\theta^{-1}(1))) \\
&= f(\sigma) \cdot \sigma(f(\tau))
\end{aligned}$$

On a alors par la remarque 2.2.3 que f est un 1-cobord : il existe donc $\beta \in L^\times$ tel que $f(\sigma) = \frac{\sigma\beta}{\beta}$. On montre à présent que $\tilde{\theta} := \beta^{-1} \cdot \theta$ est l'isomorphisme souhaité. Pour cela on

4. Si ces paramètres sont α on prends la clôture galoisienne de $K(\alpha)$.
5. On demande ici que l'application réciproque soit aussi continue pour la topologie de Zariski, cela ne peut donc pas être un p-polynôme (cf A.1.1) à part un polynôme linéaire.

montre que ses paramètres sont invariants par le groupe de Galois, autrement dit que $\tilde{\theta}^\sigma = \tilde{\theta}$ pour tout $\sigma \in Gal(L/K)$. On a donc

$$\tilde{\theta}^\sigma = \sigma\beta^{-1} \cdot \theta^\sigma = (\beta^{-1} f(\sigma)^{-1}) \cdot \theta^\sigma \circ \theta^{-1} \circ \theta = \beta^{-1} \cdot f(\sigma)^{-1} \cdot f(\sigma) \cdot \theta = \tilde{\theta}$$

Ce qui conclut la preuve du théorème. □

2.3 Le groupe vectoriel $G_{\bar{a}}$

On étudie dans cette section le groupe vectoriel défini de la façon suivante, pour $\bar{a} = (a_1, \dots a_n) \in K^{\times n}$

$$G_{\bar{a}} = \left\{ (t, x_1, \dots, x_n) \in \mathbb{K}^{n+1} | \bigwedge_{i=1,\dots,n} t = a_i \cdot (x_i^p - x_i) \right\}$$

Remarque 2.3.1 ($G_{\bar{a}}$ est un groupe vectoriel)**.** *Remarquons que $G_{\bar{a}}$ est bien un fermé de Zariski, défini par les équations $T - a_i \cdot (X_i^p - X_i)$ à paramètres dans K, de plus la caractéristique du corps K étant p, on a que si $(t, \bar{x}), (t', \bar{x}') \in G_{\bar{a}}$ alors $t - t' = a_i \cdot (x_i^p - x_i) - a_i \cdot (x_i'^p - x_i') = a_i \cdot ((x_i - x_i')^p - (x_i - x_i'))$ ainsi $G_{\bar{a}}$ est un groupe algébrique et comme c'est un sous groupe fermé du groupe vectoriel $(\mathbb{K}^{n+1}, +)$ c'est aussi un groupe vectoriel, par le lemme 2.2.2.*

Remarque 2.3.2 ($G_{\bar{a}}$ est de dimension 1)**.** *On considère le morphisme $s : G_{\bar{a}} \to \mathbb{K}^+$ donné par $s(t, x_1, \dots, x_n) = t$. C'est clairement un morphisme de variété qui est aussi un homomorphisme de groupe. On a la formule classique sur les dimensions*

$$dim G_{\bar{a}} = dim \ker s + dim \mathrm{Im} s$$

Comme s est surjective, la dimension de l'image est celle de $\mathbb{K}$ c'est à dire 1. De plus si $s(t, x_1, \dots, x_n) = 0$ on a bien sur $t = 0$ mais aussi $a_i \cdot (x_i^p - x_i) = 0$ ainsi comme $a_i \neq 0$ on a que $\ker s = 0 \times \mathbb{F}_p^n$ qui est une variété affine finie donc de dimension 0, on a donc bien $dim G_{\bar{a}} = 1$.

Remarque 2.3.3 (Définition de $G_{\bar{a}}$)**.** *Le groupe $G_{\bar{a}}$ est défini par des équations à paramètres dans le corps parfait K, on a donc que $G_{\bar{a}}$ est défini* au sens de la géométrie algébrique *sur K autant qu'il est définissable* au sens de la théorie des modèles *sur K. Suivant le deuxième sens, on se permettra de noter $G_{\bar{a}}(\mathbb{K})$ pour la réalisation dans $\mathbb{K}$ de la formule définissant $G_{\bar{a}}$, formule que l'on notera aussi $G_{\bar{a}}$. Ainsi $G_{\bar{a}}(L)$ est un groupe algébrique pour tout corps L contenant $\bar{a}$. De même $G_{\bar{a}}^0$ est définissable sur $\bar{a}$.*

Une condition pour la connexité du groupe $G_{\bar{a}}$.

Lemme 2.3.4. *Si $\bar{a}$ est un uplet d'éléments de K algébriquement indépendants (sur $\mathbb{F}_p$) alors $G_{\bar{a}}$ est connexe.*

PREUVE : La preuve est par induction sur $n = |\bar{a}|$. On commence par le cas $n = 1$, le groupe est alors

$$G_a = \{(a \cdot (x^p - x), x) | x \in \mathbb{K}\}$$

La projection sur la deuxième coordonnée nous donne un isomorphisme de groupes algébriques (dans ce cas une application polynomiale) entre G_a et $(\mathbb{K}, +)$ (de réciproque $x \mapsto (a \cdot (x^p - x), x)$)

et comme $(\mathbb{K}, +)$ est connexe il en est de même pour G_a.

Commençons l'étape d'induction. On dispose de $\bar{a} = a_1, \ldots, a_{n+1}$ algébriquement indépendants, notons $\bar{a}' = a_1, \ldots, a_n$ et par hypothèse d'induction $G_{\bar{a}'}$ est connexe. Soit $H = G^0_{\bar{a}}$ et on suppose que $H \subsetneq G_{\bar{a}}$.
Pour arriver à une contradiction on a besoin du résultat suivant :

$$\text{Pour tout } (t, \bar{x}) \in G_{\bar{a}'} \text{ il existe un unique } x_{n+1} \in \mathbb{K} \text{ tel que } (t, \bar{x}, x_{n+1}) \in H \qquad (\dagger)$$

Preuve de $(\dagger)$:
Soit $\pi : G_{\bar{a}} \twoheadrightarrow G_{\bar{a}'}$ défini par $\pi(t, x_1, \ldots, x_{n+1}) = (t, x_1, \ldots, x_n)$. La surjectivité de π est immédiate : en effet étant donné $(t, \bar{x}) \in G_{\bar{a}'}$ il s'agit de trouver une solution à $t = a_{n+1} \cdot (X^p - X)$ et donc on utilise que $\mathbb{K}$ est algébriquement clos.
Montrons que $\pi(H) = G_{\bar{a}'}$. En effet on a que $[G_{\bar{a}'} : \pi(H)] \leq [G_{\bar{a}} : H]$ (puisque $\pi(a) - \pi(b) \notin \pi(H)$ implique $a - b \notin H$ et π est surjective, à deux classes distinctes selon $\pi(H)$ correspondent deux classes distinctes selon H) et comme H est la composante connexe de $G_{\bar{a}}$ l'indice est fini, et comme $G_{\bar{a}'}$ est connexe et infini cela force $G_{\bar{a}'} = \pi(H)$. La surjectivité de $\pi_{\restriction H}$ nous assure l'existence, étant donné un $(t, \bar{x}) \in G_{\bar{a}'}$ d'un $x_{n+1} \in \mathbb{K}$ tel que $(t, \bar{x}, x_{n+1}) \in H$. Montrons à présent l'unicité. Supposons que $y_1, y_2 \in \mathbb{K}$ soient distincts et tels que $(t, \bar{x}, y_1) \in H$ et $(t, \bar{x}, y_2) \in H$. La différence $(0, \bar{0}, y_1 - y_2)$ est alors dans H ; or par définition $t = a_{n+1} \cdot (y_1^p - y_1) = a_{n+1} \cdot (y_2^p - y_2)$ et comme $a_{n+1} \neq 0$ il vient $(y_1 - y_2)^p = y_1 - y_2$ et donc $y_1 - y_2 \in \mathbb{F}_p$. Puisque $y_1 - y_2 \neq 0$ on en déduit que $(0, \bar{0}, \mathbb{F}_p) \subseteq H$. Or si $(t, \bar{x}, x_{n+1}) \in G_{\bar{a}}$ on a $(t, \bar{x}) \in G_{\bar{a}'}$ et si $x'_{n+1} \in \pi^{-1}_{\restriction H}(t, \bar{x})$ on a alors $\alpha = x'_{n+1} - x_{n+1} \in \mathbb{F}_p$ et donc

$$(t, \bar{x}, x_{n+1}) = (t, \bar{x}, x'_{n+1}) + (0, \bar{0}, \alpha)$$

et donc $G_{\bar{a}} = H$ ce qui est une contradiction. $(\dagger)$ $\square$

On fixe à présent $(1, \bar{x}) \in G_{\bar{a}'}$. On pose $L = \mathbb{F}_p(\bar{x})$. On va montrer que l'unique $y \in \mathbb{K}$ tel que $(1, \bar{x}, y) \in H$ est dans $L(a_{n+1}) \setminus L$, cela nous donnera la contradiction finale.
Pour montrer que $y \in L(a_{n+1})$ on montre qu'il est à la fois séparable et purement inséparable sur $L(a_{n+1})$. Remarquons que comme y est une racine de $f(X) = 1 - a_{n+1} \cdot (X^p - X)$ alors il en est de même pour les p éléments de l'ensemble $y + \mathbb{F}_p$ ce qui montre que le polynôme minimal de y sur $L(a_{n+1})$ est séparable puisqu'il divise f, ainsi y est séparable sur $L(a_{n+1})$. De plus par le lemme 2.1.1 y est purement inséparable sur $L(a_{n+1}) = \mathbb{F}_p(\bar{x}, a_{n+1})$ si et seulement si il est dans $dcl(\bar{x}, a_{n+1})$. Or remarquons d'une part que a_i est définissable à partir de x_i puisque $a_i \cdot (x_i^p - x_i) = 1$, a_i est l'inverse de $x_i^p - x_i$. De plus on sait par la remarque 2.3.3 que comme $G_{\bar{a}}$ est définissable à partir de $\bar{a}$, $H = G^0_{\bar{a}}$ est aussi définissable à partir de $\bar{a}$ et donc à partir de $\bar{x}, a_{n+1}$. Enfin, par $(\dagger)$, y est l'unique solution de l'équation $1 = a_{n+1} \cdot (X^p - X)$ qui gît dans H et comme l'équation et H sont définissable à partir de $\bar{x}, a_{n+1}$ on a bien que $y \in dcl(\bar{x}, a_{n+1})$ et donc y est purement inséparable sur $L(a_{n+1})$. Comme il y est aussi séparable, on conclut que $y \in L(a_{n+1})$. Enfin par hypothèse a_{n+1} est transcendant sur $\bar{a}'$ et puisque $\bar{x} \in acl(\bar{a}')$ on a que a_{n+1} est transcendant sur L et comme $a_{n+1} = (y^p - y)^{-1}$ on doit avoir $y \notin L$ on a donc bien $y \in L(a_{n+1}) \setminus L$.
On exprime alors $y = \frac{h(a_{n+1})}{g(a_{n+1})}$ avec $g, h \in L[X]$ premiers entre eux. Or l'équation que satisfait y donne :

$$a_{n+1} \cdot \left(\frac{h(a_{n+1})^p}{g(a_{n+1})^p} - \frac{h(a_{n+1})}{g(a_{n+1})} \right) = 1$$

De plus comme a_{n+1} est transcendant sur L, l'équation est purement algébrique, on l'exprime dans $L[X]$ en réduisant, ce qui donne

$$\begin{aligned} X \cdot \left(h^p - hg^{p-1}\right) &= g^p && (2.1)\\ h \cdot (X \cdot h^{p-1} - X \cdot g^{p-1}) &= g^p && (2.2)\\ X \cdot h^p &= g \cdot (g^{p-1} + X \cdot hg^{p-2}) && (2.3) \end{aligned}$$

