Théorie des modèles des corps pseudo finis

Silvain Rideau

2 avril 2020

Table des matières

1 Logique du premier ordre (des anneaux)

1.1 Ultraproduits

On fixe V un ensemble infini, qui consistera en notre ensemble de variables. On fixe aussi A un anneau.

Définition 1.1 (Formules) **:** *Soit $\overline{x}$ un uplet de V. L'ensemble $\mathcal{F}_A(\overline{x})$ des formules à paramètres dans A et à variables $\overline{x}$, est le plus petit ensemble tel que :*

- *pour tout $P \in A[\overline{x}]$, $P \simeq 0 \in \mathcal{F}_A(\overline{x})$;*
- *$\perp \in \mathcal{F}_A(\overline{x})$;*
- *si $\varphi, \psi \in \mathcal{F}_A(\overline{x})$, alors $\varphi \to \psi \in \mathcal{F}_A(\overline{x})$;*
- *si $\varphi \in \mathcal{F}_A(y, \overline{x})$, alors $\exists y\, \varphi \in \mathcal{F}_A(\overline{x})$.*

Si $\varphi \in \mathcal{F}_A(\overline{x})$, on la note souvent $\varphi(\overline{x})$. Les éléments des $\mathcal{F}_A(\varnothing)$ s'appellent les A-énoncés. Un ensemble de A-énoncés s'appelle une A-théorie. Pour toute A-algèbre B, on note $\mathrm{Th}_A(B) := \{\varphi \in \mathcal{F}_A(\varnothing) : B \vDash \varphi\}$. Si B' est une autre A-algèbre, on écrit $B \equiv_A B'$ si $\mathrm{Th}_A(B) = \mathrm{Th}_A(B')$. On dit que B et B' sont A-élémentairement équivalents.

Définition 1.2 (La vérité selon Tarski) **:** *Soit B une A-algèbre, $\overline{x}$ un uplet de variables et $\overline{b} \in B^{\overline{x}}$ — c'est à dire un uplet de même longueur que $\overline{x}$. On dit que $\overline{b}$ réalise φ dans B, et on écrit $B \vDash \varphi(\overline{b})$:*

- *quand $\varphi = P \simeq 0$ avec $P \in A[\overline{x}]$, si $P(\overline{b}) = 0$;*
- *jamais, quand $\varphi = \perp$;*
- *quand $\varphi = \psi \to \theta$, si, quand $B \vDash \psi(\overline{b})$, on a $B \vDash \theta(\overline{b})$;*
- *quand $\varphi = \exists y\, \psi$ où $\psi \in \mathcal{F}_A(y, \overline{x})$, s'il existe $c \in B$ tel que $B \vDash \psi(c, \overline{b})$.*

On définit $T_{\mathrm{f}} := \{\varphi \in \mathcal{F}_{\mathbb{Z}}(\varnothing) :$ pour tout corps fini F, $F \vDash \varphi\}$, la théorie des corps finis, et $T_{\mathrm{psf}} := T_{\mathrm{f}} \cup \{\exists x_1 \ldots x_n \bigwedge_{i \neq j} x_i - x_j \not\simeq 0\}$, la théorie des corps pseudo finis.

Définition 1.3 (Filtres et Ultrafiltres) **:** *Soit I un ensemble. Un filtre sur I est un ensemble $\mathfrak{F} \subseteq \mathfrak{P}(I)$ tel que :*

- *$I \in \mathfrak{F}$;*
- *$\varnothing \notin \mathfrak{F}$;*
- *pour tout $X \subseteq Y \subseteq I$, si $X \in \mathfrak{F}$ alors $Y \in \mathfrak{F}$;*
- *pour tout $X, Y \in \mathfrak{F}$, $X \cap Y \in \mathfrak{F}$.*

On dit que $\mathfrak{F}$ est un ultrafiltre si, de plus :

- *Pour tout $X, Y \subseteq I$, si $X \cup Y \in \mathfrak{F}$, alors $X \in \mathfrak{F}$ ou $Y \in \mathfrak{F}$.*

Théorème 1.4 (Łoś, 1955) **:** *Soit I un ensemble, A un anneau et, pour tout $i \in I$, B_i une A-algèbre. Soit $\mathfrak{U}$ un ultrafiltre sur I. Alors $\mathfrak{b} := \{(b_i)_i : \{i : b_i = 0\} \in \mathfrak{U}\} \subset \prod_i B_i$ est un idéal et pour tout $\varphi \in \mathcal{F}_A(\overline{x})$ et $\overline{b}_i \in B_i^{\overline{x}}$, on a*

$$B \vDash \varphi(\overline{b}) \text{ si et seulement si } \{i : B_i \vDash \varphi(\overline{b}_i)\} \in \mathfrak{U},$$

où $B := \prod_i B_i/\mathfrak{b}$ et $\overline{b} \in B^{\overline{x}}$ est le uplet dont les coordonnées sont les $(b_{i,j})_i + \mathfrak{b}$.

La A-algèbre B sera notée $\prod_{i \to \mathfrak{U}} B_i$ et $\overline{b}$ sera noté $\prod_{i \to \mathfrak{U}} \overline{b}_i$.

Démonstration. Soient $(x_i)_i, (y_i)_i \in \prod_i B_i$. Si $(x_i)_i \in \mathfrak{b}$, alors $\{i : x_i = 0\} \subseteq \{i : y_i x_i = 0\} \in \mathfrak{U}$ et $\{i : x_i = 0\} \subseteq \{i : x_i y_i = 0\} \in \mathfrak{U}$, puisque c'est un filtre. De même, si on a aussi $(y_i)_i \in \mathfrak{b}$, on a alors $\{i : x_i = 0\} \cap \{i : y_i = 0\} \subseteq \{i : x_i + y_i = 0\} \in \mathfrak{U}$.
On procède maintenant par induction sur φ.

- Si $\varphi = P \simeq 0$, avec $P \in A[\overline{x}]$, on a $B \vDash \varphi(\overline{b})$ si et seulement si $P(\overline{b}) = 0$, si et seulement si $(P(\overline{b}_i))_i \in \mathfrak{b}$, si et seulement si $\{B_i \vDash \varphi(\overline{b}_i)\} = \{i : P(\overline{b}_i) = 0\} \in \mathfrak{U}$.
- Si $\varphi = \bot$, on a $B \nvDash \varphi(\overline{b})$ et $\{i : B_i \vDash \bot\} = \varnothing \notin \mathfrak{U}$.
- Si $\varphi = \psi \vee \theta$, on a $B \vDash \varphi(\overline{b})$ si et seulement si $B \vDash \psi(\overline{b})$ ou $B \vDash \theta(\overline{b})$, si et seulement si $\{i : B_i \vDash \psi(\overline{b}_i)\} \in \mathfrak{U}$ ou $\{i : B_i \vDash \theta(\overline{b}_i)\} \in \mathfrak{U}$. Comme $\mathfrak{U}$ est un filtre, cela implique que $\{i : B_i \vDash \varphi(\overline{b}_i)\} = \{i : B_i \vDash \psi(\overline{b}_i)\} \cup \{i : B_i \vDash \theta(\overline{b}_i)\} \in \mathfrak{U}$. La réciproque suit du fait que $\mathfrak{U}$ est un ultrafiltre.
- Enfin, si $\varphi = \exists y\, \psi$ où $\psi \in \mathcal{F}_A(y, \overline{x})$, on a $B \vDash \varphi(\overline{b})$ si et seulement s'il existe $c_i \in B_i$, pour tout $i \in I$, tel que $\{i : B_i \vDash \psi(c_i, \overline{b}_i)\} \in \mathfrak{U}$. Ce dernier ensemble est contenu dans $\{i : B_i \vDash \varphi(\overline{b}_i)\}$ qui est donc dans $\mathfrak{U}$. Réciproquement, si $X := \{i : B_i \vDash \exists y\, \varphi(\overline{b}_i)\} \in \mathfrak{U}$, pour tout i dans X, on trouve $c_i \in B_i$ tel que $B_i \vDash \psi(c_i, \overline{b}_i)$, et pour $i \notin X$, on pose $c_i = 0$. On a alors $\{i : B_i \vDash \psi(c_i, \overline{b}_i)\} = X \in \mathfrak{U}$. Ce qui conclut la preuve. □

Une fois qu'on a vérifié que les ultrafiltres sont exactement les filtres maximaux, le résultat suivant est une conséquence immédiate du lemme de Zorn :

Proposition 1.5 (Théorème de l'ultrafiltre) **:** *Tout filtre est contenu dans un ultrafiltre.*

Démonstration. On vérifie que l'ensemble des filtres sur I contenant un filtre donné $\mathfrak{F}$ est non vide et inductif pour l'inclusion (l'union d'une chaîne de filtre pour l'inclusion est bien un filtre). Par le lemme de Zorn, on trouve un filtre maximal $\mathfrak{U}$ contenant $\mathfrak{F}$. Supposons alors que $X \cup Y \in U$. Si on a $X \notin \mathfrak{F}$, on vérifie que $V := \{Z \subseteq I : \text{ il exists } W \in U \text{ tel que } W \cap Y \subseteq Z\}$ est bien un filtre qui contient U. La seule chose non triviale à vérifier est que $\varnothing \in V$. Si c'était le cas, on aurait $W \in U$ tel que $W \cap Y = \varnothing$. On aurait donc $W \cap X \cup Y \subseteq X$, ce qui contredit que $X \notin U$. Par maximalité de U, on a $W = U$ et donc $Y \in U$. □

Proposition 1.6 : *Soit F un corps. Sont équivalents :*

1. *F est pseudo fini ;*
2. *il existe $\mathfrak{U}$ un ultrafiltre non principal sur les puissance de nombres premiers tel que $F \equiv \prod_{q \to \mathfrak{U}} \mathbb{F}_q$;*
3. *il existe I, des corps finis $(F_i)_{i \in I}$, et $\mathfrak{U}$ un ultrafiltre sur I tels que $\lim_{i \to \mathfrak{U}} |F_i| = \infty$ et tels que $F \equiv \prod_{i \to \mathfrak{U}} F_i$*

Démonstration.

$1 \Rightarrow 2$ Pour tout $\varphi \in \mathcal{F}_{\mathbb{Z}}(\varnothing)$, on note $[\![\varphi]\!] := \{q : \mathbb{F}_q \vDash \varphi\}$. On note $X := \{[\varphi] : F \vDash \varphi\}$. Pour tout $(\varphi_i)_{i<n} \in \mathcal{F}_{\mathbb{Z}}(\varnothing)$, si $[\bigwedge_i \varphi_i] = \bigcap_i [\varphi_i] = \varnothing$, on a alors $\mathbb{F}_q \nvDash \bigvee_i \neg\varphi_i$, pour tout q, et donc, comme $K \vDash T_{\mathrm{f}}$, il existe i tel que $K \nvDash \varphi_i$. Il s'ensuit que X a la propriété d'intersection finie et donc qu'il existe un ultrafiltre $\mathfrak{U}$ contenant X. Par le théorème de Łoś (Théorème **(1.4)**) on a alors $K \vDash \varphi$ si et seulement si $[\varphi] \in X$ si et seulement si $\prod_{q \to \mathfrak{U}} \mathbb{F}_q \vDash \varphi$ et donc $K \equiv \prod_{q \to \mathfrak{U}} \mathbb{F}_q$.
Si $\mathfrak{U}$ était principal, il existerait q tel que $K \equiv \prod_{q \to \mathfrak{U}} \mathbb{F}_q \cong \mathbb{F}_q$ qui est fini. Ce qui contredirait le fait que K est pseudo-fini et donc infini.

$2 \Rightarrow 3$ C'est évident.

$3 \Rightarrow 1$ Par le théorème de Łoś, $K \equiv \prod_{i \to \mathfrak{U}} F_i \vDash T_\mathrm{f}$. De plus, par hypothèse, pour tout $N \in \mathbb{Z}_{\geqslant 0}$, il existe $V \in \mathfrak{U}$ tel que pour tout $i \in V$, $|F_i| \geqslant N$. On a alors $V \subseteq \{i : F_i \vDash \exists x_1 \cdots \exists x_n \bigwedge_{i \neq j} x_i \neq x_j\}$, d'où, par le théorème de Łoś (Théorème **(1.4)**), $K \equiv \prod_{i \to \mathfrak{U}} F_i \vDash \exists x_1 \cdots \exists x_n \bigwedge_{i \neq j} x_i \neq x_j$ et donc $|K| \geqslant N$. On a donc montré que K est bien un modèle infini de T_f. □

Corollaire 1.7 : *Il existe des corps pseudo finis de toute caractéristique.*

Démonstration. Soit $\mathfrak{U}$ un ultrafiltre non principal sur $\mathbb{P}$. Par la Proposition **(1.6)**, $\prod_{p \to \mathfrak{U}} \mathbb{F}_p$ est pseudo fini. De plus, pour tout premier p_0, $\{p : \mathbb{F}_p \vDash p_0 \simeq 0\} = \{p_0\}$ et donc son complémentaire est dans $\mathfrak{U}$. Par le théorème de Łoś (Théorème **(1.4)**), $\prod_{p \to \mathfrak{U}} \mathbb{F}_p$ est de caractéristique nulle.

Fixons maintenant $p \in \mathbb{P}$ et soit $\mathfrak{U}$ un ultrafiltre non principal sur $\mathbb{Z}_{>0}$. Par la Proposition **(1.6)**, $\prod_{n \to \mathfrak{U}} \mathbb{F}_{p^n}$ est pseudo fini. De plus $\{n : \mathbb{F}_{p^n} \vDash p \simeq 0\} = \mathbb{Z}_{>0}$ est dans $\mathfrak{U}$ et donc, par le théorème de Łoś (Théorème **(1.4)**), $\prod_{n \to \mathfrak{U}} \mathbb{F}_{p^n}$ est de caractéristique p. □

1.2 Types

Définition 1.8 (Ensembles consistants) **:** *Soit $\pi \subseteq \mathcal{F}_A(\overline{x})$.*

- *On dit que π est consistant s'il exists une A-algèbre B et $\overline{b} \in B^{\overline{x}}$ tel que, pour tout $\varphi \in \pi$, $B \vDash \varphi(\overline{b})$. On écrit alors $B \vDash \pi(\overline{b})$. Un sous-ensemble consistant de $\mathcal{F}_A(\overline{x})$ est aussi appelé un A-type partiel.*
- *π est dit finiment consistant si toute partie finie de π est consistante.*

Théorème 1.9 (Compacité ; Goedel, 1930 – Maltsev, 1936) **:** *Soit $\pi \subseteq \mathcal{F}_A(\overline{x})$. Sont équivalents :*

1. *π est consistant ;*
2. *π est finiment consistant.*

Démonstration. Il est évident que si π est consistant, il est finiment consistant. Il suffit donc de prouver la réciproque. Supposons donc que π est finiment consistant. Soit $I := \mathfrak{P}_\mathrm{f}(T)$. Pour tout $i \in I$, comme π est finiment consistante, il existe une A-algèbre B_i et $\overline{b}_i \in B_i^{\overline{x}}$ tel que $B_i \vDash i(\overline{b}_i)$. Pour tout $i \in I$, on définit $X_i := \{j \in I : i \subseteq j\}$ et on vérifie que $\{X \subseteq I :$ il existe $i \in I$ tel que $X_i \subseteq X\}$ est un filtre. Soit $\mathfrak{U}$ un ultrafiltre qui le contient. Pour tout $\varphi \in \pi$, on a alors $X_\varphi \subseteq \{i : B_i \vDash \varphi(b_i)\} \in \mathfrak{U}$ et donc $\prod_{i \to \mathfrak{U}} B_i \vDash \pi(\prod_{i \to \mathfrak{U}} \overline{b}_i)$. □

Définition 1.10 (Δ-Types) **:** *Soit $\Delta \subseteq \mathcal{F}_A(\overline{x})$ clos par les opérations booléennes.*

- *Un Δ-type partiel est un ensemble consistant de formules de Δ ;*
- *Un Δ-type partiel maximal pour l'inclusion est appelé un Δ-type complet.*

On dit qu'un Δ-type partiel π engendre un Δ-type complet modulo T, si $[\pi] \subseteq \mathcal{S}_\Delta(T)$ est un singleton.

Proposition 1.11 : *Soit $\Delta \subseteq \mathcal{F}_A(\overline{x})$ clos par les opération booléennes et π un Δ-type partiel. Sont équivalents :*

1. *π est un Δ-type complet ;*
2. *Il existe une A-algèbre B et $\overline{b} \in B^{\overline{x}}$ tel que $\pi = \mathrm{tp}_\Delta^B(\overline{b}) := \{\varphi \in \Delta \cup \neg\Delta : B \vDash \varphi(\overline{b})\}$;*
3. *pour tout $\varphi \in \Delta$, $\varphi \in \pi$ ou $\neg\varphi \in \pi$.*

Si B est une A-algèbre et $b \in B^x$, on définit $\mathrm{tp}_A^B(b) := \mathrm{tp}_{\mathcal{F}_A(x)}^B(b)$ et $\mathrm{qftp}_A^B(b) := \mathrm{tp}_{\mathcal{F}_A^{\mathrm{qf}}(x)}^B(b)$. Si $b' \in B^x$, on note $b \equiv_A^B b'$ si $\mathrm{tp}_A^B(b) = \mathrm{tp}_A^B(b')$.

Démonstration. Supposons que π soit maximal. Comme π est consistant, il existe une A-algèbre B et $\overline{b} \in B^{\overline{x}}$ tel que $B \models \pi(\overline{b})$. On a alors $\pi \subseteq \mathrm{tp}^B_\Delta(\overline{b})$, qui est, par définition, consistant. Par maximalité de π, on a $\pi = \mathrm{tp}^B_\Delta(\overline{b})$. Cela prouve que 1 implique 2.
Supposons maintenant que $\pi = \mathrm{tp}^B_\Delta(\overline{b})$ où B est une A-algèbre et $\overline{b} \in B^{\overline{x}}$. Pour tout $\varphi \in \Delta$, si $B \models \varphi(\overline{b})$, on a $\varphi \in \pi$; sinon $B \models \neg\varphi(\overline{b})$, et on a alors $\neg\varphi \in \pi$. On a donc que 2 implique 3.
Supposons enfin que pour tout $\varphi \in \Delta$, $\varphi \in \pi$ ou $\neg\varphi \in \pi$. Soit ρ un Δ-type partiel contenant π. Pour tout $\varphi \in \rho$, si $\neg\varphi \in \pi \subseteq \rho$, on a à la fois φ et $\neg\varphi \in \rho$ qui ne peut donc pas être consistant. Il s'ensuit donc que $\varphi \in \pi$ et donc $\rho \subseteq \pi$ qui est donc bien maximal. Cela prouve que 3 implique 1 et conclut la preuve. □

Définition 1.12 (Espace de Stone) **:** *Soit T une A-théorie et $\Delta \subseteq \mathcal{F}_A(\overline{x})$ clos par les opérations booléennes.*

- *On note $\mathcal{S}_\Delta(T)$ l'ensemble des Δ-types complets p tels que $T \cup p$ est consistant.*
- *Pour tout $\Phi \subseteq \Delta$, on note $[\Phi] := \{p \in \mathcal{S}_\Delta(T) : \Phi \subseteq p\}$.*

On note $\mathcal{S}_{\overline{x}}(T) := \mathcal{S}_{\mathcal{F}_A(\overline{x})}(T)$ et $\mathcal{S}^{\mathrm{qf}}_{\overline{x}}(T) := \mathcal{S}_{\mathcal{F}^{\mathrm{qf}}_A(\overline{x})}(T)$

Proposition 1.13 : *Les ensembles de la forme $[\Phi]$, où $\Phi \subseteq \Delta$, forment les fermés d'une topologie sur $\mathcal{S}_\Delta(T)$. Cette topologie est totalement discontinue séparée : pour tout $p, q \in \mathcal{S}_\Delta(T)$, il existe un ensemble ouvert-fermé $U \subseteq \mathcal{S}_\Delta(T)$ tel que $p \in U$ et $q \notin U$; de plus, elle est compacte.*

Cette topologie se nomme la topologie de Stone. Les seuls sous-ensembles de $\mathcal{S}_\Delta(T)$ connexes (pour la topologie induite) sont les singletons, d'où la terminologie « totalement discontinu ».

Démonstration. On a $[\varnothing] = \mathcal{S}_\Delta(T)$ et $[\Delta] = \varnothing$ qui sont donc bien fermés. De plus pour tout $\Phi_1, \Phi_2 \subseteq \Delta$, $[\Phi_1 \vee \Phi_2] = [\Phi_1] \cup [\Phi_2]$, où $\Phi_1 \vee \Phi_2 := \{\varphi_1 \vee \varphi_2 : \varphi_i \in \Phi_i\}$. Enfin $\bigcap_i [\Phi_i] = [\bigcup_i \Phi_i]$, et donc ce sont bien les fermés d'une topologie. De plus, si $p \neq q \in \mathcal{S}_\Delta(T)$, on trouve $\varphi \in \Delta$ telle que $\varphi \in p$ et $\varphi \notin q$. On a alors $p \in [\varphi]$ et $q \notin [\varphi]$. De plus, $[\varphi] = \mathcal{S}_\Delta(T) \smallsetminus [\neg\varphi]$ est bien ouvert-fermé.
Reste à montrer que cette topologie est compacte. Notons que $[\Phi] \neq \varnothing$ si et seulement si $T \cup \Phi$ est consistant. Soit $[\Phi_i]$ une collection de fermés tels toutes les intersections finies sont non vides. On considère $\pi := \bigcup_i \Phi_i$. Toute partie finie π_0 de π est incluse dans $\bigcup_{j \leqslant n} \Phi_{i_j}$ pour un nombre fini de i_j. Comme $[\bigcup_{j \leqslant n} \Phi_{i_j}] = \bigcap_i [\Phi_{i_j}] \neq \varnothing$, $T \cup \bigcup_{j \leqslant n} \Phi_{i_j}$, et donc $T \cup \pi_0$, sont consistants. Il s'ensuit que $T \cup \pi = T \cup \bigcup_i \Phi_i$ est consistant et donc que $\bigcap_i [\Phi_i] = [\bigcup_i \Phi_i] \neq \varnothing$. Ce qui conclut la preuve de la compacité de $\mathcal{S}_\Delta(T)$. □

Proposition 1.14 : *Soit $U \subseteq \mathcal{S}_\Delta(T)$ ouvert-fermé. Il existe $\varphi \in \Delta$ tel que $U = [\varphi]$.*

Démonstration. Puisque $\mathcal{S}_\Delta(T) \smallsetminus U$ est fermé, il existe $\Phi \subseteq \Delta$ tel que $U = \mathcal{S}_\Delta(T) \smallsetminus [\Phi] = \mathcal{S}_\Delta(T) \smallsetminus (\bigcap_{\varphi \in \Phi} [\varphi]) = \bigcup_{\varphi \in \Phi} [\neg\varphi]$. Mais U est fermé, donc compact, et il s'ensuit qu'il existe un nombre fini de $\varphi_i \in \Phi$, $i \leqslant n$, tels que $U = \bigcup_{i \leqslant n} [\neg\varphi_i] = [\bigvee_{i \leqslant n} \neg\varphi_i]$. □

1.3 Morphismes

Définition 1.15 (Formules sans quantificateurs) **:** *Soit $\overline{x}$ un uplet de V. L'ensemble $\mathcal{F}^{\mathrm{qf}}_A(\overline{x})$ des formules à paramètres dans A et à variables $\overline{x}$, est le plus petit ensemble tel que :*

- *pour tout $P \in A[\overline{x}]$, $P \simeq 0 \in \mathcal{F}^{\mathrm{qf}}_A(\overline{x})$;*
- *$\bot \in \mathcal{F}^{\mathrm{qf}}_A(\overline{x})$;*

- *si* $\varphi \in \mathcal{F}_A^{\mathrm{qf}}(\overline{x})$*, alors* $\neg\varphi \in \mathcal{F}_A^{\mathrm{qf}}(\overline{x})$ *;*
- *si* $\varphi, \psi \in \mathcal{F}_A^{\mathrm{qf}}(\overline{x})$*, alors* $\varphi \vee \psi \in \mathcal{F}_A^{\mathrm{qf}}(\overline{x})$*.*

Proposition 1.16 : *Soit $f : C \to D$ un morphisme injectif de A-algèbre, alors pour tout $\varphi \in \mathcal{F}_A^{\mathrm{qf}}(\overline{x})$ et $\overline{c} \in C^{\overline{x}}$, on a $C \vDash \varphi(\overline{c})$ si et seulement si $D \vDash \varphi(f(\overline{c}))$.*

Démonstration. On procède par induction sur φ. Les équivalences étant préservées par combinaison booléennes, il suffit de vérifier le cas où $\varphi = P \simeq 0$ avec $P \in A[\overline{x}]$. On a alors $C \vDash \varphi(\overline{c})$ si et seulement si $P(\overline{c}) = 0$. Comme f est injectif et que f est un morphisme de A-algèbre, cela est équivalent à $P(f(\overline{c})) = f(P(\overline{c})) = 0$, ce qui est bien équivalent à $D \vDash \varphi(f(\overline{c}))$. □

Corollaire 1.17 : *Soient B et D deux A-algèbres, $\overline{b} \in B^{\overline{x}}$, $\overline{d} \in D^{\overline{x}}$ et $p = \mathrm{qftp}_A^B(\overline{b})$. Sont équivalents :*

1. *$D \vDash p(\overline{d})$;*
2. *Il existe un isomorphisme de A-algèbres $f : A[\overline{b}] \to A[\overline{d}]$ tel que $f(\overline{b}) = \overline{d}$.*

Démonstration. Supposons que $D \vDash p(\overline{d})$. Pour tout $P \in A[\overline{x}]$, on définit $f(P(\overline{b})) := P(\overline{d})$. Comme $P(\overline{b}) = 0$ si et seulement si $P \simeq 0 \in p$, si et seulement si $P(\overline{d}) = 0$, f est un morphisme injectif de A-algèbres. Il est clair que f est surjective.
Réciproquement, supposons qu'il existe un isomorphisme de A-algèbres $f : A[\overline{b}] \to A[\overline{d}]$ tel que $f(\overline{b}) = \overline{d}$. Comme f est injective et $B \vDash p(\overline{b})$, par la Proposition **(1.16)**, $D \vDash p(f(\overline{b})) = p(\overline{d})$. □

Définition 1.18 (Morphisme élémentaire) **:** *Soient $h : C \to B$ et $f : C \to D$ deux morphismes de A-algèbres. On dit que f est un morphisme B-élémentaire, si pour toute formule $\varphi \in \mathcal{F}_A(\overline{x})$ et $\overline{c} \in C^{\overline{x}}$, on a $B \vDash \varphi(h(\overline{c}))$ si et seulement si $D \vDash \varphi(f(\overline{c}))$.*

Si $h : C \to C = B$ est l'identité, on dit simplement que $f : B \to D$ est morphisme élémentaire de A-algèbres.

Proposition 1.19 : *Soit $f : B \to D$ un isomorphisme de A-algèbre, alors f est élémentaire.*

Démonstration. On prouve par induction sur $\varphi \in \mathcal{F}_A(\overline{x})$ que pour tout $\overline{b} \in B^{\overline{x}}$, $B \vDash \varphi(\overline{b})$ si et seulement si $D \vDash \varphi(f(\overline{d}))$. Les équivalences étant préservées par combinaison booléennes et f étant injectif, il suffit de vérifier le cas $\varphi = \exists y\, \psi$. S'il existe $c \in B^y$ tel que $B \vDash \psi(c, \overline{b})$, par induction on a $D \vDash \psi(f(c), f(\overline{b}))$ et donc $D \vDash \varphi(f(\overline{b}))$. Réciproquement, s'il existe $d \in D^y$ tel que $D \vDash \psi(d, f(\overline{b}))$, on a $B \vDash \psi(f^{-1}(d), \overline{b})$ et donc $B \vDash \varphi(\overline{b})$. □

Définition 1.20 : *Soient $\varphi \in \mathcal{F}_A(\overline{x})$ et $\overline{P} \in A[\overline{y}]^{\overline{x}}$. On définit $\varphi(\overline{P}) \in \mathcal{F}_A(\overline{y})$ par induction sur φ :*

- *si* $\varphi = Q \simeq 0$*, où* $Q \in A[\overline{x}]$*,* $\varphi(\overline{P}) := Q(\overline{P}) \simeq 0$ *;*
- *si* $\varphi = \bot$*,* $\varphi(\overline{P}) := \bot$ *;*
- *si* $\varphi = \neg\psi$*,* $\varphi(\overline{P}) := \neg\varphi(\overline{P})$ *;*
- *si* $\varphi = \psi \vee \theta$*,* $\varphi(\overline{P}) := \psi(\overline{P}) \vee \theta(\overline{P})$ *;*
- *si* $\varphi = \exists z\, \psi$*,* $\varphi(\overline{P}) := \exists z\, \psi(z, \overline{P})$*.*

Remarque 1.21 : Soient B une A-algèbre, $\varphi \in \mathcal{F}_A(\overline{x})$, $\overline{P} \in A[\overline{y}]^{\overline{x}}$ et $\overline{b} \in B^{\overline{y}}$. On a :

$$B \vDash \varphi(\overline{P})(\overline{b}) \text{ si et seulement si } B \vDash \varphi(\overline{P}(\overline{b})).$$

Lemme 1.22 : *Soient B et D deux A-algèbres, $\overline{b} \in B^{\overline{x}}$, $\overline{d} \in D^{\overline{x}}$ et $p = \mathrm{tp}_A^B(\overline{b})$. Sont équivalents :*

1. *$D \models p(\overline{d})$;*
2. *Il existe un morphisme B-élémentaire de A-algèbres $f : A[\overline{b}] \to D$ tel que $f(\overline{b}) = \overline{d}$.*

Démonstration. Supposons que $D \models p(\overline{d})$. Comme $\mathrm{qftp}_A^B(\overline{b}) \subseteq p$, par le Corollaire **(1.17)**, il existe un morphisme de A-algèbres $f : A[\overline{b}] \to D$ tel que $f(\overline{b}) = \overline{d}$. Pour tout $\varphi \in \mathcal{F}_A(\overline{y})$ et $\overline{P}(\overline{b}) \in (A[\overline{b}])^{\overline{y}}$, on a $B \models \varphi(\overline{P}(\overline{b}))$ si et seulement si $\varphi(\overline{P}) \in p$, si et seulement si $D \models \varphi(\overline{P}(\overline{d}))$. Réciproquement, supposons qu'il existe un morphisme B-élémentaire de A-algèbres $f : A[\overline{b}] \to D$ tel que $f(\overline{b}) = \overline{d}$. Pour tout $\varphi \in p$, on a $B \models \varphi(\overline{b})$ et donc $D \models \varphi(f(\overline{b})) = \varphi(\overline{d})$. D'où $D \models p(\overline{d})$. □

Définition 1.23 : *Soit B une A-algèbre.*
- *On définit* $\mathrm{Th}_A^{\mathrm{qf}}(B) := \{\varphi \in \mathcal{F}_A^{\mathrm{qf}}(\varnothing) : B \models \varphi\} = \mathrm{qftp}_A^B(\varnothing)$. *On parle du diagramme sans quantificateur de A dans B.*
- *On définit* $\mathrm{Th}_A(B) := \{\varphi \in \mathcal{F}_A(\varnothing) : B \models \varphi\} = \mathrm{tp}_A^B(\varnothing)$. *On parle du diagramme élémentaire de A dans B.*

Si $D \models \mathrm{Th}_A(B)$, on dit que D est élémentairement équivalent à B au dessus de A et on écrit $D \equiv_A B$. Une A-théorie T engendre une théorie complète si et seulement si pour tout $B, D \models T$, $B \equiv_A D$. L'espace $\mathcal{S}_\varnothing(T)$ contient alors un unique point qui est exactement $\mathrm{Th}_A(B)$ pour tout choix de $B \models T$.

Remarque 1.24 : Soient B et D deux A-algèbres de morphismes structurels $f : A \to B$ et $h : A \to D$.
- On a $D \models \mathrm{Th}_A^{\mathrm{qf}}(B)$ si et seulement si $\ker(f) = \ker(h)$.
- On a $D \models \mathrm{Th}_A(B)$ si et seulement si f est B-élémentaire.

Définition 1.25 : *Soient C une A-algèbre et $f : A \to C$ son morphisme structurel.*
- *Pour tout $\varphi \in \mathcal{F}_A(\overline{x})$, on note $f_\star\varphi \in \mathcal{F}_C(\overline{x})$ la formule définie par l'induction suivante :*
  - *pour tout $P \in A[\overline{x}]$, $f_\star(P \simeq 0) := f_\star P \simeq 0$;*
  - *$f_\star\bot := \bot$;*
  - *pour tout $\varphi \in \mathcal{F}_A(\overline{x})$, $f_\star(\neg\varphi) := \neg f_\star\varphi$;*
  - *pour tout $\varphi, \psi \in \mathcal{F}_A(\overline{x})$, $f_\star(\varphi \vee \psi) := f_\star\varphi \vee f_\star\psi$;*
  - *pour tout $\varphi \in \mathcal{F}_A(y, \overline{x})$, $f_\star(\exists y\, \varphi) := \exists y\, f_\star\varphi$.*
- *Pour tout $\pi \subseteq \mathcal{F}_A(\overline{x})$, on définit $f_\star\pi := \{f_\star\varphi : \varphi \in \pi\}$.*

On note aussi $P_C := f_\star P$, $\varphi_C := f_\star\varphi$ et $\pi_C := f_\star\pi$.