On déduit de (2.2) que h divise g^p donc comme h et g sont premiers entre eux, $h \in L[X]^\times = L^\times$. Sachant cela, (2.3) nous donne que g divise X, et donc $g = X$ car on ne peut pas avoir que $g \in L$ puisque sinon $y = \frac{h}{g}$ serait dans L. En réinjectant dans (3) on trouve $X \cdot h^p = X^p \cdot (1+h)$ ce qui nous donne une relation algébrique absurde. □

On en déduit alors

Théorème 2.3.5. *Soit K un corps parfait et $\mathbb{K}$ un corps algébriquement clos contenant K. Soit $\bar{a} \in K$ un uplet d'élément algébriquement indépendants. Alors il existe un isomorphisme de groupe algébrique θ définissable sur K*

$$\theta : G_{\bar{a}}(\mathbb{K}) \to (\mathbb{K}, +)$$

Preuve : On sait que $dim G_{\bar{a}}(\mathbb{K}) = 1$ en tant que variété par la remarque 2.3.2. $G_{\bar{a}}(\mathbb{K})$ est alors un groupe vectoriel connexe de dimension 1 par le lemme 2.3.4 et est donc isomorphe sur K à $\mathbb{K}^+$ par le théorème 2.2.4. □

3 Structures algébriques dépendantes

3.1 Interprétation dans les théories dépendantes

Les notations et conventions utilisée ici à propos de la théorie des modèles sont celles de la théorie des modèles dite géométrique. Dans un langage $\mathscr{L}$, on considère une théorie T que l'on supposera complète, dépendante et l'on dispose du monstre $\mathfrak{C}$ de la théorie, classe propre dans laquelle tous les modèles de T se plongent élémentairement, il est donc saturé en tout cardinal. On dénotera par $a \in \mathfrak{C}$ ou $\bar{a} \in \mathfrak{C}$ un uplet de taille finie d'éléments du montre.

Definition 3.1.1. *On dit qu'une formule $\varphi(x, y)$ a la* propriété d'indépendance *si il existe deux suites dans le monstre $(a_i)_{i<\omega}$ et $(b_I)_{I\subseteq\omega}$ telles que*

$$\mathfrak{C} \models \varphi(a_i, b_I) \text{ si et seulement si } i \in I$$

Une théorie est dite dépendante *ou* NIP *si aucune formule n'a la propriété d'indépendance. Une structure $\mathcal{M}$ est dite* dépendante *ou* NIP *si sa théorie l'est.*

On comprend alors que l'hypothèse de dépendance d'une théorie se traduit sur une restriction sur les ensembles définissables du monstre.

On s'intéressera à des structures algébriques ayant cette restriction logique sur les ensembles définissables. On rappelle qu'on dit qu'une théorie T *interprète* une structure $\mathscr{M}$ si pour chaque symbole logique du langage de $\mathscr{M}$ il existe une formule de $\mathscr{L}$ correspondante, représentant dans T le symbole logique en question dans le sens suivant : la vérité dans le monstre $\mathfrak{C}$ de la $\mathscr{L}$-formule définit la vérité dans la structure. Le langage de $\mathscr{M}$ est donc totalement traduisible dans le langage $\mathscr{L}$, et on peut traiter $\mathscr{M}$ comme une structure à part entière, dont les formules sont construites à partir de $\mathscr{L}$-formules qui jouent le rôle de prédicats atomiques pour le langage de $\mathscr{M}$. Si une structure est interprétée dans la théorie d'une autre, on dira que la deuxième interprète la première. Le domaine de la structure $\mathscr{M}$ est représenté par un ensemble définissable d'une puissance cartésienne de $\mathfrak{C}^{eq}$ i.e. le quotient d'un ensemble définissable par une relation d'équivalence définissable sans paramètre. Lorsque le domaine est définissable sans quotient (i.e. dans une puissance cartésienne de $\mathfrak{C}$) on parle d'*interprétation par définition.* Le cas qui nous intéresse est lorsque la structure interprétée est un groupe, ou un corps. Bien sûr comme ces groupes sont interprétées à partir de théorie arbitraire il peut y avoir plus de structure que celle de groupe ou de corps, comme des prédicats ou d'autres fonctions mais cela ne nous dérange pas, bien au contraire cela témoigne d'un taux de généralité très apréciable. Dans notre cas, qui concerne les groupes et corps interprétés dans des théories dépendantes, on a une restriction sur les ensembles définissables, par exemple on vérifie facilement que la structure $(\mathbb{N}, \cdot)$ a la propriété d'indépendance pour la formule « x divise y », on prend pour cela a_i le i-ième nombre premier et $b_I = \prod_{i\in I} a_i$, on a alors bien a_i divise b_I si et seulement si $i \in I$, on ne peut conclure qu'une chose, $(\mathbb{N}, \cdot)$ est une structure qui ne sera pas interprétée dans une théorie dépendante. Remarquons

que l'on montre facilement que si T est NIP alors T^{eq} l'est aussi, ainsi si il était clair que les structures définissablement interprétable dans une théorie NIP sont NIP, il en est de même pour les structures interprétables dans les théories NIP. On appelera *groupe* (respectivement *corps*) *dépendant* tout groupe (respectivement corps) interprétable dans une théorie dépendante.

Exemple 3.1.2 (Une extension finie d'un corps dépendant est dépendant)**.** *Soit K un corps dépendant et $L = K(\alpha)$ une extension monogène algébrique, alors soit $m(X)$ le polynôme irréductible de α sur K, et $n = [L : K]$. On interprète L dans K de la façon suivante on va interpréter $L = K \oplus \alpha K \oplus \cdots \oplus \alpha^{n-1}K$, on commence par triviallement interpréter l'espace vectoriel par K^n. Il reste alors à définir la multiplication, et elle est donnée par la table de multiplication de la base $(1, \alpha, \ldots, \alpha^{n-1})$ (qui se déduit de la division euclidienne par $m(X)$) puis on définit la multiplication entre $(u_0, \ldots, u_{n-1})$ et $(v_0, \ldots, v_{n-1})$ de la façon suivante : pour chaque i, j on a $c_l(i, j)$, $l = 0, \ldots, n-1$ tel que $\alpha_i\alpha_j = \sum_{l=1,\ldots,n-1} c_l(i, j)\alpha^l$ (suivant la table), ensuite il suffit de définir la k-ième coordonnée de l'uplet produit comme la somme des u_iv_j multipliés par les coefficients $c_l(i, j)$ correspondant. On a au final interprété $K(\alpha)$ dans K (avec éventuellement quelques coefficients). Ensuite pour une extension finie algébrique quelconque, on itère en utilisant que $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.*

On regarde maintenant la traduction algébrique de l'hypothèse de dépendance d'un groupe. On note dorénavant G un groupe interprétable dans la théorie T. Une famille de sous-groupes $(H_i)_{i\in I}$ de G sera dite *uniformément définissable* si il existe une formule $\varphi(x, y)$ ainsi qu'une suite $(a_i)_{i\in I}$ tels que $H_i = \varphi(\mathfrak{C}, a_i)$.

Proposition 3.1.3 (Condition de Baldwin-Saxl)**.** *Soit G un groupe dépendant et $(H_i)_{i\in I}$ une famille uniformément définissable de sous-groupes de G. Alors il existe un $n < \omega$ (dépendant seulement de $\varphi(x, y)$ définissant les H_i) tel que pour tout $m > n$ et pour tout $J \subseteq \omega$ tel que $|J| = m$ il existe $I \subsetneq J$ avec $|I| = n$ tels que*

$$\bigcap_{i\in J} H_i = \bigcap_{i\in I} H_i$$

En d'autres termes l'intersection d'un nombre fini de H_i est l'intersection de n d'entre eux.

Preuve : Par contradiction on suppose que ce ne soit pas le cas, ce qui signifie qu'il existe des m arbitrairement grands et des familles $(H_i)_{i\in I}$ de taille m (i.e. $|I| = m$) tels que $\bigcap_{i\in I} H_i \subsetneq \bigcap_{i\in J} H_i$ pour tout $J \subsetneq I$. Pour chaque $i \in I$, il existe $h_i \in \bigcap_{j\in I\setminus\{i\}} H_j \setminus \bigcap_{j\in I} H_j$ ie $h_i \notin H_i$ et $h_i \in H_j$ pour tout $j \in I$ tels que $j \neq i$. Pour tout $J \subsetneq I$ on pose $h_J := \prod_{j\in J} h_j$. On a alors que

$$h_J \notin H_i \iff i \in J$$

puisque si $i \in J$ alors h_i est dans le produit h_J et chaque facteur de h_J différent de h_i est dans H_i on a donc que h_J ne peut pas être dans H_i car sinon h_i serait dans H_i aussi. Réciproquement si $i \notin J$ chaque facteur de h_J est dans H_i et donc aussi h_J. Si H_i est défini disons par $\varphi(x, g_i)$ on a alors une suite $(g_i)_{i<\omega}$ on a en fait montré que pour $J \subseteq \omega$ l'ensemble

$$\{\neg\varphi(x, g_i) \mid i \in J\} \cup \{\varphi(x, g_i) \mid i \notin J\}$$

est finiment consistant et donc consistant par compacité, on obtient donc une suite $(h_J)_{J\subseteq\omega}$ telle que

$$\mathfrak{C} \models \neg\varphi(h_J, g_i) \iff i \in J$$

Donc la formule $\psi(x, y) = \neg\varphi(y, x)$ a la propriété d'indépendance. □

3.2 Groupes et corps types-définissables

Dans cette section, on s'intéressera à une légère variante de l'interprétation dans une théorie dans laquelle le domaine de base de la structure interprétée n'est ni définissable, ni un quotient d'un ensemble définissable mais un ensemble *type-définissable*. Les fonctions et relations de la structure sont définissables au sens usuel du terme. On s'interesse au cas où la structure interprétée est un groupe.

Definition 3.2.1. *On dit qu'un groupe $(G, \cdot)$ est* type-définissable *dans la théorie T si il existe une famille $(\phi_i)_{i\in I}$ de $\mathscr{L}$-formules consistante (i.e. un type partiel) telle que*

$$G = \bigcap_{i\in I} \phi_i(\mathfrak{C})$$

et tel que la multiplication $\cdot$ soit définissable.

Exemple 3.2.2 (Les groupes des infinitésimaux des réél et du tore)**.** • *On sait qu'en prenant $\mathbb{R}^* \succcurlyeq \mathbb{R} \models RCF$ suffisements saturé, le corps perds son caractère archimédien et des éléments infinitésimaux apparaissent. On peut donc considérer l'ensemble défini par l'intersection des formules $\phi_n(x) = |x| \leq \frac{1}{n}$ pour $n < \omega$, que l'on dénote I. On notera $I(\mathbb{R}^*) := \bigcap_{i<\omega} \phi_i(\mathbb{R}^*)$. Il s'avère que cet ensemble est stable par addition et clairement par opposé, c'est donc, muni de l'addition du modèle, un groupe type-définissable de RCF. Noter que ce groupe est réduit à $\{0\}$ lorsque le modèle n'est pas suffisement saturé.*

• *Soit $\mathbb{R}^* \models RCF$ et on va définir le tore $\mathbb{T}(\mathbb{R}^*)$ (de dimension 1, autrement dit le cercle !), en définissant le domaine étant $\phi(x) = 0 \leq x < 1$, et l'addition $x \dot{+} y = z \leftrightarrow (x + y = z \wedge z < 1) \vee (x + y \geq 1 \wedge z = x + y - 1)$ modulo $\mathbb{Z}$. On définit alors le tore $\mathbb{T}(\mathbb{R}^*)$ par la structure de domaine $\phi(\mathbb{R}^*)$ et avec la loi de groupe $\dot{+}$. On peut aussi définir le type des infinitésimaux de $\mathbb{T}(\mathbb{R}^*)$ comme conjonction des $x < \frac{1}{n} \vee x > 1 - \frac{1}{n}$ pour tout $n < \omega$, on le note $I(\mathbb{T}(\mathbb{R}^*))$, c'est un sous groupe de $T(\mathbb{R}^*)$ pour $\dot{+}$.*

On voit dans l'exemple précédent que la saturation du modèle va jouer un rôle important dans ce type d'interprétation. On aura besoin de la notion d'*indice borné*. Lorsque un groupe G est type-définissable dans la théorie T et $\mathscr{M} \models T$ on adoptera la notation $G(\mathscr{M})$ pour la réalisation du type définissant G dans $\mathscr{M}$, on considère dans ce cas que $\mathscr{M}$ contient les paramètres nécessaires à définir le type partiel.

Definition 3.2.3. *Soit H un sous groupe type-définissable d'un groupe type-définissable G. On dit que H est d'*indice borné dans G *si il existe un cardinal κ tel que pour tout modèle $\mathscr{M}$ de T l'indice $[G(\mathscr{M}) : H(\mathscr{M})]$ soit borné par κ.*

Exemple 3.2.4. • *Dans le premier exemple, on pose $G = (\mathbb{R}^*, +)$ et $H = I(\mathbb{R}^*, +)$ on voit facilement que le quotient G/H va dépendre du nombre d'élément infinis*[1] *qui ne sont pas I-équivalent. Si le modèle est suffisament saturé on peut mettre autant d'élément infinis non I-équivalent que le cardinal du modèle et ainsi faire que le cardinal du quotient $\mathbb{R}^*/I(\mathbb{R}^*)$ soit égal au cardinal de $\mathbb{R}^*$. On conclut donc que I est un sous groupe type-définissable du groupe additif de RCF qui n'est pas d'indice borné.*
• *Dans le second exemple, toujours dans RCF on a $G = \mathbb{T}(\mathbb{R}^*)$ et $H = I(\mathbb{T}(\mathbb{R}^*))$ on a que le*

1. Rappelons que dans un modèle non standard de RCF les inverses des éléments infinitésimaux sont plus grand que tout élément de ω ; on les appelle les éléments *infinis*.

quotient G/H est isomorphe à $\mathbb{T}(\mathbb{R})$ [2] *et donc le sous groupe $I(\mathbb{T}(\mathbb{R}^*))$ est d'indice borné dans $\mathbb{T}(\mathbb{R}^*)$.*

Remarquons qu'une intersection de groupes types-définissables est encore type-définissable. On considère à présent le cas où le groupe G est type-définissable sans paramètre, où encore 0-type-définissable.

Definition 3.2.5. *Soit A un ensemble de paramètres et G un groupe 0-type-définissable, on note G^{00}_A l'intersection de tous les sous-groupes de G qui sont types-définissableis à paramètres dans A et d'indice borné. Si on a pour n'importe quel A que $G^{00}_A = G^{00}_\emptyset$ alors on le note G^{00} et on l'appelle la* composante type-connexe *de G.*

Noter qu'un tel G^{00} n'a aucune raison d'exister, mais il s'avère que si la théorie est dépendante, alors il existe.

Definition 3.2.6. *On dit qu'un groupe G type-définissable est* fortement connexe *si $G^{00} = G$.*

Un groupe G fortement connexe n'a pas de sous-groupes type-définissables d'indice borné. Par exemple $(\mathbb{R}^*, +)$ est fortement connexe.

2. De la même façon que, si l'on regarde, dans le modèle $\mathbb{R}^*$ l'ensemble des éléments *finis* i.e. $x \in \mathbb{R}^*$ tel que il existe $n < \omega$ tel que $|x| < n$, alors c'est un sous anneau $F(\mathbb{R}^*)$ de $\mathbb{R}^*$ dont $I(\mathbb{R}^*)$ est un idéal maximal. Le quotient $F(\mathbb{R}^*)/I(\mathbb{R}^*)$ est alors isomorphe à $\mathbb{R}$ donc on pourrait dire que le sous groupe $I(\mathbb{R}^*)$ est d'indice borné dans $F(\mathbb{R}^*)$ mais hélas ce dernier n'est pas définissable dans le langage de RCF.

4 Corps définissables et type-définissables dans une théorie dépendante

4.1 Extensions d'Artin-Schreier dans les corps dépendants

Cette section est consacrée au résultat principal de ce mémoire, la seule caractérisation connue des corps dépendants : ils n'admettent pas d'extensions d'Artin-Schreier.

Lemme 4.1.1. *Soit $\mathbb{K}$ un corps algébriquement clos et $f : \mathbb{K} \to \mathbb{K}$ un polynôme additif tel que $V(f) = \mathbb{F}_p$, alors f est de la forme*

$$u \cdot (x^p - x)^{p^m}$$

pour un $u \in \mathbb{K}$ et $m < \omega$.

Preuve : Si le polynôme est additif, comme le corps est algébriquement clos, il est infini et c'est un résultat classique que f soit de la forme $\sum a_i X^{p^i}$ (cf lemme A.1.1 en appendice). On a donc que la dérivée formelle f' est égale à a_0. Si $a_0 \neq 0$, on a nécessairement que le pgcd de f et f' est 1 donc le polynôme est séparable, et donc comme il a p racines, il est de degré p et donc $f = a_0 X + a_1 X^p$, de plus comme $f(1) = 0$ on trouve $a_0 = -a_1$ et donc $f(X) = a_1 \cdot (X^p - X)$. Si $a_0 = 0$ on a $f = \sum_{i>0} a_i X^{p^i} = (\sum_{j\geq 0} b_j X^{p^j})^p = (g(X))^p$ avec g additif aussi. Si $b_0 \neq 0$ on conclut, sinon on procède par induction jusqu'à trouver un terme en X non nul. Les b_j existent car $\mathbb{K}$ est algébriquement clos. □

Théorème 4.1.2. *Tout corps infini dépendant de caractéristique positive est Artin-Schreier clos.*

Preuve : Soit K un corps infini dépendant de caractéristique $p > 0$ et $\mathbb{K}$ un corps algébriquement clos tel que $|\mathbb{K}| > |K|$. On doit montrer que $\wp : K^+ \to K^+$ est surjective. Comme la propriété d'être Artin-Schreier clos est élémentaire, on suppose que l'on se place dans une extension élémentaire $K' \succcurlyeq K$ suffisamment saturée ($\aleph_0$ suffit) que l'on notera encore K et telle que $k = K^{p^\infty}$ soit non vide, infini et contienne des familles finies arbitrairement grandes d'éléments algébriquement indépendants. k est un corps parfait.
On commence par traduire l'hypothèse de dépendance du corps K. La famille de sous-groupes additifs définis par la formule $\phi(x, a) = \exists y\ x = a \cdot (y^p - y)$ pour $a \in K$ est uniformément définissable. On note $\phi(K, a) = H_a$. Par la condition de Baldwin-Saxl sur le groupe dépendant K^+ il existe un n tel que toute intersection finie des H_a est l'intersection de n d'entre eux. En particulier, pour tout $\bar{a} \in K$ avec $|\bar{a}| = n + 1$ il existe $\bar{a}' \subsetneq \bar{a}$ avec $|a|' = n$ et tel que

$$\bigcap_{a\in\bar{a}} H_a = \bigcap_{a\in\bar{a}'} H_a$$

Appelons cette condition (BS) sans nul doute sur l'origine de ces initiales.

On extirpe à présent un homomorphisme $\rho : \mathbb{K}^+ \to \mathbb{K}^+$ définissable sur k. Pour cela, on fixe – pour le n de la condition (BS)– un uplet $\bar{a} \in k$ de $n+1$ éléments algébriquement indépendants. Il existe alors par (BS) un sous uplet $\bar{a}'$ de taille n vérifiant (BS) et quitte à réindexer et permuter on supposera que $\bar{a}' = \bar{a} \restriction_n$. Soient $G_{\bar{a}}(\mathbb{K})$ et $G_{\bar{a}'}(\mathbb{K})$ les groupes vectoriels de 2.3 :

$$G_{\bar{a}} = \left\{ (t, x_1, \ldots, x_n) \in \mathbb{K}^{n+2} | \bigwedge_{i=1,\ldots,n+1} t = a_i \cdot (x_i^p - x_i) \right\}$$

Ils sont définis sur le corps parfait k et on a donc par le théorème 2.3.5 l'existence de deux isomorphismes k-définissable θ (respectivement θ') entre $G_{\bar{a}}(\mathbb{K})$ (resp. $G_{\bar{a}'}(\mathbb{K})$) et $\mathbb{K}^+$. De plus, on dispose de l'homomorphisme additif $\pi : G_{\bar{a}}(\mathbb{K}) \to G_{\bar{a}'}(\mathbb{K})$ qui est surjectif car $\mathbb{K}$ est algébriquement clos. Enfin, en posant $\rho = \theta' \circ \pi \circ \theta^{-1}$ également surjective, on dispose du diagramme suivant :

$$\begin{array}{ccc} G_{\bar{a}}(\mathbb{K}) & \xrightarrow{\pi} & G_{\bar{a}'}(\mathbb{K}) \\ \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta'} \\ \mathbb{K}^+ & \xrightarrow{\rho} & \mathbb{K}^+ \end{array}$$

L'idée de la preuve consiste d'une part à restreindre ce diagramme au corps K en conservant la surjectivité de ρ dans K et d'autre part à donner une expression de ρ qui fera apparaître $\wp$.

Dans le diagramme précédent, on constate que π est définissable sans paramètres et que θ, θ', $G_{\bar{a}}$ et $G_{\bar{a}'}$ sont des formules avec paramètres dans k. On peut donc considérer la réalisation de toutes ces formules dans la sous-structure [1] K. On note f_A la restriction d'une fonction f à un sous-ensemble A de son domaine. On a que θ_K et θ'_K restent des isomorphismes à valeur dans K. On vérifie que π_K est surjectif, en effet si $(t, x_1, \ldots, x_n) \in G_{\bar{a}'}(K)$ alors par construction $K \models \bigwedge_{i=1,\ldots,n} t = a_i \cdot (x_i^p - x_i)$ et donc $t \in \bigcap_{i=1,\ldots,n} H_{a_i}$. On a donc par la condition (BS) que $t \in \bigcap_{i=1,\ldots,n+1} H_{a_i}$ et donc il existe un $x_{n+1} \in K$ tel que $t = a_{n+1}\wp(x_{n+1})$ autrement dit $\pi(t, x_1, \ldots, x_{n+1}) = (t, x_1, \ldots, x_n)$ et donc π_K est surjectif. On conclut donc que ρ_K est surjective, et on a

$$\begin{array}{ccc} G_{\bar{a}}(K) & \xrightarrow{\pi_K} & G_{\bar{a}'}(K) \\ \downarrow{\scriptstyle \theta_K} & & \downarrow{\scriptstyle \theta'_K} \\ K^+ & \xrightarrow{\rho_K} & K^+ \end{array}$$

Montrons à présent que $|\ker \rho| = p$. Comme $\ker \rho$ et $\ker \pi$ sont en bijection par l'isomorphisme θ on détermine $\ker \pi$. Si $(t, \bar{x}, y) \in \ker \pi$ il est clair que $(t, \bar{x}) = (0, \bar{0})$ de plus, on a l'équation $0 = a_{n+1} \cdot (y^p - y)$ ce qui implique, puisque $a_{n+1} \neq 0$ que $y^p = y$ et donc $y \in \mathbb{F}_p$. L'autre inclusion étant évidente, on a $\ker \pi = (0, \bar{0}) \times \mathbb{F}_p$ et donc $|\ker \rho| = p$. On a que $\ker \rho$ est un sous groupe de K^+ de cardinal p, si l'on montre qu'il contient 1, ce sera nécessairement $\mathbb{F}_p$. Soit $c \in \ker \rho$ et on pose $\tilde{\rho}(x) = \rho(c \cdot x)$, alors il est clair que $\tilde{\rho}(1) = 0$ donc $\ker \tilde{\rho} = \mathbb{F}_p$. À présent, puisque $\tilde{\rho}$ est un morphisme défini sur la variété $\mathbb{K}$ régulier sur tout $\mathbb{K}$, c'est un polynôme par la remarque 2.1.2 et par le lemme 4.1.1 il existe $u \in \mathbb{K}^\times$ et $m < \omega$ tels que

$$\tilde{\rho}(x) = u \cdot (x^p - x)^{p^m}$$

1. On est ici dans le cas où l'on a une sous-structure K d'un modèle $\mathbb{K}$ de ACF_p, on regarde donc la réalisation de ces formules dans K.