Lemme 1.26 : *Soit $f : C \to D$ un morphisme de A-algèbres. On note D_f la C-algèbre de morphisme structurel f. Soient $\varphi \in \mathcal{F}_A(\overline{x})$ et $\overline{d} \in D^{\overline{x}}$. On a alors :*

$$D \models \varphi(\overline{d}) \text{ si et seulement si } D_f \models \varphi_C(\overline{d}).$$

En particulier, pour tout $\pi \subseteq \mathcal{F}_A(\overline{x})$ et $\overline{d} \in D^{\overline{x}}$, on a :

$$D \models \pi(\overline{d}) \text{ si et seulement si } D \models \pi_C(\overline{d}).$$

Démonstration. On procède par induction sur φ. Comme les équivalences sont préservées par combinaisons booléennes, il suffit de vérifier le cas où $\varphi = P \simeq 0$ et le cas $\varphi = \exists y\, \psi$. Si $\varphi = P \simeq 0$, puisque f est un morphisme de A-algèbres, on a $P(\overline{d}) = P_C(\overline{d})$. Si $\varphi = \exists y, \psi$, on a $D \models \varphi(\overline{d})$ si et seulement s'il existe $d_0 \in D$ tel que $D \models \psi(d_0, \overline{d})$, ce qui est équivalent à $D_f \models \psi_C(d_0, \overline{d})$, et donc a $D_f \models \varphi_C(\overline{d})$. □

Définition 1.27 : *Soit $\pi \subseteq \mathcal{F}_A(\overline{x})$ un A-type partiel et $\varphi \in \mathcal{F}_A(\overline{x})$. On dit que π implique φ, et on écrit $\pi \models \varphi$ si pour toute A-algèbre B et tout $\overline{b} \in B^{\overline{x}}$, si $B \models \pi(\overline{b})$, $B \models \varphi(\overline{b})$.*

Définition 1.28 (Élimination des quantificateurs) **:** *Soit T une A-théorie, on dit que T élimine les quantificateurs si pour tout $\varphi \in \mathcal{F}_A(\overline{x})$, il existe $\psi \in \mathcal{F}_A^{\mathrm{qf}}(\overline{x})$ tel que $T \models \forall \overline{x}\,(\varphi \leftrightarrow \psi)$.*

Remarque 1.29 : Soit T une A-théorie qui élimine les quantificateurs. Pour tous $B, D \models T$ et $f : B \to D$ un morphisme injectif de A-algèbres, f est élémentaire. On dit que T est modèle complète.

Théorème 1.30 (Union de chaîne, Tarski) **:** *Soient I un ensemble filtrant et pour tout $i < j$, $f_{i,j} : B_i \to B_j$ une collection compatible de morphismes élémentaires de A-algèbres. Alors pour tout $i \in I$, $h_i : B_i \to B := \varinjlim_i B_i$ est élémentaire.*

Démonstration. Remarquons tout d'abord que comme les $f_{i,j}$ sont élémentaires, ils sont injectifs. Il s'ensuit que les h_i sont injectifs. Prouvons maintenant par induction sur $\varphi \in \mathcal{F}_A(\overline{x})$ que pour tout i et tout $\overline{b}_i \in B_i^{\overline{x}}$, $B_i \models \varphi(\overline{b}_i)$ si et seulement si $B \models \varphi(h_i(\overline{b}_i))$. Puisque que les équivalences sont préservées par les combinaisons booléennes, et que les h_i sont injectifs, il suffit de considérer le cas $\varphi = \exists y\,\psi$. Supposons tout d'abord qu'il existe $c_i \in B_i$ tel que $B_i \models \psi(c_i, \overline{b}_i)$ et donc, par induction $B \models \psi(h_i(c_i), h_i(\overline{b}_i))$. En particulier, $B \models \varphi(h_i(\overline{b}_i))$. Réciproquement, s'il existe $c \in B = \varinjlim_i B_i$ tel que $B \models \psi(c, h_i(\overline{b}_i))$, il existe $j \in I$ et $c_j \in B_j$ tel que $c = h_j(c_j)$. Comme $h_i = h_j \circ f_{i,j}$, par induction, on a $B_j \models \psi(c_j, f_{i,j}(\overline{b}_i))$ et donc $B_j \models \varphi(f_{i,j}(\overline{b}_i))$. Comme $f_{i,j}$ est élémentaire, il s'ensuit que $B_i \models \varphi(\overline{b}_i)$. □

Proposition 1.31 : *Soit T une A-théorie. Sont équivalents :*

1. *T élimine les quantificateurs ;*
2. *pour tout $B, D \models T$, tous morphismes injectifs de A-algèbres $h : C \to B$ et $f : C \to D$ et tout $\varphi \in \mathcal{F}_C^{\mathrm{qf}}(x)$, si $B_h \models \exists x\,\varphi$, alors $D_f \models \exists x\,\varphi$;*
3. *pour tout $B, D \models T$, tous morphismes injectifs de A-algèbres $h : C \to B$ et $f : C \to D$ et tout $b \in B$, il existe $l : D \to D^\star$ un morphisme élémentaire de A-algèbres et $g : C[b] \to D^\star$ un morphisme injectif de C-algèbres ;*
4. *pour tout $B, D \models T$, et tous morphismes injectifs de A-algèbres $h : C \to B$ et $f : C \to D$ et tout $b \in B$, l existe $l : D \to D^\star$ un morphisme élémentaire de A-algèbres et $g : B \to D^\star$ un morphisme injectif de C-algèbres ;*
5. *pour tout $B, D \models T$ et tout morphisme injectif de A-algèbres $h : C \to B$, tout morphisme injectif de A-algèbe $f : C \to D$ est B-élémentaire ;*
6. *pour tout $B \models T$ et tout morphisme injectif de A-algèbres $h : C \to B$, la théorie $T_C^{\mathrm{qf}} := T_C \cup \mathrm{Th}_C^{\mathrm{qf}}(B_h)$ engendre une théorie complète.*

Démonstration.

$1 \Rightarrow 2$ Soit $\psi \in \mathcal{F}_A^{\mathrm{qf}}(x, \overline{y})$ et $\overline{c} \in C^{\overline{y}}$ tel que $\varphi = \psi_C(x, \overline{c})$. Comme T élimine les quantificateurs, il existe $\theta \in \mathcal{F}_A^{\mathrm{qf}}(\overline{y})$ telle que $T \models \forall \overline{y}\,((\exists x\,\psi) \leftrightarrow \theta)$. On a alors que $B_h \models \exists x\,\varphi$ si et seulement si $B \models \theta(h(\overline{c}))$, si et seulement si $C \models \theta(\overline{c})$, si et seulement si $D \models \theta(f(\overline{c}))$, si et seulement si $D_f \models \exists x\,\varphi$.

$2 \Rightarrow 3$ Soit $p(x) \coloneqq \mathrm{qftp}_C^{B_h}(b)$. Pour tout $p_0 \subseteq p$ fini, on a $B_h \vDash \exists x \bigwedge_{\varphi \in p_0} \varphi(x)$ et donc, $D_f \vDash \exists x \bigwedge_{\varphi \in p_0} \varphi(x)$. Il s'ensuit que $q \coloneqq \mathrm{Th}_D(D) \cup f_\star p$ est finitment consistant et donc, par compacité, il existe une D-algèbre $D^\star$ et $d \in (D^\star)^x$ tel que $D^\star \vDash q(d)$. Soit $l : D \to D^\star$ son morphisme structurel qui est élémentaire. Soit $D_C^\star$ la C-algèbre de morphisme structurel $l \circ f$. Comme $D_C^\star \vDash p(d)$, par le Corollaire **(1.17)**, on trouve un morphisme injectif de C-algèbre $g : C[b] \to D^\star$ tel que $g(b) = d$.

$3 \Rightarrow 4$ Soit $(b_i)_{i \in \kappa}$ une énumération de B. On construit par induction, pour tout $j < i$, $l_{j,i} : D_j \to D_i$ un morphisme élémentaire de A-algèbre et $g_i : C[\overline{b}_{<i}] \to D_i$ un morphisme injectif de A-algèbres, tels que, pour tout $j < i$, $g_i \circ h_{j,i} = l_{j,i} \circ g_j$, où $h_{j,i} : C[b_{<j}] \to C[b_{<i}]$ est le morphisme naturel. On pose $D_0 = D$ et $g_0 = f$. Pour construire $l_{i,i+1}$ et g_{i+1}, on applique 3 à l'inclusion de $C[b_{<i}]$ dans B et g_i. Pour construire l_i et g_i quand i est limite, on pose $D_i = \varinjlim_{j<i} D_j$, $l_{j,i} : D_j \to D_i$ le morphisme élémentaire naturel, et $g_i : C[\overline{b}_{<i}] = \bigcup_{j<i} C[\overline{b}_{<j}] \to D_i$ le morphisme universel. On obtient donc au final $l \coloneqq l_{0,\kappa} : D \to D^\star = D_\kappa$ et $g \coloneqq g_\kappa : B \to D^\star$ qui ont les propriétés requises.

$4 \Rightarrow 5$ On construit par induction sur $i < \omega$ des morphismes injectifs de A-algèbres $f_i : B_i \to D_i$, $g_i : D_i \to B_{i+1}$ tels que $g_i \circ f_i : B_i \to B_{i+1}$ et $f_{i+1} \circ g_i : D_i \to D_{i+1}$ sont des morphismes élémentaires. On pose $B_0 = B$ et $f_0 : B_0 \to D_0$ le morphisme obtenu en appliquant 4 à h et f. Par construction, il existe un morphisme élémentaire $l : D \to D_0$ tel que $f_0 \circ h = l \circ f$. Supposons que f_i est construit. Soit $E_i \coloneqq f_i(B_i) \leqslant D_i$. On obtient alors $g_i : D_i \to B_{i+1}$ en appliquant 4 à l'inclusion de E_i dans D_i et $f_i^{-1} : E_i \to B_i$. Soit alors $C_{i+1} \coloneqq g_i(D_i) \leqslant B_{i+1}$. On obtient f_{i+1} en appliquant 4 à l'inclusion de C_{i+1} dans B_{i+1} et $g_i^{-1} : C_{i+1} \to D_i$.

On note $B_\omega = \varinjlim_i B_i$, $D_\omega \coloneqq \varinjlim_i D_i$, $f_\omega \coloneqq \varinjlim_i f_i : B_\omega \to D_\omega$ et $g_\omega \coloneqq \varinjlim_i g_i : D_\omega \to B_\omega$. Soient $h_\omega : B \to B_\omega$ et $l_\omega : D \to D_\omega$, les morphismes élémentaires naturels. On vérifie facilement que f_ω et g_ω sont des isomorphismes inverses l'un de l'autre. En particulier, f_ω est élémentaire. On vérifie aussi que $f_\omega \circ h_\omega \circ h = l_\omega \circ f$ et donc que f est B-élémentaire.

$5 \Rightarrow 6$ Remarquons que $B \vDash T_C^{\mathrm{qf}}$. Il suffit donc de vérifier que pour tout $D \vDash T_C^{\mathrm{qf}}$, $B \equiv_C D$. Comme $D \vDash T_C$, on a $D \vDash T$, et comme $D \vDash \mathrm{Th}_C^{\mathrm{qf}}(B_h)$, il existe un morphisme injectif de A-algèbres $f : C \to D$. Par 5, f est B-élémentaire. On a donc bien, $B \equiv_C D$.

$6 \Rightarrow 1$ Fixons un uplet de variables $\overline{x}$. Pour tout $p \in \mathcal{S}_{\overline{x}}(T)$, soit $\mathrm{qf}(p) \coloneqq \{\varphi \in \mathcal{F}_A^{\mathrm{qf}}(\overline{x}) : \varphi \in p\} \in \mathcal{S}_{\overline{x}}^{\mathrm{qf}}(T)$. On peut vérifier que la fonction $\mathrm{qf} : \mathcal{S}_{\overline{x}}(T) \to \mathcal{S}_{\overline{x}}^{\mathrm{qf}}(T)$ est une fonction continue. Soit $q \in \mathcal{S}_{\overline{x}}(T)$ tel que $\mathrm{qf}(q) = \mathrm{qf}(p) \eqqcolon r$. Soit $B, D \vDash T$, $\overline{b} \in B^{\overline{x}}$ et $\overline{d} \in D^{\overline{x}}$ tels que $B \vDash p(\overline{b})$ et $D \vDash q(\overline{d})$. Soit $C = A[\overline{b}] \leqslant B$. Comme $D \vDash r(\overline{d})$, il existe un morphisme injectif de A-algèbre $f : C \to D$ tel que $f(\overline{b}) = \overline{d}$. On a alors $D_f \vDash T_C^{\mathrm{qf}}$ et donc, par 6, $D_f \equiv_C B$, autrement dit, $p = \mathrm{tp}_A^B(\overline{b}) = \mathrm{tp}_A^D(\overline{d}) = q$. Il s'ensuit que qf est injectif. Comme $\mathcal{S}_{\overline{x}}(T)$ et $\mathcal{S}_{\overline{x}}^{\mathrm{qf}}(T)$ sont compacts, c'est un homémorphisme.

Pour tout $\varphi \in \mathcal{F}_A(\overline{x})$, l'ensemble $\mathrm{qf}([\varphi]) \subseteq \mathcal{S}_{\overline{x}}^{\mathrm{qf}}(T)$ est donc ouvert-fermé. Il s'ensuit qu'il existe $\psi \in \mathcal{F}_A^{\mathrm{qf}}(\overline{x})$ tel que $\mathrm{qf}([\varphi]) = [\psi]$ et donc $[\varphi] = \mathrm{qf}^{-1}([\psi]) = [\psi] \subseteq \mathcal{S}_{\overline{x}}(T)$, c'est-à-dire, $T \vDash \forall \overline{x}\, (\varphi \leftrightarrow \psi)$. □

2 Un peu de géométrie algébrique

2.1 La topologie de Zariski

Soit F un corps et K un corps algébriquement clos contenant F.

Définition 2.1 (Fermés de Zariski) **:** *Pour tout $R \subseteq F[\overline{X}]$, où $\overline{X}$ est un uplet, on définit :*

$$\mathcal{V}_K(R) := \{a \in K^{\overline{X}} : \textit{pour tout } P \in R,\ P(a) = 0\}.$$

Réciproquement, pour tout $S \subseteq K^{\overline{X}}$, on définit :

$$\mathcal{I}_F(S) := \{P \in F[\overline{X}] : \textit{pour tout } a \in S,\ P(a) = 0\}.$$

Les ensembles de la forme $\mathcal{V}_K(R)$ s'appellent les F-fermés de Zariski.

On peut facilement vérifier les propriétés suivantes :

Lemme 2.2 : *Soient $Q, R \subseteq F[\overline{X}]$ et $S, T \subseteq K^{\overline{X}}$.*

- *$\mathcal{I}_F(S) \subseteq F[\overline{X}]$ est un idéal radical : pour tout $f \in F[\overline{X}]$ et $n \in \mathbb{Z}_{>0}$, si $f^n \in \mathcal{I}_F(S)$ alors $f \in \mathcal{I}_F(S)$;*
- *$R \subseteq \mathcal{I}_F(\mathcal{V}_K(R))$ et $S \subseteq \mathcal{V}_K(\mathcal{I}_F(S))$;*
- *Si $Q \subseteq R$ alors $\mathcal{V}_K(R) \subseteq \mathcal{V}_K(Q)$ et si $S \subseteq T$ alors $\mathcal{I}_F(T) \subseteq \mathcal{I}_F(S)$;*
- *$\mathcal{I}_F(\mathcal{V}_K(\mathcal{I}_F(S))) = \mathcal{I}_F(S)$ et $\mathcal{V}_K(\mathcal{I}_F(\mathcal{V}_K(R))) = \mathcal{V}_K(R) = \mathcal{V}_K((R))$;*
- *$\mathcal{I}_F(\varnothing) = (1)$, $\mathcal{I}_F(K^{\overline{X}}) = (0)$, $\mathcal{V}_K(\varnothing) = \mathcal{V}_K((0)) = K^{\overline{X}}$ et $\mathcal{V}_K((1)) = \varnothing$;*
- *$\mathcal{V}_K(Q \cup R) = \mathcal{V}_K(Q) \cap \mathcal{V}_K(R)$ et $\mathcal{V}_K((Q) \cap (R)) = \mathcal{V}_K(Q) \cup \mathcal{V}_K(R)$;*
- *$\mathcal{I}_F(S \cup T) = \mathcal{I}_F(S) \cap \mathcal{I}_F(T)$ et $\mathcal{I}_F(S) \cup \mathcal{I}_F(T) \subseteq \mathcal{I}_F(S \cap T)$.*

Démonstration. Montrons tout d'abord que $\mathcal{I}_F(S) \subseteq F[\overline{X}]$ est un idéal radical. Pour tout $f, g \in \mathcal{I}_F(S)$ et $\overline{x} \in R$, $f_g(\overline{x}) = f(\overline{x}) + g(\overline{x}) = 0$ et donc $f + g \in \mathcal{I}_F(S)$. Pour tout $h \in F[\overline{X}]$, on alors $hf(\overline{x}) = h(\overline{x})f(\overline{x}) = 0$ et donc $hf \in \mathcal{I}_F(S)$. C'est donc bien un idéal. Enfin, si pour un certain $n \in \mathbb{Z}_{>0}$, on a $h^n \in \mathcal{I}_F(S)$, on a alors $(h(\overline{x}))^n = h^n(\overline{x}) = 0$ et donc, comme $F[\overline{X}]$ est intègre, $h(\overline{x}) = 0$. D'où $h \in \mathcal{I}_F(S)$ qui est bien radical.
Démontrons aussi une des égalités qui sera utile par la suite : $\mathcal{V}_K((Q) \cap (R)) = \mathcal{V}_K(Q) \cup \mathcal{V}_K(R)$. Puisque $(Q) \cap (R) \subseteq (Q)$, on a $\mathcal{V}_K(Q) = \mathcal{V}_K((Q)) \subseteq \mathcal{V}_K((Q) \cap (R))$. De manière symétrique, $\mathcal{V}_K(R) \subseteq \mathcal{V}_K((Q) \cap (R))$. Il suffit donc de démontrer que $\mathcal{V}_K((Q) \cap (R)) \subseteq \mathcal{V}_K(Q) \cup \mathcal{V}_K(R)$. Soit $\overline{x} \in \mathcal{V}_K((Q) \cap (R))$ tel que $\overline{x} \notin \mathcal{V}_K(Q)$. Soit $f \in Q$ tel que $f(\overline{x}) \neq 0$. Pour tout $g \in R$, on a $fg \in (Q) \cap (R)$ et donc $f(\overline{x})g(\overline{x}) = 0$. Il s'ensuit que $g(\overline{x}) = 0$ et donc $\overline{x} \in \mathcal{V}_K(R)$. □

Rappelons qu'un anneau est noethérien si tous ses idéaux sont finiment engendrés — ou de maniére équivalente, toute chaîne croissante d'idéaux est stationnaire. L'anneau $F[\overline{X}]$ est noethérien. Une topologie est noethérienne si toute chaîne décroissante de fermés est stationnaire.

Proposition 2.3 : *L'ensemble des F-fermés de Zariski forme les fermés d'une toplologie noethérienne sur $K^{\overline{X}}$.*

Démonstration. Comme on a démontré dans le Lemme **(2.2)**, $K^{\overline{X}}$ et $\varnothing$ sont bien des F-fermés de Zariski. Dans le même lemme, on a aussi démontré que l'union de deux F-fermés de Zariski est bien un F-fermé de Zariski. Il reste donc à démontrer qu'étant donné une collection de sous-ensembles $(R_i)_i \subseteq F[\overline{X}]$, $\bigcap_i \mathcal{V}_K(R_i)$ est bien un F-fermé de Zariski. Montrons que $\bigcap_i \mathcal{V}_K(R_i) = \mathcal{V}_K(\bigcup_i R_i)$. Comme $R_i \subseteq \bigcup_i R_i$, on a bien $\mathcal{V}_K(\bigcup_i R_i) \subseteq \mathcal{V}_K(R_i)$. Choisissons donc $\overline{x} \in \mathcal{V}_K(R_i)$ pour tout i. Pour tout $f \in \bigcup_i R_i$, on a alors $f(\overline{x}) = 0$ et donc $\bigcap_i \mathcal{V}_K(R_i) \subseteq \mathcal{V}_K(\bigcup_i R_i)$.

Montrons maintenant que cette topologie est noethérienne. Considérons une chaîne décroissante $(\mathcal{V}_K(R_i))$ de F-fermés de Zariski — où $R_i \subseteq F[\overline{X}]$. Pour tout $i \leqslant j$, on a $\mathcal{V}_K(R_j) \leqslant \mathcal{V}_K(R_i)$ et donc $\mathcal{I}_F(\mathcal{V}_K(R_i)) \subseteq \mathcal{I}_F(\mathcal{V}_K(R_i))$. Par noetherianité de $F[\overline{X}]$, cette chaîne d'idéaux est stationnaire et il existe donc i_0 tel que pour tout $j \geqslant i_0$, on ait $\mathcal{I}_F(\mathcal{V}_K(R_j)) = \mathcal{I}_F(\mathcal{V}_K(R_{i_0}))$, et donc $\mathcal{V}_K(R_j) = \mathcal{V}_K(\mathcal{I}_F(\mathcal{V}_K(R_j))) = \mathcal{V}_K(\mathcal{I}_F(\mathcal{V}_K(R_{i_0}))) = \mathcal{V}_K(R_{i_0})$. □

Cette topologie est appelée la F-topologie de Zariski. On peut facilement vérifier que pour tout $S \subseteq K^{\overline{X}}$, $\mathcal{V}_K(\mathcal{I}_F(S))$ est la clôture de R pour cette topologie. On l'appelle la F-clôture de Zariski de R. On parle aussi du F-locus algébrique de R. La K-topologie de Zariski sur $K^{\overline{X}}$ est simplememt appelée la topologie de Zariski.

2.2 La théorie des modèles des corps algébriquement clos

On note ACF la $\mathbb{Z}$-théorie des corps algébriquement clos. Elle contient :

- L'énoncé $\forall x\, x \not\simeq 0 \to \exists y\, xy - 1 \simeq 0$;
- Pour tout $n \in \mathbb{Z}_{>0}$, l'énoncé $\forall x_0 \dots x_n\, x_n \not\simeq 0 \to \exists y\, \sum_i x_i y^i \simeq 0$.

Lemme 2.4 : *Soit $F, K \vDash$ ACF, $A \leqslant F$, $f : A \to K$ un morphisme d'anneaux injectif et $a \in F$ un élément algébrique sur A — c'est à dire tel qu'il existe $P \in A[X]$ non nul tel que $P(a) = 0$. Alors il existe $g : A[a] \to K$ un morphism d'anneau injectif qui étend f.*

Démonstration. Soit $h : A_{(0)} \to K$ l'unique morphisme d'anneau (injectif) qui étend f et soit $P \in A_{(0)}[X]$ le polynôme minimal (unitaire) de a sur $A_{(0)}$. Comme K est algébriquement clos, il existe $b \in K$ tel que $h(P)(b) = 0$. Rappelons que, puisque a est algébrique sur A et donc sur $A_{(0)}$, P est non nul et irréductible. Il s'ensuit que $h(P)$ est non nul et irréductible et c'est donc le polynôme minimal unitaire de b sur $h(A_{(0)})$. Le morphisme que l'on recherche est donc $g : A_{(0)}[a] \cong A_{(0)}[X]/(P) \cong h(A_{(0)})[X]/(h(P)) \cong h(A_{(0)})[b] \subseteq K$. □

Corollaire 2.5 : *Soit $f : A \to K \vDash$ ACF un morphisme d'anneaux injectif et $A \leqslant C$ une extension algébrique. Il existe alors $g : C \to K$ un morphism d'anneau injectif qui étend f.*

Démonstration. L'ensemble des morphismes injectifs $D \to K$ qui étendent f, où $A \leqslant D \leqslant C$, ordonné par l'extension est un ensemble inductif non vide. Il a donc un élément maximal $g : D \to K$. Par le Lemme **(2.4)**, comme g est maximal, $D = C$. □

Lemme 2.6 : *Soit $F, K \vDash$ ACF, $A \leqslant F$, $f : A \to K$ un morphisme d'anneaux injectif et $a \in F$. Alors il existe $h : K \to K^\star$ un morphisme élémentaire d'anneaux et $g : A[a] \to K^\star$ un morphisme injectif d'anneaux qui étend $h \circ f$.*

Démonstration. Si a est algébrique sur A, on applique le Lemme **(2.4)** avec $K^\star = K$. On peut donc supposer a transcendant sur A. Comme dans le Lemme **(2.4)**, on peut supposer que $A = A_{(0)}$ est un corps. Pour tout nombre fini de $P_i \in A[X] \smallsetminus (0)$, soit $c \in K$ tel que $P_i(c) \neq 0$ pour tout $i \leqslant n$. Un tel c exists puisque que K est infini. Alors c satisfait dans K le K-type

$Th[K](K) \cup \{\neg P_i(x) \simeq 0 : i \leqslant n\}$. On considère alors le K-type partiel $p(x) := \mathrm{Th}_K(K) \cup \{\neg P(x) \simeq 0 : P \in A[X] \setminus (0)\}$, qui est bien finiment satisfaisble.
Soit $K^\star$ une K-algèbre et $c \in K^\star$ une réalisation de p dans $K^\star$. Comme $K^\star \vDash \mathrm{Th}_K(K)$, le morphisme structurel $h : K \to K^\star$ est un morphisme élémentaire de A-algèbres. De plus, comme $K^\star \vDash p(c)$, c est transcendant sur F. Le morphisme que l'on recherche est donc $g : A[a] \cong A[X] \cong f(A)[X] \cong f(A)[c] \subseteq K^\star$. □

Théorème 2.7 (Tarski – Chevalley) **:** *La théorie* ACF *élimine les quantificateurs.*

Démonstration. On applique la Proposition **(1.31)** et le Lemme **(2.6)**. □

Corollaire 2.8 : *Deux corps algébriquement clos K et L sont élémentairement équivalents si et seulement s'ils ont la même caractéristique.*

Démonstration. Deux corps élémentairement équivalents ont la même caractéristique, il suffit de vérifier les énoncés de la forme $p \simeq 0$. Réciproquement, soit $K, L \vDash$ ACF de même caractéristique. Leurs corps premiers sont isomorphes. On a donc $L \vDash \mathrm{ACF}_F$, où F est le corps premier de K. Par élimination des quantificateurs, cette théorie est complète et donc $L \equiv_F K$, en particulier $L \equiv_{\mathbb{Z}} K$. □

Remarque 2.9 :

- L'espace $\mathcal{S}_\varnothing(\mathrm{ACF})$ est le compactifié d'Alexandrov de l'ensemble des nombres premiers muni de la topologie discrète. À chaque nombre premier p on associe ACF_p, la théorie des corps algébriquement clos de caractéristique p. Le point à l'infini est ACF_0, la théorie des corps algébriquement clos de caractéristique nulle.
- la théorie ACF_p est engendrée par $\mathrm{ACF} \cup \{p \simeq 0\}$. La théorie ACF_0 est engendrée par $\mathrm{ACF} \cup \{p \not\simeq 0 : p \text{ premier}\}$.
- En particulier, pour tout énoncé φ, $\mathbb{C} \vDash \varphi$ si et seulement $\varphi \in \mathrm{ACF}_0$, si et seulement s'il existe $P \subseteq \mathbb{P}$ fini tel que $\varphi \in \mathrm{ACF}_p$, pour tout $p \notin P$, si et seulement s'il existe $P \subseteq \mathbb{P}$ fini tel que $\mathbb{F}_p^{\mathrm{a}} \vDash \varphi$. C'est le principe de Lefschetz.

On revient à nos notations précédentes. Soit F un corps et K un corps algébriquement clos contenant F.

Théorème 2.10 (Nullstellensatz, Hilbert) **:** *Pour tout $R \subseteq F[\overline{X}]$, on a $\mathcal{I}_F(\mathcal{V}_K(R)) = \sqrt{R}$.*

On rappelle que $\sqrt{R} := \bigcap_{R \subseteq \mathfrak{p} \text{ premier}} \mathfrak{p}$ est le plus petit idéal radical contenant R.

Démonstration. Comme $\mathcal{I}_F(\mathcal{V}_K(R))$ est un idéal radical, on a $\sqrt{R} \subseteq \mathcal{I}_F(\mathcal{V}_K(R))$. Soit $f \in \mathcal{I}_F(\mathcal{V}_K(R))$ et $R \subseteq \mathfrak{p}$ un idéal premier de $F[\overline{X}]$. On pose $L := F[\overline{X}]/\mathfrak{p}$. Par élimination des quantificateurs dans ACF, il existe des morphismes élémentaires $h : K \to K^\star$ et $g : L \to K^\star$ de F-algèbre.
Rappelons que $F[\overline{X}]$ est noethérien, et donc (R) est engendré par des polynômes $g_i \in F[\overline{X}]$, $i \leqslant n$. Comme $f \in \mathcal{I}_F(\mathcal{V}_K(R)) = \mathcal{I}_F(\mathcal{V}_K((R))) = \mathcal{I}_F(\mathcal{V}_K(\{g_i : i \leqslant n\}))$, on a $K \vDash \forall \overline{x} \bigwedge_i g_i(\overline{x}) \simeq 0 \to f(x) \simeq 0$, donc $K^\star \vDash \forall \overline{x} \bigwedge_i g_i(\overline{x}) \simeq 0 \to f(x) \simeq 0$ et, finalement, $L \vDash \forall \overline{x} \bigwedge_i g_i(\overline{x}) \to f(x)$. En particulier, comme $g_i \in (R) \subseteq \mathfrak{p}$, pour tout $i \leqslant n$, il s'ensuit que $L \vDash f(\overline{X}) \simeq 0$ et ainsi $f \in \mathfrak{p}$. On a donc bien $\mathcal{I}_F(\mathcal{V}_K(R)) \subseteq \bigcap_{R \subseteq \mathfrak{p} \text{ premier}} \mathfrak{p} = \sqrt{R}$. □

Corollaire 2.11 (Nullstellensatz faible, Hilbert) **:** *Pour tout $R \subseteq F[\overline{X}]$, si $\mathcal{V}_K(R) = \varnothing$ alors* $1 \in (R)$.

Démonstration. Si $\mathcal{V}_K(R) = \varnothing$, par le nullstellensatz, on a $\sqrt{R} = \mathcal{I}_F(\mathcal{V}_K(R)) = (1)$. D'où $1 \in \sqrt{R}$ et il existe donc $n \in \mathbb{Z}_{>0}$ tel que $1 = 1^n \in (R)$. □

Corollaire 2.12 : *L'espace $K^{\overline{X}}$ muni de la topologie de Zariski est quasi-compact.*

Comme on le verra plus tard, La compacité de la topologie de Zariski peut aussi être vue comme une conséquence de la compacité de la topologie de Stone sur l'espace des types dans ACF.

Démonstration. Soit $\mathcal{V}_K(R_i)$ une famille de F-fermés de Zariski telle que $\mathcal{V}_K(\bigcup_i R_i) = \bigcap_i \mathcal{V}_K(R_i) = \varnothing$. Par le Nullstelensatz failble, $1 \in (\bigcup_i R_i)$. Il existe donc $I_0 \subseteq I$ fini et $f_i \in (R_i)$ pour tout $i \in I_0$ tel que $1 = \sum_i f_i$. On a alors que $\bigcap_{i \in I_0} \mathcal{V}_K(R_i) = \mathcal{V}_K(\bigcup_{i \in I_0} R_i) = \varnothing$. □

La topologie de Zariski n'est, en général, pas séparée.