De plus comme $\tilde{\rho}$ est défini sur k ($c \in \ker \rho \subseteq k$) et comme k est parfait, $u \in k$ (par les remarques après le lemme 2.1.1). Comme la restriction $\tilde{\rho}_K$ est toujours surjective, on a que pour tout $y \in K$ il y a une préimage pour uy^{p^m}, i.e. il existe $x \in K$ tel que $u \cdot (x^p - x)^{p^m} = u \cdot y^{p^m}$ et par injectivité de $x \mapsto x^{p^m}$ en caractéristique positive, on conclut que $x^p - x = y$ et donc K est Artin-Schreier clos. □

Nota. *La fin de la preuve peut être légèrement simplifiée de la façon suivante : on remarque d'abord que ρ est séparable car π l'est. En effet, pour un générique $\bar{x}$ de $G_{\bar{a}}$ sur K, $K(\bar{x})/K(\pi(\bar{x}))$ est séparable (c'est même une extension d'Artin-Schreier). Pour y algébriquement indépendant sur K, (autrement dit un générique de $\mathbb{K}$ sur K), comme θ et θ' induisent respectivement des isomorphismes de $K(\bar{x})$ dans $K(y)$ et de $K(\pi(\bar{x}))$ dans $K(y)$ on a bien que $K(y)/K(\rho(y))$ est séparable, autrement dit ρ est séparable. Il en est de même pour $\tilde{\rho}$. Ensuite comme ce dernier un polynôme additif il est de la forme $\sum_i u_i X^{p^i}$ et comme il est séparable et a p racines on a $u_i = 0$ pour tout $i > 1$. Il est alors la forme $u_0 X + u_1 X^p$ mais comme $\tilde{\rho}(1) = 0$ on a que $\tilde{\rho}(X) = u_1 \cdot (X^p - X)$, on remarque de même que $u_1 \in K$ (et même à k) et on conclut à la surjectivité de $\wp$ immédiatement.*

Corollaire 4.1.3. *Si K est un corps infini dépendant de caractéristique $p > 0$ et L/K est une extension finie séparable, alors p ne divise pas $[L : K]$.*

PREUVE : Supposons en effet que p divise $[L : K]$. Alors si L^{gal} est la clôture galoisienne de L/K, l'extension est Galoisienne et on a toujours que p divise $[L^{gal} : K]$ mézalor par théorie de Galois, il existe une extension intermédiaire $K \subseteq F \subseteq L^{gal}$ avec L^{gal}/F d'Artin-Schreier, ce qui est une contradiction puisque comme F est de degré fini sur K, F est interprétable dans K et donc F est dépendant. □

Exemple 4.1.4. *On déduit de l'exemple 1.1.10 qu'un ultraproduit non-principal de corps finis de caractéristique $p > 0$ a toujours la propriété d'indépendance.*

Revenons sur la conjecture énoncée dans l'introduction. Comme les corps dépendants ne sont pas en général séparablement clos (les corps réels clos sont dépendants), si l'on considère un corps K dépendant et non séparablement clos, on dispose donc d'une extension L/K de degré l premier et quitte à changer K en $K(\zeta)/K$ avec ζ une racine primitive l-ième de l'unité, on obtient alors que K a une extension de Kummer. Il serait intéressant de trouver une restriction logique sur la théorie impliquant que les corps interprétés dans cette dernière soient Kummer clos. Il serait heureux que la propriété en question soit une conséquence de la stabilité (on aurait alors la conjecture). Que le découpage algébrique/logique soit parfait —i.e. que la simplicité soit cette fameuse propriété, cela semble trop beau pour être vrai.

4.2 Extensions d'Artin-Schreier dans les corps dépendants type-définissables

On s'intéresse à présent aux corps types-définissable dans une théorie dépendante.

Proposition 4.2.1. *Soit K un corps infini type-définissable dans une théorie dépendante, alors K est additivement fortement connexe, i.e. $(K^+)^{00} = K^+$.*

PREUVE : Si K^{00} est la composante fortement connexe du groupe additif, alors si $\lambda \in K^\times$ on a que λK^{00} est un sous groupe type-définissable de même indice que K^{00} (donc borné) et

ainsi $K^{00} = \lambda K^{00}$ et donc K^{00} est un idéal de K. Si $K^{00} = \{0\}$ alors $[K : K^{00}] = |K|$ et donc l'indice de K^{00} n'est pas borné car K est infini. On conclut donc que $K^{00} = K$. □

Corollaire 4.2.2. *Soit K un corps type-définissable dans une théorie dépendante, alors soit K est Artin-Schreier clos, soit il a une infinité d'extension d'Artin-Schreier.*

PREUVE : Par la proposition précédente, K est additivement fortement connexe. Or comme $K = \cap_{i\in I}\phi_i$ on a que $\wp K = \cap_{i\in I}\wp(\phi_i)$ est aussi type-définissable, et c'est un sous groupe additif. On conclut suivant deux cas, si $[K^+ : \wp K]$ est borné, alors par forte connexité $\wp K = K$ ainsi $\wp$ est surjective et K est Artin-Schreier clos. Si $[K^+ : \wp K]$ est non borné il est en particulier infini et alors par la remarque 1.1.7 et le théorème 1.1.6 le nombre d'extension d'Artin-Schreier est aussi infini. □

Remarquons que le preuve montre plus que l'énoncé, si il existe une extension d'Artin-Schreier alors le nombre d'extension d'Artin-Schreier est non borné, comme dans la remarque 1.1.7 cela suit du fait que les orbites pour l'action considérée sont de cardinal fini.

On aura pas hélas de résultat plus précis concernant les corps type-définissables dépendants. En revanche si l'on impose une hypothèse supplémentaire sur K on peut montrer un résultat similaire à celui de la section précédente.

Théorème 4.2.3. *Soit K un corps type-définissable dans une théorie dépendante. On suppose de plus que tout modèle de la théorie de K satisfait la propriété suivante :*

Il n'existe pas de chaine infinie décroissante de sous-groupes additifs type-définissables d'indice non bornés l'un dans l'autre

Alors K est Artin-Schreier clos.

PREUVE : L'idée de la preuve est vraiment très similaire à celle du théorème 4.1.2. On commence par se placer dans un corps $\aleph_0$-saturé K vérifiant la propriété du théorème, et on pose $k = K^{p^\infty}$ le plus gros sous-corps parfait de dans K. On suppose aussi que ces deux corps sont dans un corps $\mathbb{K}$ algébriquement clos tel que $|\mathbb{K}| > |K|$. Soit $(a_i)_{i<\omega}$ un uplet infini d'élément de k algébriquement indépendant et $H_a = a \cdot \wp K$. Remarquons que H_a est type-définissable. On cherche donc a avoir une condition de Baldwin-Saxl sur les groupes H_a. On a toujours

$$G_{\bar{a}}(\mathbb{K}) = \left\{ (t, x_1, \ldots, x_{|\bar{a}|}) \in \mathbb{K}^{|\bar{a}|+1} \mid \mathbb{K} \models \bigwedge_{i=1,\ldots,|\bar{a}|} t = a_i \cdot \wp x_i \right\}$$

c'est un groupe type-définissable. On veut montrer la condition

Il existe un n tel que pour tout $\bar{a} \subsetneq (a_i)_{i<\omega}$ avec $|a| = n+1$ il existe $\bar{a}' \subsetneq \bar{a}$ avec $|\bar{a}'| = n$ et tels que

$$\bigcap_{a\in\bar{a}} H_a = \bigcap_{a\in\bar{a}'} H_a$$

On l'appelle encore (BS), mais cette fois on n'a pas la propriété de Baldwin-Saxl car ces ensembles sont types-définissable. On suivra donc un autre chemin. On a par le théorème 2.3.5 que pour chaque $\bar{a}$, $G_{\bar{a}}(\mathbb{K})$ est définissablement isomorphe sur k à $\mathbb{K}^+$, disons par θ et on peut restreindre cet isomorphisme θ à θ_K de façon à ce que l'on ait $G_{\bar{a}}(K)$ qui soit définissablement isomorphe sur k à K^+. Par la proposition 4.2.1 K est additivement fortement connexe

il en est donc de même pour $G_{\bar{a}}(K)$, puisque sinon l'image par θ_K de $G_{\bar{a}}(K)^{00}$ serait un sous groupe strict (car θ_K est un isomorphisme) de K^+ type-définissable et d'indice borné. On considère à présent $\pi_1 : G_{\bar{a}}(K) \to K$ qui est la projection sur la première coordonnée. C'est un homomorphisme et son image est par définition $\bigcap_{a\in\bar{a}} H_a$. Montrons que $H := \bigcap_{a\in\bar{a}} H_a$ est fortement connexe. Soit donc H^{00} la composante fortement connexe. Comme H^{00} est type-définissable, il en est de même de $\pi_1^{-1}(H^{00})$ (puisque π_1 est clairement définissable) et de plus on a [2] $[G_{\bar{a}}(K) : \pi_1^{-1}(H^{00})] \leq [H : H^{00}]$ donc $\pi_1^{-1}(H^{00})$ est d'indice borné et par forte connexité on a que $G_{\bar{a}}(K) = \pi_1^{-1}(H^{00})$ et donc $H = \pi_1(G_{\bar{a}}(K)) = H^{00}$. On a ainsi montré que pour tout $\bar{a} \subsetneq (a_i)_{i<\omega}$, $H_{\bar{a}} := \bigcap_{a\in\bar{a}} H_a$ est connexe. Si on considère alors la famille $(H_{a_1,\ldots,a_n})_{n<\omega}$, chaque $H_{\bar{a}}$ est connexe et donc ils sont d'indice non borné l'un dans l'autre, par la condition du théorème, il existe un n tel que l'on ait (BS).
Maintenant pour un uplet algébriquement indépendant de taille ω de k, il existe un n tel que pour $\bar{a}$ un sous uplet de taille $n+1$ il existe un sous uplet $\bar{a}'$ de taille n vérifiant (BS). On fixe donc n $\bar{a}$ et $\bar{a}'$ et on peut supposer que $\bar{a} = a_1, \ldots, a_{n+1}$ et $\bar{a}' = \bar{a} \restriction_n$. On a alors de la même façon que dans la preuve du théorème 4.1.2 $\pi : G_{\bar{a}}(\mathbb{K}) \to G_{\bar{a}'}(\mathbb{K})$ la projection sur les $n+1$ premières coordonnées qui est surjective, des isomorphismes θ et θ' avec $\mathbb{K}^+$, une surjection $\rho = \theta' \circ \pi \circ \theta^{-1}$ et ce diagramme se réalise dans K car tout est défini sur k, on obtient en récapitulant les deux diagrammes suivant :

$$\begin{array}{ccc} G_{\bar{a}}(\mathbb{K}) & \xrightarrow{\pi} & G_{\bar{a}'}(\mathbb{K}) \\ \downarrow{\scriptstyle\theta} & & \downarrow{\scriptstyle\theta'} \\ \mathbb{K}^+ & \xrightarrow{\rho} & \mathbb{K}^+ \end{array} \qquad \begin{array}{ccc} G_{\bar{a}}(K) & \xrightarrow{\pi_K} & G_{\bar{a}'}(K) \\ \downarrow{\scriptstyle\theta_K} & & \downarrow{\scriptstyle\theta'_K} \\ K^+ & \xrightarrow{\rho_K} & K^+ \end{array}$$

La fin de la preuve est exactement la même que celle du théorème 4.1.2, on établit d'une part que ρ_K est surjective puisque π_K l'est grâce à (BS) puis on trouve une expression polynômiale de $\tilde{\rho} = \rho(c\cdot)$ avec $c \in \ker\rho$ tel que $\tilde{\rho}(x) = u \cdot (\wp(x))^{p^m}$, avec $u \in k$. $\tilde{\rho}_K$ est aussi surjective et comme $u \in k$, $\tilde{\rho}_K$ est aussi de la forme polynômiale souhaité et on conclut que $\wp : K \to K$ est surjective, donc K est Artin-Schreier clos. □

2. Cela vient du fait que si $x - y \notin \pi_1^{-1}(H^{00})$ alors $\pi(x) - \pi(y) \notin H^{00}$, et donc deux classes distinctes selon $\pi_1^{-1}(H^{00})$ restent distinctes selon H^{00}.

5 Corps ayant la propriété d'indépendance

5.1 Les corps PAC

On introduit ici la notion de corps pseudo-algébriquement clos. Soit $\mathbb{K}$ un corps algébriquement clos et soit K un sous corps de $\mathbb{K}$. Soit V une variété affine définie sur K. La question de l'existence d'un point rationnel de V sur K est toujours intéressante, et supposons par exemple que K vérifie que toute variété affine irréductible sur K définie sur K admette un point rationnel sur K. Soit donc $f(X) \in K[X]$ un polynôme irréductible sur K, la variété affine $V(f)$ admet donc un point rationnel sur K et ce point est une racine de f, i.e. K est *algébriquement clos*. La réciproque est une conséquence du Nullstellensatz. On pourrait prendre cet propriété comme définition d'un corps algébriquement clos. Mais ici l'irréductibilité de la variété affine considérée dépend intrinsèquement du corps K considéré. On pourrait donc se restreindre au cas où la variété affine est *absolument irréductible*, et regarder les corps sur lesquels toute variété affine absolument irréductible admettent un point rationnel, ce sont ces derniers que l'on appelle *pseudo-algébriquement clos*. On va montrer ici que contrairement aux corps algébriquement clos qui sont stables, les corps pseudo-algébriquement clos (ou PAC) non séparablement clos ont la propriété d'indépendance. Le terme *variété* dénote à partir de maintenant une *variété affine*.

Definition 5.1.1. *Une variété définie sur K est dite* absolument irréductible *si elle est irréductible sur toute extension du corps K. Un corps K est dit* pseudo-algébriquement clos *si toute variété absolument irréductible définie sur K admet un point rationnel sur K.*

Remarque 5.1.2. *On vérifie immédiatement qu'une variété V est absolument irréductible si et seulement si $I(V)$ est absolument premier. On en déduit, grâce au lemme 1.2.2, que V est absolument irréductible si et seulement si $K(V)/K$ est régulière, pour V définie sur K.*

Lemme 5.1.3. *Soit K un corps, alors les assertions suivantes sont équivalentes :*

1. *K est pseudo-algébriquement clos*
2. *Pour tout polynôme f dans $K[\bar{X}, T]$ absolument irréductible, de degré non nul en T et $g \in K[\bar{X}]$; il existe $\bar{\alpha}, \beta$ dans K tels que*

$$\begin{aligned} f(\bar{\alpha}, \beta) &= 0 \\ g(\bar{\alpha}) &\neq 0 \end{aligned}$$

3. *K est existentiellement clos dans toute extension régulière.*

Preuve : $1 \Rightarrow 2$ Soient donc f, g comme dans l'énoncé. On a que $V(f)$ est absolument irréductible, et on veut montrer que $V(f) \cap (\{\bar{x} \in \mathbb{K}\ g(\bar{x}) \neq 0\} \times \mathbb{K})$ a un point à coordonnée dans K. On considère pour cela une variété dans l'espace affine de dimension supérieur $\mathbb{K}^{n+2}$. Si $W = V(f(\bar{X}, T), g(\bar{X}) \cdot Z - 1)$ alors si $(\bar{\alpha}, \beta, \gamma)$ est dans W on a $(\bar{\alpha}, \beta) \in V(f)$ et comme $\gamma g(\bar{\alpha}) = 1$

$g(\bar{\alpha}) \neq 0$ (c'est l'astuce classique de géométrie algébrique pour passer d'une variété quasi-affine à une variété affine de dimension supérieur). Il suffit donc de montrer que W qui est clairement définie sur K, est absolument irréductible et c'est le cas car W est isomorphe à un ouvert principal d'une variété absolument irréductible, qui est donc aussi absolument irréductible.
$2 \Rightarrow 3$ Il suffit de montrer le résultat pour une extension régulière L/K finiment engendrée, puisque si K est existentiellement clos dans toute extension intermédiaire finiment engendrée alors K est existentiellement clos dans l'extension totale (le nombre de paramètre d'une formule est fini et toute extension intermédiaire est aussi régulière). Si donc L/K est finiment engendrée, comme en particulier l'extension est séparable, il existe une base de transcendance séparante, i.e. $\bar{t} \in L$ algébriquement indépendant sur K et tel que $L/K(\bar{t})$ soit séparable et algébrique. En particulier, comme L/K est finiment engendré, $L/K(\bar{t})$ est finie et donc par le théorème de l'élément primitif il existe $b \in L$ tel que $L = K(\bar{t}, b)$. À présent on se donne une formule sans quantificateur $\phi(\bar{x})$, et comme le corps est infini, on peut supposer que c'est une conjonction de $P_i(\bar{x}) = 0$ $(i < s)$ et soit $\bar{a} \in L$ tel que $L \models \phi(\bar{a})$. On écris alors $a_j = \frac{f_j(\bar{t},b)}{g(\bar{t})}$ (b est algébrique sur K) pour f_j, g à coefficients dans K, on a donc, pour chaque $i < s$ et $j < |\bar{a}|$

$$G_{i,j}(\bar{t}, b) := g(\bar{t})^{m_i} \cdot P_i(f_j(\bar{t}, b)) = 0$$

avec G à coefficients dans K. On a d'autre part que $I(\bar{t}, b/K)$ est un idéal principal par la remarque 1.2.3 , disons engendré par $f(\bar{X}, Y)$ et comme c'est l'idéal de la variété de générique $(\bar{t}, b)$, f est absolument irréductible par le lemme 1.2.2 puisque $K(\bar{t}, b)/K$ est régulière, on conclut qu'il existe $\bar{\alpha}, \beta$ dans K qui s'annulent en f mais $\bar{\alpha}$ ne s'annule pas en g, en particulier ils annulent les $G_{i,j}$ et donc l'uplet des $\frac{f_j(\bar{\alpha},\beta)}{g(\bar{\alpha})}$ est le témoins dans K pour la formule ϕ.
$3 \Rightarrow 1$ Si V est une variété absolument irréductible définie sur K alors si $\bar{\alpha}$ est un générique de V sur K, comme $K(\bar{\alpha})/K$ est régulière et que $\bar{\alpha}$ vérifie les équations définissant V il en est de même pour un élément de K. □

Remarque 5.1.4. *On peut en fait montrer que dans le critère 2 du lemme précédent l'uplet $\bar{X}$ peut être choisi de taille 1, autrement dit qu'un corps K est PAC si et seulement si toute courbe affine absolument irréductible admet un point rationnel sur K. (la condition sur g devient trivial car g n'a qu'un nombre fini de zéro, et un corps PAC est nécessairement infini).*

On déduit du lemme précédent une chose qui ne saute pas aux yeux à première vue des définitions.

Théorème 5.1.5. *La classe des corps PAC est élémentaire.*

PREUVE : On utilise le critère 2 du lemme précédent. Il s'agit donc de vérifier que l'absolue irréductibilité d'un polynôme $f(\bar{X}, T)$ est une propriété élémentaire de ses coefficients. En effet dans ce cas on peut quantifier sur les coefficients de f, de g et demander l'existence de témoins $f(\bar{\alpha}, \beta) = 0 \wedge g(\bar{\alpha}) \neq 0$. Or si $a_1, \ldots, a_l$ sont les coefficients d'un polynôme f de degré d en n variables (par exemple écrit en composantes homogènes) de K, on a une formule (dépendant de d et n) de K^{alg} qui dit « f est irréductible »puisqu'il suffit de quantifier sur les coefficients des polynômes de degré inferieur, appelons cette formule $\phi_{n,d}(x_1, \ldots, x_l)$ (l est une fonction de n et d). Par élimination des quantificateurs dans ACF_p, cette formule est dans K^{alg} équivalente à une formule $\tilde{\phi}_{n,d}(x_1, \ldots, x_l)$. À présent

$$\begin{aligned} K \models \tilde{\phi}_{n,d}(\bar{a}) &\iff K^{alg} \models \tilde{\phi}_{n,d}(\bar{a}) \\ &\iff K^{alg} \models \phi_{n,d}(\bar{a}) \\ &\iff \text{« } f \text{ est absolument irréductible »} \end{aligned}$$

On conlut donc le théorème. Notez que $\tilde{\phi}_{n,d}$ et $\phi_{n,d}$ ne sont pas en générale équivalente selon la théorie de K. □

Proposition 5.1.6. *Toute extension algébrique séparable d'un corps PAC est encore un corps PAC.*

PREUVE : On procède en deux étapes. D'abord on considère un corps K PAC et une extension finie L/K séparable. Soit V une variété absolument irréductible définie sur L. On considère la restriction de Weil (remarque 2.1.3) W de V sur K. On a alors que W est absolument irréductible, en effet on a que W est isomorphe à V^d et on peut choisir des génériques $x_1, \ldots, x_d$ de V sur K algébriquements indépendants sur K^{alg}, par les propriétés de $\perp$, on a que $K(x_1, \ldots, x_n)/K$ est régulière. On conclut, puisque K est PAC, que W admet au moins un point rationnel sur K et donc V admet un point rationnel sur L, donc L est PAC. Enfin si l'on considère une extension L/K séparable quelconque, alors si V est une variété absolument irréductible définie sur L, son plus petit corps de définition est une extension séparable (et même régulière) de degrée fini sur K donc V a un point rationnel sur ce dernier, et donc dans L. □

5.2 La propriété d'indépendance dans les corps PAC

Les corps séparablement clos sont NIP, il en résulte que l'on va s'intéresser aux corps PAC non séparablement clos.