Corollaire 2.13 : *Les idéaux maximaux de $K[X_1, \ldots, X_n]$ sont exactement ceux de la forme $(X_1 - x_1, \ldots, X_n - x_n)$ avec $x_i \in K$.*

Démonstration. Soit $\mathfrak{m} \subseteq K[X_1, \ldots, X_n]$ un idéal maximal. Comme $1 \notin \mathfrak{m}$, par le nullstellensatz faible, il existe $\overline{x} \in \mathcal{V}_K(\mathfrak{m})$. On a donc $\mathfrak{m} \subseteq \mathcal{I}_K(\mathcal{V}_K(\mathfrak{m})) \subseteq \mathcal{I}_K(\overline{x}) \supseteq (X_1 - x_1, \ldots, X_n - x_n)$. Mais ce dernier idéal est le noyau du morphisme surjectif $K[\overline{X}] \to K$ qui envoie X_i sur x_i, c'est donc un idéal maximal. Il s'ensuit que $\mathfrak{m} = \mathcal{I}_K(\overline{x}) = (X_1 - x_1, \ldots, X_n - x_n)$. □

2.3 Les fermés intègres

Définition 2.14 (Intégrité) **:** *Soit $V \subseteq K^{\overline{X}}$ un F-fermé de Zariski. On dit que V est dit F-intègre si ce n'est pas l'union de deux F-fermés propres de Zariski.*

La proposition suivante est une conséquence facile de la noethérianité :

Proposition 2.15 : *Soit V un F-fermé de Zariski de $K^{\overline{X}}$. Alors il existe $V_i \subseteq V$, $i \leqslant n$, des F-fermés F-intègres de Zariski tels que $V = \bigcup_i V_i$. De plus, on peut supposer que pour tout i, j, $V_i \subseteq V_j$ implique $i = j$. On a alors unicité des V_i à permutation près.*

Démonstration. On construit par induction un arbre de F-fermés de Zariski $W_\varepsilon \subseteq V$, $\varepsilon \in 2^{(\omega)}$ tels que, pour tout ε $W_\varepsilon = W_{\varepsilon 0} \cup W_{\varepsilon 1}$ et si W_ε n'est pas F-intègre, $W_{\varepsilon i} \subset W_\varepsilon$. Comme la topologie de Zariski est noethérienne, pour tout $\varepsilon \in 2^\omega$, la suite décroissante $V_{\varepsilon|_i}$ est stationnaire égale à un certain F-fermé de Zariski, que l'on nomme V_ε. Par construction, V_ε est F-intègre. Par le lemme de Koenig, $\{V_\varepsilon : \varepsilon \in 2^\omega\}$ est fini et on a bien $V = \bigcup_\varepsilon V_\varepsilon$.
On a donc montré qu'il existe $V_i \subseteq V$, $i \leqslant n$, des F-fermés F-intègres de Zariski tels que $V = \bigcup_i V_i$. Si on choisit n minimal, on a bien $V_i \subseteq V_j$ implique $i = j$. Soit alors $W \subseteq V$ un F-fermé F-intègre de Zariski. Il est alors couvert par les fermés $W \cap V_i$. Il existe donc i tel que $W = W \cap V_i$ et donc $W \subseteq V_i$. Soit alors $V = \bigcup_j W_j$ un autre recouvrement fini de V par des F-fermés F-intègres de Zariski. Pour tout i, on trouve alors un j tel que $V_i \subseteq W_j$ et, donc, un i' tel que $V_i \subseteq W_j \subseteq V_{i'}$. Par minimalité, $i = i'$ et donc $W_j = V_i$. Ceci prouve l'unicité à permutation près.
□

Lemme 2.16 : *Soit $V \subseteq K^{\overline{X}}$ un F-fermé de Zariski. L'ensemble V est F-intègre si et seulement si $\mathcal{I}_F(V) \subseteq F[\overline{X}]$ est premier.*

Démonstration. Supposons que V est F-intègre. Et soient $f_i \in F[\overline{X}]$ tels que $f_1 f_2 \in \mathfrak{p} := \mathcal{I}_F(V)$. On a $\mathcal{V}_K(\mathfrak{p}, f_i) \subseteq \mathcal{V}_K(\mathfrak{p}) = V$. De plus, pour tout $\overline{x} \in V$, on a $f_1 f_2(\overline{x}) = 0$ et donc il existe i tel que $f_i(\overline{x}) = 0$, c'est-à dire $\overline{x} \in \mathcal{V}_K(\mathfrak{p}, f_i)$. Puisque V est F-intègre, il existe i tel que $V \subseteq \mathcal{V}_K(\mathfrak{p}, f_i)$ et donc tel que $f_i \in \mathcal{I}_F(\mathcal{V}_K(\mathfrak{p}, f_i)) \subseteq \mathcal{I}_F(V) = \mathfrak{p}$.
Réciproquement, supposons que $\mathfrak{p}$ est premier. Soit $\mathcal{V}_K(R_i) \subset V$ deux fermés. Comme $\mathfrak{p} \subset (R_i)$, soit $f_i \in R_i \setminus \mathfrak{p}$. Comme $f_1 f_2(\overline{x}) = 0$ pour tout $\overline{x} \in V$, on a $f_1 f_2 \in \mathfrak{p}$ et donc il existe i tel que $f_i \in \mathfrak{p}$, une contradiction. □

Remarque 2.17 :

- On définit $\mathrm{Spec}(F[\overline{X}]) := \{\mathfrak{p} \subset F[\overline{X}] : \mathfrak{p} \text{ premier}\}$. On munit $\mathrm{Spec}(F[\overline{X}])$ de la topologie de Zariski dont les fermés sont de la forme $\mathcal{V}(R) := \{\mathfrak{p} : R \subseteq \mathfrak{p}\}$, où $R \subseteq F[\overline{X}]$. On peut vérifier que cette topologie est noethérienne quasi-compacte.
- Il existe une bijection continue $\mathcal{S}_{\overline{X}}(F) := \mathcal{S}_{\overline{X}}(\mathrm{Th}_F^{\mathrm{qf}}(K)) = \mathcal{S}_{\overline{X}}(\mathrm{ACF}_F^{\mathrm{qf}}) \to \mathrm{Spec}(F[\overline{X}])$ qui à tout type complet $p \in \mathcal{S}_{\overline{X}}(F)$ associe $\mathcal{I}(p) := \{P \in F[\overline{X}] : P \simeq 0 \in p\}$. Ce n'est pas un homéomorphisme.
- L'image par cette fonction d'un ouvert-fermé de $\mathcal{S}_{\overline{X}}(F)$ est une combinaison booléenne de fermés de Zariski. On dit que la topologie de Stone est la topologie constructible associée à la topologie de Zariski.
- On note $\mathcal{S}_{\overline{X}}^{\mathrm{Zar}}(F)$ l'ensemble $\mathcal{S}_{\overline{X}}(F)$ muni de la topologie induite par la bijection avec $\mathrm{Spec}(F[\overline{X}])$ muni de la topologie de Zariski. Les fermés de $\mathcal{S}_{\overline{X}}^{\mathrm{Zar}}(F)$ sont exactement ceux de la forme $\mathcal{V}(R) := [\{P \simeq 0 : P \in R\}]$.

Remarque 2.18 : Soit $V \subseteq K^{\overline{X}}$ un F-fermé de Zariski et $\overline{x} \in V$. On a alors :

- $\mathcal{V}_K(\mathcal{I}_F(\overline{x})) \subseteq V$;
- $\mathcal{I}_F(V) \subseteq \mathcal{I}_F(\overline{x})$;
- un morphisme surjectif de F-algèbres $F[\overline{X}]/\mathcal{I}_F(V) \to F[\overline{x}] = F[\overline{X}]/\mathcal{I}_F(\overline{x})$.

Définition 2.19 : *Soit V un F-fermé de Zariski.*

- *L'anneau $F[V] := F[\overline{X}]/\mathcal{I}_F(V)$ est appelé l'anneau de fonctions régulières de V.*
- *Si V est F-intègre, $F[V]$ est intègre et son corps des fractions $F(V) := F[V]_{(0)}$ est appelé le corps de fonctions rationnelles de V.*

Lemme 2.20 : *Soit $V \subseteq K^{\overline{x}}$ un F-fermé de Zariski et $\overline{x} \in V$. Sont équivalents :*

1. *$\mathcal{V}_K(\mathcal{I}_F(\overline{x})) = V$, c'est à dire que $\overline{x}$ est F-dense dans V ;*
2. *$\mathcal{I}_F(\overline{x}) = \mathcal{I}_F(V)$;*
3. *Le morphisme naturel $F[V] \to F[\overline{x}] \subseteq K$ est un isomorphisme.*

Démonstration. Supposons que $\mathcal{V}_K(\mathcal{I}_F(\overline{x})) = V$, on a alors $\mathcal{I}_F(\overline{x}) = \mathcal{I}_F(\mathcal{V}_K(\mathcal{I}_F(\overline{x}))) = \mathcal{I}_F(V)$. Réciproquement, si $\mathcal{I}_F(\overline{x}) = \mathcal{I}_F(V)$, $\mathcal{V}_F(\mathcal{I}_F(\overline{x})) = \mathcal{V}_F(\mathcal{I}_F(V)) = V$m ce qui prouve l'équivalence de 1 et 2. Puisque le noyau du morphisme surjectif $F[V] \to F[\overline{x}] \subseteq K$ est $\mathcal{I}_F(V)/\mathcal{I}_F(\overline{x})$, on a aussi équivalence entre le 2 et le 3. □

Définition 2.21 (Point générique) **:** *Un uplet $\overline{x} \in K^{\overline{X}}$ vérifiant les conditions équivalentes du Lemme* ***(2.20)*** *est dit F-générique dans V.*

On suppose maintenant que K est de degré de transcendance infini sur F.

Lemme 2.22 : *Soit $V \subseteq K^{\overline{X}}$ un F-fermé de Zariski. Sont équivalents :*

1. *V est F-intègre ;*
2. *Il existe $\overline{x} \in K$ F-générique dans V.*

Démonstration. Supposons que V est F-intègre et soit $\mathfrak{p} := \mathcal{I}_F(V)$. C'est un idéal premier. Soit $L := F[\overline{X}]/\mathfrak{p}$. Le degré de transcendance de L sur F est borné par $|\overline{X}|$ et donc il existe un morphisme injectif de F-algèbres $f : L \to K$. Soit $\overline{x} = f(\overline{X}) \in K^{\overline{X}}$. Pour tout $P \in F[\overline{X}]$, on a $P(\overline{x}) = 0$ si et seulement si $P \in \mathfrak{p}$ et donc $\mathcal{I}_F(\overline{x}) = \mathfrak{p}$.
Réciproquement, soit $\overline{x} \in K$ tel que $V = \mathcal{V}_K(\mathcal{I}_F(\overline{x}))$ et soient $V_i \subseteq V$ deux F-fermés de Zariski qui couvrent V. Comme $\overline{x} \in V$, il existe i tel que $\overline{x} \in V_i$. On a donc $V = \mathcal{V}_K(\mathcal{I}_F(\overline{x})) \subseteq \mathcal{V}_K(\mathcal{I}_F(V_i)) = V_i$. □

Remarque 2.23 :

- La fonction $\mathcal{I}_F : K^{\overline{X}} \to \mathcal{S}^{\mathrm{Zar}}_{\overline{X}}(F)$ qui a tout $\overline{x} \in K^{\overline{x}}$ associe $\mathrm{tp}^K_F(\overline{x})$ est une surjection continue. De plus la F-topologie de Zariski est la topologie la moins fine telle que cette fonction soit continue.
- Si $\overline{x}$ et $\overline{y}$ sont F-génériques dans V alors $\mathrm{tp}^K_F(\overline{x}) = \mathrm{tp}^K_F(\overline{y})$.

On fixe $F \leqslant E \leqslant K$ un corps intermédiaire. On suppose que K est de degré de transcendance infini sur E.

Remarque 2.24 : Soit $V \subseteq K^{\overline{X}}$ un F-fermé de Zariski. Alors V est aussi un E-fermé de Zariski. Cependant, même si V est F-intègre, il se peut que V ne soit pas E-intègre.

Soit $L \vDash \mathrm{ACF}$ contenant K.

Remarque 2.25 :

- À tout $V \subseteq K^{\overline{X}}$ F-fermé de Zariski, on associe $V_L = \mathcal{V}_L(\mathcal{I}_F(V))$. On a $V_L \cap K^{\overline{x}} = V$, $\mathcal{I}_F(V_L) = \mathcal{I}_F(V)$.
- Réciproquement, à tout $V \subseteq L^{\overline{X}}$ F-fermé de Zariski, on associe $V_K = V \cap K^{\overline{X}} = \mathcal{V}_K(\mathcal{I}_F(V))$. On a $\mathcal{I}_F(V_K) = \mathcal{I}_F(V)$ et $(V_K)_L = V$.
- De même, pour tout $V \subseteq K^{\overline{X}}$, $(V_L)_K = V$

Lemme 2.26 : *Soit $V \subseteq K^{\overline{X}}$ un F-fermé de Zariski. Sont équivalents :*

1. *V_L est F-intègre ;*
2. *V est F-intègre ;*

Démonstration. Ces énoncés sont équivalents au fait que $\mathcal{I}_F(V) = \mathcal{I}_F(V_L)$ est premier. □

Lemme 2.27 : *Soit $V \subseteq K^{\overline{X}}$ un fermé de Zariski. Sont équivalents :*

1. *V_L est L-intègre ;*
2. *V_L est K-intègre ;*
3. *V est K-intègre.*

Démonstration.

1⇒2 Évident.

2 ⇒3 *cf.* Lemme **(2.26)**.

3⇒1 Soient $f_i \in K[\overline{X}]$ un ensemble fini de générateurs de $\mathcal{I}_K(V)$. Puisque V est K-intègre, $\mathcal{I}_K(V)$ est premier et donc pour tout $n \in \mathbb{Z}_{>0}$, $K \vDash \varphi_n := \forall \overline{y}\overline{z}\, (\forall \overline{x} \bigwedge f_i(\overline{x}) = 0 \to$

$(\sum_{|I|\leqslant n} y_I \overline{x}^I)(\sum_{|I|\leqslant n} z_I \overline{x}^I) = 0) \to ((\forall \overline{x} \bigwedge f_i(\overline{x}) = 0 \to \sum_{|I|\leqslant n} y_I \overline{x}^I = 0) \vee (\forall \overline{x} \bigwedge f_i(\overline{x}) = 0 \to \sum_{|I|\leqslant n} z_I \overline{x}^I = 0))$. Comme ACF élimine les quantificateurs, on a aussi $L \vDash \varphi_n$ et donc $L\mathcal{I}_K(V)$ est premier. Il est donc égal à $\mathcal{I}_L(V_L)$ et V_L est -intègre.

□

Remarque 2.28 : On vient de montrer que l'irréductibilité du locus algébrique d'un nombre fini borné de polynômes de degré borné peut s'exprimer comme la conjonction d'un nombre dénombrable de formule sur les coefficients de ces polynômes — un type partiel en les coefficients des polynômes. On verra plus tard qu'elle peut en fait s'exprimer par une unique formule en les coefficients des polynômes.

2.4 Disjonction linéaire

Soient C un F-algèbre $A, B \leqslant C$ deux sous-F-algèbres.

Définition 2.29 (Disjonction linéaire) **:** *On dit que A est linéairement disjointe de B sur F si tout $\overline{a} \in A$ linéairement indépendant sur F reste linéairement indépendant sur B. On le note $A \downarrow^{\mathrm{lin}}_F B$.*

Remarque 2.30 : Par définition, $A \downarrow^{\mathrm{lin}}_F B$ si et seulement si $A_0 \downarrow^{\mathrm{lin}}_F B_0$ pour toutes sous-F-algèbres de type fini $A_0 \leqslant A$ et $B_0 \leqslant B$.

On rappelle que la fonction F-bilinéaire $A \times B \to A \otimes_F B$ qui a (a, b) associe $a \otimes_F b$ a la propriété universelle suivante : pour tout morphisme F-bilinéaire $A \times B \to C$, où C est une F-algèbre, il existe un unique morphisme de F-algèbres $g : A \otimes_F B$ tel que $f(a, b) = g(a \otimes_F b)$. Ceci définit (à unique isomorphisme près) la paire $A \otimes_F B, \otimes_F : A \times B \to A \otimes_F B$.

Proposition 2.31 : *Sont équivalents :*

1. *$A \downarrow^{\mathrm{lin}}_F B$;*
2. *le morphisme naturel $A \otimes_F B \to C$ est injectif.*

Démonstration. Le noyau du morphisme $A \otimes_F B \to K$ est constitué exactement des éléments $\sum_i a_i \otimes b_i$ avec $a_i \in A$, linéairement indépendants sur F, et $b_i \in B$ tels que $\sum_i a_i b_i = 0$. Le morphisme $A \otimes_F B \to C$ est donc injectif si et seulement si, pour tous $a_i \in A$, linéairement indépendants sur F et $b_i \in B$ tels que $\sum_i a_i b_i = 0$, $\sum_i a_i \otimes b_i = 0$. Ce qui est équivalent au fait que $b_i = 0$ pour tout i puisque $(\bigoplus_i F a_i) \otimes_F B \cong \bigoplus_i (F a_i \otimes_F B)$. Ceci conclut la preuve. □

En combinant la Proposition **(2.31)** avec les propriétés du produit tensoriel, on obtient :

Lemme 2.32 :

- *$A \downarrow^{\mathrm{lin}}_F B$ si et seulement si $B \downarrow^{\mathrm{lin}}_F A$.*
- *Si $F \leqslant E \leqslant A$ est un corps, $A \downarrow^{\mathrm{lin}}_F B$ si et seulement si $E \downarrow^{\mathrm{lin}}_F B$ et $A \downarrow^{\mathrm{lin}}_F EB$.*
- *Soit a_i une base de A sur F, $A \downarrow^{\mathrm{lin}}_F B$ si et seulement si a_i est aussi libre sur B.*
- *Supposons que C est un corps, alors $A \downarrow^{\mathrm{lin}}_F B$ si et seulement si $A \downarrow^{\mathrm{lin}}_F B_{(0)}$.*

Démonstration. Les trois premiers points sont des conséquences de la commutativité des diagrammes suivants :

$$
\begin{tikzcd}
A \otimes_F B \arrow[r] \arrow[d, leftrightarrow] & C \\
B \otimes_F A \arrow[ur] &
\end{tikzcd}
\qquad
\begin{tikzcd}
A \otimes_E (E \otimes_F B) \arrow[r] \arrow[d, leftrightarrow] & A \otimes_E EB \arrow[d] \\
A \otimes_F B \arrow[r] & C
\end{tikzcd}
\qquad
\begin{tikzcd}
\bigoplus_i (Fa_i \otimes B) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \bigoplus Ba_i \arrow[d] \\
A \otimes_F B \arrow[r] & C
\end{tikzcd}
$$

Le commutativité du premier diagramme est une conséquence de la commutativité du produit, celle du deuxième suit de son associativité et celle du troisième de la distributivité. Pour ce qui est de la dernière équivalence, soit $a_i \in A$ de éléments linéairement indépendants sur F et $b_i \in B_{(0)}$ tels que $\sum_i a_i b_i = 0$. Il existe $b \in B \setminus \{0\}$ tel que, pour tout i, $bb_i \in B$. On a alors $b(\sum_i a_i b_i) = \sum_i a_i bb_i = 0$ et donc, comme $A \mathop{\downarrow}^{\mathrm{lin}}_{F} B$, $bb_i = 0$ pour tout i, d'où $b_i = 0$. □

Définition 2.33 : *Soit F un corps.*
- *F est parfait si $F = F^p := \{a^p : a \in F\}$, où p est la caractéristique de F si elle est positive et 1 sinon.*
- *La clôture parfaite de F, notée $F^{p^{-\infty}}$, est la plus petite extension parfaite de F.*

Définition 2.34 : *Soit L une F-algèbre intègre. On dit que*
- *L est régulière si $L \mathop{\downarrow}^{\mathrm{lin}}_{F} F^{\mathrm{a}}$;*
- *L est séparable si $L \mathop{\downarrow}_{F} F^{p^{-\infty}}$.*

On rappelle qu'une extension algébrique $F \leqslant L$ est normale si pour tout $a \in L$, le polynôme minimal de a sur F se décompose en facteurs linéaires sur L. L'extension $F \leqslant L$ est galoisienne si elle est séparable et normale. Toute extension algébrique $F \leqslant L$ contient une sous extension séparable maximale L_s. Si $F \leqslant L$ est une extension normale, $F \leqslant L_s$ est une extension galoisienne. On note $L_i = L \cap F^{p^{-\infty}}$, on a alors $L_s \mathop{\downarrow}^{\mathrm{lin}}_{F} L_i$ et $L = L_s L_i$. On note F^{s} la sous extension maximale séparable de F^{a}. On a $F^{\mathrm{a}} = F^{\mathrm{s}} F^{p^{-\infty}}$ et $F^{\mathrm{s}} \mathop{\downarrow}^{\mathrm{lin}}_{F} F^{p^{-\infty}}$.

Lemme 2.35 : *Soit $L \leqslant K$ une extension normale de K et H_1, H_2 deux sous-F-algèbres isomorphes de K. On a alors :*

$$H_1 \mathop{\downarrow}^{\mathrm{lin}}_{F} L \text{ si et seulement si } H_2 \mathop{\downarrow}^{\mathrm{lin}}_{F} L.$$

Démonstration. Supposons que $H_1 \mathop{\downarrow}^{\mathrm{lin}}_{F} L$. Par élimination des quantificateurs, l'injection $f : H_2 \to K$ induite par l'isomorphisme est K-élémentaire. Soient $x_i \in H_2$ des éléments linéairement indépendants sur F. Comme f est un morphisme injectif de f-algèbre, les $f(x_i)$ sont aussi linéairement indépendants sur F, et donc sur L. Soient $e_i \in L$ tels que $\sum_i e_i x_i = 0$. On note $g_i \in F[\overline{X}]$ le polynôme minimal de e_i sur F. On a alors $K \models \varphi(\overline{x}) := \exists \overline{e} \bigwedge_i g_i(e_i) = 0 \wedge \sum_i e_i x_i = 0$ et donc $K \models \varphi(f(\overline{x}))$. Comme L est normal, toutes les racines des g_i sont dans L et donc, pour tout i, $e_i = 0$. □

On remarque que le Lemme **(2.35)** implique que les notions d'extension régulière et d'extension séparable ne dépendent pas d'un choix de plongement.

Proposition 2.36 : *Soit $L, H \subseteq K$ deux sous-corps contenant F et supposons que L est une extension galoisienne de F. On a alors :*

$$H \mathop{\downarrow}^{\mathrm{lin}}_{F} L \text{ si et seulement si } H \cap L = F.$$

Démonstration. Supposons que $H \downarrow^{\text{lin}}_F L$, alors si $x \in H \cap L$, on a $x - x \cdot 1 = 0$ donc la famille $(x, 1)$ de points de H n'est pas linéairement indépendant sur L, il s'ensuit qu'elle n'est pas linéairement indépendante sur F non plus, et donc $x \in F \cdot 1 = F$. Réciproquement, si $H \cap L = F$, pour montrer que $H \downarrow^{\text{lin}}_F L$, il suffit de montrer que $H \downarrow^{\text{lin}}_F L_0$ pour toute sous$F$-algèbre de type fini $L_0 \leqslant L$. On peut donc supposer que L est une extension finie galoisienne de F, et donc, par le théorème de l'élément primitif, que $L = F[a]$. Soit $P \in F[X]$ le polynôme minimal de a sur F et $Q \in H[x]$ son polynôme minimal sur H. Les racines de Q sont toutes dans L, puisque ce sont aussi des racines de P. Les coefficients de Q sont donc dans $H \cap L = F$. D'où $Q = P$ et les puissances de a de degré strictement inférieur à $\deg(P)$ restent libres sur H. Il s'ensuit que $L \downarrow^{\text{lin}}_F H$ et donc $H \downarrow^{\text{lin}}_F L$. □

Corollaire 2.37 : *Soit $F \leqslant L$ une extension de corps. Si F est parfait, sont équivalents :*

1. *l'extension $F \leqslant L$ est régulière ;*
2. *$L \cap F^{\mathrm{a}} = F$.*

Démonstration. On applique la Proposition **(2.36)** a l'extension galoisienne $F \leqslant F^{\mathrm{s}} = F^{\mathrm{a}}$. □

2.5 Variétés

Définition 2.38 : *Un idéal $I \subseteq E[\overline{X}]$ est défini sur F si $I = E(I \cap F[\overline{X}])$.*

Proposition 2.39 : *Soient $\overline{x} \in K^{\overline{X}}$ et $\mathfrak{p} = \mathcal{I}_E(\overline{x}) \subseteq E[\overline{X}]$. Sont équivalents :*

1. *$\mathfrak{p}$ est défini sur F ;*
2. *$F(\overline{x}) \downarrow^{\text{lin}}_F E$.*

Démonstration. Supposons tout d'abord que $\mathfrak{p}$ est défini sur F. Notons qu'il suffit de montrer que $F[\overline{x}] \downarrow^{\text{lin}}_F E$. Soient $f_i \in F[\overline{X}]$ tels que les $f_i(\overline{x}) \in F[\overline{x}]$ sont linéairement indépendants sur F et $g_j \in \mathcal{I}_F(\overline{x})$ qui sont linéairement indépendants sur F. S'il existe $c_i, d_j \in F$, presque partout 0, tels que $\sum_i c_i f_i = \sum_j d_j g_j$, on a $\sum_i c_i f_i(x) = \sum_j d_j g_j(x) = 0$ et donc $c_i = 0$, pour tout i. Il s'ensuit que $\sum_j d_j g_j = 0$ et donc $d_j = 0$, pour tout j. Puisque $F[\overline{X}] \downarrow^{\text{lin}}_F E$, dans $E[X]$, les f_i et g_j restent indépendants sur E.

Supposons maintenant qu'on a des $c_i \in E$ presque partout 0 tels que $\sum_i c_i f_i(x) = 0$. On a donc $\sum_i c_i f_i \in \mathcal{I}_E(\overline{x}) = \mathfrak{p} = E(\mathfrak{p} \cap F[\overline{X}])$. On peut donc trouver un nombre fini de $g_j \in \mathfrak{p} \cap F[\overline{X}]$, linéairement indépendants sur F, et des $d_j \in E$, presque partout 0, tels que $\sum_i c_i f_i = \sum_j d_j g_j$. Par indépendance linéaire sur E, on a alors $c_i = 0$ pour tout i.

Réciproquement, supposons que $F(\overline{x}) \downarrow^{\text{lin}}_F E$. Soit $f \in \mathfrak{p}$. On peut écrire $f = \sum_i e_i g_i$ où $e_i \in E$ sont linéairement indépendants sur F et $g_i \in F[\overline{X}]$. On a alors $\sum_i e_i g_i(x) = f(\overline{x}) = 0$. Comme $E \downarrow^{\text{lin}}_F F[\overline{x}]$, les $e_i \in E$ sont linéairement indépendants sur $F(\overline{x})$ et donc $g_i(x) = 0$, pour tout i, c'est-à dire $g_i \in \mathcal{I}_F(\overline{x}) = \mathfrak{p} \cap F[\overline{X}]$. On a donc bien que $\mathfrak{p} = E(\mathfrak{p} \cap F[\overline{X}])$ est défini sur F. □

Corollaire 2.40 : *Soit $V \subseteq K^{\overline{X}}$ un F-fermé F-intègre de Zariski. Sont équivalents :*

1. *V est E-intègre et $\mathcal{I}_E(V)$ est défini sur F ;*
2. *il existe un point F-générique $\overline{x}$ de V tel que $F(\overline{x}) \downarrow^{\text{lin}}_F E$.*

Démonstration. Supposons que V est E-intègre et $\mathcal{I}_E(V)$ est défini sur F et soir $\overline{x}$ générique sur E. Comme $\mathcal{I}_E(V) = \mathcal{I}_E(\overline{x})$ est défini sur F, par la Proposition **(2.39)**, $F(\overline{x}) \downarrow^{\text{lin}}_F E$. Réciproquement, soit $\overline{x}$ un point F-générique $\overline{x}$ de V tel que $F(\overline{x}) \downarrow^{\text{lin}}_F E$. Par la Proposition **(2.39)**,

$\mathcal{I}_E(V) \subseteq \mathcal{I}_E(\overline{x}) = E\mathcal{I}_F(\overline{x}) = E\mathcal{I}_F(V) \subseteq \mathcal{I}_E(V)$. D'où $\mathcal{I}_E(V)$ est premier défini sur F. En particulier, V est E-intègre. □

Proposition 2.41 : *Soit $V \subseteq K^{\overline{X}}$ un F-fermé F-intègre de Zariski. Sont équivalents :*

1. *V est K-intègre et $\mathcal{I}_K(V)$ est défini sur F ;*
2. *il existe un point F-générique $\overline{x}$ de V tel que $F(\overline{x}) \downarrow^{\mathrm{lin}}_F F^{\mathrm{a}}$;*
3. *pour tout point F-générique $\overline{x}$ de V, $F(\overline{x}) \downarrow^{\mathrm{lin}}_F F^{\mathrm{a}}$.*

Démonstration. Puisque V est K-intègre si et seulement si il est F^{a}-intègre, l'équivalence de 1 et 2 est un conséquence, étant donné $L \vDash \mathrm{ACF}$ contenant K et $\overline{x}$ K-générique dans V_L, de l'équivalence entre $F(\overline{x}) \downarrow^{\mathrm{lin}}_F F^{\mathrm{a}}$ et $F(\overline{x}) \downarrow^{\mathrm{lin}}_F K$. Supposons, $F(\overline{x}) \downarrow^{\mathrm{lin}}_F F^{\mathrm{a}}$. Soient $f_i \in F[\overline{X}]$ une famille finie de générateurs de $\mathcal{I}_F(V)$ et $g_j \in F[\overline{X}]$ de polynômes tels que les $g_j(\overline{x})$ soient linéairement indépendants sur F. On a $F^{\mathrm{a}} \vDash \forall e_j\, (\forall \overline{x} \bigwedge_i f_i(\overline{x}) \to \sum_j e_j g_j(\overline{x}) = 0) \to \bigwedge_j e_j = 0$ et cette même formule est donc vraie dans K. On a donc $F(\overline{x}) \downarrow^{\mathrm{lin}}_F K$. L'implication réciproque est évidente.
L'équivalence entre 2 et 3 est une conséquence du Lemme **(2.35)**. □

Définition 2.42 : *Une F-variété affine est un fermé de $\mathcal{S}^{\mathrm{Zar}}_{\overline{X}}(F)$, pour un certain $\overline{X}$.*

Remarque 2.43 : Soit $V \subseteq \mathcal{S}^{\mathrm{Zar}}_{\overline{X}}(F)$ une F-variété affine et E un corps contenant F. On définit :

- $V_E := \{p \in \mathcal{S}^{\mathrm{Zar}}_{\overline{X}}(E) : p \cap \mathcal{F}_F(\overline{X}) \in V\}$;
- $\mathcal{I}_E(V) := \{f \in E[\overline{X}] :$ pour tout $p \in V_E$, $f \simeq 0 \in p\} = \bigcap_{p \in V_E} \mathcal{I}(p)$;
- $V(E) := \{\overline{x} \in E^{\overline{X}} : \mathrm{qftp}_F(\overline{x}) \in V\} = V_E(E) = \mathcal{V}_E(\mathcal{I}_E(V)) = \mathcal{V}_E(\mathcal{I}_F(V))$, l'ensemble des points E-rationels de V ;
- $E[V] := E[\overline{X}]/\mathcal{I}_E(V)$;
- si $\mathcal{I}_E(V)$ est premier, on note $E(V) := E[V]_{(0)}$

Définition 2.44 : *On dit qu'une F-variété affine $V \subseteq \mathcal{S}^{\mathrm{Zar}}_{\overline{X}}(F)$ est géométriquement intègre définie sur F si pour tout corps E contenant F, $E\mathcal{I}_F(V) \subseteq E[\overline{X}]$ est premier.*

Proposition 2.45 : *Soit $V \subseteq \mathcal{S}^{\mathrm{Zar}}_{\overline{X}}(F)$ une F-variété affine. Sont équivalents :*

1. *V est géométriquement intègre définie sur F ;*
2. *pour tout $K \vDash \mathrm{ACF}^{\mathrm{qf}}_F$, $V(K) \subseteq K^{\overline{X}}$ est K-intègre et $\mathcal{I}_K(V)$ est défini sur F ;*
3. *il existe $K \vDash \mathrm{ACF}^{\mathrm{qf}}_F$, $V(K) \subseteq K^{\overline{X}}$ est K-intègre et $\mathcal{I}_K(V)$ est défini sur F ;*
4. *$F[V]$ est une F-algèbre intègre régulière.*

Démonstration. Supposons tout d'abord que V est géométriquement intègre définie sur F. Alors, pour tout $K \vDash \mathrm{ACF}^{\mathrm{qf}}_F$, $\mathcal{I}_K(V(K)) = \mathcal{I}_K(V) = \sqrt[K]{\mathcal{I}_F(V)} = K\mathcal{I}_F(V)$ est premier et défini sur F. Par le Lemme **(2.16)**, $V(K)$ est K-intègre. On a donc que 1 implique 2, qui implique trivialement 3. Si $V(K)$ est F-intègre, Comme $F[V]$ est isomorphe au dessus de F à la F-algèbre engendrée par un élément F-générique de $V(K)$, il découle de la Proposition **(2.41)** que 3 implique 4. Enfin, supposons que $F[V]$ est une F-algèbre intègre régulière. Soit $F \leqslant E \leqslant K \vDash \mathrm{ACF}$ une tour d'extension. Par la Proposition **(2.41)**, $V(K)$ est K-intègre défini sur F et donc $\mathcal{I}_K(V(K)) = K\mathcal{I}_F(V)$ est premier. Il s'ensuit que $E\mathcal{I}_F(V) = (K\mathcal{I}_F(V)) \cap E[\overline{X}]$ est aussi premier. □

Remarque 2.46 : Cette dernière égalité n'est pas entièrement triviale. Mais pour tout $I \subseteq E[\overline{X}]$, on a $KI \cap E = I$. En effet, soit f_i ne base de I sur E que l'on complète en une base g_i de $E[\overline{X}]$ sur E. Alors les g_i forment aussi une base de $K[\overline{X}]$ sur K. En écrivant un élément de $KI \cap E[\overline{X}]$ dans cette base, on voit qu'il doit être une combinaison E-linéaire des f_i, c'est-à-dire un élément de I.
On verra plus tard que ce résultat est lié au fait que le $E[\overline{X}]$-module $K[\overline{X}]$ est fidèlement plat.

2.6 Disjonction algébrique

Définition 2.47 : *Soient $F \leqslant L, H \leqslant K$ des corps. On dit que L est algébriquement disjoint de H sur F, et on écrit $L \downarrow^{\mathrm{alg}}_F H$ si pour tout uplet $\overline{a} \in L$, $\mathrm{trdeg}_H(\overline{a}) = \mathrm{trdeg}_F(\overline{a})$.*

Lemme 2.48 : *Soient $F \leqslant L, H \leqslant K$ des corps.*

- *$L \downarrow^{\mathrm{alg}}_F H$ si et seulement si $H \downarrow^{\mathrm{alg}}_F L$.*
- *Si $L \downarrow^{\mathrm{lin}}_F H$ alors $L \downarrow^{\mathrm{alg}}_F H$.*

Démonstration.

- Supposons que $L \downarrow^{\mathrm{alg}}_F H$ et soit $\overline{c} \in H$ un uplet. Pour tout uplet $\overline{a} \in L$, on a $\mathrm{trdeg}_{F(\overline{c})}(\overline{a}) = \mathrm{trdeg}_F(\overline{a})$. On a alors $\mathrm{trdeg}_F(\overline{c}) + \mathrm{trdeg}_{F(\overline{c})}(\overline{a}) = \mathrm{trdeg}_F(\overline{ac}) = \mathrm{trdeg}_F(\overline{a}) + \mathrm{trdeg}_{F(\overline{a})}(\overline{c})$ et donc $\mathrm{trdeg}_F(\overline{c}) = \mathrm{trdeg}_{F(\overline{a})}(\overline{c})$, *i.e.* $F(\overline{c}) \downarrow^{\mathrm{alg}}_F F(\overline{a})$ et donc $H \downarrow^{\mathrm{alg}}_F L$.
- Supposons maintenant $L \downarrow^{\mathrm{lin}}_F H$. Soit $\overline{a} \in L$ algébriquement indépendant sur F. La famille des monômes en $\overline{a}$ est alors linéairement indépendante sur F. En effet, si $\sum_I \overline{a}^I = 0$, on a $P(\overline{a}) = 0$, où $P = \sum_I \overline{X}^I \in F[\overline{X}]$, et donc $P = 0$. Elle est donc linéairement indépendante sur H et donc si $P(\overline{a}) = 0$ avec $P \in H[\overline{x}]$, on a aussi $P = 0$.

□

Définition 2.49 (Dimension d'une variété) **:** *Soit $V \subseteq \mathcal{S}^{\mathrm{Zar}}_{\overline{X}}(F)$ une F-variété F-intègre. La dimension de V est $\dim(V) := \mathrm{trdeg}(F(V)/F)$.*

Proposition 2.50 : *Soient $F \leqslant K$ des corps, V une F-variété F-intègre et $\overline{a} \in V(K)$. On a alors $\mathrm{trdeg}_F(\overline{a}) \leqslant \dim(V)$. De plus, $\mathrm{trdeg}_F(\overline{a}) = \dim(V)$ si et seulement si $\overline{a}$ est F-générique dans V.*

Démonstration. Comme $\overline{a} \in V(K)$, on a morphisme surjectif $\varphi : F(V) \to F(\overline{a})$. Il s'ensuit que l'image d'une base de transcendance de $F(V)$ par φ génère $F(\overline{a})$ et donc $\mathrm{trdeg}_F(\overline{a}) \leqslant \mathrm{trdeg}(F(V)/F) = \dim(V)$.
Comme $\overline{a}$ est F-générique si et seulement si φ est injectif, il suffit de démontrer que ce dernier énoncé est équivalent à $\mathrm{trdeg}_F(\overline{a}) = \dim(V)$. Si φ est injective, les F-algèbres $F(\overline{a})$ et $F(V)$ sont isomorphes et ont donc le même degré de transcendance. Réciproquement, si $\mathrm{trdeg}_F(\overline{a}) = \mathrm{trdeg}(F(V)/F) := n$, soit $\overline{c}$ une base de transcendance de $F(V)$ sur F. Alors $\varphi(\overline{c})$ est une base de transcendance de $F(\overline{a})$ sur F, en particulier $\varphi(\overline{c})$ est algébriquement indépendante sur F. Pour tout $b = P(\overline{c}) \in F[\overline{c}]$, on a $\varphi(b) = P(\varphi(\overline{c}))$ et donc $\varphi(b) = 0$ si et seulement si $P = 0$ et donc $b = 0$. Soit maintenant $b \in F(V)$ et P son polynôme minimal sur $F(\overline{c})$. Si $\varphi(b) = 0$, on a $\varphi_\star P(0) = \varphi_\star P(\varphi(b)) = \varphi(P(b)) = 0$. Le coefficient constant de $\varphi_\star P$ est donc nul, mais par injectivité de φ restreint à $F(\overline{c})$ cela implique que le coefficient constant de P est aussi nul. Par irreductibilité, on a $P = X$ et $b = 0$. Ce qui prouve que φ est injective. □

Proposition 2.51 : *Soient $F \leqslant E \leqslant K$ des corps, V une F-variété et $\overline{a} \in V(K)$ tel que* $\mathrm{trdeg}_E(\overline{a}) \geqslant \dim(V)$. *On a alors que $\overline{a}$ E-générique dans V et de plus* $\dim(V) = \mathrm{trdeg}_F(\overline{a}) = \mathrm{trdeg}_E(\overline{a}) = \dim(V_E)$.

Démonstration. On a $\mathrm{trdeg}_E(\overline{a}) \leqslant \mathrm{trdeg}_F(\overline{a}) \leqslant \dim(V) \leqslant \mathrm{trdeg}_E(\overline{a})$ et donc ils sont égaux. De plus si $\overline{b} \in V(K)$ est E-générique, $\dim(V_E) = \mathrm{trdeg}_E(\overline{b}) \leqslant \mathrm{trdeg}_F(\overline{b}) = \dim(V) = \mathrm{trdeg}_E(\overline{a}) \leqslant \dim(V_E)$ et donc on a bien $\mathrm{trdeg}_E(\overline{a}) = \dim(V_E)$. Il s'ensuit que $\overline{a}$ est E-générique dans V. □

Lemme 2.52 : *Soient F un corps et K, L deux F-algèbres intègres. Pour toute L-algèbre $M \vDash \mathrm{ACF}_L$ telle que* $\mathrm{trdeg}(M/L) \geqslant \mathrm{trdeg}(K/F)$, *il existe un morphisme de F-algèbres $\varphi : K \to M$ tel que $\varphi(K) \downarrow^{\mathrm{alg}}_F L$.*

Démonstration. Soit c une base de transcendance de K sur F et $d \in M^c$ algébriquement indépendant sur L. On considère alors le morphisme de F-algèbres $\varphi : F[c] \to M$ qui envoie c sur d. Par le Corollaire **(2.5)**, on peut l'étendre en un morphisme $\varphi : K \to M$. Par construction, $\varphi(c) = d$ est algébriquement indépendant sur L et donc $\varphi(K) \downarrow^{\mathrm{alg}}_F L$. □

Corollaire 2.53 : *Soient $F \leqslant E$ des corps et V une F-variété E-intègre. On a alors* $\dim(V) = \dim(V_E)$.

Démonstration. Soit $E \leqslant K \vDash \mathrm{ACF}$ un corps de degré de transcendance infini sur E et $\overline{a}$ un point F-générique dans $V(K)$. On peut supposer $F(\overline{a}) \downarrow^{\mathrm{alg}}_F E$ et donc $\mathrm{trdeg}_E(\overline{b}) = \mathrm{trdeg}_F(\overline{b}) = \dim(V)$. Par la Proposition **(2.51)**, $\dim(V) = \mathrm{trdeg}_F(\overline{b}) = \mathrm{trdeg}_E(\overline{b}) = \dim(V_E)$. □

Corollaire 2.54 : *Soient $F \leqslant L, H \leqslant K$ des corps tels que l'extension $K \leqslant L$ soit régulière. Alors $L \downarrow^{\mathrm{alg}}_F H$ si et seulement si $L \downarrow^{\mathrm{lin}}_F H$.*

Démonstration. Il suffit de démontrer que $L \downarrow^{\mathrm{alg}}_F H$ implique que $L \downarrow^{\mathrm{lin}}_F H$. Soit $\overline{a} \in L$ un uplet. Comme l'extension $F \leqslant F[\overline{a}]$ est régulière, $V := \mathrm{loc}_F(\overline{a})$ est une F-variété géométriquement intègre définie sur F. Comme, de plus $F(\overline{a}) \downarrow^{\mathrm{alg}}_F H$, $\mathrm{trdeg}_H(\overline{a}) = \mathrm{trdeg}_F(\overline{a}) = \dim(V)$ et donc $\overline{a}$ est H-générique dans V, c'est-à-dire $\mathrm{id}_H(\overline{a}) = \mathrm{id}_H(V) = H\mathrm{id}_F(V) = H\mathrm{id}_F(\overline{a})$. Par la Proposition **(2.39)**, on a $F[\overline{a}] \downarrow^{\mathrm{lin}}_F H$. On a donc bien montré que $L \downarrow^{\mathrm{lin}}_F H$. □

Corollaire 2.55 : *Soit $F \leqslant E$ une extension régulière et $\mathfrak{p} \subseteq F[\overline{X}]$ un idéal premier. Alors $E\mathfrak{p} \subseteq E[\overline{X}]$ est aussi premier.*

Démonstration. Soient $V := \mathcal{V}_F(\mathfrak{p})$, $E \leqslant K$ et $\overline{a} \in V(K)$ F-générique. On peut supposer que $F(\overline{a}) \downarrow^{\mathrm{alg}}_F E$ et donc $F(\overline{a}) \downarrow^{\mathrm{lin}}_F E$. On a alors $\mathrm{id}_E(V) = \mathrm{id}_E(\overline{a}) = E\mathrm{id}_F(\overline{a}) = E\mathrm{id}_F(V) = E\mathfrak{p}$. En particulier, $E\mathfrak{p}$ est premier. □

3 Les corps pseudo algébriquement clos

3.1 Définition et premières propriétés

Définition 3.1 : *Soit $f : B \to D$ un morphisme injectif de A-algèbres. On dit que f est existentiellement clos si pour tout $\varphi \in \mathcal{F}^{\mathrm{qf}}_B(\overline{x})$, $D_f \vDash \exists \overline{x}\, \varphi$ implique $B \vDash \exists \overline{x}\, \varphi$.*

Lemme 3.2 : *Soit $f : B \to D$ un morphisme injectif de A-algèbres. Sont équivalents :*

1. *f est existentiellement clos ;*
2. *il existe un morphisme injectif de A-algèbres $g : D \to B^\star$ tel que $g \circ f$ soit élémentaire ;*
3. *$D_f \vDash \mathrm{Th}_B^\forall(B) := \{\varphi \in \mathcal{F}_B(\varnothing)$ universelle $: B \vDash \varphi\}$.*

Démonstration.

$1 \Rightarrow 2$ Soit $\overline{X} := (X_d)_{d \in D}$ et $h : B[\overline{X}] \to D$ le morphisme qui envoie X_d sur d. On considère alors la $B[\overline{X}]$-théorie $T := \mathrm{Th}_B(B)_{B[\overline{X}]} \cup \mathrm{Th}_{B[\overline{X}]}(D_h)$. Soit $T_0 \subseteq T$ finie. On a $T_0 \subseteq \mathrm{Th}_B(B)_{B[\overline{X}]} \cup \{\varphi_i(\overline{X}) : i \leqslant n\}$ où $\psi_i \in \mathcal{F}_B(\overline{x})$ et $D \vDash \varphi_i(h(\overline{X}))$, pour tout i. On trouve donc $\overline{b} \in \bigcap_i \varphi_i(B)$. Soit $g : B[\overline{X}] \to B$ tel que $g(\overline{X}) = \overline{b}$. On a alors $B_g \vDash T_0$. Par compacité, on trouve une $D[\overline{X}]$-algèbre $B^\star \vDash T$. Comme $B^\star \vDash \mathrm{Th}_{B[\overline{X}]}(D_h)$, le noyau du morphisme structurel $l : B[\overline{X}] \to B^\star$ est égal au noyau de $h : B[\overline{X}] \to D$ et l se factorise donc à travers un morphisme injectif $g : D \to B^\star$. Comme $B^\star_{g \circ f} \vDash \mathrm{Th}_B(B)$, le morphisme $g \circ f : B \to B^\star$ est bien élémentaire.

$2 \Rightarrow 3$ Soit $\varphi \in \mathcal{F}_B^\forall(\overline{x})$ telle que $B \vDash \varphi$. Puisque $g \circ f$ est elementaire, $B^\star_{g \circ f} \vDash \varphi$ et donc, comme φ est universelle, $D \vDash \varphi$.

$3 \Rightarrow 1$ Soit $\varphi \in \mathcal{F}_B^{\mathrm{qf}}(\overline{x})$. Si $B \nvDash \exists \overline{x}\, \varphi$, on a alors $\forall \overline{x} \neg\varphi \in \mathrm{Th}_B^\forall(B) \Dashv D_f$. Il s'ensuit que $D_f \vDash \forall \overline{x} \neg\varphi$, d'où $D \nvDash \exists \overline{x}\, \varphi$. □

Proposition 3.3 : *Soit F un corps. Sont équivalents :*

1. *toute F-variété géométriquement intègre définie sur F admet un point F-rationnel ;*
2. *F est existentiellement clos dans toute extension régulière $F \leqslant L$.*

Démonstration.

1⇒2 Soit $F \leqslant L$ une extension régulière. Soit $\varphi \in \mathcal{F}_F^{\mathrm{qf}}(\overline{x})$ et $\overline{a} \in L$ tel que $L \vDash \varphi(\overline{a})$. On peut supposer que φ est (à equivalence près) de la forme $\bigvee_i (\bigwedge_j P_{i,j} \simeq 0 \wedge \bigwedge_l Q_{i,l} \not\simeq 0)$. Soit i tel que $L \vDash \bigwedge_j P_{i,j}(\overline{a}) \simeq 0 \wedge \bigwedge_l Q_{i,l}(\overline{a}) \not\simeq 0$. Quite à remplacer L par $L_{(0)}$ et les $Q_{i,j} \not\simeq 0$ par $y_j Q_j - 1 \simeq 0$ et agrandir $\overline{a}$, on peut supposer que φ est de la forme $\bigwedge_j P_j \simeq 0$.
Comme $F(\overline{a}) \downarrow_F^{\mathrm{lin}} F^{\mathrm{a}}$, la F-variété $V := \mathcal{I}_F(\overline{a}) \subseteq \mathcal{S}_{\overline{x}}^{\mathrm{Zar}}(F)$ est géométriquement intègre définie sur F. Par 1, elle admet un point F-rationnel $\overline{c} \in F^{\overline{x}}$. Comme $P_j \in \mathcal{I}_F(\overline{a})$, pour tout j, on a bien $F \vDash \varphi(\overline{c})$.

2⇒1 Soit V une F-variété géométriquement intègre définie sur F. Alors $L := F[V]$ est une F-algèbre regulière. Soit $f_i \in F[\overline{X}]$ des générateurs de $\mathcal{I}_F(V)$ et $\overline{x} := \overline{X} + \mathcal{I}_F(V) \in L$. On a alors $L \vDash \bigwedge_i f_i(\overline{x}) \simeq 0$ et donc, comme F est existentiellement clos dans L, $F \vDash \exists \overline{x} \bigwedge_i f_i(\overline{x}) \simeq 0$. Et donc $V(F) \neq \varnothing$.

□

Définition 3.4 (PAC) **:** *Un corps F est dit pseudo algébriquement clos (*PAC*) s'il vérifie les conditions équivalentes de la Proposition (3.3).*

Lemme 3.5 : *Soit K un corps* PAC*et V un K-variété géométriquement intègre définie sur K. L'ensemble $V(K)$ est alors K-Zariski dense dans $V(K^{\mathrm{a}})$.*

Démonstration. TO DO □

Exemple 3.6 :

- Les corps algébriquement clos sont PAC.
- On verra que tout sous-corps infini de $\mathbb{F}_p^{\mathrm{a}}$ est PAC.

- On verra aussi que tout corps pseudo fini est PAC.

Lemme 3.7 : *Tout corps a une extension régulière qui est* PAC.

Démonstration. Soit F un corps et $(V_i)_{\alpha<\kappa}$ une énumération de toutes les F-variétés géométriquement intègres définies sur F. On construit par induction $(F_\alpha)_{i<\kappa}$ tels que $F_0 = F$, $V_\alpha(F_{\alpha+1}) \neq \varnothing$ et pour tout $\alpha \leqslant \beta$, $F_\alpha \leqslant F_\beta$ est régulière. Supposons que pour tout $\beta < \alpha$, F_β est construit. Si α est limite, $F_\alpha := \bigcup_\beta F_\beta$ convient. Sinon $\alpha = \beta + 1$ et $F_\alpha := F_\beta(V_\beta)$ convient.
On note $K_1 := F_\kappa$. C'est un extension régulière de $K_0 := F$ dans laquelle toutes les F-variétés géométriquement intègres définies sur F ont un point rationnel. En itérant, on construit $(K_i)_{i<\omega}$ tel que pour tout $i < j$ $K_i \leqslant K_j$ est régulière et toute K_i-variété géométriquement intègre définie sur K_i a un point K_{i+1}-rationnel. Soit alors $L := K_\omega = \bigcup_i K_i$. C'est bien une extension régulière de F.
Soit $V \subseteq \mathcal{S}_X^{\mathrm{Zar}}(L)$ une L-variété géométriquement intègre définie sur L. Par noethérianité, $\mathcal{I}(V)$ est finiment engendré. Il existe donc i tel que $\mathcal{I}(V) = L \cdot (\mathcal{I}(V) \cap K_i[X])$. Soit alors $W \subseteq \mathcal{S}_X^{\mathrm{Zar}}(K_i)$ la K_i-variété d'idéal $\mathcal{I}(V) \cap K_i[X]$. Elle est géométriquement intègre définie sur K_i et $W_L = V$. Par construction $\varnothing \neq W(K_{i+1}) \subseteq W(L) = V(L)$. □

Lemme 3.8 : *Tout corps* PAC *est infini.*

Démonstration. La preuve suit aisément du fait suivant :

Assertion 3.9 : *Soit F un corps, l'extension $F \leqslant F(X)$ est régulière.*

Démonstration. C'est une conséquence immédiate du fait que $F^{\mathrm{a}}(X) \simeq F^{\mathrm{a}} \otimes_F F(X)$. ◊

Soit alors F un corps fini et $(a_i)_{i<n}$ une énumération de ses éléments. Soit $\varphi := \exists x \bigvee_i x - a_i \neq 0$. On a $F(X) \vDash \varphi$ et $F \nvDash \varphi$. L'extension $F \leqslant F(X)$ bien que régulière n'est donc pas existentiellement close et F n'est pas PAC. □

3.2 L'algèbre des polynômes non standards

On fixe une famille de. corps $(K_i)_{i\in I}$ et $\mathfrak{U}$ un ultrafiltre sur I. On note $K := \prod_{i\to\mathfrak{U}} K_i$ et $K[\overline{X}]_{\mathfrak{U}} := \prod_{i\to\mathfrak{U}} K_i[\overline{X}]$. On plonge $K[\overline{X}]$ dans $K[\overline{X}]_{\mathfrak{U}}$ en envoyant X_j sur $\prod_{i\to\mathfrak{U}} X_j$.

Proposition 3.10 (Bourbaki, *Algèbre commutative*, Ch. I, §2, n°3 et n°11) **:** *Soit B une A-algèbre. Sont équivalents :*

1. *pour tout A-modules M_0 et M_1, si $f : M_0 \to M_1$ est injective alors $f_B := \mathrm{id}_B \otimes_A f : B \otimes_A M \to B \otimes_A M_1$ est injective ;*
2. *pour tout idéal $\mathfrak{a} \subseteq A$, le morphisme naturel $B \otimes_A \mathfrak{a} \to B$ est injectif ;*
3. *pour tous $f_i \in A$, les solutions dans B de $\sum_i f_i X_i = 0$ sont combinaisons B-linéaires de solutions dans A : pour tous $b_i \in B$ tels que $\sum_i f_i b_i = 0$, il existe $a_{i,j} \in A$ et $c_j \in B$ tels que, pour tout j, $\sum_i f_i a_{i,j} = 0$ et, pour tout i, $b_i = \sum_j c_j a_{i,j}$.*

On dit alors que B est une A-algèbre plate.

Proposition 3.11 (Bourbaki, *Algèbre commutative*, Ch. I, §3, n°5 et n°7) **:** *Soit B une A-algèbre plate de morphisme structurel $f : A \to B$. Sont équivalents :*

1. *pour tout idéal $\mathfrak{a} \subseteq A$, $f^{-1}(\mathfrak{a}B) = \mathfrak{a}$;*
2. *pour tout idéal maximal $\mathfrak{m} \subseteq A$, $1 \notin f(\mathfrak{m}) \cdot B$;*

3. *pour tous $f_i \in A$ et $g \in A$, si $\sum_i f_i X_i = g$ a une solution dans B, il a une solution dans A.*

On dit alors que B est une A-algèbre fidèlement plate.

Remarque 3.12 :

- Une A-algèbre B est plate si et seulement si pour toute suite exacte de A-modules $M_0 \to M_1 \to M_2$, la suite naturelle $B \otimes_A M_0 \to B \otimes_A M_1 \to B \otimes_A M_2$ est exacte.
- Une A-algèbre B est fidèlement plate si et seulement si l'exactitude de toute suite de A-modules $M_0 \to M_1 \to M_2$ et équivalente à l'exactitude de la suite naturelle $B \otimes_A M_0 \to B \otimes_A M_1 \to B \otimes_A M_2$.

Proposition 3.13 : *Soit B une A-algèbre plate. Alors, pour toute A-algèbre C, la C-algèbre $B \otimes_A C$ est plate.*

Démonstration. Soit $f : M_1 \to M_2$ un morphisme injectif de C-modules. Par transitivité du produit tensoriel, $f_{B\otimes_A C} : (B \otimes_A C) \otimes_C M_1 \to (B \otimes_A C) \otimes_C M_2 = f_B : B \otimes_A M_1 \to B \otimes_A M_2$ qui est bien injectif. □

Théorème 3.14 (van den Dries-Schmidt, 1984) **:** *$K[X]_{\mathfrak{U}}$ est une $K[X]$-algèbre fidèlement plate.*

Démonstration. Montrons tout d'abord que c'est une algèbre plate. On procède par induction sur $|X|$. Soient $(f_j)_{j<n} \in K[X]$ et $(g_j)_{j<n} \in K[X]_{\mathfrak{U}}$ tels que $\sum_j f_j g_j = 0$. On veut montrer que g_j est une combinaison $K[X]$-linéaire de solutions de cette equation dans $K[X]$. Supposons tout d'abord que f_0 est unitaire en X_0 — s'il ne l'est pas, il suffit de faire le changement de variable inversible $X_i \mapsto X_i + X_0$, pour $i > 0$, pour qu'il le devienne. On remarque que $(-f_j, 0, \ldots, 0, f_0, 0 \ldots)$ est une solution pour tout j. Soit $g_{i,j} = f_{i,0} q_{i,j} + r_{i,j}$, avec $\deg_0(r_{i,j}) < d := \deg_0(f_0)$ sa division euclidienne dans $K_i[X_{>0}][X_0]$. Pour tout $j > 0$, soit $r_j = \prod_{i\to\mathfrak{U}} r_{i,j} \in K[X]_{\mathfrak{U}}$. On trouve alors $r_0 \in K[X]_{\mathfrak{U}}$ tel que les r_j soient une solution. On a alors aussi $\deg_0(r_0) < d$. En particulier, on a trouvé des solutions dans $K[X_{>0}]_{\mathfrak{U}}[X_0]$ dont les g_j sont combinaison $K[X]_{\mathfrak{U}}$-linéaire.
Par induction, $K[X_{>0}]_{\mathfrak{U}}$ est une $K[X_{>0}]$-algèbre plate. Il suit de la Proposition **(3.13)** que $K[X_{>0}]_{\mathfrak{U}}[X_0]$ est une $K[X] = K[X_{>0}][X_0]$-algèbre plate et donc les r_j sont des combinaisons $K[X]_{\mathfrak{U}}$-linéaires de solutions dans $K[X]$.
Montrons maintenant que c'est une algèbre fidèlement plate. Soit $\mathfrak{m} \subseteq K[X]$ maximal. En particulier, $1 \notin \mathfrak{m}$ et donc par le Nullstellensatz, il existe $x \in \mathcal{V}_{K^{\mathrm{a}}}(\mathfrak{M}) \subseteq (K^{\mathrm{a}})^X \subseteq (\prod_{i\to\mathfrak{U}} K_i^{\mathrm{a}})^X$. Pour tout $f \in \mathfrak{m} \cdot K[X]_{\mathfrak{U}}$, $f(x) = 0$ et donc $f \neq 1$. □

On note $K(\overline{X})_{\mathfrak{U}} := \prod_{i\to\mathfrak{U}} K_i(\overline{X})$. On note que le plongement de $K[\overline{X}] \to K[\overline{X}]_{\mathfrak{U}}$ s'étend en un plongement $K(\overline{X}) \to K(\overline{X})_{\mathfrak{U}}$.

Théorème 3.15 (van den Dries-Schmidt, 1984) **:** *Soit $\mathfrak{p} \subseteq K[X]$ un idéal. Sont équivalents :*

1. *$\mathfrak{p} \subseteq K[X]$ est premier ;*
2. *$\mathfrak{p} \cdot K[X]_{\mathfrak{U}} \subseteq K[X]_{\mathfrak{U}}$ est premier.*

Démonstration.

1 ⇒2 On procède par induction sur $n := |X|$. Supposons tout d'abord que pour tout $j < n$, il existe $f_j \in \mathfrak{p} \cap K[X_j] \setminus (0)$. Pour tout $g \in K[X]_{\mathfrak{U}}$, par division euclidienne itérée par les $f_{i,j}$, on trouve $r_j \in K_i[X]$ de degré total borné par le produit des $d_j = \deg(f_j)$ tel que $g_i - r_i \in (f_{i,j} : j < n)$. C'est donc une K-algèbre de type finie engendrée par les puissances

de X. Il s'ensuit que le morphisme naturel $K[X]/\mathfrak{p} \to K[X]_{\mathfrak{U}}/(\mathfrak{p} \cdot K[X]_{\mathfrak{U}})$ est surjectif. Par platitude fidèle, $K[X]_{\mathfrak{U}}/(\mathfrak{p} \cdot K[X]_{\mathfrak{U}})$ est non triviale et donc, comme $K[X]/\mathfrak{p}$ est un corps (c'est une K-algèbre intègre de dimension finie), ce morphisme est injectif. Il s'ensuit que $\mathfrak{p} \cdot K[X]_{\mathfrak{U}}$ est premier puisque maximal.

Supposons maintenant que $\mathfrak{p} \cap K[X_0] = (0)$. Par localisation, $\mathfrak{p} \cdot K(X_0)[X_{>0}] \subseteq K(X_0)[X_{>0}]$ est premier.

Assertion 3.16 : *La $K(\overline{X})$-algèbre $K(\overline{X})_{\mathfrak{U}}$ est régulière.*

Démonstration. TO DO ◊

Par le Corollaire **(2.55)** et l'Assertion **(3.16)**, $\mathfrak{p} \cdot K(X_0)_{\mathfrak{U}}[X_{>0}] \subseteq K(X_0)_{\mathfrak{U}}[X_{>0}]$ est premier. Par induction, $\mathfrak{p} \cdot K(X_0)_{\mathfrak{U}}[X_{>0}]_{\mathfrak{U}} \subseteq K(X_0)_{\mathfrak{U}}[X_{>0}]_{\mathfrak{U}}$ est premier et il en est de même de son intersection avec $K[X]_{\mathfrak{U}}$.

Assertion 3.17 : $(\mathfrak{p} \cdot (K(X_0)_{\mathfrak{U}}[X_{>0}]_{\mathfrak{U}})) \cap K[X]_{\mathfrak{U}} = \mathfrak{p} \cdot K[X]_{\mathfrak{U}}$.

Démonstration. La preuve est technique et passe par une suite de résultats intermédiaires.

Assertion 3.18 : *Soit $I \leqslant K[X]$ un idéal tel que, pour tout $f \in K[X_0]$ irréductible, $\{a \in K[X] : fa \in I\} = I$ alors, pour tout $f \in K[X_0]_{\mathfrak{U}} \smallsetminus \{0\}$, $\{a \in K[X]_{\mathfrak{U}} : fa \in K[X]_{\mathfrak{U}} \cdot I\} = K[X]_{\mathfrak{U}} \cdot I$.*

On remarque que comme $\mathfrak{p}$ est premier et $\mathfrak{p} \cap K[X_0] = (0)$, l'Assertion **(3.18)** s'applique.

Démonstration. TO DO △

Soient $g \in (\mathfrak{p} \cdot (K(X_0)_{\mathfrak{U}}[X_{>0}]_{\mathfrak{U}})) \cap K[X]_{\mathfrak{U}}$, $(f_j)_{j<n} \in K[X]$ des générateurs de $\mathfrak{p}$. Comme $K(X_0)_{\mathfrak{U}} = (K[X_0]_{\mathfrak{U}})_{(0)}$, il existe $h_j, l \in K[X]_{\mathfrak{U}}$ tels que $g = \sum_j h_j l^{-1} f_j$ et donc $lg \in \mathfrak{p} \cdot K[X]_{\mathfrak{U}}$. Par l'Assertion **(3.18)**, $g \in \mathfrak{p} \cdot K[X]_{\mathfrak{U}}$. ◊

On a donc bien que $\mathfrak{p} \cdot K[X]_{\mathfrak{U}} = (\mathfrak{p} \cdot (K(X_0)_{\mathfrak{U}}[X_{>0}]_{\mathfrak{U}})) \cap K[X]_{\mathfrak{U}}$ est premier. Ce qui conclut la preuve de 1 ⇒2.

2 ⇒1 C'est une conséquence immédiate de la platitude fidèle : $\mathfrak{p} = (\mathfrak{p} \cdot K[X]_{\mathfrak{U}}) \cap K[X]$ est premier. □

Corollaire 3.19 (Hermann, 1926 – Seidenberg, 1974) **:** *Soient $n, d \in \mathbb{Z}_{\geqslant 0}$. Il existe $D \in \mathbb{Z}_{\geqslant 0}$ tel que pour tout $m \in \mathbb{Z}_{\geqslant 0}$ corps K et tout idéal $I \subseteq K[X]$, avec $|X| = n$, généré par des polynômes $(f_i)_{i<m}$ de degré total au plus d, on ait :*

(1) pour tout $h \in K[X]_{\leqslant d}$, $h \in I$ si et seulement s'il existe $g_i \in K[X]_{\leqslant D}$, $h = \sum g_i f_i$;

(2) I est premier si et seulement si $1 \notin I$pour tout $g, h \in K[X]_{\leqslant D}$, $gh \in I$ implique $g \in I$ ou $h \in I$.

Démonstration.

(1) Si un tel D n'existe pas, alors pour tout $D \in \mathbb{Z}_{\geqslant 0}$, il existe un corps K_D et $h, (f_{D,i})_{i<m} \in K_D[X]_{\leqslant d}$ tels que $h \in I_D := K_D[X](f_{D,i} : i < m)$ mais pour tout $(g_i)_{i<m} \in K_D[X]_{\leqslant D}$, $h \neq \sum_i g_i f_{D,i}$. Soit $\mathfrak{U}$ un ultrafiltre sur $\mathbb{Z}_{\geqslant 0}$. On définit $K = \prod_{D \to \mathfrak{U}} K_D$, $f_i = \prod_{D \to \mathfrak{U}} f_{D,i} \in K[X]$ et $h := \prod_{D \to \mathfrak{U}} h_D \in K[X]$. Par Łoś, il existe $g_i \in K[X]_{\mathfrak{U}}$ tels que $h = \sum_i g_i f_i$. Par le Théorème **(3.14)**, on peut supposer $g_i \in K[X]$. Par Łoś, pour tout $D \in U$, où $U \in \mathfrak{U}$, il existe $(g_{D,i})_{i<m} \in K_D[X]_{\leqslant E}$, où $E \geqslant \max_i \deg(g_i)$, tels que $h_D = \sum_i g_{D,i} f_{D,i}$. Notons que $U_{\geqslant E} := \{D \in U : D \geqslant E\} \in \mathfrak{U}$. En particulier, $U_{\geqslant E} \neq \varnothing$ et soit $D \in U_{\geqslant E}$. On a alors

$h_D = \sum_i g_{D,i} f_{D,i}$ avec $g_{D,i} \in K_D[X]_{\leqslant E} \subseteq K_D[X]_{\leqslant D}$, ce qui contredit notre hypothèse sur h_D.

(2) Si un tel D n'existe pas, alors pour tout $D \in \mathbb{Z}_{\geqslant 0}$, il existe un corps K_D et $(f_{D,i})_{i<m} \in K_D[X]_{\leqslant d}$ tels que $1 \notin I_D := K_D[X](f_{D,i} : i < m)$ et pour tous $g, h \in K_D[X]_{\leqslant D}$ si $gh \in I_D$ alors $g \in I_D$ ou $h \in I_D$; ainsi que $g_D, h_D \in K_D[X]$ tels que $g_D \notin I_D$, $f_D \notin I_D$ et $g_D h_D \in I_D$. Soit $\mathfrak{U}$ un ultrafiltre sur $\mathbb{Z}_{\geqslant 0}$. On définit $K = \prod_{D \to \mathfrak{U}} K_D$, $f_i = \prod_{D \to \mathfrak{U}} f_{D,i} \in K[X]$, $I := K[X](f_i : i < m)$, $g := \prod_{D \to \mathfrak{U}} g_D \in K[X]_{\mathfrak{U}}$ et $h := \prod_{D \to \mathfrak{U}} h_D \in K[X]_{\mathfrak{U}}$.