Lemme 5.2.1. *Soit K un corps non séparablement clos, alors il existe un nombre premier $l \neq 1$ et une extension séparable K' de K telle que K' ai une extension galoisienne L qui soit cyclique de degré l. De plus on peut choisir K' contenant une racine primitive l-ième de l'unité.*

PREUVE : On suppose que K est non séparablement clos, il admet donc une extension séparable non triviale et quitte à passer à la clôture galoisienne, on peut supposer que cette extension est galoisienne, on la note L. Si l'on prend $l \neq 1$ un facteur premier de $[L : K]$, on sait par théorie de Galois qu'il existe K' avec $K \subseteq K' \subseteq L$ tel que $[L : K'] = l$ et L/K' est galoisienne. L'extension K'/K est finie séparable car L/K et L/K' le sont. Si de plus K' ne contient pas de racine primitive l-ième de l'unité, alors L non plus. En effet si il y en avait une, disons $\zeta \in L$ on aurait que $K'(\zeta)$ est une extension intermédiaire entre K' et L or $[K'(\zeta) : K'] \leq l - 1$ devra diviser $[L : K'] = l$ ce qui est absurde. On a alors que $L \cap K'(\zeta) = K'$ et comme L/K' est galoisienne on a que L et $K'(\zeta)$ sont linéairement disjoint sur K'. On conclut que $[L(\zeta) : K'(\zeta)] = l$. □

Théorème 5.2.2. *Si K est un corps pseudo-algébriquement clos non séparablement clos, alors K a la propriété d'indépendance.*

PREUVE : On va montrer la chose suivante : il existe une formule $\varphi(x, y)$ telle que pour $n < \omega$ et pour tout $I \subseteq \{1, \ldots, n\}$ on peut trouver $a_I, b_1, \ldots, b_n \in K$ tels que

$$\varphi(a_I, b_i) \iff i \in I$$

Par le lemme 5.2.1, pour montrer que K a la propriété d'indépendance, on peut quitte à remplacer K par K' supposer qu'il existe une extension radicielle L de K et un nombre premier $l \neq 1$ tel que $[L : K] = l$, cela suit de 3.1.2 et de 5.1.6. On traite alors deux cas selon la remarque 1.1.11

Cas $p \neq l$. Comme l'extension L/K est radicielle c'est une extension de Kummer, qui est donc engendré par une racine l-ième d'un élément de K, disons $\alpha \in K^{alg} \setminus K$ et $\alpha^l \in K$. On considère ensuite, $y_1, \ldots, y_n$ des éléments algébriquement indépendants au dessus de K^{alg} et $(x_I)_{I \subseteq \{1,\ldots,n\}}$ algébriquement indépendants au dessus de $K(y_1, \ldots, y_n)$. On pose ensuite

$$M_I = K(x_I, \sqrt[l]{x_I + y_i}, \sqrt[l]{\alpha \cdot (x_I + y_j)})_{i \in I \ j \notin I}$$

On considère ensuite $\varphi(u, v) = \exists w \ w^l = u + v$. On a que si $i \in I$ alors $M_I \models \varphi(x_I, y_i)$. Dans la phrase qui suit et uniquement dans celle-ci, M_I^l désigne l'ensemble des puissances l-ème des éléments de M_I. Maintenant, si $j \in \{1, \ldots, n\} \setminus I$, on a que $\alpha \cdot (x_I + y_j) \in M_I^l$ et comme $\alpha \notin M_I^l$ il est nécessaire que $x_I + y_j \notin M_I^l$ (car sinon on a $x_I + y_j = r^l$ et comme $\alpha \cdot (x_I + y_j) = s^l$ on a $\alpha = \left(\frac{s}{r}\right)^l$ ce qui contredit nos hypothèses sur α). On conclut que $M_I \models \varphi(x_I, y_i) \iff i \in I$. On a donc que la formule $\bigwedge_{i \in I} \varphi(u, v_i) \wedge \bigwedge_{j \in \{1,\ldots,n\} \setminus I} \varphi(u, v_j)$ est réalisée dans M_I, on la note $\Phi_I(u, \bar{v})$.
Soit M le compositum des M_I pour $I \subseteq \{1, \ldots, n\}$. L'extension $K(y_1, \ldots, y_n)/K$ est régulière clairement, et de plus comme les x_I sont indépendants sur $K(y_1, \ldots, y_n)$ on a que $M/K(y_1, \ldots, y_n)$ est régulière et par transitivité de la relation $\perp_K$, M/K est régulière. On sait alors par le lemme 5.1.3 que K est existentiellement clos dans M et donc la formule $\exists (u_I)_{I \subseteq \{1,\ldots,n\}} \exists \bar{v} \bigwedge_{I \subseteq \{1,\ldots,n\}} \Phi_I(u_I, \bar{v})$ qui est vraie dans M, est vrai dans K. Soient donc $(a_I)_{I \subseteq \{1,\ldots,n\}}, b_1, \ldots, b_n$ les témoins dans K, ils vérifient ce que l'on veut par construction.

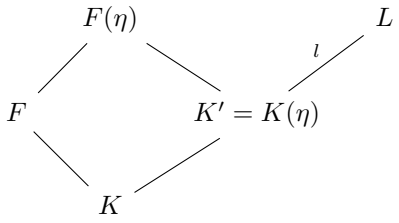
Cas $l = p$. L'extension est donc d'Artin-Schreier et donc il existe $\alpha \in K^{alg} \setminus K$ avec $\wp\alpha \in K$ et tel que $L = K(\alpha)$. On considère alors des éléments $y_1, \ldots, y_n$ algébriquement indépendant sur K^{alg} ainsi que $(x_I)_{I \subseteq \{1,\ldots,n\}}$ algébriquements indépendants sur $K(y_1, \ldots, y_n)$. Soit

$$M_I = K(x_I, \wp^{-1}(x_I y_i), \wp^{-1}(\alpha + x_I y_j))_{i \in I \ j \notin I}$$

On s'intéresse alors à la formule $\varphi(u, v) = \exists w \ w^p - w = u \cdot v$. Maintenant si $i \in I$ il suit par construction que $M_I \models \varphi(x_I, y_i)$. Ensuite si $j \notin I$ il existe $\beta \in M_I$ tel que $\beta^p - \beta = \alpha + x_I \cdot y_j$. Si $x_I \cdot y_j$ était dans $\wp M_I$ disons $x_I \cdot y_j = \gamma^p - \gamma$ alors $\alpha = (\beta - \gamma)^p - (\beta - \gamma) \in \wp M_I$ ce qui est absurde, et on conclut que $x_I \cdot y_j \notin \wp M_I$ et donc $\neg\varphi(x_I, y_j)$. On a donc à nouveau $M_I \models \varphi(x_I, y_i) \iff i \in I$. Soit M le compositum des M_I pour $I \subseteq \{1, \ldots, n\}$. Pour les même raisons que le cas précédent, M/K est régulière et donc K est existentiellement clos dans M. On en déduit qu'il existe $(a_I)_{I \subseteq \{1,\ldots,n\}}, b_1, \ldots, b_n \in K$ tels que $\varphi(a_I, b_i) \iff i \in I$.

On conlut maintenant par compacité. □

Remarque 5.2.3. *On peut modifier la preuve du théorème précédent pour avoir un résultat légèrement plus fort. On considère donc K un corps PAC non séparablement clos et algébriquement clos dans F. On obtient par le lemme 5.2.1 deux extensions $K \subseteq K' \subseteq L$ telle que L/K' soit cyclique radicielle galoisienne de degrée l premier, de plus comme L/K est séparable, il en est de même pour K'/K qui est donc engendrée par un élément primitif η. On vérifie alors que K' est algébriquement clos dans $F(\eta)$ et on se retrouve dans la même configuration que nos hypothèses avec cette fois-ci une extension cyclique L/K, on peut donc supposer que l'on a K PAC algébriquement clos dans F et L/K extension cyclique de degré l.*



À présent on refait la même preuve que précédemment sachant que dans les deux cas respectifs $p \neq l$ *et* $p = l$ *l'élément* α *vérifiera encore* $\alpha^l \in L$ *respectivement* $\wp\alpha \in L$*, ainsi que* $\alpha \notin L$*. Avec les mêmes arguments que précédemment, on s'aperçoit que c'est bien dans* L *que la formule* φ *aura la propriété d'indépendance. On conclut alors que* si K est un corps PAC non séparablement clos et algébriquement clos dans L alors $Th(L)$ a la propriété d'indépendance.

Remarque 5.2.4. *(Sur le nombre de point rationnel d'une courbe sur un corps fini, estimée de Lang-Weil) On considère un corps* $\mathbb{K}$ *algébriquement clos ainsi qu'un polynôme* $f(X, Y)$ *absolument irréductible de degré* d *définie sur un corps fini* $\mathbb{F}_q \subseteq \mathbb{K}$ *et* $V = V(f) \subseteq \mathbb{K}^2$ *la courbe associée. On a alors que l'ensemble* $V(\mathbb{F}_q)$ *des points rationnels de* V *sur* $\mathbb{F}_q$ *vérifie*

$$|V(\mathbb{F}_q)| \geq q + 1 - (d-1)(d-2)\sqrt{q} - d$$

On a alors pour $q > (d-1)^4$ *que* $V(\mathbb{F}_q)$ *est non vide. Si l'on considère donc un sous-corps infini* k *de* F_p^{alg} *et une courbe absolument irréductible* V *définie sur* k*, elle est alors définie sur un corps fini* l_0 *inclu dans* k *(le corps de définition est de dimension finie sur le corps premier) et donc dans un corps fini plus grand* l_1 *contenant* l_0 *par ce qui précéde, on a un point rationnel. Comme* k *est infini, on peut choisir un autre corps fini contenant* l_1 *et inclu dans* k*, et on a montré que pour toute courbe absolument irréductible définie sur* k*, il existe un point rationnel sur* k*. Par la remarque 5.1.4 on conclut que tout sous corps infini de* $\mathbb{F}_p^{alg}$ *est PAC.*

Corollaire 5.2.5. *Soit* K *un corps infini dépendant de caractéristique* $p > 0$*, alors* K *contient* $\mathbb{F}_p^{alg}$*.*

PREUVE : On pose $k = K \cap \mathbb{F}_p^{alg}$, la clôture algébrique de $\mathbb{F}_p$ dans K. On sait que K est Artin-Schreier clos par le théorème 4.1.2. Si $a \in k$, alors comme $a \in \mathbb{F}_p^{alg}$, si $\alpha \in \wp^{-1}a$ on a aussi $\alpha \in \mathbb{F}_p^{alg}$ mais on a aussi $\alpha \in K$ puisque K est Artin-Schreier clos, on conclut que $\alpha \in k$ et donc k est Artin-Schreier clos. Par l'exemple 1.1.10 k est donc infini. Il est de plus parfait, puisque si $a \in k$ alors a est algébrique sur $\mathbb{F}_p$ donc $\mathbb{F}_p(a)$ est fini et dans k. Or tout corps fini est parfait donc il existe $\alpha \in \mathbb{F}_p(a) \subseteq k$ tel que $\alpha^p = a$. Enfin comme sous-corps infini de $\mathbb{F}_p^{alg}$, k est PAC par la remarque précédente. Comme k est PAC alors par la remarque 5.2.3 on doit avoir que k est séparablement clos car sinon K aurais la propriété d'indépendance. On a donc que k est parfait et séparablement clos, il n'a aucune extension algébriques non triviale donc il est algébriquement clos, ce qui force $k = \mathbb{F}_p^{alg}$. □

On peut remarquer que si K est un corps dépendant infini différent de $\mathbb{F}_p^{alg}$ alors l'extension $K/\mathbb{F}_p^{alg}$ n'est pas finiment engendrée. En effet si $x \in K \setminus \mathbb{F}_p^{alg}$ alors x est transcendant sur $\mathbb{F}_p^{alg}$ et comme K est Artin-Schreier clos, $\wp^{-1}x \in K \setminus \mathbb{F}_p^{alg}(x)$ et on a donc

$$\mathbb{F}_p^{alg} \subsetneq \mathbb{F}_p^{alg}(x) \subsetneq \cdots \subsetneq \mathbb{F}_p^{alg}(\wp^{-n}x) \subsetneq \cdots \subseteq K$$

A Appendice

A.1 Sous-groupe fermé connexe d'un groupe vectoriel

Dans cette section on montre le lemme 2.2.2, qui stipule qu'un sous-groupe fermé connexe d'un groupe vectoriel est encor un groupe vectoriel dans le cadre d'un corps ambiant $\mathbb{K}$ algébriquement clos de caractéristique $p > 0$.
On commence par quelques résultats à propos des p-polynômes, ce sont les polynômes en variable $X_1, ..., X_n$ qui sont combinaisons linéaires de monômes $X_i^{p^r}$. Ces polynômes sont clairement additifs [1] et en fait on montre que tout polynôme additif est un p-polynôme. Il est claire qu'un p-polynôme f induit un morphisme de groupe algébrique additif $\mathbb{K}^n \to \mathbb{K}^+$ et donc la variété $V(f)$ est un sous-groupe algébrique du groupe vectoriel K^n. On montre dans le lemme qui suit une réciproque de ce résultat.