Assertion 3.20 : *$I \subseteq K[X]$ est premier.*

Démonstration. Par Łoś, $1 \notin I$. De plus, si $ab \in K[X]$ sont tels que $ab \in I$, c'est à dire $ab = \sum_i c_i f_i$ où $c_i \in K[X]$. Alors par Łoś encore, pour tout $D \in U$, où $U \in \mathfrak{U}$, $a_D b_D = \sum_i c_{D,i} f_{D,i} \in I_D$ où $a_D, b_D \in K_D[X]_{\leqslant E}$ et $\deg(a), \deg(b) \leqslant E$. Par hypothèse, pour tout $D \in U_{\geqslant E} \in \mathfrak{U}$, on a alors $a_D \in I_D$ ou $b_D \in I_D$. Par Łoś toujours, on a $a \in IK[X]_{\mathfrak{U}}$ ou $b \in IK[X]_{\mathfrak{U}}$. Comme $IK[X]_{\mathfrak{U}} \cap K[X] = I$, on a donc bien $a \in I$ ou $b \in I$. $\Diamond$

Cependant, par Łoś, on a $g \notin IK[X]_{\mathfrak{U}}$, $h \notin IK[X]_{\mathfrak{U}}$ et $gh \in IK[X]_{\mathfrak{U}}$ et donc $IK[X]_{\mathfrak{U}}$ n'est pas premier. Ceci contredit le Théorème **(3.15)**. $\square$

Corollaire 3.21 : *Soient $n, m, d \in \mathbb{Z}_{\geqslant 0}$. Il existe une formule $\theta_{n,m,d} \in \mathcal{F}_{\mathbb{Z}}(\overline{x}_1, \ldots, \overline{x}_m)$ telle que pour tout corps F et tout $\overline{a}_i \in F$, $F \vDash \theta_{n,m,d}(\overline{a}_1, \ldots, \overline{a}_m)$ si et seulement si $F[X](f_{\overline{a}_1}, \ldots, f_{\overline{a}_m})$ est premier, où $f_{\overline{a}_i} = \sum_{|I| \leqslant d} a_{I,i} X^I$, où $|X| = n$.*

Démonstration. Soit D la constante associée par le Corollaire **(3.19)** à n ,m et d, et E celle associée à n ,m et D^2. On a alors que $I := F[X](f_{\overline{a}_i} : i \leqslant m)$ est premier si et seulement si $1 \notin I$ et pour tout $g, h \in F[X]_{\leqslant D}$, $gh \in I$ implique $g \in I$ ou $h \in I$. Par le (1) du Corollaire **(3.19)**, $gh \in I$ si et seulement s'il existe $(c_i)_{i \leqslant m} \in F[X]_{\leqslant E}$ tels que $gh = \sum_i c_i f_i$. On peut donc écrire $\theta_{n,m,d}$ en quantifiant sur les coefficients et en remplaçant les égalités de polynômes par des égalités sur leurs coefficients. $\square$

Corollaire 3.22 : *Soient $n, m, d \in \mathbb{Z}_{\geqslant 0}$. Il existe une formule $\psi_{n,m,d} \in \mathcal{F}^{\mathrm{qf}}_{\mathbb{Z}}(\overline{x}_1, \ldots, \overline{x}_m)$ telle que pour tout corps F et tout $\overline{a}_i \in F$, $F \vDash \psi_{n,m,d}(\overline{a}_1, \ldots, \overline{a}_m)$ si et seulement si $V(f_{\overline{a}_1}, \ldots, f_{\overline{a}_2}) := \bigcap_i [f_{\overline{a}_i} \simeq 0] \subseteq \mathcal{S}^{\mathrm{Zar}}_X(F)$ est géométriquement intègre définie sur F.*

Démonstration. Soit $\psi_{n,m,d} \in \mathcal{F}^{\mathrm{qf}}_{\mathbb{Z}}(\overline{x}_1, \ldots, \overline{x}_m)$ équivalente à $\theta_{n,m,d}$ dans ACF. On a alors $F \vDash \psi_{n,m,d}(\overline{a}_1, \ldots, \overline{a}_m)$ si et seulement si $F^{\mathrm{a}} \vDash \psi_{n,m,d}(\overline{a}_1, \ldots, \overline{a}_m)$ si et seulement si $F^{\mathrm{a}} \vDash \theta_{n,m,d}(\overline{a}_1, \ldots, \overline{a}_m)$ si et seulement si $F^{\mathrm{a}}[X](f_{\overline{a}_i} : i \leqslant m)$ est premier si et seulement si $V(f_{\overline{a}_1}, \ldots, f_{\overline{a}_2})$ est géométriquement intègre définie sur F — *cf.* Proposition **(2.45)**. $\square$

Corollaire 3.23 : *Les corps* PAC *forment une classe élémentaire.*

Démonstration. Un corps est PAC si et seulement s'il vérifie $\forall x \exists y\, x \not\simeq 0 \vee xy - 1 \simeq 0$ et $\chi_{n,m,d} := \forall \overline{x}\, \theta_{n,m,d}(\overline{x}) \to \exists \overline{y} \bigwedge_i \sum_{|I| \leqslant d} x_{I,i} \overline{y}^I \simeq 0$, pour tout $n, m, d \in \mathbb{Z}_{\geqslant 0}$. $\square$

3.3 les corps pseudo finis

Lemme 3.24 : *Les corps pseudo finis sont parfaits.*

Démonstration. Les corps finis sont parfaits. On a donc $p \simeq 0 \to \forall x \exists y\, y^p - x \simeq 0 \in T_{\mathrm{f}}$, la théorie des corps finis qui est contenue dans T_{psf} celle des corps pseudo finis. $\square$

Définition 3.25 (Interprétation) **:**

- *Soit B une A-algèbre et D une C-algèbre. Une interprétation (avec paramètres) de B dans D est la donnée :*
  - *d'une formule $\delta \in \mathcal{F}_C(\overline{xy})$;*
  - *d'un uplet $\overline{b} \in D^{\overline{y}}$;*
  - *d'une fonction surjective $f : \delta(D, \overline{b}) \to B$;*
  - *pour tout $\varphi \in \mathcal{F}_A(\overline{z})$, d'une formule $\theta_\varphi \in \mathcal{F}_C(\overline{v}, \overline{y})$;*

  tels que pour tout $\varphi \in \mathcal{F}_A(\overline{z})$, $f^{-1}(\varphi(B)) = \theta_\varphi(D, \overline{b})$.
- *Soit $\mathcal{D}$ une classe de C-algèbres et, et pour tout $D \in \mathcal{D}$, $\mathcal{B}_D$ une classe de A-algèbres. Une interprétation uniforme de la famille $\mathcal{B} := (\mathcal{B}_D)_{D \in \mathcal{D}}$ et la donnée :*
  - *d'une formule $\delta \in \mathcal{F}_C(\overline{xy})$;*
  - *pour tout $\varphi \in \mathcal{F}_A(\overline{z})$, d'une formule $\theta_\varphi \in \mathcal{F}_C(\overline{v}, \overline{y})$;*
  - *d'une formule $\chi \in \mathcal{F}_C(\overline{y})$;*

  telles que pour tout $D \in \mathcal{D}$ et tout $B \in \mathcal{B}_D$, il existe $\overline{b}_B \in \chi(D)$ et une fonction $f_B : \delta(D, \overline{b}_B) \to B$ tels que $(\delta, \overline{b}_B, f_B, \theta_\varphi)$ soit une interprétation de B dans D et de plus, pour tout $\overline{b} \in \chi(D)$, il existe $B \in \mathcal{B}_D$ et $f_B : \delta(D, \overline{b}_B) \to B$ tels que $(\delta, \overline{b}_B, f_B, \theta_\varphi)$ soit une interprétation de B dans D.

Remarque 3.26 : Pour trouver une interpretation (uniforme), il suffit de trouver, pour tout $a \in A$ $\theta_a(v)$ associée à $z - a \simeq 0$, $\theta_+(v_1, v_2, v_3)$ associée à $z_1 + z_2 - z_3 \simeq 0$ et $\theta_\times(v_1, v_2, v_3)$ associée à $z_1 \cdot z_2 - z_3 \simeq 0$.

Proposition 3.27 : *Pour tout $d \in \mathbb{Z}_{\geqslant 0}$ les extensions monogènes de degré d d'un corps sont uniformément interprétables.*

Démonstration. Soit $\chi_d(y) := \forall r \forall s\, X^d + \sum_{i<d} y_i X^i \not\simeq (\sum_{i<d} r_i X^i)(\sum_{i<d} s_i X^i)$. Pour tout corps F et toute extension $F[a]$ de de degré d, soit $b \in F^d$ tel que $P_b = X^d + \sum_{i<d} b_i X^i$ est le polynôme minimal de a sur F. Sot $\delta_d(x, y) = \top$ où $|x| = d$ et $f : F^d \to F[a]$ la fonction $c_i \mapsto \sum_{i<d} c_i a^i$ qui est bien surjective. On a alors $\theta_{n,d} n(x, y) := x_0 \simeq n \wedge \bigwedge_{i>0} x_i \simeq 0$, $\theta_{+,d}(x_1, x_2, -x_3)$ qui est l'addition coordonnées par coordonnées et $\theta_{\times,d}(x_1, x_2, x_3)$ qui exprime qu'il existe $Q \in F[X]_{<d}$ $(\sum_i x_{i,1} X_i)(\sum_i x_{i,2} X_i) = Q P_b + \sum_i x_{i,3} X_i$. On remarque enfin que le corps de rupture d'un polynôme irréductible de degré d étant toujours une extension monogène de degré d, on a bien une interprétation uniforme. □

Remarque 3.28 :

- Pour tout $d \in \mathbb{Z}_{\geqslant 0}$ les extensions séparables de degré d d'un corps sont uniformément interprétables.
- Pour tout $d \in \mathbb{Z}_{\geqslant 0}$ les extensions de degré d d'un corps sont uniformément interprétables.

Corollaire 3.29 : *Soit F un corps pseudo fini. Pour tout $\mathrm{d} \in \mathbb{Z}_{>0}$, F a exactement une extension de degré d (dans une clôture algébrique donnée).*

Démonstration. Soit $\xi_d := \exists y\, \chi_d(y) \wedge \forall x\, \chi(x) \to \theta_{\exists t_1 \cdots \exists t_d \bigwedge_j t_j^d + \sum_{i<d} z_i t_j^i \simeq 0 \wedge \bigwedge_{j_1 \neq j_2} t_{j_1} \not\simeq t_{j_2}, d}(\hat{x}, y)$ où $\hat{x}_i$ est le uple $(x_i, 0, \ldots, 0)$. On a $F \vDash \xi_d$ si et seulement si F une extension monogène de degré d qui et le corps de décomposition de tous les polynômes irréductibles de degré d ; c'est à dire que F a une unique extension de degré d. Comme c'est le cas de tous les corps finis, on $\xi_d \in T_{\mathrm{f}} \subseteq T_{\mathrm{psf}}$. □

Théorème 3.30 (Lang-Weil, 1954) **:** *Pour tout $n, m, e \in \mathbb{Z}_{\geqslant 0}$, il existe $C \in \mathbb{Z}_{\geqslant 0}$ tel que pour tout corps fini F de cardinal q et $f_1 \ldots, f_m \in F[X_1, \ldots, X_n]$ de degré total au plus e, si $V = V(f_1, \ldots, f_m)$ est géométriquement intègre définie sur F de dimension d, alors :*

$$\left||V(F)| - q^d\right| < Cq^{d-1/2}.$$

Corollaire 3.31 : *Pour tout $n, m, e \in \mathbb{Z}_{\geqslant 0}$, il existe $Q \in \mathbb{Z}_{\geqslant 0}$ tel que pour tout corps fini F de cardinal $q \geqslant Q$ et $f_1 \ldots, f_m \in F[X_1, \ldots, X_m]$ de degré total au plus e, si $V = V(f_1, \ldots, f_m)$ est géométriquement intègre définie sur F, $V(F) \neq \varnothing$.*

Démonstration. Si $V(F) = \varnothing$, alors, par le Théorème **(3.30)**, $q^d < Cq^{d-1/2}$ et donc $q < C^2$ Il suffit donc de choisir $Q = C^2$. □

Corollaire 3.32 : *Les sous corps infinis de $\mathbb{F}_p^{\mathrm{a}}$ sont* PAC.

Démonstration. Soit $F \leqslant \mathbb{F}_p^{\mathrm{a}}$ un sous corps infini. On a alors $F := \bigcup_{i \in I} \mathbb{F}_{p^i}$ où $I \subseteq \mathbb{Z}_{>0}$ est infini. On peut supposer que pour tout $i, j \in I$, $ij \in I$. Soit V une F-variété géométriquement intègre définie sur F. Comme $I_F(V)$ est finiment engendré, il existe $i \in I$ tel que V soit définie sur F_i. Par le Corollaire **(3.31)**, $V(F) \supseteq V(F_i) \neq \varnothing$. □

Corollaire 3.33 : *Les corps pseudo finis sont* PAC.

Démonstration. Pour tout $n, m, e \in \mathbb{Z}_{\geqslant 0}$, la formule $\exists x_1 \cdots \exists x_Q \bigwedge_{i \neq j} x_i \neq x_j \to \chi_{n,m,e}$ est dans T_{f} par le Corollaire **(3.31)**. Comme $\exists x_1 \cdots \exists x_Q \bigwedge_{i \neq j} x_i \neq x_j \in T_{\mathrm{psf}}$ par définition, il s'ensuit que $T_{\mathrm{psf}} \vDash \chi_{n,m,e}$, et donc $T_{\mathrm{psf}} \vDash \mathrm{PAC}$. □

Soit PSF la théorie des corps PAC parfaits avec exactement une extension de degré d pour tout $d \in \mathbb{Z}_{>0}$. Nous avons donc prouvé :

Proposition 3.34 : *Les corps pseudo-finis sont des modèles de* PSF.

Démonstration. C'est le contenu du Lemme **(3.24)** et des Corollaires **(3.29)** et **(3.33)**. □

3.4 Théorie de Galois

Soit $F \leqslant K$ une extension de Galois (potentiellement infinie). On définit $\mathcal{G}(K/F) := \{\sigma \in \mathrm{Aut}(K) : \sigma|_F = \mathrm{id}_F\}$. On note $\mathcal{G}(F) := \mathcal{G}(F^{\mathrm{s}}/F)$ le groupe de galois absolu de F.

Proposition 3.35 : *Soit $F \leqslant K$ et $E \leqslant L$ des extensions galoisiennes et $f : K \to L$ un morphisme tel que $f(F) \leqslant E$. Il existe un unique morphisme de groupe $f^\star : \mathcal{G}(L/E) \to \mathcal{G}(K/F)$ tel que pour tout $\sigma \in \mathcal{G}(L/E)$, le diagramme suivant commute :*

$$\begin{tikzcd} K \arrow[r, "f^\star(\sigma)"] \arrow[d, "f"'] & K \arrow[d, "f"] \\ L \arrow[r, "\sigma"'] & L \end{tikzcd}$$

De plus, si $D \leqslant M$ est une extension galoisienne et $g : L \to M$ est un morphisme tel que $g(E) \leqslant D$, alors $(g \circ f)^\star = f^\star \circ g^\star$.

Démonstration. L'existence de $f^\star(\sigma)$ suit du fait suivant :

Assertion 3.36 : $\sigma(f(K)) \leqslant f(K)$.

Démonstration. L'extension $f(F) \leqslant f(K)$ est normale et donc, pour tout $x \in f(K)$, $\sigma(x)$, qui est une autre racine du polynôme minimal de x sur $f(F)$ est aussi dans $f(K)$. ◊

On définit alors $f^\star(\sigma) := f^{-1} \circ \sigma \circ f$ qui est bien un morphisme (injectif) $K \to K$ qui fixe F. Il est surjectif sur les extensions finies intermédiaires et donc c'est un élément de $\mathcal{G}(K/F)$. On vérifie facilement que $f^\star$ est un morphisme de groupe (c'est essentiellement la conjugaison) et que, par unicité, il commute à la composition. □

Remarque 3.37 : Un cas particulier de cette construction est le morphisme de restriction. Étant donné des extensions $F \leqslant E, K \leqslant L$ avec $F \leqslant K$ et $E \leqslant L$ galoisiennes, on a un morphisme res : $\mathcal{G}(L/E) \to \mathcal{G}(K/F)$ qui a $\sigma \in \mathcal{G}(L/E)$ associe $\sigma|_K$.

Proposition 3.38 : *Les groupes $\mathcal{G}(L/K)$ avec $F \leqslant L \leqslant K$ et $F \leqslant L$ galoisienne finie forment une famille projective filtrante où, pour tout $F \leqslant L_1 \leqslant L_2 \leqslant K$, $\mathcal{G}(L_2/F) \to \mathcal{G}(L_1/F)$ est donné par la restriction. De plus, on a un isomorphisme $\mathcal{G}(K/F) \cong \varprojlim_L \mathcal{G}(L/F)$, induit par la restriction.*

Démonstration. Le fait que la famille est filtrante est une conséquence du fait que si, pour $i = 1, 2$, $F \leqslant L_1 \leqslant K$ est galoisienne finie, alors $F \leqslant L_1L_2$ est aussi galoisienne finie. Le fait qu'elle est séparable est une conséquence du fait que $F \leqslant K$ l'est. Pour ce qui est de la normalité, comme L_i est normale, pour tout $\sigma \in \mathcal{G}(F)$, on a $\sigma(L_i) = L_i$ et donc $\sigma(L_1L_2) = L_1L_2$. Si a, c sont deux racines d' un polynôme irréductible sur F avec $a \in L_1L_2$, alors le morphisme de F-algèbre $F[a] \to F[b]$ qui envoie a sur b s'étend en un élément de $\mathcal{G}(F)$, par exemple par le Corollaire **(2.5)**. On a donc bien $b \in L_1L_2$ qui est normale.
Le fait que le morphisme $\mathcal{G}(K/F) \to \varprojlim_L \mathcal{G}(L/F)$ induit par la restriction est un isomorphisme suit aisément du fait que K est couvert par ses sous extensions normales finies de F : le corps de décomposition du polynôme minimal de tout $x \in K$ est une extension normale finie qui contient K. Tout système compatibles d'éléments de $\mathcal{G}(L/F)$ se recolle donc en un unique élément de $\mathcal{G}(K/L)$. □

Soit $G = \varprojlim_i G_i$ où les G_i sont finis. On munit chaque G_i de la topologie discrète et G de la topologie induite par la topologie produit sur $\prod_i G_i$. Cette topologie est nommée la topologie profinie.

Définition 3.39 : *Un groupe topologique est dit profini s'il est (homéomorphe à) la limite d'une famille projective filtrante de groupes finis.*

Proposition 3.40 : *Les groupes profinis sont des groupes topologiques compacts totalement discontinus.*

Démonstration. Supposons que G est homéomorphe à $\varprojlim_i G_i$. On note $f_{j,i} : G_j \to G_i$ les fonctions de transition pour tout $i < j$ et $f_i : \varprojlim_i G_i \to G_i$. Le produit $\prod_i G_i$ est compact par Tychonov. On rappelle que $\varprojlim_i G_i = \{(x_i)_i : \forall i < j\ f_{j,i}(x_j) = x_i\} = \bigcap_{i<j}(\pi_j \times \pi_i)^{-1}(\Gamma_{f_{j,i}})$ où $\Gamma_{f_{j,i}} \leqslant G_j \times G_i$ est le graphe de $f_{j,i}$. On a donc que $\varprojlim_i G_i$ est un fermé de $\prod_i G_i$ qui est donc bien compact.

Soit $U_i := f_i^{-1}(0) \subseteq \varprojlim_i G_i$. C'est un voisinage ouvert-fermé de 0 et comme $\bigcap_i U_i = \{0\}$, 0 a un système de voisinages ouverts-fermés. Leurs translatés forment une base d'ouverts-fermés de la topologie qui est donc bien totalement discontinue. $\square$

Remarque 3.41 :

- Un groupe fini est profini et la topologie profinie sur un groupe fini est exactement la topologie discrète.
- Les groupes profinis sont exactement les groupes topologiques compacts totalement discontinus.
- Dans un groupe profini, les sous-groupes normaux ouverts-fermés (et donc d'indice fini) forment une base de voisinages de l'identité.

Pour toute extension galoisienne $F \leqslant K$, on munit $\mathcal{G}(K/F) \cong \varprojlim_L \mathcal{G}(L/K)$ de la topologie profinie. Une base de voisinages ouverts-fermés de l'identité est donnée par les sous-groupes $\mathcal{G}(K/L)$ où $F \leqslant L \leqslant K$ et $F \leqslant L$ est une extension galoisienne finie.

Lemme 3.42 : *Soit $F \leqslant K$ et $E \leqslant L$ des extensions galoisiennes et $f : K \to L$ un morphisme tel que $\varphi(F) \leqslant E$. Le morphisme $f^\star : \mathcal{G}(L/E) \to \mathcal{G}(K/F)$ est continu.*

Démonstration. Soit $F \leqslant D \leqslant K$ avec $F \leqslant D$ galoisienne finie. Pour tout $\sigma \in \mathcal{G}(L/E)$, $f^\star(\sigma) \in \mathcal{G}(K/D)$ si et seulement si $\sigma \in \mathcal{G}(L/E\varphi(D))$ qui est ouvert. En effet, pour tout $d \in D$, $\varphi^{-1}(\sigma(\varphi(d))) = d$ si et seulement si $\sigma(\varphi(d)) = \varphi(d)$. $\square$

Théorème 3.43 (Galois, 1830 – Krull, 1928) **:** *Soit $F \leqslant K$ une extension galoisienne. On a une bijection qui inverse les inclusions :*

$$\begin{array}{rcc} \{L : F \leqslant L \leqslant K\} & \cong & \{H \leqslant G : H \textit{ fermé}\} \\ L & \mapsto & \mathcal{G}(K/L) \\ K^H := \{x \in K : \forall \sigma \in H\, \sigma(x) = x\} & \leftarrow\!\shortmid & H \end{array}$$

De plus $F \leqslant L \leqslant K$ est galoisienne si et seulement si $\mathcal{G}(K/L) \leqslant \mathcal{G}(K/F)$ est normale. On a alors une suite exacte courte naturelle : $1 \to \mathcal{G}(K/L) \to \mathcal{G}(K/F) \to \mathcal{G}(L/F) \to 1$.

Proposition 3.44 : *Soient $F \leqslant K$, $E \leqslant L$ et $D \leqslant M$ des extensions galoisiennes telles que $F \leqslant E \cap D$, $K \leqslant L \cap M$ et $L \downarrow_K^{\mathrm{lin}} M$. On a alors un homéomorphisme $\varphi : \mathcal{G}(LM/ED) \to \mathcal{G}(L/E) \times_{\mathcal{G}(K/F)} \mathcal{G}(M/D)$.*

On rappelle que si B et C sont des A-algèbres, alors $B \otimes_A C$ est leur somme amalgamée.

Démonstration. Comme la restriction est fonctorielle, on a un morphisme $\varphi : \mathcal{G}(LM/ED) \to \mathcal{G}(L/E) \times_{\mathcal{G}(K/F)} \mathcal{G}(M/D) = \{(\sigma, \tau) : \sigma|_K = \tau|_K\} \leqslant \mathcal{G}(L/E) \times \mathcal{G}(M/D)$ tel que $\varphi(\sigma) = (\sigma|_L, \sigma|_M)$. Ce morphisme est évidemment injectif. Comme $L \downarrow_K^{\mathrm{lin}} M$, on a $LM \cong L \otimes_K M$ et donc pour toute paire $(\sigma, \tau) \in \mathcal{G}(L/E) \times_{\mathcal{G}(K/F)} \mathcal{G}(M/D)$, $\sigma \otimes_K \tau$ est un automorphisme de $L \otimes_K M$ dont l'action sur L est donnée par σ et celle sur M par τ. Le morphisme φ est donc surjectif.

Soit $E \leqslant E_0 \leqslant L$ et $D \leqslant D_0 \leqslant M$ tels que $E \leqslant E_0$ et $D \leqslant D_0$ soient galoisiennes finies et $\sigma \in \mathcal{G}(LM/ED)$. On a alors $\sigma|_L \in \mathcal{G}(L/E_0)$ et $\sigma|_M \in \mathcal{G}(M/D_0)$ si et seulement si $\sigma \in \mathcal{G}(LM/E_0D_0)$ et φ est continue. Comme $\mathcal{G}(L/E) \times \mathcal{G}(M/D)$ est compact, c'est un homéomorphisme sur son image. $\square$

Proposition 3.45 : *Soient $F \leqslant K$ et $E \leqslant L$ des extensions galoisiennes et $f : K \to L$ un morphisme tel que $\varphi(F) \leqslant E$. On a :*

1. *$f^\star : \mathcal{G}(L/E) \to \mathcal{G}(K/F)$ est surjectif si et seulement si $E \cap f(K) = f(F)$;*
2. *$f^\star : \mathcal{G}(L/E) \to \mathcal{G}(K/F)$ est injectif si et seulement si $L = Ef(K)$.*

Démonstration.

1. Supposons tout d'abord que $f^\star$ est surjectif. et soit $x \in K$ tel que $f(x) \in E$. Pour tout $\sigma \in \mathcal{G}(K/F)$, il existe $\tau \in \mathcal{G}(L/E)$ tel que $f^\star(\tau) = \sigma$. Il s'en suit que $\sigma(x) = f^{-1}(\tau(f(x))) = x$ et donc $x \in K^{\mathcal{G}(K/F)} = F$. On a donc $E \cap f(K) \leqslant f(F)$. L'inclusion réciproque est évidente.
   On suppose maintenant que $E \cap f(K) = f(F)$. Comme $f(F) \leqslant f(K)$ est galoisienne, par la Proposition **(2.36)**, $E \downarrow^{\mathrm{lin}}_{f(F)} f(K)$. Comme $Ef(K) \cong E \otimes_F K$, tout $\sigma \in \mathcal{G}(K/F)$ induit un (unique) automorphisme $\tau \in \mathcal{G}(Ef(K)/Ef(F))$ qui s'étend à E^{a} et donc à $E \leqslant L \leqslant E^{\mathrm{a}}$ qui est normale.
2. Supposons tout d'abord que $f^\star$ est injectif. Pour tout $\sigma \in \mathcal{G}(L/Ef(K))$, on a $f^\star(\sigma) = \mathrm{id}_K$ et donc $\sigma = \mathrm{id}_L$. Il s'ensuit que $Ef(K) = L$. Réciproquement, si $L = Ef(K)$, pour tout $\sigma \in \mathcal{G}(L/E)$ tel que $f^\star(\sigma) = \mathrm{id}_K$ et tout $x = \sum_i e_i f(k_i)$ où $e_i \in E$ et $k_i \in K$, on a $\sigma(x) = \sum_i \sigma(e_i)\sigma(f(k_i)) = \sum_i e_i f(k_i) = x$ et donc $\sigma = \mathrm{id}_L$. □

3.5 Presque elimination des quantificateurs

Théorème 3.46 (Lemme de plongement, Jarden-Kiehne, 1975) **:** *Soient $F \leqslant K$ et $E \leqslant L$ des extensions de corps parfaits telles que L est* PAC. *Soit, de plus $\varphi : F^{\mathrm{a}} \to E^{\mathrm{a}}$ un isomorphisme tel que $\varphi(F) = E$ et $\Psi : \mathcal{G}(L) \to \mathcal{G}(K)$ un morphisme continu tel que le diagramme suivant commute :*

$$\begin{tikzcd} \mathcal{G}(L) \arrow[r, "\Psi"] \arrow[d, "\mathrm{res}"'] & \mathcal{G}(K) \arrow[d, "\mathrm{res}"] \\ \mathcal{G}(E) \arrow[r, "\varphi^\star"'] & \mathcal{G}(F). \end{tikzcd}$$

Il existe alors une extension élémentaire $L \preccurlyeq M$ et un morphisme $\psi : K^{\mathrm{a}} \to M^{\mathrm{a}}$ qui étend φ tel que le diagramme suivant commute :

$$\begin{tikzcd} \mathcal{G}(M) \arrow[d, "\mathrm{res}"'] \arrow[dr, "\psi^\star"] & \\ \mathcal{G}(L) \arrow[r, "\Psi"] & \mathcal{G}(K) \end{tikzcd}$$

Démonstration. Par le Lemme **(2.52)**, il existe $\Omega \vDash \mathrm{ACF}$ contenant L et $\xi : K^{\mathrm{a}} \to \Omega$ qui étend φ et tel que $\xi(K^{\mathrm{a}}) \downarrow^{\mathrm{alg}}_{E^{\mathrm{a}}} L^{\mathrm{a}}$. Soit $N = \xi(K)$. On a alors $N^{\mathrm{a}} \downarrow^{\mathrm{lin}}_{E^{\mathrm{a}}} L^{\mathrm{a}}$. Il s'ensuit que $\mathcal{G}(N^{\mathrm{a}}L^{\mathrm{a}}/NL) \cong \mathcal{G}(N) \times_{\mathcal{G}(E)} \mathcal{G}(L)$ et on a donc un morphisme injectif continu $\Upsilon := \Xi \times_{\mathcal{G}(E)} \mathrm{id}_{\mathcal{G}(L)} : \mathcal{G}(L) \to \mathcal{G}(N^{\mathrm{a}}L^{\mathrm{a}}/NL)$ où $\Xi := (\xi^\star)^{-1} \circ \Psi$. Le sous-groupe $\Upsilon(\mathcal{G}(L)) \leqslant \mathcal{G}(N^{\mathrm{a}}L^{\mathrm{a}}/NL)$ est fermé et soit $D := (N^{\mathrm{a}}L^{\mathrm{a}})^{\Upsilon(\mathcal{G}(L))}$. Par la correspondance de Galois, $\mathcal{G}(N^{\mathrm{a}}L^{\mathrm{a}}/D) = \Upsilon(\mathcal{G}(L))$. Donc Υ induit un homéomorphisme entre $\mathcal{G}(L)$ et $\mathcal{G}(N^{\mathrm{a}}L^{\mathrm{a}}/D)$. Par construction, le diagrame suivant commute :

$$\begin{tikzcd}
\mathcal{G}(L) \arrow[r, "\Upsilon"] \arrow[rrrd, bend right, "\mathrm{id}"'] & \mathcal{G}(L^{\mathrm{a}}N^{\mathrm{a}}/D) \arrow[r, "\mathrm{res}"] \arrow[rrd, "\mathrm{res}"] & \mathcal{G}(L^{\mathrm{a}}N^{\mathrm{a}}/LN) \arrow[r, "\mathrm{res}"] \arrow[rd, "\mathrm{res}"] & \mathcal{G}(L)\times_{\mathcal{G}(E)}\mathcal{G}(N) \arrow[d, "\pi_L"] \\
 & & & \mathcal{G}(L)
\end{tikzcd}$$

et donc $\mathrm{res}\circ\Upsilon = \mathrm{id}_{\mathcal{G}(L)}$. Comme Υ est surjective sur $\mathcal{G}(L^{\mathrm{a}}N^{\mathrm{a}}/D)$, $\mathrm{res} : \mathcal{G}(N^{\mathrm{a}}L^{\mathrm{a}}/D) \to \mathcal{G}(L)$ est aussi l'inverse à droite de Υ. En particulier, $\mathrm{res} : \mathcal{G}(D) \to \mathcal{G}(L^{\mathrm{a}}N^{\mathrm{a}}/D) \to \mathcal{G}(L)$ est surjectif, et donc, comme L est parfait, $L \leqslant D$ est régulière. Comme L est PAC, il est existentiellement clos dans D et donc par le Lemme **(3.2)**, il existe une L-algèbre élémentaire M et un morphisme de L-algèbres $\theta : D \to M$. Comme $D \downarrow^{\mathrm{lin}}_{L} L^{\mathrm{a}}$, on peut étendre θ en un morphisme L^{a}-algèbre $\theta : DL^{\mathrm{a}} \to ML^{\mathrm{a}}$ et enfin en un morphisme L^{a}-algèbre $\theta : D^{\mathrm{a}} \to M^{\mathrm{a}}$. Soit $\psi = \theta\circ\xi$. On a donc le diagramme commutatif suivants au niveau des corps :

$$\begin{tikzcd}
K^{\mathrm{a}} \arrow[rr, "\xi"'] \arrow[rrrrrr, bend left, "\psi"] \arrow[rd, dotted, dash] \arrow[dd, dotted, dash] & & N^{\mathrm{a}} \arrow[rr, dotted, dash] \arrow[rd, dotted, dash] \arrow[dd, dotted, dash] & & D^{\mathrm{a}} \arrow[rr, "\theta"'] \arrow[rd, dotted, dash] \arrow[dd, dotted, dash] & & M^{\mathrm{a}} \arrow[rd, dotted, dash] \arrow[ld, dotted, dash] & \\
 & K \arrow[rr] \arrow[dd, dotted, dash] & & N \arrow[rr, dotted, dash] \arrow[dd, dotted, dash] & & D \arrow[rr] \arrow[dd, dotted, dash] & & M \\
F^{\mathrm{a}} \arrow[rr, "\varphi"'] \arrow[rd, dotted, dash] & & E^{\mathrm{a}} \arrow[rr, dotted, dash] \arrow[rd, dotted, dash] & & L^{\mathrm{a}} \arrow[rd, dotted, dash] \arrow[ru, dotted, dash] & & & \\
 & F \arrow[rr] & & E \arrow[rr, dotted, dash] & & L \arrow[rruu, bend right, dotted, dash] & &
\end{tikzcd}$$

et celui-ci au niveau des groupes de Galois :

$$\begin{tikzcd}
 & & \mathcal{G}(N^{\mathrm{a}}L^{\mathrm{a}}/NL) \arrow[ld, dotted] & & \\
\mathcal{G}(K) \arrow[d, dotted] & \mathcal{G}(N) \arrow[l, "\xi^\star"'] \arrow[d, dotted] & \mathcal{G}(N^{\mathrm{a}}L^{\mathrm{a}}/D) \arrow[l, dotted] \arrow[u, dotted] \arrow[d, dotted] & \mathcal{G}(D) \arrow[l, dotted] & \mathcal{G}(M) \arrow[l, "\theta^\star"'] \arrow[llll, bend right, "\psi^\star"'] \arrow[lld, dotted] \\
\mathcal{G}(F) & \mathcal{G}(E) \arrow[l, "\varphi^\star"] & \mathcal{G}(L) \arrow[l, dotted] \arrow[u, "\Upsilon"] \arrow[lu, "\Xi"] \arrow[llu, "\Psi"] & &
\end{tikzcd}$$

ce qui conclut la preuve. $\square$

Définition 3.47 (Corps borné) **:** *Une extension galoisienne $F \leqslant K$ est dite bornée si pour chaque $d \in \mathbb{Z}_{\leqslant 0}$, il y a un nombre fini d'extensions intermédiaires $F \leqslant L \leqslant K$ avec $[L : K] = d$. Le corps F est dit borné si $F \leqslant F^{\mathrm{s}}$ est bornée.*

Exemple 3.48 :

- Les corps algébriquement clos sont bornés.
- $\mathbb{R}$ est borné. Plus généralement les corps réels clos, c'est-à-dire les corps élémentairement équivalents à $\mathbb{R}$, sont bornés. En fait, K est réel clos si et seulement si $[K^{\mathrm{a}} : K] < 2$ — si et seulement si $[K^{\mathrm{a}} : K] < \infty$.