Lemme A.1.1. *1. Soit $f \in \mathbb{K}[\bar{X}]$ un polynôme additif; alors f est un p-polynôme.*

2. Soit $f \in \mathbb{K}[\bar{X}]$ un polynôme sans carré tel que $V(f)$ est un sous-groupe additif de $\mathbb{K}^n$ alors f est un p-polynôme.

Preuve : 1. Par induction sur le degré (total) de f. Soit D_i l'opérateur de dérivée partielle formelle suivant la variable X_i et soit $\bar{a} \in \mathbb{K}^n$. On a immédiatement que $(D_i f)(\bar{X} + \bar{a}) = (D_i f)(\bar{X})$, et donc pour chaque $i = 1, \ldots, n$ $D_i f$ est un polynôme constant, disons égal à $c_i \in \mathbb{K}$. On a de plus que $D_i(f(\bar{X}) - (c_1 X_1 + \cdots + c_n X_n)) = 0$, puisque tout simplement $D_i(c_j X_j) = \delta_{i,j} c_i = \delta_{i,j} D_i f$ (avec $\delta_{i,j} = 0$ si $i \neq j$ et 1 si $i = j$). On a alors que $f(\bar{X}) - \sum_i c_i X_i$ est de la forme $g(X_1^p, \ldots, X_n^p)$, en effet on écrit $f(\bar{X}) - \sum_i c_i X_i$ comme $\sum_k g_k(X_1, \ldots, X_{n-1}) X_n^k$ et la dérivée n-ième vaut 0 donc on conclut que soit $g_i(X_1, \ldots, X_{n-1}) = 0$ soit (et c'est un « ou »exclusif) $i \equiv 0 \ mod\ p$, on conclut bien que $f(\bar{X}) - \sum_i c_i X_i$ est un polynôme en $X_1, \ldots, X_{n-1}, X_n^p$ puis on répete l'argument pour chaque variable. Enfin on conclut le 1. par reccurence si $g(Y_1, \ldots, Y_n)$ est lui-même additif, ce qui est vrai car $\mathbb{K}$ est algébriquement clos : pour $\bar{a}, \bar{b} \in \mathbb{K}$ il existe $\bar{a}', \bar{b}' \in \mathbb{K}$ tels que $a_i = a_i'^p$ et $b_i = b_i'^p$ et donc $g(\bar{a} + \bar{b}) = f(\bar{a}' + \bar{b}') - \sum_i c_i(a_i' + b_i') = f(\bar{a}') - \sum_i c_i a_i' + f(\bar{b}') - \sum_i c_i b_i' = g(\bar{a}) + g(\bar{b})$.
2. Supposons donc que $f(\bar{X}) \in \mathbb{K}[\bar{X}]$ soit un polynôme sans carré tel que $G := V(f)$ soit un sous-groupe additif de $\mathbb{K}^n$. Montrons que f est additif, et le 1. nous donnera le résultat. On déduit d'abord du fait que G soit un groupe que pour un $\bar{a} \in G$ on a que $f(\bar{X} + \bar{a})$ et $f(\bar{X})$ ont le même ensemble de zéro, donc $V(f(\bar{X})) = V(f(\bar{X} + \bar{a}))$. Le Nullstellensatz nous dit alors que $f(\bar{X} + \bar{a}) \in \sqrt{(f)} = (f)$ puisque f est sans carré. Une considération sur le degré nous donne qu'il existe un scalaire $\gamma(\bar{a}) \in \mathbb{K}$ tel que $f(\bar{X} + \bar{a}) = \gamma(\bar{a}) f(\bar{X})$. Si $\bar{b} \in G$, on utilise la propriété universelle des polynômes pour voir que $f(\bar{X} + \bar{a} + \bar{b}) = \gamma(\bar{a} + \bar{b}) f(\bar{X}) = \gamma(\bar{a})\gamma(\bar{b}) f(\bar{X})$ et donc γ est un homomorphisme de groupe entre $\mathbb{K}^+$ et $\mathbb{K}^\times$; comme $\mathbb{K}^\times$ est sans torsion cela force $\gamma = x \mapsto 1$,

1. Un polynôme $P(\bar{X}) \in \mathbb{K}[\bar{X}]$ est *additif* si pour tout $\bar{x}, \bar{y} \in \mathbb{K}^{|\bar{X}|}$ on a $P(\bar{x} + \bar{y}) = P(\bar{x}) + P(\bar{y})$.

on a donc pour tout $\bar{a} \in G$ $f(\bar{X} + \bar{a}) = f(\bar{X})$. Soit $\bar{a} \in \mathbb{K}$, on a que $f(\bar{X} + a) - f(\bar{a})$ s'annule sur G et est de même degré que f donc par un argument similaire à celui fait précédemment on a encore une fonction $\mu : \mathbb{K}^{n+} \to \mathbb{K}$ telle que $f(\bar{X} + \bar{a}) = f(\bar{a}) + \mu(\bar{a})f(\bar{X})$, puis en calculant $f(\bar{X} + \bar{a} + \bar{b})$ de deux manière différentes on en déduit que μ est aussi un homomorphisme dans le groupe multiplicatif et donc c'est l'application constante égale à 1, on en déduit que pour tout $\bar{a} \in \mathbb{K}^n$ $f(\bar{X} + \bar{a}) = f(\bar{X}) + f(\bar{a})$, et on conclut le lemme. □

Proposition A.1.2. *Soit G un sous-groupe fermé de $\mathbb{K}^{+n}$ de codimension 1 ; alors il existe un p-polynôme f tel que $G = V(f)$.*

PREUVE : Soit donc G un tel sous-groupe algébrique ; la remarque 1.2.3 nous dit précisément que l'idéal annulateur est principal, donc il existe un $f \in \mathbb{K}[\bar{X}]$ tel que $G = V(f)$ et il est clair qu'on peut le supposer sans carré. Le 2 du lemme précédent nous assure que f est un p-polynôme. □

Dans ce qui suit un automorphisme de $\mathbb{K}^n$ est un morphisme bijectif de variété doublé d'un homomorphisme de groupe (donc c'est une application additive et polynômiale puisque définie sur $\mathbb{K}^n$, donc une application p-polynômiale par le lemme A.1.1).

Lemme A.1.3. *Si $f \in \mathbb{K}[\bar{X}]$ est un p-polynôme alors il existe un automorphisme $\sigma : \mathbb{K}^n \to \mathbb{K}^n$ tel que $\sigma(\mathbb{K} \times \bar{0}) \subseteq V(f)$.*

PREUVE : Soit donc $f(\bar{X}) = \sum_{i,j} c_{i,j} X_i^{p^j}$, on considère la *partie principale de f*, i.e. le polynôme $c_{1,r(1)} X_1^{p^{r(1)}} + \cdots + c_{n,r(n)} X_n^{p^{r(n)}}$, où $c_{i,r(i)}$ est le coefficient ($\neq 0$) de la plus grande puissance de X_i dans f (et la puissance en question est $r(i)$).
On procède par induction sur $\sum_{i=1,\ldots,n} r(i)$. Quitte à considérer un premier automorphisme de $\mathbb{K}^n$ qui serait une permutation des coordonnées on peut supposer que $r(1) \geq \cdots \geq r(n)$. De plus on peut supposer que tous les c_i sont non nuls car sinon on pourrais procèder par récurrence sur n (le cas $n = 1$ étant evident). Si $\sum_i r(i) = 0$ alors le polynôme f est linéaire, de la forme $c_1 X_1 + \cdots + c_n X_n$ et l'automorphisme $x_1, \ldots, x_n \mapsto c_1 x_1 + \cdots + c_n x_x, x_2, \ldots x_n$ fait l'affaire. Pour l'étape de récurrence, on considère $\bar{a}$ une racine de $\sum_{i=1,\ldots,n} c_i X_i^{p^{r(i)}}$ et soit $m \in 1, \ldots, n$ minimal tel que $a_m \neq 0$. On considère alors l'automorphisme $\sigma : \mathbb{K}^n \to \mathbb{K}^n$ défini par un changement linéaire de coordonnées, par

$$(x_1, \ldots, x_n) \longmapsto (x_1, \ldots, x_{m-1}, a_m x_m, x_{m+1} + a_{m+1} x_m^{p^{r(m)-r(m+1)}}, \ldots, x_n + a_n x_m^{p^{r(m)-r(n)}})$$

Remarquons que c'est bien un automorphisme puisque c'est une application p-polynômiale, et de plus l'appliquer revient a effectuer le changement de variable $Y_1, \ldots, Y_n = \sigma(X_1, \ldots, X_n)$. On constate alors, en regroupant la partie principale de $f(\sigma(X_1, \ldots, X_n)$ que

$$f(\sigma(X_1, \ldots, X_n)) = \sum_{i \neq m} c_i X^{p^{r(i)}} + \left(\sum_{i=m,\ldots,n} c_i a_i^{p^{r(i)}} \right) X_m^{p^{r(m)}} + g(X_1, \ldots, X_n)$$

avec g de degré inferieur. On a alors puisque $(0, \ldots, 0, a_m, \ldots, a_n)$ est une racine de la partie principale de f que la deuxième somme s'annule et donc la partie principale de $f(\sigma(X_1, \ldots, X_n))$ est $\sum_{i \neq m} c_i X^{p^{r(i)}}$. Par induction, il existe un automorphisme $\tau : \mathbb{K}^n \to \mathbb{K}^n$ tel que $\tau(\mathbb{K} \times \bar{0}) \subseteq V(f(\sigma(\bar{X})))$ et donc $\sigma \circ \tau$ est l'automorphisme tant désiré. □

Théorème A.1.4. *Tout sous-groupe fermé et connexe d'un groupe vectoriel est encore un groupe vectoriel.*

PREUVE : Soit G un sous-groupe fermé et connexe de $\mathbb{K}^n$. On procède par induction sur n. Pour $n = 1$ comme G est un fermé de Zariski de $\mathbb{K}$, il ne peut pas être fini puisque un groupe fini n'est pas connexe, c'est donc un fermé de Zariski infini de $\mathbb{K}$, c'est donc $\mathbb{K}$ tout entier.
On suppose donc que tout sous-groupe fermé connexe de $\mathbb{K}^m$ avec $m < n$ est un groupe vectoriel. Si G est un sous-groupe fermé connexe de $\mathbb{K}^n$, on suppose d'abord que G est de dimension $n-1$. Par la proposition A.1.2, il existe un p-polynôme $f \in \mathbb{K}[X_1, \ldots, X_{n-1}]$ tel que $G = V(f)$. Par le lemme précédent il existe un automorphisme $\sigma : \mathbb{K}^n \to \mathbb{K}^n$ tel que $\mathbb{K} \times \bar{0} \subseteq V(f \circ \sigma^{-1})$ et donc $\mathbb{K} \times \bar{0} \subseteq \sigma G$. Soit donc H la projection de σG sur $0 \times \mathbb{K}^{n-1}$, H est fermé et connexe, sous-groupe fermé du groupe vectoriel $\mathbb{K}^{n-2}$ et par induction c'est aussi un groupe vectoriel, et il en est de même pour $\mathbb{K} \times H = \sigma G$, donc G est un groupe vectoriel. Si maintenant on suppose que G est de dimension strictement inferieure à $n-1$, en ce cas on projette G sur un sous-groupe fermé connexe de $0 \times \mathbb{K}^{n-1}$ disons G' qui est alors un sous groupe fermé connexe d'un groupe vectoriel de dimension strictement inferieur à n et donc G' est un groupe vectoriel (de dimension strictement inferieur à $n-1$), G est donc un sous-groupe fermé connexe de $\mathbb{K} \times G'$ qui est de dimension inferieur ou égale à $n-1$, et on applique l'hypothèse de reccurence. □

A.2 Descente de Weil

On démontre ici le résultat énoncé dans la remarque 2.1.3. On se place toujours dans le contexte de la géométrie algébrique avec un gros corps ambiant $\mathbb{K}$ algébriquement clos et $K \subsetneq \mathbb{K}$ avec $|\mathbb{K}| > |K|$. On rappelle le résultat.
Considérons une variété affine irréductible V définie sur L une extension séparable finie de K de degré d. Alors il existe une variété W définie sur K appelée *réduction de Weil* de V sur K, telle que :