- Les corps pseudo finis sont bornés.
- $\mathbb{Q}$ n'est pas borné.

Soit $\mathfrak{d} : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$. On note $C_{\mathfrak{d}} := \mathbb{Z}[X_n : n \in \mathbb{Z}_{>0}]$ avec $|X_n| = \mathfrak{d}(n)$, $P_n := Y^{\mathfrak{d}(n)} + \sum_{i<\mathfrak{d}(n)} X_{n,i}Y^i \in C_{\mathfrak{d}}[Y]$, $\mathrm{IRR}_{\mathfrak{d}}$ la $C_{\mathfrak{d}}$-théorie qui contient la théorie des corps et énonce que P_n est séparable irréductible pour tout n, et $\mathrm{GAL}_{\mathfrak{d}}$ la $C_{\mathfrak{d}}$-théorie qui contient $\mathrm{IRR}_{\mathfrak{d}}$ et énonce que tout polynôme Q séparable irréductible de degré n a n racines distinctes modulo P_n.

Lemme 3.49 : *Soit K un corps, sont équivalents :*

1. *K est borné ;*
2. *il existe $\mathfrak{d} : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ et un morphisme $f : C_{\mathfrak{d}} \to K$ tel que $K_f \vDash \mathrm{GAL}_{\mathfrak{d}}$.*

Démonstration.

$1 \Rightarrow 2$ TO DO

$2 \Rightarrow 1$ TO DO □

Lemme 3.50 : *Soit $K \vDash \mathrm{GAL}_{\mathfrak{d}}$ et $f : A \to K$ un morphisme de $C_{\mathfrak{d}}$-corps. Le morphisme $f^\star : \mathcal{G}(K) \to \mathcal{G}(A)$ est injectif.*

Démonstration. Soit □

Lemme 3.51 : *Soit $f : F^{\mathrm{s}} \to K^{\mathrm{s}}$ un morphisme de corps tel que $f(F) \leqslant K$ et $f^\star : \mathcal{G}(K) \to \mathcal{G}(F)$ est surjectif. Soit $P \in F[Y]$, $|Y| = 1$ un polynôme séparable, sont équivalents :*

1. *$f(P)$ est irréductible sur K ;*
2. *P est irréductible sur F.*

Démonstration. TO DO □

Lemme 3.52 : *Soit $f : F^{\mathrm{s}} \to K^{\mathrm{s}}$ un morphisme de $C_{\mathfrak{d}}$-corps tel que $f(F) \leqslant K$, avec $F \vDash \mathrm{GAL}_{\mathfrak{d}}$. Sont équivalents :*

1. *$K \vDash \mathrm{IRR}_{\mathfrak{d}}$;*
2. *$f^\star : \mathcal{G}(K) \to \mathcal{G}(F)$ est surjectif.*

Démonstration.

$1 \Rightarrow 2$ Soit $e_n \in F^{\mathrm{s}}$ une racine de $P_n := Y^{\mathfrak{d}(n)} + \sum_{i<\mathfrak{d}(n)} X_{n,i}Y^i \in C_{\mathfrak{d}}[Y]$. Comme $F \vDash \mathrm{GAL}_{\mathfrak{d}}$, les $F[e_n]$ forment une famille filtrante. En effet $F[e_{n_1}, e_{n_2}]$ est une extension séparable de degré $m < \infty$ et donc $F[e_{n_1}, e_{n_2}] \leqslant F[e_m]$. De plus, comme $f(P_n)$ est irréductible sur K, pour tout extensoin de f à $F^{\mathrm{s}} \to K^{\mathrm{s}}$, $f(F[e_n]) \downarrow^{\mathrm{lin}}_{f(F)} K$ et donc $f(F^{\mathrm{s}}) = \bigcup_n f(F[e_n]) \downarrow^{\mathrm{lin}}_{f(F)} K$. En particulier, $f(F^{\mathrm{s}}) \cap K = f(F)$ et donc, par la Proposition **(3.45)**, $f^\star$ est surjectif.

$2 \Rightarrow 1$ Comme P_n est séparable et irréductible sur F, il l'est aussi sur K par le Lemme **(3.51)**. □

Lemme 3.53 : *Soit $f : F^{\mathrm{s}} \to K^{\mathrm{s}}$ un morphisme de $C_{\mathfrak{d}}$-corps tel que $f(F) \leqslant K$, sont équivalents :*

1. *$K \vDash \mathrm{GAL}_{\mathfrak{d}}$ et $f^\star : \mathcal{G}(K) \to \mathcal{G}(F)$ est surjectif ;*
2. *$F \vDash \mathrm{GAL}_{\mathfrak{d}}$ et $f^\star : \mathcal{G}(K) \to \mathcal{G}(F)$ est un homéomorphisme ;*
3. *$K \vDash \mathrm{GAL}_{\mathfrak{d}}$ et $F \vDash \mathrm{GAL}_{\mathfrak{d}}$;*
4. *$K \vDash \mathrm{GAL}_{\mathfrak{d}}$, $F \vDash \mathrm{GAL}_{\mathfrak{d}}$ et $f^\star : \mathcal{G}(K) \to \mathcal{G}(F)$ est un homéomorphisme.*

Démonstration.

$1 \Rightarrow 3$ Si $P_n := Y^{\mathfrak{d}(n)} + \sum_{i<\mathfrak{d}(n)} X_{n,i}Y^i \in C_{\mathfrak{d}}[Y]$ et $\mathrm{GAL}_{\mathfrak{d}}$ est irréductible sur K il l'est aussi sur F et donc $F \models \mathrm{IRR}_{\mathfrak{d}}$. Soit $Q \in F[Y]$ un polynôme séparable irréductible de degré n et $a \in F^{\mathrm{s}}$ une de ses racines. Par le Lemme **(3.51)**, Q est irréductible sur K et donc $a \in K[e_n]$ où $e_n \in F^{\mathrm{s}}$ est une racine de P_n. On a donc $a \in K[e_n]$ et donc $\mathcal{G}(K[e_n]) \leqslant \mathcal{G}(K[a])$. Il s'ensuit que $f^\star\mathcal{G}(K[e_n]) \leqslant f^\star\mathcal{G}(K[a])$. On remarque que $(f^\star)^{-1}(\mathcal{G}(F[a])) = \mathcal{G}(K[a])$ et donc, comme $f^\star$ est surjectif, $f^\star(\mathcal{G}(K[a])) = \mathcal{G}(F[a])$. De même, $f^\star(\mathcal{G}(K[e_n])) = \mathcal{G}(F[e_n]) \leqslant \mathcal{G}(F[a])$ et donc $F[a] \leqslant F[e_n]$.

$2 \Rightarrow 4$ Par le Lemme **(3.52)**, $K \models \mathrm{IRR}_{\mathfrak{d}}$. Soit $Q \in K[Y]$ un polynôme séparable irréductible de degré n et $a \in F^{\mathrm{s}}$ une de ses racines. Soit $H := f^\star(\mathcal{G}(K[a])) \leqslant \mathcal{G}(F)$. Comme $f^\star$ est un homéomorphisme, $[\mathcal{G}(F) : H] = [\mathcal{G}(K) : \mathcal{G}(K[a])] = n$ et donc $F \leqslant L := (F^{\mathrm{s}})^H$ est une extension de degré n. Il s'ensuit que $L \leqslant F[e_n]$, d'où $\mathcal{G}(F[e_n] \leqslant H)$ et donc $\mathcal{G}(K[e_n]) = (f^\star)^{-1}(\mathcal{G}(F[e_n])) \leqslant (f^\star)^{-1}(H) = \mathcal{G}(K[a])$, comme $f^\star$ est injective. On a donc bien $K[a] \leqslant K[e_n]$.

$3 \Rightarrow 4$ Par le Lemme **(3.50)**, $f^\star$ est injectif et par le Lemme **(3.52)**, il est surjectif.

Comme 4 implique clairement tous les autres énoncés, cela conclut la preuve. □

Lemme 3.54 : *Soit K une $C_{\mathfrak{d}}$-algèbre, sont équivalents :*

1. $K \models \mathrm{GAL}_{\mathfrak{d}}$ *;*
2. *pour toute $C_{\mathfrak{d}}$-corps F et tout morphisme de $C_{\mathfrak{d}}$-algèbres $f : F^{\mathrm{s}} \to K^{\mathrm{s}}$ tel que $f(F) \leqslant K$, on a $f(F^{\mathrm{s}}) \cap K \models \mathrm{GAL}_{\mathfrak{d}}$ et $f_\star : \mathcal{G}(K) \to \mathcal{G}(F)$ est injectif ;*
3. *$F^{\mathrm{s}} \cap K \models \mathrm{GAL}_{\mathfrak{d}}$, où F est sous corps de K engendré par C, et $\mathrm{res} : \mathcal{G}(K) \to \mathcal{G}(F)$ est injectif.*

Démonstration.

$1 \Rightarrow 2$ TO DO

$2 \Rightarrow 3$ On applique 2 à la C-algèbre $F^{\mathrm{s}} \cap K$ et au choix de morphisme structurel $F^{\mathrm{s}} \to K^{\mathrm{s}}$.

$3 \Rightarrow 1$ TO DO □

Si L est une K-algèbre alors L^{s} est naturellement (mais non canoniquement) une L^{s}-algèbre et on note $\mathrm{res} : \mathcal{G}(L) \to \mathcal{G}(K)$ le morphisme associé au morphisme structurel choisi.

Corollaire 3.55 : *Soit F un corps borné et K une F-algèbre élémentaire. Le morphisme res : $\mathcal{G}(K) \to \mathcal{G}(F)$ est alors un homéomorphisme et K est borné.*

Démonstration. Par le Lemme **(3.49)**, il existe $\mathfrak{d}$ tel que $F \models \mathrm{GAL}_{\mathfrak{d}}$. On a alors $K \models \mathrm{GAL}_{\mathfrak{d}}$, en particulier il est borné, Par le Lemme **(3.49)**. De plus, par le **??**, $\mathrm{res} : \mathcal{G}(K) \to \mathcal{G}(F)$ est un homéomorphisme. □

Proposition 3.56 : *Soient $F \leqslant K$ et $E \leqslant L$ des extensions de corps parfaits telles que K et L soient* PAC *bornés. Soit, de plus, $\varphi : F^{\mathrm{a}} \to E^{\mathrm{a}}$ un isomorphisme tel que $\varphi(F) = E$ et $\Psi : \mathcal{G}(L) \to \mathcal{G}(K)$ un homéomorphisme tel que le diagramme suivant commute :*

$$\begin{tikzcd}
\mathcal{G}(L) \arrow[r, "\Psi"] \arrow[d, "\mathrm{res}"'] & \mathcal{G}(K) \arrow[d, "\mathrm{res}"] \\
\mathcal{G}(E) \arrow[r, "\varphi^\star"'] & \mathcal{G}(F).
\end{tikzcd}$$

Le morphisme $\varphi : F \to L$ est alors K-élémentaire.

Démonstration. On construit par induction K_{i+1}, une K_i-algèbre élémentaire, où $K_0 := K$, L_{i+1} une L_i-algèbre élémentaire, où $L_{-1} := L$, et des morphismes $\varphi_i : K_i^{\mathrm{a}} \to L_i^{\mathrm{a}}$ et $\psi_i : L_i^{\mathrm{a}} \to K_{i+1}^{\mathrm{a}}$ tels que $\varphi_i(K_1) \leqslant L_i$, $\psi_i(L_i) \leqslant K_{i+1}$ et les diagrammes suivants commutent :

$$\begin{tikzcd} K_0^{\mathrm{a}} \arrow[r, "\varphi_0"] \arrow[d, dash] & L_0^{\mathrm{a}} \\ F^{\mathrm{a}} \arrow[r, "\varphi"'] & E^{\mathrm{a}} \arrow[u] \end{tikzcd} \qquad \begin{tikzcd} \mathcal{G}(L_0) \arrow[r, "\varphi_0^\star"] \arrow[d, "\mathrm{res}"'] & \mathcal{G}(K_0) \\ \mathcal{G}(L) \arrow[ur, "\Psi"'] & \end{tikzcd} \qquad \begin{tikzcd} K_{i+1}^{\mathrm{a}} \arrow[r, "\varphi_{i+1}"] & L_{i+1}^{\mathrm{a}} \\ K_i^{\mathrm{a}} \arrow[u] \arrow[r, "\varphi_i"'] & L_i^{\mathrm{a}} \arrow[u] \arrow[ul, "\psi_i"'] \end{tikzcd}$$

On obtient φ_0 en appliquant le Théorème **(3.46)**. On remarque que, puisque L_0 est une L-algèbre élémentaire, par le Corollaire **(3.55)**, $\mathrm{res} : \mathcal{G}(L_0) \to \mathcal{G}(L)$ est un homéomorphisme. Comme Ψ en est aussi un, c'est donc aussi le cas de $\varphi_0^\star$.
Supposons maintenant que φ_i est construit (et que $\varphi_i^\star$ est un homéomorphisme). On applique alors le Théorème **(3.46)** à $\varphi_i^{-1} : \varphi_i(K_i^{\mathrm{a}}) \to K_i$ et $(\varphi_i^\star)^{-1} : \mathcal{G}(K_i) \to \mathcal{G}(L_i)$ pour obtenir ψ_i. Comme précédemment, puisque $(\varphi_i^\star)^{-1}$ est un homéomorphisme, c'est aussi le cas de $\mathcal{G}(\psi_i)$. On applique alors de nouveau le Théorème **(3.46)** à $\psi_i^{-1} : \psi_i(L_i^{\mathrm{a}}) \to L_i$ et $\mathcal{G}(\psi_i)^{-1} : \mathcal{G}(L_i) \to \mathcal{G}(K_{i+1})$ pour obtenir φ_{i+1}. On vérifie, de même, que $\varphi_{i+1}^\star$ est un homéomorphisme.
On définit alors $\varphi_\infty := \bigcup_i \varphi_i : K_\infty \to L_\infty$ et $\psi_\infty := \bigcup_i \psi_i : L_\infty \to K_\infty$ et on vérifie que ce sont des isomorphismes inverses l'un de l'autre. En particulier, φ_∞ est élémentaire. Comme le diagramme suivant commute par construction,

$$\begin{tikzcd} F \arrow[r, dash] \arrow[d, "\varphi"'] & K \arrow[r] & K_\infty \arrow[d, "\varphi_\infty"] \\ E \arrow[r, dash] & L \arrow[r] & L_\infty \end{tikzcd}$$

et que, par le théorème d'union de chaîne (Théorème **(1.30)**), K_∞ est une K-algèbre élémentaire et L_∞ est une L-algèbre élémentaire, on a bien que $\varphi : F \to L$ est K-élémentaire. □

Corollaire 3.57 : *Soit $F \leqslant K$ et $E \leqslant L$ des extensions de corps parfaits telles que K et L soient* PAC *bornés, et les morphismes* $\mathrm{res} : \mathcal{G}(K) \to \mathcal{G}(F)$ *et* $\mathrm{res} : \mathcal{G}(L) \to \mathcal{G}(E)$ *sont des homéomorphismes. Alors tout morphisme $\varphi : F \to L$ tel que $\varphi(F) = E$ est K-élémentaire.*

Démonstration. Par hypothèse $\mathcal{G}(K) \cong \mathcal{G}(F) \cong \mathcal{G}(E) \cong \mathcal{G}(L)$. On peut donc appliquer la Proposition **(3.56)**. □

Proposition 3.58 : *Soient F un corps infini, $F \leqslant L$ une extension de corps, K une extension algébrique de F et $A \subseteq K$ un ensemble de générateurs de K. Sont équivalents :*

1. *Il existe un morphisme de F-algèbres $\varphi : K \to L$;*
2. $L \vDash \{\exists x\, P \simeq 0 : P \in F[x]$ *avec* $|x| = 1$ *et P a une racine dans K*$\}$.
3. $L \vDash \{\exists x\, P \simeq 0 : P$ *est le polynôme minimal de $c \in A$ sur F*$\}$.

Démonstration.

1 ⇒ 2 Pour tout $P \in F[X]$ et $a \in K$ tel que $P(a) = 0$, on a $L \vDash P(\varphi(a)) \simeq 0$ et donc on a bien $L \vDash \{\exists x\, P \simeq 0 : P \in F[X]$ a une racine dans $K\}$.

2 ⇒ 3 C'est évident.

3 ⇒ 1 On suppose tout d'abord que A est fini, et donc $F \leqslant K$ est finie. Soit $E \geqslant K$ telle que $F \leqslant E$ est normale finie. Pour tout $a \in A$, il existe $b \in L \cap E$ une racine du polynôme minimal de a sur F. L'isomorphisme $F[b] \cong F[a]$ s'étend en un élément $\sigma \in \mathcal{G}(E/F)$. On a alors $a \in \sigma(L \cap E)$ et donc $K \subseteq \bigcup_{\sigma \in \mathcal{G}(E/F)} \sigma(L \cap E) \leqslant E$.

Assertion 3.59 : *Soit F un corps infini, W un espace vectoriel sur F et $V, (V_i)_{i<n} \leqslant W$ des sous-F-espaces vectoriels. Si $V \subseteq \bigcup_{i<n} V_i$, il existe alors i tel que $V \leqslant V_i$.*

Démonstration. On procède par induction sur n. Si $V \subseteq \bigcup_{0<i<n} V_i$, on conclut par induction. On peut donc supposer qu'il existe $a \in V \setminus (\bigcup_{0<i<n} V_i)$, en particulier, $a \in V_0$. Soit $b \in V$, comme F est infini, il existe $i < n$ et $\lambda, \mu \in F$ tels que $a + \lambda b, a + \mu b \in V_i$. On a alors $a = (\mu - \lambda)^{-1}(\mu(a + \lambda b) - \lambda(a + \mu b)) \in V_i$ et donc $i = 0$. Il s'ensuit que $b = (\lambda - \mu)^{-1}(a + \lambda b - (a + \mu b)) \in V_0$. On a donc bien $V \leqslant V_0$. ◊

Comme $K \subseteq \bigcup_{\sigma \in \mathcal{G}(E/F)} \sigma(L \cap E) \leqslant E$, par l'Assertion **(3.59)**, il existe $\sigma \in \mathcal{G}(E/F)$ tel que $K \leqslant \sigma(L \cap E)$ et donc σ^{-1} induit un morphisme de F-algèbres $K \to L$.

En général, soit $p(x) := \mathrm{qftp}(a/F)$. Soit $a_0 \subseteq a$ fini. Par le cas précédent, il existe $\varphi : F[a_0] \to L$. Il s'ensuit que $p(x)$ est finiment satisfaisable dans L et donc il existe une L-algèbre élémentaire $L^\star$ et un morphisme de F-algèbres $\varphi : K \to L^\star$. Comme K est une F-algèbre algébrique séparable, $\varphi(K) \leqslant L^{\mathrm{s}}$. Par le Corollaire **(3.55)** et la Proposition **(3.45)**, $L^{\mathrm{s}} \cap L^\star = L$ et donc $\varphi(A) \leqslant L$. □

Remarque 3.60 : Si F est fini, l'existence et l'unicité des extensions de chaque degré (et une induction sur $|A|$), nous permettent de conclure que la Proposition **(3.58)** est aussi vraie.

Soit PPAC la $\mathbb{Z}$-théorie des corps PAC parfaits et $\mathrm{PPAC}_{\mathfrak{d}}$ la $C_{\mathfrak{d}}$-théorie $\mathrm{PPAC} \cup \mathrm{GAL}_{\mathfrak{d}}$.

Proposition 3.61 : *Soient $K, L \vDash \mathrm{PPAC}_{\mathfrak{d}}$, $A \subseteq K$ un sous-ensemble et $f : A \to L$ une fonction. Sont équivalents :*

1. *pour tout $P \in C_{\mathfrak{d}}[x, y]$, où $|y| = 1$, et $a \in A^x$ tel que $P(a, y)$ a une racine dans K, $P(\varphi(a), y)$ a une racine dans L.*
2. *il existe un morphisme de $C_{\mathfrak{d}}$-algèbres $g : C_{\mathfrak{d}}[A]^{\mathrm{a}}_{(0)} \cap K \to L$ qui étend f.*
3. *il existe un morphisme K-élémentaire de F-algèbres $g : C_{\mathfrak{d}}[A] \cap K \to L$ qui étend f.*

Démonstration.

1 ⇒ 2 On remarque que si $P \in C_{\mathfrak{d}}[x]$ et $a \in A^x$, $P(a) = 0$ si et seulement si le polynôme constant $f(a)$ a une racine (dans K), si et seulement si $P(f(a)) = 0$; et $P(a) \neq 0$ si et seulement si $P(a)y - 1$ a une racine, si et seulement si $P(f(a)) \neq 0$. On a donc un morphisme injectif de $C_{\mathfrak{d}}$-algèbres $g : C_{\mathfrak{d}}[A] \to L$ qui étend f. Par la Proposition **(3.58)**, g s'étend encore en un morphisme $F^{\mathrm{a}} \cap K \to L$.

2 ⇒ 3 Soit $F := C_{\mathfrak{d}}[A]^{\mathrm{a}}_{(0)} \cap K$. On a $F^{\mathrm{s}} \cap K = C_{\mathfrak{d}}[A]^{\mathrm{s}}_{(0)} \cap K = F$ et donc $\mathrm{res} : \mathcal{G}(K) \to \mathcal{G}(F)$ est surjectif. Comme $K \vDash \mathrm{GAL}_{\mathfrak{d}}$, par le Lemme **(3.53)**, $\mathrm{res} : \mathcal{G}(K) \to \mathcal{G}(F)$ est un homéomorphisme et $F \vDash \mathrm{GAL}_{\mathfrak{d}}$. On a donc aussi $g(F) \vDash \mathrm{GAL}_{\mathfrak{d}}$ et donc, par le Lemme **(3.53)**, comme $L \vDash \mathrm{GAL}_{\mathfrak{d}}$, $\mathrm{res} : \mathcal{G}(L) \to \mathcal{G}(g(F))$ est aussi un homéomorphisme. On peut donc appliquer le Corollaire **(3.57)** pour conclure que $g : F \to L$ est K-élémentaire.

3 ⇒ 1 C'est évident. □

Proposition 3.62 : *Soit T une A-théorie, $\Delta(\overline{x}) \subseteq \mathcal{F}_A(\overline{x})$ un ensemble clos par disjonctions et conjonctions finies (modulo T) et $\varphi(\overline{x}) \in \mathcal{F}_A(\overline{x})$ une formule. Sont équivalents :*

1. *il existe $\psi \in \Delta$ tel que $T \vDash \forall \overline{x}\, \varphi(\overline{x}) \leftrightarrow \psi(\overline{x})$;*
2. *pour tout $B, C \vDash T$, $\overline{b} \in \varphi(B)$ et $\overline{c} \in C^{\overline{x}}$ tels que pour tout $\psi \in \Delta$, $B \vDash \psi(\overline{b})$ implique $C \vDash \psi(\overline{c})$, alors $C \vDash \varphi(\overline{c})$.*

Démonstration.

$1 \Rightarrow 2$ Soit $\pi(x) := \{\psi \in \Delta : T \vDash \forall x\, \varphi(x) \to \psi(x)\}$. Soit $C \vDash T$ et $c \in C$ tel que $C \vDash \pi(c)$. Soit $\rho(x) := \{\neg\theta : \theta \in \Delta \text{ et } B \vDash \neg\theta\}$. Si $\rho \cup \{\varphi\}$ est inconsistent (dans T), par compacité, il existe $(\neg\psi_i)_{i<n} \in \rho$ tel que $T \vDash \forall x\, \varphi \to (\bigvee_{i<n} \psi_i)$. On a alors $\bigvee_{i<n} \psi_i \in \pi$ et donc, pour un certain i, $C \vDash \psi_i(c)$, ce qui contredit que $\neg\psi_i \in \rho$.
Soit donc $B \vDash T$ et $b \in B$ tel que $B \vDash \rho(b)$ et $C \vDash \varphi(c)$. On remarque que, pour tout $\psi \in \Delta$, si $C \vDash \neg\psi(b)$ alors $\neg\psi \in \rho$ et donc $B \vDash \neg\psi(b)$. Par hypothèse, on a donc $C \vDash \varphi(c)$.
On a donc $\pi(x) \vDash \varphi(x)$ et donc, par compacité, $T \vDash \forall x\, \varphi(x) \leftrightarrow (\bigwedge_{i \leqslant m} \psi_i(x))$ où $\psi_i \in \pi \subseteq \Delta$.

$2 \Rightarrow 1$ C'est évident. □

Théorème 3.63 : *Toute formule $\varphi \in \mathcal{F}_{C_{\mathfrak{d}}}(x)$ est équivalente modulo* $\mathrm{PPAC}_{\mathfrak{d}}$ *à une formule de la forme $\exists y \bigwedge_i f_i(x, y_i) \simeq 0$ où $f_i \in C_{\mathfrak{d}}[x, y_i]$ et $|y_i| = 1$.*

En particulier, $\mathrm{PPAC}_{\mathfrak{d}}$ est modèle complète.

Démonstration. Soit $K, L \vDash \mathrm{PPAC}_{\mathfrak{d}}$, $b \in \varphi(K)$ et $c \in L^x$ tels que, pour tout $P(x, y) \in C_{\mathfrak{d}}[x, y]$, où $|y| = 1$, si $P(b, y)$ a une racine dans K alors $P(c, y)$ a une racine dans L. Par la Proposition **(3.61)**, il existe un morphisme K-élémentaire de $C_{\mathfrak{d}}$-algèbres $g : C_{\mathfrak{d}}[b] \to C_{\mathfrak{d}}[c]$ qui envoie b sur c. On a donc $c \in \varphi(L)$.
Par la Proposition **(3.62)**, φ est équivalente modulo $\mathrm{PPAC}_{\mathfrak{d}}$ à une conjonction finie de disjonctions finies de formules $\exists f(x, y) \simeq 0$ avec $f \in F[x, y]$, $|y| = 1$. Mais on remarque que $\bigvee_i \exists y_i\, f_i(x, y_i) \simeq 0$ est équivalent (modulo la théorie des anneaux intègres), à $\exists y \prod_i f_i(x, y) \simeq 0$. Ce qui conclut la preuve. □

On définit $\mathrm{PSFG} := \mathrm{PPAC}_{\mathrm{id}} = \mathrm{PSF} \cap \mathrm{GAL}_{\mathrm{id}}$. Par la Proposition **(3.34)**, les modèles infinis de $T_{\mathrm{f}} \cup \mathrm{IRR}_{\mathrm{id}}$ sont des modèles de PSFG.

Corollaire 3.64 : *Pour toute formule $\varphi \in \mathcal{F}_{C_{\mathrm{id}}}(x)$, il existe $N \in \mathbb{Z}_{\leqslant 0}$ et $(f_i)_{i<m} \in C_{\mathrm{id}}[x, y_i]$, avec $|y_i| = 1$, tels que pour toute corps fini F muni d'une structure de C_{id}-algèbre avec $F \vDash \mathrm{IRR}_{\mathrm{id}}$, si $|F| \geqslant N$, $F \vDash \forall x\, \varphi \leftrightarrow \exists y \bigwedge_i f_i(\overline{x}, y_i) \simeq 0$.*

Soit $F \leqslant E$ une extension galoisienne bornée. Pour tout $n \in \mathbb{Z}_{\geqslant 0}$, il existe un nombre fini de $a_{i,n} \in E$ de degré n tels que pour tout $c \in E$ de degré n, $c \in F[\overline{a}_n]$. Soit $e_n \in E$ un générateur de $F[\overline{a}_n]$ sur F et $P_n \in F[Y]$ son polynôme minimal. Soit $\mathfrak{d}(n)$ le degré de P_n. On munit F de l'unique structure de $C_{\mathfrak{d}}$-algèbre telle que $P_n = Y^{\mathfrak{d}(n)} + \sum_{i<n} X_{n,i} Y^i$ et on note $\mathrm{GAL}_F^E := (\mathrm{GAL}_{\mathfrak{d}})_F$.

Lemme 3.65 : *Soit K une F-algèbre, sont équivalents :*

1. *$K \vDash \mathrm{GAL}_F^E$;*
2. *pour tout morphisme de F-algèbre $f : E \to K^{\mathrm{s}}$, $f_\star : \mathcal{G}(K) \to \mathcal{G}(E/F)$ est un homéomorphisme.*

3. *il existe un morphisme de F-algèbre $f : E \to K^s$ tel que $f_\star : \mathcal{G}(K) \to \mathcal{G}(E/F)$ est un homéomorphisme.*

Démonstration.
1 ⇒ 2 TO DO
2 ⇒ 3 Cela suit du fait qu'un morphisme de F-algèbres $f : E \to K^s$ existe toujours.
3 ⇒ 1 TO DO □

Soit $\mathrm{PPAC}_F^E := \mathrm{PPAC} \cup \mathrm{GAL}_F^E = (\mathrm{PPAC}_\mathfrak{d})_F$.

Proposition 3.66 : *Toute formule $\varphi \in \mathcal{F}_F(x)$ est équivalente modulo PPAC_F^E à une formule de la forme $\exists y \bigwedge_i f_i(x, y_i) \simeq 0$ où $f_i \in F[x, y_i]$ et $|y_i| = 1$.*

En particulier, PPAC_F^E est modèle complète.

Démonstration. C'est une conséquence immédiate du Théorème **(3.63)** □

3.6 Le groupe de Galois des corps pseudo finis

Soit F un corps fini de cardinal q. Soit $\sigma_q : F^s \to F^s$ le morphisme de Frobenius qui envoie x sur x^q. Soit $F \leqslant E$ l'extension de degré n. Pour tout $m \in \mathbb{Z}_{>0}$, on a $\varphi^n|_E = \mathrm{id}_E$ si et seulement si $n|m$. Donc $\sigma \in \mathcal{G}(E/F)$ engendre un groupe de taille n. Mais $[E : F] = n$ et donc $\mathcal{G}(E/F)$ est cyclique engendré par σ. Il s'ensuit que $\mathcal{G}(F) = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$. De plus, le groupe engendré par $\sigma \in \mathcal{G}(F)$ intersecte chaque coset de $\mathcal{G}(E) \leqslant \mathcal{G}(F)$. Il est donc dense dans $\mathcal{G}(F)$. On dit que σ est un générateur topologique de $\mathcal{G}(F)$. On remarque que σ^n est un générateur topologique de $\mathcal{G}(E) \leqslant \mathcal{G}(F)$.

Définition 3.67 : *On note $\widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}$.*

Proposition 3.68 : *Soit G un groupe profini et $g \in G$. Sont équivalents :*
1. *g est un générateur topologique de G ;*
2. *pour tout sous groupe ouvert $H \leqslant G$, $G = \langle g \rangle H$;*
3. *pour tout sous-groupe ouvert $H \leqslant G$, l'action de $\langle g \rangle$ sur G/H est transitive ;*
4. *les sous-groupes ouverts de G sont de la forme $\overline{\langle g^n \rangle}$.*

De plus, si g est un générateur topologique de G et $H \leqslant G$ est ouvert d'indice n alors $H = \overline{\langle g^n \rangle}$. Réciproquement, si $n \in \mathbb{Z}_{>0}$ est minimal tel que $g^n \in H$ alors $[G : H] = n$.

Démonstration.
1 ⇒ 2 Pour tout $a \in G$, aH est un ouvert et donc $g^n \in aH$ pour un $n \in \mathbb{Z}$. On a alors $a \in aH = g^n H \subseteq \langle g \rangle H$.
2 ⇒ 3 Pour tout $a \in G$, il existe $n \in \mathbb{Z}$ tel que $a \in g^n H$, c'est-à-dire $aH = g^n H$.
3 ⇒ 1 Comme les sous-groupes (normaux) ouverts forment une base de voisinages de 1, il suffit de montrer que pour tout sous-groupe ouvert $H \leqslant G$ et tout $a \in G$, $aH \cap \langle g \rangle \neq \varnothing$, c'est à dire $aH = g^n H$, ce qui est bien l'énoncé 3.
1 ⇒ 4 Comme H est ouvert et G est compact, $[G : H] < \infty$. Il s'ensuit que, comme $\langle g \rangle / (H \cap \langle g \rangle)$ se plonge dans G/H, $H \cap \langle g \rangle$ est d'indice fini, n, dans $\langle g \rangle$, et est donc égal à $\langle g^n \rangle$. D'où $\overline{\langle g^n \rangle} \leqslant H$. De plus, pour tout i, $\overline{\{g^{i+nj} : j \in \mathbb{Z}\}} \leqslant g^i H$. Par ailleurs, $\bigcup_i \overline{\{g^{i+nj} : j \in \mathbb{Z}\}} = \overline{\langle g \rangle} = G$ et donc, pour tout i, $g^i H = \overline{\{g^{i+nj} : j \in \mathbb{Z}\}}$. En particulier $H = \overline{\langle g^n \rangle}$.

4 ⇒ 1 G est un sous-groupe ouvert de G et donc il est de la forme $\overline{\langle g^n \rangle}$ pour un certain $n \in \mathbb{Z}$. Mais on a alors $G = \overline{\langle g^n \rangle} \leqslant \overline{\langle g \rangle} \leqslant G$ et donc g est un générateur topologique. □

De plus, si g est un générateur topologique de G, on a vu dans la preuve de 1 ⇒ 4 que si $H \leqslant G$ ouvert d'indice n alors $H = \overline{\langle g^n \rangle}$. La réciproque suit de l'énoncé 3.

Proposition 3.69 : *Soit G un groupe profini. Sont équivalents :*

1. *G a au plus un sous groupe ouvert d'indice n pour tout n ;*
2. *tous les sous groupes ouverts $H \leqslant G$ sont normaux et G/H est cyclique ;*
3. *il existe un générateur topologique $g \in G$.*

On dit que G est *procyclique*.

Démonstration.

1⇒2 Soit $H \leqslant G$ un sous-groupe ouvert. On a $n := [G : H] < \infty$ et pour tout $g \in G$, $[G : gHg^{-1}] = n$. Par unicité du sous-groupe ouvert d'indice n, on a $gHg^{-1} = H$ et donc H est normal. Montrons maintenant que G/H est cyclique. Comme il y a une bijection entre les sous-groupes de G/H et les sous-groupes $H \leqslant L \leqslant G$, il suffit de montrer que si G est fini alors il est cyclique.

On procède par induction sur $|G|$. Soit p premier qui divise $|G|$. On trouve alors $g \in G$ d'ordre p. Par induction, $G/\langle g \rangle$ est cyclique et soit $h \in G$ un générateur. Si $\langle g \rangle \leqslant \langle h \rangle$, $G = \langle h \rangle$ est cyclique. sinon $G = \langle g \rangle \langle h \rangle$. De plus, si p divise l'ordre de $\langle h \rangle$ on aurait un deuxième sous-groupe de G d'ordre p ce qui est impossible. Il s'ensuit que gh est un générateur de G qui est donc bien cyclique.

2⇒3 Pour tout sous groupe ouvert (normal) H, on définit $X_H := \{g \in G : g \text{ génère } G/H\}$. C'est un fermé non vide. Pour tous $(H_i)_{i<n} \leqslant G$ ouverts, on a $X_{\bigcap_{i<n} H_i} \subseteq \bigcap_{i<n} X_{H_i}$ qui est donc non vide. Par compacité $\bigcap_H X_H \neq \emptyset$. On remarque que tout élément de cet ensemble est un générateur topologique de G par la Proposition **(3.68)**.

3⇒1 Soit $H \leqslant G$ un sous-groupe ouvert. Par la Proposition **(3.68)**, $H = \overline{\langle g^n \rangle}$ pour un $n \in \mathbb{Z}$. On peut supposer n minimal tel que $H = \overline{\langle g^n \rangle}$. On a alors $G = \bigsqcup_{0 \leqslant i < n} g^i H$ et donc $[G : H] = n$. Il s'en suit que l'unique sous-groupe d'indice n de G s'il existe, est $\overline{\langle g^n \rangle}$. □

Remarque 3.70 : Les groupes procycliques sont abéliens.

Par la correspondance de Galois, on a l'équivalence suivante :

Corollaire 3.71 : *Soit F un corps. Sont équivalents :*

1. *F a au plus une extension séparable de degré n pour tout n ;*
2. *toutes les extensions finies séparables de K sont galoisiennes et leur groupe de Galois sur F est cyclique ;*
3. *il existe $\sigma \in \mathcal{G}(F)$ tel que $F = (F^{\mathrm{s}})^{\sigma}$.*

De plus, pour toute extension séparable finie $F \leqslant E$, on a alors que $\sigma|_E$ engendre $\mathcal{G}(E/F)$ et $E = (F^{\mathrm{s}})^{\sigma^{[E:F]}}$.

Démonstration. Par la correspondance de Galois, l'énoncé 1 est équivalent à $\mathcal{G}(F)$ a un plus un sous-groupe d'indice n pour tout $n \in \mathbb{Z}_{>1}$. L'énoncé 2 est équivalent à tout sous-groupe ouvert $\mathcal{G}(E) \leqslant \mathcal{G}(F)$ est normal et $\mathcal{G}(E/F) \cong \mathcal{G}(F)/\mathcal{G}(E)$ est cyclique. Pour ce qui est du 3, on remarque d'abord que si $H \leqslant \mathcal{G}(F)$ alors $F^H = F^{\overline{H}}$. En effet, comme $F^{\overline{H}} \leqslant F^H$, on a

$H \leqslant \mathcal{G}(F^H) \leqslant \overline{H}$ et donc $\mathcal{G}(F^H) = \overline{H}$. L'énoncé 3 est donc équivalent à l'existence de $\sigma \in \mathcal{G}(F)$ tel que $\overline{\langle\sigma\rangle} = \mathcal{G}(F)$. L'équivalence entre ces énoncés est donc une conséquence de la Proposition **(3.69)**.
De plus, on a vu dans la Proposition **(3.68)**, que pour tout sous groupe ouvert (normal) $\mathcal{G}(E) \leqslant \mathcal{G}(F)$, $\mathcal{G}(F)/\mathcal{G}(E) = \mathcal{G}(E/F)$ est engendré par l'image de σ, à savoir $\sigma|_E$. Enfin, toujours par la Proposition **(3.68)**, $\mathcal{G}(E) = \overline{\sigma^{[E:F]}}$ et donc $E = F^{\mathcal{G}(E)} = F^{\sigma^{E:F}}$. □

Revenons à $\widehat{\mathbb{Z}}$. On fixe $\sigma \in \widehat{\mathbb{Z}}$ un générateur topologique. La paire $(\widehat{\mathbb{Z}}, \sigma)$ a la propriété universelle suivante :

Proposition 3.72 : *Soient G un groupe profini et $g \in G$. Il existe alors un unique morphisme continu $\varphi : \widehat{\mathbb{Z}} \to G$ tel que $\varphi(\sigma) = g$.*

Démonstration. Soit $H \leqslant G$ un sous groupe ouvert normal. Soit n_H l'ordre de gH dans G/H. On note $\varphi_H : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}/\overline{\langle\sigma^{n_H}\rangle} \cong \mathbb{Z}/n_H\mathbb{Z} \to G/H$ le morphisme naturel qui envoit σ sur gH. Ces morphismes sont compatibles et on obtient alors bien un morphisme $\varphi : \widehat{\mathbb{Z}} \to \varprojlim_H G/H \cong G$ qui envoie σ sur g. De plus, φ est continu puisque que pour tout $H \leqslant G$ ouvert normal, $\varphi^{-1}(H) = \ker(\varphi_H) = \overline{\langle\sigma^{n_H}\rangle}$ qui est ouvert. □

Corollaire 3.73 : *Soit G un groupe profini. Sont équivalents :*

1. *G a exactement un sous groupe ouvert d'indice n pour tout n ;*
2. *$G \cong \widehat{\mathbb{Z}}$.*

Démonstration.

$1 \Rightarrow 2$ Par la Proposition **(3.69)**, on trouve $g \in G$ un générateur topologique. Par la Proposition **(3.72)**, il existe $\varphi : \widehat{\mathbb{Z}} \to G$ un morphisme continu qui envoie un générateur topologique $\sigma\widehat{\mathbb{Z}}$ sur g. En reprenant les notations de la preuve de la Proposition **(3.72)**, $\ker(\varphi) = \bigcap_{H \leqslant G \text{ ouvert}} \ker(\varphi_H) = \bigcap_H \overline{\langle\sigma^{n_H}\rangle}$. Par la Proposition **(3.68)**, l'unique sous groupe ouvert $H \leqslant G$ d'indice n est de la forme $\overline{g^n}$ et donc $n_H = n$. On a donc $\ker(\varphi) \leqslant \bigcap_n \overline{\langle\sigma^n\rangle} = \{0\}$.

$2 \Rightarrow 1$ Cela suit immédiatement de la Proposition **(3.68)**. □

Par la correspondance de Galois, on a l'équivalence suivante :

Corollaire 3.74 : *Soit F un corps. Sont équivalents :*

1. *F a exactement une extension séparable de degré n pour tout n ;*
2. *$\mathcal{G}(F) \cong \widehat{\mathbb{Z}}$.*

Proposition 3.75 : *Soit G et H deux groupes procycliques et $\varphi : G \to H$ un morphisme continu surjectif. Pour tout générateur topologique $h \in H$, il existe un générateur topologique $g \in G$ tel que $\varphi(g) = h$.*

Démonstration. Supposons tout d'abord que G est fini, ce qui implique que H l'est aussi. Soit $m, n \in \mathbb{Z}_{>0}$ avec m maximal tel que $cardG = mn$ et $m \wedge |H| = 1$. On remarque que $|H|$ divise n et donc $\varphi(g^n) = \{0\}$. Comme $G = \langle g^n\rangle\langle g^m\rangle$, Il s'ensuit que $\varphi : \langle g^m\rangle \to H$ est surjective. Il existe donc i premier à $|H|$ (et donc à n) tel que $\varphi(g^m)^i = h$. On vérifie alors que g^{mi+n} est un générateur de G et que $\varphi(g^{mi+n}) = h$.
Revenons au cas général. Pour tout sous-groupe ouvert $L \leqslant H$, φ induit un morphisme $G/\varphi^{-1}(L) \to H/L$. L'ensemble $X_L := \{g \in G : g$ est un générateur topologique de G et $\varphi(g) \in hL\}$ est un

fermé non vide. Pour tous $L_i \leqslant H$ ouverts, on a $X_{\bigcap_{i\leqslant n} L_i} \subseteq \bigcap_{i\leqslant n} X_{L_i}$ qui est donc non vide. Par compacité $\bigcap_L X_L \neq \varnothing$. On remarque que tout élément de cet ensemble est un générateur topologique de $g \in G$ tel que $\varphi(g) = h$. □

Théorème 3.76 : *Soient $K, L \vDash \mathrm{PSF}$, $A \leqslant K$ et $\varphi : A \to L$ un morphisme injectif. Sont équivalents :*

1. *φ est K-élémentaire ;*
2. *φ s'étend en un isomorphisme $A_{(0)} \cap K \cong_A \varphi(A)^{\mathrm{a}}_{(0)} \cap L$.*

Démonstration.

1 ⇒ 2 TO DO

2 ⇒ 1 Soit $F := A^{\mathrm{a}}_{(0)} \cap K$, $E = \varphi(A)^{\mathrm{a}}_{(0)} \cap L$. On note encore φ l'isomorphisme $F \cong E$ qui étend φ. Comme $\mathrm{res} : \widehat{\mathbb{Z}} \cong \mathcal{G}(K) \to \mathcal{G}(F)$ est surjectif, l'image d'un générateur topologique $\sigma \in \mathcal{G}(K)$ est un générateur topologique $\tau \in \mathcal{G}(F)$. Comme $\varphi^\star : \mathcal{G}(E) \to \mathcal{G}(F)$ est un homéomorphisme, $\varphi^\star(\tau) \in \mathcal{G}(E)$ est un générateur topologique. Par la Proposition **(3.75)**, on trouve $\rho \in \mathcal{G}(L) \cong \widehat{\mathbb{Z}}$ tel que $\mathrm{res}(\rho) = \varphi^\star(\tau)$. Par la Proposition **(3.72)**, il existe $\Psi : \mathcal{G}(L) \to \mathcal{G}(K)$ qui envoie ρ sur σ ; c'est un homéomorphisme d'inverse l'unique morphisme $\mathcal{G}(K) \to \mathcal{G}(L)$ qui envoie σ sur ρ. De plus, comme $\mathrm{res}(\Psi(\rho)) = \varphi^\star(\tau) = \varphi^\star(\mathrm{res}(\sigma))$, on a, par unicité, que $\mathrm{res} \circ \Psi = \varphi^\star \circ \mathrm{res}$. Par la Proposition **(3.56)**, φ est K-élémentaire. □

Corollaire 3.77 : *Soient $K, L \vDash \mathrm{PSF}$, k et ℓ leurs corps premiers respectifs. Sont équivalents :*

1. *$K \equiv L$;*
2. *$k^{\mathrm{a}} \cap K \cong \ell^{\mathrm{a}} \cap L$.*

Démonstration.

1 ⇒ 2 Comme $K \equiv L$ ils ont la même caractéristique et donc il existe un morphisme K-élémentaire $\varphi : k \cong \ell \leqslant L$. Par le Théorème **(3.76)**, Il s'étend en un isomorphisme $k^{\mathrm{a}} \cap K \cong \ell^{\mathrm{a}} \cap L$.

2 ⇒ 1 Le morphisme $k^{\mathrm{a}} \cap K \cong \ell^{\mathrm{a}} \cap L \leqslant L$ est K-élémentaire par le Théorème **(3.76)**. Il s'ensuit immédiatement que $K \equiv L$. □

3.7 Extensions procycliques des corps premiers

Proposition 3.78 : *Soit $F \leqslant \mathbb{F}_p^{\mathrm{a}}$. Il existe un ultraproduit non principal $\mathfrak{U}$ sur $\mathbb{Z}_{>0}$ tel que $(\prod_{n\to\mathfrak{U}} \mathbb{F}_{p^n}) \cap \mathbb{F}_p^{\mathrm{a}} \cong F$.*

Démonstration. Si F est infini, soient $I \subseteq \mathbb{Z}_{>0}$ tel que $F \cong \bigcup_i \mathbb{F}_{p^i}$ et pour tout $i < j \in I, \mathbb{F}_{p^i} \subseteq \mathbb{F}_{p^j}$. Si F est fini de degré n sur $\mathbb{F}_p$, soit I l'ensemble (infini) des entiers de la forme nq où q ne divise pas n. Soit $\mathfrak{U}$ un ultrafiltre non principal sur $\mathbb{Z}_{>0}$ qui contient I et $K := \prod_{i\to\mathfrak{U}} \mathbb{F}_{p^i}$. Pour tout $m \in \mathbb{Z}_{>0}$, on a $\mathbb{F}_{p^m} \leqslant K$ si et seulement si $X^{p^m} - X$ a une racine dans K si et seulement s'il existe $V \in \mathfrak{U}$ tel que $V \subseteq I$ et pour tout $i \in V$, $X^{p^m} - X$ a une racine dans $\mathbb{F}_{p^i}$, c'est à dire $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^i} \subseteq F$. Si F est infini, comme les $(\mathbb{F}_{p^i})_{i\in I}$ forment une chaîne, cela est équivalent au fait que $\mathbb{F}_{p^m} \subseteq \bigcup_{i\in I} \mathbb{F}_{p^i} = F$. Si F est fini, comme, pour tout $i \neq j \in I$, $\mathbb{F}_{p^i} \cap \mathbb{F}_{p^j} = F$, cela est aussi équivalent au fait que $\mathbb{F}_{p^m} \subseteq \bigcap_{i\in I} \mathbb{F}_{p^i} = F$. On a donc bien $K \cap \mathbb{F}_p^{\mathrm{a}} \cong F$. □

Le résultat équivalent en caractéristique nulle nécessite des outils supplémentaires.

Soit $\mathbb{Q} \leqslant F$ une extension finie normale. On note $\mathcal{O} \leqslant F$ la clôture intégrale de $\mathbb{Z}$ dans F — c'est l'ensemble des racines dans F de polynômes unitaires $f \in \mathbb{Z}[X]$. On a $\mathcal{O}_{(0)} = F$. Pour tout premier $p \in \mathbb{Z}$, il existe un idéal maximal $\mathfrak{p} \subseteq \mathcal{O}$ tel que $\mathfrak{p} \cap \mathbb{Z} = (p)$. On note $k_\mathfrak{p} = \mathcal{O}/\mathfrak{p}$. C'est une extension finie de $\mathbb{F}_p$. De plus les idéaux maximaux $\mathfrak{p} \subseteq \mathcal{O}$ au dessus de p sont conjugués sous l'action de $\mathcal{G}(F/\mathbb{Q})$. On note $\mathcal{D}_\mathfrak{p} := \{\sigma \in \mathcal{G}(F/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}$, le groupe de décomposition de $\mathfrak{p}$, et $F_\mathfrak{p} = F^{\mathcal{D}_\mathfrak{p}}$, le corps de décomposition de $\mathfrak{p}$. On peut vérifier que le morphisme naturel $\mathrm{res}_\mathfrak{p} : \mathcal{D}_\mathfrak{p} \to \mathcal{G}(k_\mathfrak{p}/\mathbb{F}_p)$ est surjectif. Si c'est un homéomorphisme, on dit que F est non ramifié en p. On peut vérifier que F n'est ramifié qu'en un nombre fini de premiers.

Si F est non ramifié en p et $\mathfrak{p} \subseteq F$ est au dessus de p, on note $\left[\frac{F/\mathbb{Q}}{\mathfrak{p}}\right] \in \mathcal{D}_\mathfrak{p}$ l'unique relèvement du morphisme de Frobenius sur $k_\mathfrak{p}$. Comme les idéaux maximaux au dessus de p sont conjugués par $\mathcal{G}(F/\mathbb{Q})$, la classe de conjugaison de $\left[\frac{F/\mathbb{Q}}{\mathfrak{p}}\right] \in \mathcal{D}_\mathfrak{p}$ dans $\mathcal{G}(F/\mathbb{Q})$ ne dépend que de p. On la note $\left(\frac{F/\mathbb{Q}}{p}\right) \subseteq \mathcal{G}(F/\mathbb{Q})$.

Soit $A \subseteq \mathbb{P}$, on note $\delta(A)$ la limite $\lim_{s\to 1^+} \frac{\sum_{p\in A} p^{-s}}{\sum_{p\in\mathbb{P}} p^{-s}}$, quand elle existe. On remarque que, puisque $\sum_{p\in\mathbb{P}} p^{-1} = \infty$, si A est fini, $\delta(A) = 0$.

Théorème 3.79 (Théorème de Densité, Chebotarev, 1922) **:** *Soit $C \subseteq \mathcal{G}(F/\mathbb{Q})$ une classe de conjugaison. On a :*

$$\delta(\{p \in \mathbb{P} : \left(\frac{F/\mathbb{Q}}{p}\right) = C\}) = |C|/[F : \mathbb{Q}]$$

Corollaire 3.80 : *Soit $E \leqslant F$ tel que $\mathcal{G}(F/E)$ est cyclique. L'ensemble des p tels qu'il existe $\mathfrak{p} \subseteq \mathcal{O}$ maximal au dessus de p avec $F_\mathfrak{p} = E$ est infini.*

Démonstration. Soit $\tau \in \mathcal{G}(F/E)$ un générateur. Pour tout $p \in \mathbb{P}$ et $\mathfrak{p} \subseteq \mathcal{O}$ maximal au dessus de p, si $\tau = \left[\frac{F/\mathbb{Q}}{\mathfrak{p}}\right]$, on a alors $E = F^\tau = F^{\mathcal{D}_\mathfrak{p}} = F_\mathfrak{p}$. Il s'ensuit que $\{p \in \mathbb{P} : \exists \mathfrak{p}$ maximal au dessus de p tel que $E = F_\mathfrak{p}\} \supseteq \{p \in \mathbb{P} : \tau \in \left(\frac{F/\mathbb{Q}}{p}\right)\} \neq \emptyset$, par le théorème de densité de Chebotarev — Théorème **(3.79)**. □

Proposition 3.81 : *Soient $f \in \mathbb{Z}[X]$ scindé sur F et p premier tel que f a $\deg(f)$ racines simples modulo p. Soit aussi $\mathfrak{p} \subseteq F$ maximal au dessus de p. Sont équivalents :*

1. *f a une racine dans $F_\mathfrak{p}$;*
2. *f a une racine dans $\mathbb{F}_p$.*

Démonstration. Soient $(a_i)_{i<\deg(f)} \in F$ les racines de f, avec multiplicité. Comme $\mathcal{O}$ est intégralement clos, $a_i \in \mathcal{O}$. Soit $\pi : \mathcal{O} \to k_\mathfrak{p}$ la surjection canonique. On alors $f(\pi(a_i)) = \pi(f(a_i)) = 0$ et donc les $\pi(a_i)$ sont les $\deg(f)$ racines distinctes de f dans $k_\mathfrak{p}$. Il s'ensuit que si $\pi(a_i) = \pi(a_j)$, on a alors $i = j$.

On a alors $a_i \in F_\mathfrak{p}$ si et seulement si, pour tout $\sigma \in \mathcal{D}_\mathfrak{p}$, $\sigma(a_i) = a_i$. On a alors $\mathrm{res}_\mathfrak{p}(\sigma)(\pi(a_i)) = \pi(\sigma(a_i)) = a_i$ et donc, comme $\mathrm{res}_\mathfrak{p}$ est surjectif, $\pi(a_i) \in \mathbb{F}_p$. Réciproquement, si $\pi(a_i) \in \mathbb{F}_p$, $\pi(\sigma(a_i)) = \mathrm{res}_\mathfrak{p}(\sigma)(\pi(a_i)) = \pi(a_i)$ et donc $\sigma(a_i) = a_i$, d'où $a_i \in F_\mathfrak{p}$. □

Corollaire 3.82 : *Soient $F \leqslant \mathbb{Q}^{\mathrm{a}}$ un sous-corps dont le groupe de Galois est procyclique, $f_i, g_j \in \mathbb{Z}[X]$ tels que $F \vDash \bigwedge_{i\leqslant n} \exists x\, f_i(x) \simeq 0 \wedge \bigwedge_{j\leqslant m} \forall x\, g_j(x) \not\simeq 0$. Alors l'ensemble des p tels que $\mathbb{F}_p \vDash \bigwedge_{i\leqslant n} \exists x\, f_i(x) \simeq 0 \wedge \bigwedge_{j\leqslant m} \forall x\, g_j(x) \not\simeq 0$ est infini.*

Démonstration. Soit $\mathbb{Q} \leqslant N_0$ une extension normale au dessus de laquelle tous les f_i et g_j sont scindés. Comme $\mathcal{G}(F)$ est procyclique, $F \leqslant FN_0$ est normale cyclique. On trouve alors $F_0 \leqslant F$ une extension finie de $\mathbb{Q}$ telle $F_0 \leqslant F_0N_0$ est normale cyclique et F_0 contient une racine de chaque f_i. Soient alors $\mathbb{Q} \leqslant N$ une extension normale finie contenant F_0N_0, $\tau \in \mathcal{G}(N/\mathbb{Q})$ qui étend un générateur de $\mathcal{G}(F_0N_0/F_0)$ et $M := N^{\tau}$. L'extension $M \leqslant N$ est alors cyclique. Comme $F_0 \leqslant M$, $M \vDash \bigwedge_{i \leqslant n} \exists x\, f_i(x) \simeq 0$. De plus, si M contient une racine a d'un des g_j, on a alors $a \in N_0 \cap M \leqslant F_0N_0 \cap M = F_0 \leqslant F$, une contradiction. Il s'ensuit que $M \vDash \forall x\, g_j(x) \not\simeq 0$. Par le Corollaire **(3.80)**, l'ensemble des premiers p tels que N est non ramifié en p, tous les f_i et g_j n'ont que des racines simples, et leur degré ne diminue pas, modulo p et tels que $N_{\mathfrak{p}} = M$ pour un $\mathfrak{p} \subseteq N$ au dessus de p est infini. Pour de tels p, par la Proposition **(3.81)**, $\mathbb{F}_p \vDash \bigwedge_{i \leqslant n} \exists x\, f_i(x) \simeq 0 \wedge \bigwedge_{j \leqslant m} \forall x\, g_j(x) \not\simeq 0$. □

Corollaire 3.83 : *Soit $F \leqslant \mathbb{Q}^{\mathrm{a}}$ un sous-corps dont le groupe de Galois est procyclique. Il existe un ultraproduit non principal $\mathfrak{U}$ sur $\mathbb{P}$ tel que $(\prod_{p \to \mathfrak{U}} \mathbb{F}_p) \cap \mathbb{Q}^{\mathrm{a}} \cong F$.*

Démonstration. Pour tout $P \in \mathbb{Z}[x]$, $|x| = 1$, soit $[\![P]\!] := \{p \in \mathbb{P} : \mathbb{F}_p \vDash \exists x\, P \simeq 0\}$ et $[\![\neg P]\!] := \{p \in \mathbb{P} : \mathbb{F}_p \vDash \forall x\, P \not\simeq 0\}$. Pour tout $N \in \mathbb{Z}_{\geqslant 0}$, soit $[\![\geqslant N]\!] := \{p \in \mathbb{P} : p \geqslant N\}$. Soit $X = \{[\![P \simeq 0]\!] : F \vDash \exists x\, P \simeq 0\} \cup \{[\![\neg P]\!] : F \vDash \forall x\, P \not\simeq 0\} \cup \{[\![\geqslant N]\!] : N \in \mathbb{Z}_{\geqslant 0}\}$. Par le Corollaire **(3.82)**, X est une base de filtre et on trouve donc un ultrafiltre $\mathfrak{U}$ qui le contient. Soit $K := \prod_{p \to \mathfrak{U}} \mathbb{F}_p$. Pour tout $P \in \mathbb{Z}[X]$, par Łoś, $F \vDash \exists x\, P \simeq 0$ si et seulement si $K \vDash \exists x\, P \simeq 0$. Par la Proposition **(3.58)**, il existe des morphismes d'anneaux $f : F \to K$ et $g : K \to F$. La composition $g \circ f$ est un plongement de F dans lui-même. Comme F est une extension algébrique de $\mathbb{Q}$, $g \circ f$ doit être surjectif, et donc f est un isomorphisme. □

Théorème 3.84 (Ax, 1968) **:** *Soit K un corps de caractéristique p positive. Sont équivalents :*

1. *$K \vDash$ PSF ;*
2. *Il existe un ultrafiltre non principal $\mathfrak{U}$ sur $\mathbb{Z}_{>0}$ tel que $K \equiv \prod_{n \to \mathfrak{U}} \mathbb{F}_{p^n}$.*

Si K est de caractéristique nulle, sont équivalents :

1. *$K \vDash$ PSF ;*
2. *Il existe un ultrafiltre non principal $\mathfrak{U}$ sur $\mathbb{P}$ tel que $K \equiv \prod_{p \to \mathfrak{U}} \mathbb{F}_p$.*

Démonstration. Soit $K \vDash$ PSF de caractéristique $p > 0$. Par la Proposition **(3.78)**, il existe un ultrafiltre non principal $\mathfrak{U}$ sur $\mathbb{Z}_{>0}$ tel que $(\prod_{n \to \mathfrak{U}} \mathbb{F}_{p^n}) \cap \mathbb{F}_p^{\mathrm{a}} \cong K \cap \mathbb{F}_p^{\mathrm{a}}$. Par la Proposition **(3.34)**, $\prod_{n \to \mathfrak{U}} \mathbb{F}_{p^n} \vDash$ PSF et donc, par le Corollaire **(3.77)**, $K \equiv \prod_{n \to \mathfrak{U}} \mathbb{F}_{p^n}$. Réciproquement, si $\mathfrak{U}$ est non principal, on a $K \equiv \prod_{n \to \mathfrak{U}} \mathbb{F}_{p^n} \vDash$ PSF.
Soit $K \vDash$ PSF de caractéristique 0. Comme $\mathcal{G}(K) \to \mathcal{G}(K \cap \mathbb{Q}^{\mathrm{a}})$ est surjectif, ce dernier groupe est procyclique et donc, par le Corollaire **(3.83)**, il existe un ultrafiltre non principal $\mathfrak{U}$ sur $\mathbb{P}$ tel que $(\prod_{p \to \mathfrak{U}} \mathbb{F}_p) \cap \mathbb{Q}^{\mathrm{a}} \cong K \cap \mathbb{F}_p^{\mathrm{a}}$. Comme $\prod_{p \to \mathfrak{U}} \mathbb{F}_p \vDash$ PSF, on a donc $K \equiv \prod_{p \to \mathfrak{U}} \mathbb{F}_p$. Réciproquement, si $\mathfrak{U}$ est non principal, on a $K \equiv \prod_{p \to \mathfrak{U}} \mathbb{F}_p \vDash$ PSF. □

Corollaire 3.85 : *Soit φ un $\mathbb{Z}$-énoncés. Sont équivalents :*

1. *PSF $\vDash \varphi$;*
2. *il existe $N \in \mathbb{Z}_{>0}$ tel que, pour tout corps fini F avec $|F| \geqslant N$, $F \vDash \varphi$.*

Démonstration. TO DO □

Soit $\mathrm{PSF}_0 := \mathrm{PSF} \cup \{p \not\simeq 0 : p \in \mathbb{P}\}$.

Corollaire 3.86 : *Soit φ un $\mathbb{Z}$-énoncés. Sont équivalents :*

1. $\mathrm{PSF}_0 \models \varphi$;
2. *il existe* $N \in \mathbb{Z}_{>0}$ *tel que, pour tout corps fini* F *avec* $\mathrm{car}(F) \geqslant N$, $F \models \varphi$.
3. *il existe* $N \in \mathbb{Z}_{>0}$ *tel que, pour tout* $p \in \mathbb{P}$ *avec* $p \geqslant N$, $\mathbb{F}_p \models \varphi$.

Démonstration. TO DO □

Soit $\mathrm{PSF}_p := \mathrm{PSF} \cup \{p \simeq 0\}$.

Corollaire 3.87 : *Soit* φ *un* $\mathbb{Z}$*-énoncés. Sont équivalents :*

1. $\mathrm{PSF}_p \models \varphi$;
2. *il existe* $N \in \mathbb{Z}_{>0}$ *tel que, pour tout* $n \in \mathbb{Z}_{>0}$ *avec* $n \geqslant N$, $\mathbb{F}_{p^n} \models \varphi$.

Démonstration. TO DO □

4 Comptage dans les corps finis

4.1 Approximations de Chatzidakis-van den Dries-Macintyre

On commence par généraliser la notion de dimension à tous les ensembles définissables dans ACF.

Définition 4.1 : *Soit* $K \models \mathrm{ACF}$ *et* $\varphi \in \mathcal{F}_K(\overline{x})$. *On définit* $\dim_K(\varphi) := \{\mathrm{trdeg}(\overline{a}/K) : \overline{a} \in \varphi(N)$ *où* $K \preccurlyeq N\}$.

Lemme 4.2 : *Soit* $K \preccurlyeq N \models \mathrm{ACF}$ *et* $\varphi \in \mathcal{F}_K(\overline{x})$. *On a alors* $\dim_K(\varphi) = \dim_N(\varphi)$.

On la notera donc simplement $\dim(\varphi)$.

Démonstration. Soit $M \succcurlyeq N$ et $c \in \varphi(M)$ tel que $\mathrm{trdeg}(c/N) = \dim_N(\varphi)$. On a alors $M \succcurlyeq K$ et $\mathrm{trdeg}(c/K) \geqslant \dim_N(\varphi)$ et donc $\dim_K(\varphi) \geqslant \dim_N(\varphi)$.
Soit maintenant $M \succcurlyeq K$ et $c \in \varphi(M)$ tel que $\mathrm{trdeg}(c/K) = \dim_K(\varphi)$. Par le Lemme **(2.52)**, il existe un morphisme (élémentaire) de K-algèbre $f : M \to N^\star$, où $N^\star \succcurlyeq N$, tel que $f(M) \downarrow_K^{\mathrm{alg}} N$. On a donc $N^\star \models \varphi(f(c))$ et $\mathrm{trdeg}(f(c)/N) = \mathrm{trdeg}(c/K) = \dim_K(\varphi)$ et donc $\dim_N(\varphi) \geqslant \dim_K(\varphi)$. □

Remarque 4.3 :

- $\dim(\varphi) \leqslant |\overline{x}|$.
- Si $\varphi(K)$ est un K-fermé de Zariski K-intègre, les dimensions de φ en tant qu'ensemble définissable et en tant que variété coincident.