1. W est isomorphe à V^d sur $(L/K)^{gal}$

2. Il existe une bijection entre les points rationnels de V sur L et les points rationnels de W sur K

Comme le degré de séparabilité de L/K est d, on considère les K-plongements $\sigma_1, \ldots, \sigma_d$ de L dans une clôture algébrique de K. On considère aussi une base $e_1, \ldots, e_d$ du K-espace vectoriel L. V étant définie sur L, on dispose de $I_L(V) \subseteq L[\bar{X}]$ et on pose $V^{\sigma_i} = V(\sigma_i I_L(V))$. On constate que si $\bar{x}$ est un point L-rationnel de V alors $(\bar{x}, \ldots, \bar{x})$ est un point L-rationnel de la variété $V^{\sigma_1} \times \cdots \times V^{\sigma_d}$. Réciproquement pour un point L-rationnel $(\bar{x}_1, \ldots, \bar{x}_d)$ de $V^{\sigma_1} \times \cdots \times V^{\sigma_d}$ on a que $\sigma_1^{-1}\bar{x}_1$ est un point L-rationnel de V. Noter qu'ici lorsqu'on prend un point quelconque de $V^{\sigma_1} \times \cdots \times V^{\sigma_d}$, on ne peut pas nécessairement lui appliquer σ_i puisque $V^{\sigma_1} \times \cdots \times V^{\sigma_d}$ gît dans $\mathbb{K}^{nd}$. L'idée de la preuve est d'appliquer un isomorphisme linéaire à $V^{\sigma_1} \times \cdots \times V^{\sigma_d}$ de façon à rendre cette variété définie sur K et transformer ses points L-rationnels en des points K-rationnels.

On commence par définir la variété W. Soit $e = e_1, \ldots, e_d$ une base du K-espace vectoriel L. Soient $P_1, \ldots, P_s$ les équations de $V \subseteq \mathbb{K}^n$ sur L, autrement dit les générateurs de $I_L(V) \subseteq L[X_1, \ldots, X_n]$. On prend ensuite des symboles transcendants $Y_{1,1}, \ldots, Y_{1,d}, Y_{2,1}, \ldots, Y_{n,d}$ (que

l'on notera aussi $\bar{Y}_1, \ldots, \bar{Y}_d$ donc $\bar{Y}_1 = Y_{1,1}, \ldots, Y_{n,1})$ et pour $i = 1, \ldots, s$ on pose

$$Q_i(\bar{Y}_1, \ldots, \bar{Y}_d) = P(\sum_{j=1,\ldots,d} Y_{1,j}e_j, \ldots, \sum_{j=1,\ldots,d} Y_{n,j}e_j)$$

En écrivant les coefficients des $Q_i(\bar{Y})$ de $L[\bar{Y}]$ dans la base $e_1, \ldots, e_d$ il existe pour chaque $i = 1, \ldots, s$ $Q_{i,j} \in K[\bar{Y}]$ tels que

$$Q_i = \sum_{j=1,\ldots,d} Q_{i,j}e_j$$

Si J est l'idéal de $K[\bar{Y}]$ engendré par les polynômes $(Q_{i,j})_{i=1,\ldots,s}^{j=1,\ldots,d}$, on définit alors $W_e := V(J) \subseteq \mathbb{K}^{nd}$. On vérifie alors deux choses :

1. Pour tout $i = 1, \ldots, d$ on a $W_{\sigma_i e} = W_e$

2. Si $(y_{1,1}, \ldots, y_{1,d}, \ldots, y_{n,d}) \in W_e$ alors $(\sum_{i=1,\ldots,d} y_{1,i}e_i, \ldots, \sum_{i=1,\ldots,d} y_{n,i}e_i) \in V^{\sigma_1} \times \cdots \times V^{\sigma_d}$.

On montre que W_e et $V^{\sigma_1} \times \cdots \times V^{\sigma_d}$ sont deux variétés isomorphes. Pour cela, on considère la matrice

$$M = \begin{pmatrix} \sigma_1 e_1 & \ldots & \sigma_1 e_d \\ \vdots & \ddots & \vdots \\ \sigma_d e_1 & \ldots & \sigma_d e_d \end{pmatrix}$$

On définit alors une application $f : \mathbb{K}^{nd} \to \mathbb{K}^{nd}$ telle que pour $(\bar{y}_1, \ldots, \bar{y}_d) \in \mathbb{K}^{nd}$ on créé la matrice $d \times n$ $\begin{pmatrix} \bar{y}_1 \\ \vdots \\ \bar{y}_d \end{pmatrix}$ on calcule alors $(x_{i,j}) = M \cdot \begin{pmatrix} \bar{y}_1 \\ \vdots \\ \bar{y}_d \end{pmatrix}$ et on pose $f(\bar{y}_1, \ldots, \bar{y}_d) = (x_{1,1}, \ldots, x_{1,n}, \ldots, x_{d,n}) = (\bar{x}_1, \ldots, \bar{x}_d)$ avec $\bar{x}_1 = x_{1,1}, \ldots, x_{n,1}$.

Par 1. et 2. $f(W_e) \subseteq V^{\sigma_1} \times \cdots \times V^{\sigma_d}$, et f est un morphisme de variété algébrique. On montre à présent que f est inversible et que sa réciproque est bien un morphisme, on aura donc bien que W_e et $V^{\sigma_1} \times \cdots \times V^{\sigma_d}$ sont isomorphes et on pourra conclure.
Si M n'est pas inversible, on a une relation linéaire sur les lignes disons $\sum_i \lambda_i \sigma_i e_j = 0$ avec $\lambda_i \in K^{alg}$, pour $j = 1, \ldots, d$. On a donc que pour n'importe que $a_1e_1 + \cdots + a_de_d \in L$ $(a_i \in K)$ on a $(\sum_i \lambda_i \sigma_i)(a_1e_1 + \cdots + a_de_d) = 0$ donc les applications K-linéaires $\sigma_1, \ldots, \sigma_d$ ne sont pas indépendant sur K^{alg} ce qui contredit le théorème d'indépendence des caractères. On définit alors $g : V^{\sigma_1} \times \cdots \times V^{\sigma_d} \to \mathbb{K}^{nd}$ par $g(\bar{x}_1, \ldots, \bar{x}_d) = (\bar{y}_1, \ldots, \bar{y}_d)$ $(\bar{x}_1 = x_{1,1}, \ldots, x_{1,n}$ et $\bar{y}_1 = y_{1,1}, \ldots, y_{n,1}$ cette convention est étrange mais c'est ce qui marche) de sorte que $(y_{i,j}) = M^{-1} \cdot \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_d \end{pmatrix}$ Montrons que g est à valeurs dans W_e. Pour $(\bar{y}_1, \ldots, \bar{y}_d) \in V^{\sigma_1} \times \cdots \times V^{\sigma_d}$ on pose $q_{i,j} = Q_{i,j}(\bar{y})$. On a alors $\sum_{j=1,\ldots,d} q_{i,j}\sigma_k e_j = \sigma_k(Q_i)(\bar{y}) = \sigma_k(P_i)(x_{k,1}, \ldots, x_{k,n}) = 0$, car $x_{k,1}, \ldots, x_{k,n} \in V^{\sigma_i}$. On a donc

$$M \cdot \begin{pmatrix} q_{1,1} & \cdots & q_{s,1} \\ \vdots & \ddots & \vdots \\ q_{1,d} & \cdots & q_{s,d} \end{pmatrix} = (0)$$

Comme M est inversible, cela force $q_{i,j} = 0$ pour $i = 1, \ldots, s$ et $j = 1, \ldots, d$. On conclut que g est à valeur dans W_e puisque les $Q_{i,j}$ sont les équations de W_e. On a clairement que g est

un morphisme de variétés et que $g \circ f = Id_{W_e}$ on conclut que W_e et $V^{\sigma_1} \times \cdots \times V^{\sigma_d}$ sont isomorphes.
Remarquons que si $\tilde{L}$ est la clôture galoisienne de L/K, les σ_i s'étendent en les éléments de $Gal(\tilde{L}/K)$ et de plus tous les $\sigma_i e_j$ sont dans $\tilde{L}$ donc les isomorphismes f et g sont bien définis sur $\tilde{L}$.

Références

[1] Elisabeth Bouscaren. *Model Theory and Algebraic Geometry.* Springer, 1998.

[2] Zoé Chatzidakis. Model theory of finite fields and pseudo-finite fields. *Annals of Pure and Applied Logic*, 88 :95–108, 1997.

[3] Jean-Louis Duret. Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendance. *Lecture Notes in Mathematics*, Model theory of Algebra and Arithmetic(834) :136–162, 1979.

[4] Jean Fresnel. *Géométrie Algébrique.* Université Bordeaux 1, UFR Mathématiques et informatique, 1985.

[5] Michael Fried and Moshe Jarden. *Field Arithmetic (1st edition).* Springer-Verlag, 1986.

[6] James E. Humphreys. *Linear Algebraic Groups.* Springer-Verlag, 1975.

[7] Bruno Kahn. *Formes quadratiques sur un corps.* Société Mathématique de France, 2008.

[8] Itay Kaplan, Thomas Scanlon, and FrankO. Wagner. Artin-schreier extensions in nip and simple fields. *Israel Journal of Mathematics*, 185(1) :141–153, 2011.

[9] Serge Lang. *Introduction to algebraic geometry.* Interscience publisher, inc. New York, 1958.

[10] Serge Lang. *Algebra (Revised Third Edition).* Springer, 2002.

[11] David Marker. *Model Theory : An Introduction.* Springer Graduate Texts in Mathematics, 2002.

[12] Patrick Morandi. *Field and Galois Theory.* Springer, 1996.

[13] David Marker Margit Messmer Anand Pillay. *Model Theory of Fields.* ASL, 2006.

[14] Thomas Scanlon. Infinite stable fields are artin-schreier closed. *non publié, page de Scanlon*, 1999.

[15] Jean-Pierre Serre. *Corps Locaux.* Hermann, Paris, 1968.

[16] Pierre Simon. *A guide to NIP theories.* Association for Symbolic Logic, 2015.

[17] Lou van den Dries. *Tame Topology and o-minimal structures.* Cambridge University Press, 1998.

[18] Katrin Tent Martin Ziegler. *A course in Model Theory.* Association for Symbolic Logic, 2012.

Les résultats classiques concernant les extensions d'Artin-Schreier (section 1.1) viennent de [10] et de [12]. Ceux sur le nombre d'extension d'Artin-Schreier sont dans [8] et utilisent [15], ainsi que [5] en ce qui concerne la théorie de Galois infinie. La sous-section 1.2 s'appuie sur [5] et [9] pour les définitions, la preuve du théorème 1.2.2 est inspirée de [18] et [12].

Concernant la géométrie algébrique, les rappels de base viennent de [4], [9] et [6]. Quelques liens avec la théorie des modèles sont exposés dans [1], et l'approche sur les groupes algébriques

est tirée de [6]. La sous-section sur les groupes vectoriels est issue de [6], la preuve du théorème 2.2.4 est indiquée dans [8] et utilise des résultats élémentaires de cohomologie galoisienne que l'on trouve dans [10], [15] ou [7]. L'étude du groupe $G_{\bar{a}}$ est entièrement tirée de [8].

Concernant la section 3, une bonne introduction à l'interprétation peut être trouvée dans [11] ou [18]. La plupart des choses que l'on sait concernant les théories NIP apparaissent dans [16].

La section 4 est entièrement issue de [8]. Enfin l'étude des corps PAC est faite dans [18] et [5], tandis que la preuve que les corps PAC ont la propriété d'indépendance est dûe à Duret dans [3].

La première annexe est tirée de [6] et la deuxième de [3] et [5].