Proposition 4.4 (Définissabilité de la dimension) **:** *Pour tout* $\varphi \in \mathcal{F}_{\mathbb{Z}}(x, y)$ *et* $d \leqslant |x|$, *il existe* $\theta_d(y) \in \mathcal{F}_{\mathbb{Z}}^{\mathrm{qf}}(y)$ *telle que pour tout corps* $K \models \mathrm{ACF}$ *et tout* $a \in K^y$, $K \models \theta_d(a)$ *si et seulement si* $\dim(\varphi(x, a)) = d$.

Démonstration. On prouve par induction sur $|x|$ que pour tout $d < |x|$, il existe $\theta_{>d} \in \mathcal{F}_{\mathbb{Z}}(y)$ telle que pour tout corps $K \models \mathrm{ACF}$ et tout $a \in K^y$, $K \models \theta_{>d}(a)$ si et seulement si $\dim(\varphi(x, a)) > d$.

Assertion 4.5 : *Soient* $K \models \mathrm{ACF}$ *et* $a \in K^y$. *Sont équivalents :*

1. $\varphi(K, a)$ *est fini ;*
2. *pour tout* $N \succcurlyeq K$, $\varphi(N, a) \subseteq F^x$, *où* $F := \mathbb{Z}[a]^{\mathrm{a}}_{(0)} \leqslant K$;

3. $\dim(\varphi(x,a)) = 0$.

Si, de plus, $|x| = 1$*, ces énoncés sont équivalents à :*

4. $\neg\varphi(K,a)$ *est infini.*

Démonstration.

$1 \Rightarrow 2$ Comme $F \preccurlyeq K \preccurlyeq N$, $|\varphi(N,a)| \leqslant |\varphi(F,a)|$ et donc $\varphi(N,a) = \varphi(F,a) \subseteq F^x$.

$2 \Rightarrow 3$ Pour tout $c \in \varphi(N,a)$ on a alors $\operatorname{trdeg}(c/K) = 0$ et donc, $\dim(\varphi(x,a)) = 0$.

$3 \Rightarrow 1$ Par définition de dim, le type partiel $\pi(x) \coloneqq \{\varphi(x,a)\} \cup \{x \neq c : c \in K^x\}$ est inconsistant. Il est donc finiment inconsistant : il existe $(c_i)_{i<m} \in F^x$ tels que $K \vDash \forall x, \varphi(x,a) \to \bigvee_{i<m} x \simeq c_i$ et donc $\varphi(K,a) \subseteq \{c_i : i < m\}$ est fini.

$1 \Rightarrow 4$ Cela suit immédiatement du fait que K est infini.

$4 \Rightarrow 2$ Si $b \in N \succcurlyeq K$ et $c \in M \succcurlyeq K$ ne sont pas dans F, $F[b] \cong F[x] \cong F[c]$ et donc, par élimination des quantificateurs and ACF, $N \vDash \neg\varphi(b,a)$ si et seulement si $M \vDash \neg\varphi(c,a)$. De plus, comme $\neg\varphi(K,a)$ est infini, par compacité, il existe $c \in M \succcurlyeq K$ tel que $c \notin F$ et $M \vDash \neg\varphi(c,a)$. On a donc bien $\varphi(N,a) \subseteq F$. ◊

Assertion 4.6 : *Il existe* $d \in \mathbb{Z}_{\geqslant 0}$ *— qui ne dépend que de* φ *— tel que, pour tout* $K \vDash$ ACF*, si* $|\varphi(K,a)| \geqslant d$ *alors* $\varphi(K,a)$ *est infini.*

Démonstration. On suppose tout d'abord que $|x| = 1$. Si un tel d n'existe pas, pour tout $d \in \mathbb{Z}_{\geqslant 0}$, il existe $K_d \vDash$ ACF et $a_d \in K_d^y$ tel que $\varphi(K_d, a_d)$ est fini — en particulier, $\neg\varphi(K_d, a_d)$ est infini— mais $|\varphi(K_d, a_d)| \geqslant d$. Soit $\mathfrak{U}$ un ultrafiltre non principal sur $\mathbb{Z}_{\geqslant 0}$, $K \coloneqq \prod_{d \to \mathfrak{U}} K_d$ et $a \coloneqq \prod_{d \to \mathfrak{U}} a_d \in K^y$. Par Łoś, $|\varphi(K,a)| \geqslant d$ pour tout $d \in \mathbb{Z}_{\geqslant 0}$ et $\neg\varphi(K,a)$ est infini, ce qui contredit l'équivalence de 1 et 4 and l'Assertion **(4.5)**.

Dans le cas général, soit $(\pi_i)_{i<|x|}$ la projection sur la i-ème coordonnée et soit d_i la constant associée à $\pi_i(\varphi(K,a))$. On a alors que si $\varphi(K,a) \geqslant \prod_i d_i$, il existe alors i tel que $\pi_i(\varphi(K,a))$ est infini et donc $\varphi(K,a)$ est infini. ◊

On a donc $\dim(\varphi(x,a)) > 0$ si et seulement si $|\varphi(K,a)| \geqslant d$, *i.e.* $K \vDash \exists x_1 \cdots \exists x_d \bigwedge_i \varphi(x_i, a) \wedge \bigwedge_{i \neq j} x_i \neq x_j$. Si $|x| = 1$ on a donc fini. On suppose donc $|x| > 1$ et on note x_0 la première coordonnée de x.

Assertion 4.7 : *Soient* $K \vDash$ ACF *et* $a \in K^y$*. Sont équivalents :*

1. $\dim(\varphi(x,a)) > d$*;*

2. l'un des deux énoncés suivant (au moins) est vrai :

- $\dim(\exists x_0\, (\varphi(x,a))) > d$*;*
- $\dim(\zeta(x_{>0}, a)) \geqslant d$ *où* $\zeta(x_{>0}, y)$ *est tel que pour tout* $N \vDash$ ACF*, et tout* $c_{>0} \in N^{x_{>0}}$ *et* $a \in N^y$*,* $N \vDash \zeta(c_{>0}, a)$ *si et seulement si* $\dim(\varphi(x_0, c_{>0}, a)) = 1$.

Démonstration.

$1 \Rightarrow 2$ Soit $N \succcurlyeq K$ et $c \in \varphi(N,a)$ tels que $\operatorname{trdeg}(c/K) > d$. Si $\operatorname{trdeg}(c_0/K(c_{>0})) = 0$, puisque $\operatorname{trdeg}(c/K) = \operatorname{trdeg}(c_0/K(c_{>0})) + \operatorname{trdeg}(c_{>0}/K)$, on a alors $\operatorname{trdeg}(c_{>0}/K) > d$ et donc $\dim(\exists x_0\, (\varphi(x,a))) > d$. Si $\operatorname{trdeg}(c_0/K(c_{>0})) = 1$, on a $\zeta_0(c_{<0}, a)$ et $\operatorname{trdeg}(c_{>0}/K) \geqslant d$, d'où $\dim(\zeta_0(x_{>0}, a)) \geqslant d$.

$2 \Rightarrow 1$ Supposons tout d'abord que $\dim(\exists x_0\, (\varphi(x,a))) > d$. On trouve alors $N \succcurlyeq K$ et $c_{>0} \in \exists x_0\, \varphi(x_0, N, a)$ tel que $\operatorname{trdeg}(c_{>0}/K) > d$. Soit $c_0 \in N$ tel que $N \vDash \varphi(c,a)$. On a alors $\operatorname{trdeg}(c/K) = \operatorname{trdeg}(c_0/K(c_{>0})) + \operatorname{trdeg}(c_{>0}/K) > d$.

Supposons maintenant $\dim(\zeta_0(x_{>0},a)) \geqslant d$. Il existe donc $N \succcurlyeq K$ et $c_{>0} \in \zeta_0(F,a)$ tels que $\operatorname{trdeg}(c_{>0}/K) \geqslant d$. On a alors $\dim(\varphi(x_0,c_{>0},a)) = 1$ et on trouve donc $M \succcurlyeq K$ et $c_0 \in \varphi(M,c_{>0},a)$. Il s'ensuit que $\operatorname{trdeg}(c/K) = \operatorname{trdeg}(c_0/K(c_{>0})) + \operatorname{trdeg}(c_{>0}/K) > d$ et donc, comme $c \in \varphi(M,a)$, donc $\dim(\varphi(x,a)) > d$.

◊

L'existence de $\theta_{>d}$ est alors évidente. On pose alors $\theta_d \coloneqq \theta_{>d-1} \wedge \neg\theta_{>d}$. □

Proposition 4.8 : *Soit F un corps et V une F-variété. Il existe un plus petit corps $k \leqslant F$ tel que $\mathcal{I}_F(V) = F \cdot \mathcal{I}_k(V) \subseteq F[\overline{x}]$. De plus, pour tout $\sigma \in \operatorname{Aut}(F)$, sont équivalents :*

1. $\sigma(V) = V$ — i.e. *l'homéomorphisme induit par σ sur $\mathcal{S}^{\mathrm{Zar}}(F)$ fixe V globalement ;*
2. $\sigma|_k = \mathrm{id}_k$.

Démonstration. Soit M l'ensemble des monômes en $\overline{x}$ et $B \subseteq M$ une base de $F[\overline{x}]/\mathfrak{a}$ où $\mathfrak{a} \coloneqq \mathcal{I}_F(V)$. Pour tout $\gamma \in M$, on trouve des $a_{\gamma,\beta} \in F$ tels que $f_\gamma \coloneqq \gamma - \sum_{\beta\in B} a_{\gamma,\beta}\beta \in \mathfrak{a}$.

Assertion 4.9 : $\mathfrak{a} = (f_\gamma : \gamma \in M)$.

Démonstration. Soit $f \in \mathfrak{a}$. On peut écrire $f = \sum_{\gamma\in M} c_\gamma\gamma = \sum_{\gamma\in M} c_\gamma(\gamma - \sum_{\beta\in B} a_{\gamma,\beta}\beta) + \sum_{\beta\in B} d_\beta\beta$, où $d_\beta \coloneqq \sum_{\gamma\in M} c_\gamma a_{\gamma,\beta}$. On a alors $\sum_{\beta\in B} d_\beta\beta = f - \sum_{\gamma\in M} f_\gamma \equiv 0 \mod \mathfrak{a}$ et donc, comme B est une base de $F[\overline{x}]/\mathfrak{a}$, $d_\beta = 0$. Il s'ensuit que $f = \sum_{\gamma\in M} c_\gamma f_\gamma$. ◊

Soit $k \leqslant F$ le corps engendré par les $a_{\gamma,\beta}$. On vient de montrer que $\mathfrak{a}$ est défini sur k.

Assertion 4.10 : *Soit $E \leqslant F$ tel que $\mathfrak{a}$ soit défini sur E, on a $k \leqslant E$.*

Démonstration. Soient $g_i \in E[\overline{x}]$ tels que $\mathfrak{a} = F(g_i : i \leqslant n)$. Pour tout $\delta \in M$, il on trouve alors des $h_i = \sum_{\gamma\in M} c_{i,\gamma}\gamma \in F[\overline{x}]$ tels que $f_\delta = \sum_i h_i g_i$. Soit $H_i = \sum_\gamma Y_{i,\gamma}\gamma \in E[\overline{x},\overline{Y}]$ et $L \in E[\overline{Y}]_{\leqslant 1}$ tels que $\sum_i H_i g_i = \sum_\gamma L_\gamma\gamma$. Les $c_{i,\gamma}$ sont une solution du système d'équations sur E, $L_\delta = 1$ et $L_\gamma = 0$ pour tout $\gamma \in M \smallsetminus (B \cup \{\delta\})$. Comme l'extension $E \leqslant F$ est fidèlement plate, on trouve une solution dans E. Il existe donc $l_i \in E[\overline{x}]$ et $b_\beta \in E$ tels que $\sum_{\beta\in B} a_{\delta,\beta}\beta \equiv \delta = \sum_i l_i g_i + \sum_{\beta\in B} b_\beta\beta \equiv \sum_{\beta\in B} b_\beta\beta \mod \mathfrak{a}$. Par unicité des b_β, on a $a_{\delta,\beta} = b_\beta \in E$. ◊

Soit maintenant $\sigma \in \operatorname{Aut}(F)$. On peut vérifier que $\sigma(V) = V$ si et seulement si $\sigma(\mathfrak{a}) = \mathfrak{a}$ — en effet, $V = \bigcap_{P\in\mathfrak{a}}[P \simeq 0]$ et $\mathcal{I}_F(\sigma(V)) = \sigma(\mathcal{I}_F(V)) = \sigma(\mathfrak{a})$. Comme $\mathfrak{a}$ est défini sur k, $\sigma|_k = \mathrm{id}_k$ implique bien que $\sigma(\mathfrak{a}) = \mathfrak{a}$. Réciproquement, si $\sigma(\mathfrak{a}) = \mathfrak{a}$, σ induit un morphisme de F-espace vectoriel sur $F[\overline{x}]/\mathfrak{a}$ qui fixe M point par point. Il fixe donc les coefficients $a_{\gamma,\beta}$ de $\gamma \in M$ dans la base B, et il fixe donc k point par point. □

Proposition 4.11 : *Soit F un corps parfait et V une F-variété. Il existe des F-variétés $W_i \subseteq V$ géométriquement intègres définie sur F, tels que $V(F) = \bigcup_{i\leqslant n} W_i(F)$.*

Démonstration. On procède par induction sur $\dim(V)$. Soient $(V_j)_{j<m}$ les composantes F^{a}-intègres de V — *i.e.* les $V_j \subseteq V$ sont des F^{a}-fermés F^{a}-intègres et $V = \bigcup_{j<m} V_j$. Pour tout j, on note $W_j = \bigcap_{\sigma\in\mathcal{G}(F)} \sigma(V_j)$. Pour tout $\sigma \in \operatorname{Gal}(F)$, $\sigma(W_j) = W_j$ et donc le plus petit corps de définition de W_i est inclus dans F. En particulier, W_j est définie sur F. De plus, pour tout $a \in V(F)$, il existe j tel que $a \in V_j$ et donc, pour tout $\sigma \in \mathcal{G}(F)$, $a = \sigma(a) \in \sigma(V_j)$, on a donc $a \in W_j$.

Pour tout j, si $\mathcal{G}(F) \cdot V_j = \{V_j\}$, alors $W_j = V_j$ est géométriquement intègre définie sur F. Sinon $\dim(W_j) < \dim(W)$ et on conclut par induction. □

Corollaire 4.12 : *Soit $\varphi := \bigwedge_j f_j(x,y) \simeq 0$, où $f_i \in \mathbb{Z}[x,y]$. Il existe $(\psi_i)_{i<n} \in \mathcal{F}^{\mathrm{qf}}_{\mathbb{Z}}(x,z)$ telles que pour tout corps F parfait et tout $a \in F^y$, il existe $b \in F^z$ tels que $\psi_i(x,b)$ définit une F-variété géométriquement intègre définie sur F (ou vide) incluse dans $\varphi(x,a)$ et $\varphi(F,a) = \bigcup_i \psi_i(F,b)$.*

Démonstration. Pour tout F parfait et $a \in F^y$, par la Proposition **(4.11)**, il existe $(\psi_{i,F,a})_{i<n} \in \mathcal{F}^{\mathrm{qf}}(x,z)$ et $b \in F^z$ tels que $\psi_{i,F,a}(x,b)$ définit une F-variété géométriquement intègre définie sur F incluse dans $\varphi(x,a)$ et tels que $\varphi(F,a) = \bigcup_i \psi_{i,F,a}(F,b)$. L'espace compact $\mathcal{S}_x(\mathrm{PERF})$, où PERF est la $\mathbb{Z}$-théorie des corps parfaits, est donc couvert par les ouverts $[\chi_{F,a}]$ où $\chi_{F,a}(y) := \exists z \bigwedge_i \theta_{i,F,a}(z) \wedge \forall x\, \varphi(x,a) \leftrightarrow \bigvee_i \psi_{i,F,a}(x,z)$ avec $\theta_{i,F,a} \in \mathcal{F}^{\mathrm{qf}}_{\mathbb{Z}}(z)$ qui exprime que $\psi_{i,F,a}(x,z)$ définit une F-variété géométriquement intègre définie sur F.
Par compacité, il existe un sous-recouvrement fermé, c'est à dire qu'il existe $(\psi_{i,j})_{i<n_j,j<m} \in \mathcal{F}^{\mathrm{qf}}(x,z_j)$ tels que pour tout F parfait et $a \in F^y$, il existe $j_0 < m$ et $b_{j_0} \in F^{z_{j_0}}$ tel que $\psi_{i,j_0}(x,b_{j_0})$ définit une F-variété géométriquement intègre définie sur F et $\varphi(F,a) = \bigcup_i \psi_{i,j_0}(F,b_{j_0})$. On peut supposer que $z := (z_j)_{j<m}$ contient y. Soit $\psi'_{i,j}(x,z) := \psi_{i,j}(x,z) \wedge \theta_{i,j}(z) \wedge \xi_{i,j}(z)$ où $\theta_{i,j} \in \mathcal{F}^{\mathrm{qf}}_{\mathbb{Z}}(z)$ exprime que $\psi_{i,j}(x,z)$ définit une F-variété géométriquement intègre définie sur F et $\xi_{i,j} \in \mathcal{F}^{\mathrm{qf}}_{\mathbb{Z}}(z)$ est équivalente, modulo ACF, à $\forall x\, \psi_{i,j}(x,z) \to \varphi(x,y)$. On a donc $\psi'_{i,j_0}(F,b) = \psi_{i,j_0}(F,b_{j_0})$, $\psi'_{i,j}(x,b)$ définit une F-variété géométriquement intègre définie sur F, ou vide, incluse dans $\varphi(x,a)$ et $\varphi(F,a) = \bigcup_i \psi_{i,j_0}(F,b_{j_0}) = \bigcup_{i,j} \psi'_{i,j}(F,b)$. □

Corollaire 4.13 : *Soit $\varphi := \bigwedge_i f_i(x,y) \simeq 0$, où $f_i \in \mathbb{Z}[x,y]$. Il existe $C \in \mathbb{R}_{\geqslant 0}$, un ensemble fini $D \subseteq \{0,\dots,|x|\} \times \mathbb{Z}_{>0} \cup \{(0,0)\}$ et, pour tout $(d,\mu) \in D$, une formule $\theta_{d,\mu} \in \mathcal{F}_{\mathbb{Z}}(y)$ tels que, pour tout corps fini F et tout $a \in F^y$,*

$$F \vDash \theta_{d,\mu}(a) \text{ si et seulement si } \left||\varphi(F,a)| - \mu|F|^d\right| < C|F|^{d-1/2},$$

et

$$F^y \subseteq \bigcup_{(d,\mu)\in D} \theta_{d,\mu}(F).$$

Démonstration. TO DO □

Lemme 4.14 : *Soit $\varphi \in \mathcal{F}_{\mathbb{Z}}(x)$ une conjonction d'égalités et d'inégalités. Il existe $\psi \in \mathcal{F}_{\mathbb{Z}}(x,y)$ une conjonction d'égalités telle que, pour tout corps F, la projection sur x induit une bijection $\psi(F) \to \varphi(F)$.*

Démonstration. TO DO □

Proposition 4.15 : *Pour tout $\varphi \in \mathcal{F}_{\mathbb{Z}}(x)$, il existe $N \in \mathbb{Z}_{\geqslant 0}$, $\psi_i \in \mathcal{F}_{\mathbb{Z}}(x,z_i,t)$ une conjonction d'égalités et $\theta \in \mathcal{F}_{\mathbb{Z}}(t)$ tels que pour tout corps fini F avec $|F| \geqslant N$, on ait $\theta(F) \neq \varnothing$ et pour tout $c \in \theta(F)$ et $a \in F^x$, on ait $|\psi_i(a,F,c)| \leqslant e$ et $\varphi(F) = \bigsqcup_i \exists z_i\, \psi_i(F,z_i,c)$.*

Démonstration. TO DO □

Théorème 4.16 (Chatzidakis–van den Dries–Macintyre, 1992) **:** *Pour tout $\varphi \in \mathcal{F}_{\mathbb{Z}}(x,y)$, il existe $C \in \mathbb{R}_{\geqslant 0}$, un ensemble fini $D \subseteq \{0,\dots,|x|\} \times \mathbb{Q}_{>0} \cup \{(0,0)\}$ et pour tout $(d,\mu) \in D$, une formule $\varphi^{d,\mu} \in \mathcal{F}_{\mathbb{Z}}(y)$ tels que, pour tout corps fini F et tout $a \in F^y$,*

$$F \vDash \varphi^{d,\mu}(a) \text{ si et seulement si } \left||\varphi(F,a)| - \mu|F|^d\right| < C|F|^{d-1/2},$$

et

$$F^y \subseteq \bigcup_{(d,\mu)\in D} \varphi^{d,\mu}(F).$$

Démonstration. Supposons tout d'abord que $\varphi := \exists z\, \psi(x,y,z)$ avec $\psi \in \mathcal{F}_{\mathbb{Z}}^{\mathrm{qf}}(x,y,z)$ et qu'il existe $e \in \mathbb{Z}_{\geqslant 0}$ tel que pour tout choix de $F \vDash \mathrm{IRR}_{\mathrm{id}}$, $b \in F^x$ et $a \in F^y$, $|\psi(b,a,F)| \leqslant e$. On fixe $a \in F^y$. Par le Corollaire **(4.13)** et le Lemme **(4.14)**, il existe (d,ν) et C tels que :

$$\big||\psi(F,a,F)| - \nu|F|^d\big| < C|F|^{d-1/2}.$$

On remarque que $|\varphi(F,a,F)| \geqslant |\psi(F,a)|/e$ et donc, pour $|F| \gg 0$, on doit avoir $d \leqslant |x|$. Pour tout $0 < i \leqslant e$, on note $X_i(F,a) := \{b \in \varphi(F,a) : |\psi(b,a,F)| = i\}$. On a alors $|\varphi(F,a)| = \sum_i |X_i(F,a)|$.

On définit aussi $\psi_i(x,y,z_1,\ldots,z_i) := \bigwedge_i \psi(x,y,z_i,t) \wedge \bigwedge_{j\neq l} z_j \neq z_l$. En appliquant, de nouveau, le Corollaire **(4.13)** et le Lemme **(4.14)**, on trouve (d_i,ν_i) et C_i — ainsi que $\psi_i^{d_i,\nu_i}$ — tels que $\big||\psi_i(F,a,F,\ldots,F)| - \nu_i|F|^{d_i}\big| < C_i|F|^{d_i-1/2}$. Comme $m_i \leqslant e!|\psi(F,a,F)|$, si $|F| \gg 0$, on doit avoir $d_i \leqslant d$ et donc $\big||\psi_i(F,a,F,\ldots,F)| - \mu_i|F|^d\big| < C_i|F|^{d-1/2}$, où $\mu_i = \nu_i$ si $d_i = d$ et $\mu_i = 0$ sinon.

Par ailleurs, chaque élément de $X_i(F,a)$ donne lieu à $i!/(i-j)!$ éléments de $\psi_j(F,a,F,\ldots,F)$ pour tout $j \leqslant i$. On a donc $|\psi_j(F,a,F,\ldots,F)| = \sum_{j\leqslant i\leqslant e} i!/(i-j)! \cdot |X_i(F,a)|$. C'est un système triangulaire d'équations linéaires à coefficients dans $\mathbb{Q}$ et on trouve donc $r_{i,j} \in \mathbb{Q}$ qui ne dépendent que de e tels que $|X_i(F,a)| = \sum_j r_{i,j}|\psi_j(F,a,F,\ldots,F)|$. Il s'ensuit que :

$$\Big||\varphi(F,a)| - \big(\sum_{i,j} r_{i,j}\mu_j\big)|F|^d\Big| \leqslant \sum_{i,j} r_{i,j}\,\big||\psi_j(F,a,F,\ldots,F)| - \mu_j|F|^d\big| < \big(\sum_{i,j} r_{i,j}C_j\big)|F|^{d-1/2}.$$

Si $\mu := \sum_{i,j} r_{i,j}\mu_j = 0$, on a $\nu|F|^d - C|F|^{d-1/2} \leqslant |\psi(F,a)| \leqslant e|\varphi(F,a)| < e(\sum_{i,j} r_{i,j}C_j)|F|^{d-1/2}$. Pour $|F| \gg 0$, on doit donc avoir $\nu = 0$ et donc $d = 0$. On vérifie aisément l'existence des $\varphi^{d,\mu}$ en utilisant les $\psi_i^{d_i,\mu_i}$.

Revenons au cas général. Soient θ et ψ_i tels que dans la Proposition **(4.15)**. Pour tout F tel que $|F| \gg 0$, $a \in F^y$ et $c \in \theta(F)$, on a $|\varphi(F,a)| = \sum_i |\exists z_i\, \psi_i(F,a,z_i,c)|$. Par le cas précédent, on trouve donc D et $\theta_{d,\mu} \in \mathcal{F}_{\mathbb{Z}}(y,t)$ tels que dans le théorème. On remarque que pour $|F| \gg 0$, il existe un unique $(d,\mu) \in D$ tel que $F \vDash \theta_{d,\mu}(a,c)$, et ce (d,μ) ne dépend que de a, et pas de $c \in \theta(F)$. Il s'ensuit que $\theta'_{d,\mu}(y) := \exists t\, \theta(t) \wedge \theta_{d,\mu}(y,t)$ a les propriétés requises pour $|F| \gg 0$. □

Corollaire 4.17 : *Soit $\varphi \in \mathcal{F}_{\mathbb{Z}}(x,y)$. Il existe $N \in \mathbb{Z}_{>0}$ tel que, pour tout corps fini F et $a \in F^y$ tel que $\varphi(F,a)$ définit un sous-corps de F, si $|F| \geqslant N$, $|\varphi(F,a)| \leqslant N$ ou $\varphi(F,a) = F$.*

Démonstration. TO DO □

4.2 Dimension et mesure pseudo finie

On fixe $K \vDash \mathrm{PSF}$. Notre but est de comprendre les conséquences sur les corps pseudo finis du Théorème **(4.16)**. Puisque l'on passe à la limite des résultat de comptage, il est naturel de s'attendre à voir apparaître des mesures. Mais comme on l'a vu, le comportement asymptotique du nombre de points dépend de deux paramètre d — essentiellement la dimension — et μ. On a donc voir apparaître toute une famille de mesures paramètrées par la dimension.

Lemme 4.18 : *Soit $\varphi \in \mathcal{F}_{\mathbb{Z}}(x,y)$. Pour tout $a \in K^y$, il existe un unique (d,μ) tel que $K \vDash \varphi^{d,\mu}(a)$.*

Démonstration. Comme on l'a vu précédemment, pour F fini avec $|F| \gg 0$, et $a \in F^y$, $|\varphi(F,a)|$ a un unique équivalent de la forme $\mu|F|^d$. Il existe donc un unique (d,μ) tel que $F \vDash \varphi^{d,\mu}(a)$. Il s'ensuit que, pour tout $(d,\mu) \neq (e,\nu) \in D$ $T_{\mathrm{psf}} \vDash \forall y\, \varphi^{d,\mu}(y) \to \neg\varphi^{e,\nu}(y)$. Ce qui prouve l'unicité. Comme, de plus, $T_{\mathrm{f}} \vDash \forall y \bigvee_{(d,\mu)\in D} \varphi^{d,\mu}(y)$, on a aussi l'existence. □

Attention la notation $\theta_{d,\mu}$ a changé ; *cf.* **(4.16)**.

On note $(d(\varphi(x,a)), \mu(\varphi(x,a)))$ l'unique paire (d,μ) telle que $K \vDash \varphi^{d,\mu}(a)$ — si $(d,\mu) = (0,0)$, par convention, on pose $d(\varphi(x,a)) = -\infty$. On remarque que $(d(\varphi(x,a)), \mu(\varphi(x,a)))$ ne dépend que du type de a dans K, d'où le fait que l'on se permet de ne pas spécifier K dans la notation.
Les lemmes qui viennent suivent tous les même schéma : on prouve que certains propriétés des mesures (en particulier la mesure de comptage dans le cas des corps finis), se transmettent des corps finis aux corps pseudo-finis.

Lemme 4.19 : *Soit $\varphi, \psi \in \mathcal{F}_K(x)$ tels que $\varphi(K) \subseteq \psi(K)$. On a :*

- *$d(\varphi) \leqslant d(\psi)$.*
- *si $d(\varphi) = d(\psi)$, on a alors $\mu(\varphi) \leqslant \mu(\psi)$.*

En particulier, d et μ sont bien définis sur les classes d'équivalences modulo K, c'est à dire sur les ensembles définissables.

Démonstration. Pour tous $\varphi \in \mathcal{F}_{\mathbb{Z}}(x,y)$, $\psi \in \mathcal{F}_{\mathbb{Z}}(x,z)$, F fini, $a \in F^y$ et $b \in F^z$, tels que $F \vDash \varphi^{d,\mu}(a) \wedge \psi^{e,\nu}(b) \wedge \forall x\, \varphi(x,a) \to \psi(x,b)$, on a $|\varphi(F,a)| \leqslant |\psi(F,b)|$, et donc, puisque ce sont leurs équivalents, si $|F| \gg 0$, $\mu|F|^d \leqslant \nu|F|^e$. On a donc nécessairement $(d,\mu) \leqslant (e,\nu)$ pour l'ordre lexicographique. Il s'ensuit que pour tout $(d,\mu) > (e,\nu)$, $T_{\mathrm{psf}} \vDash \forall y \forall z\, \neg((\forall x\, \varphi(x,y) \to \psi(x,z)) \wedge \varphi^{d,\mu}(y) \wedge \psi^{e,\nu}(z))$. Le lemme est alors évident. □

Lemme 4.20 : *Soit $\varphi, \psi \in \mathcal{F}_K(x)$. On a :*

- *$d(\varphi \vee \psi) = \max\{d(\varphi), d(\psi)\}$.*
- *Si $d(\varphi) < d(\psi)$, on a alors $\mu(\varphi \vee \psi) = \mu(\psi)$.*
- *Si $d(\varphi) = d(\psi)$ et $\varphi(F) \cap \psi(F) = \varnothing$, on a alors $\mu(\varphi \vee \psi) = \mu(\varphi) + \mu(\psi)$.*

Démonstration. Soient $\varphi \in \mathcal{F}_{\mathbb{Z}}(x,y)$, $\psi \in \mathcal{F}_{\mathbb{Z}}(x,z)$, F fini, $a \in F^y$ et $b \in F^z$, tels que $F \vDash \varphi^{d,\mu}(a) \wedge \psi^{e,\nu}(b) \wedge (\varphi \vee \psi)^{r,\rho}(a,b)$.

- On a vu dans le Lemme **(4.19)** que, pour $|F| \gg 0$, $m := \max\{d,e\} \leqslant r$. De plus, $|\varphi(F,a) \cup \psi(F,b)| \leqslant |\varphi(F,a)| + |\psi(F,b)| = o(|F|^{m+1/2})$ et donc $r < m+1$; d'où $m = r$. Il s'ensuit que $T_{\mathrm{psf}} \vDash \forall y \forall z\, \varphi^{d,\mu}(y) \to \psi^{e,\nu}(b) \to \bigvee_\rho (\varphi \vee \psi)^{m,\rho}(a,b)$. L'égalité voulue en découle.
- Supposons $d < e$. Par le Lemme **(4.19)** et le point précédent, $e = r$ et $\nu \leqslant \rho$. De plus, $|\psi(F,a)| \sim \mu|F|^d = o(|F|^e) = o(\psi(F,b))$ et donc $|\varphi(F,a) \cup \psi(F,b)| \leqslant |\varphi(F,a)| + |\psi(F,b)| \sim |\psi(F,b)| \sim \nu|F|^e$; d'où $\rho \leqslant \nu$. On a donc $T_{\mathrm{psf}} \vDash \forall y \forall z\, \varphi^{d,\mu}(y) \to \psi^{e,\nu}(b) \to (\varphi \vee \psi)^{e,\nu}(a,b)$. L'égalité voulue en découle.
- Supposons $d = e$ et $\varphi(F,a) \cap \psi(F,b) = \varnothing$. Comme précédemment, on a $d = e = r$ et, pour $|F| \gg 0$, $|\varphi(F,a) \cup \psi(F,b)| = |\varphi(F,a)| + |\psi(F,b)| \sim (\mu+\nu)|F|^d$, d'où $\rho = \mu + \nu$. On a donc $T_{\mathrm{psf}} \vDash \forall y \forall z\, \varphi^{d,\mu}(y) \to \psi^{e,\nu}(b) \to (\varphi \vee \psi)^{e,\mu+\nu}(a,b)$. L'égalité voulue en découle. □

Lemme 4.21 : *Soit $f : X \to Y$ une fonction K-définissable surjective.*

- *Si pour tout $a \in Y$, $d(f^{-1}(a)) = n$, on a alors $d(X) = n + d(Y)$.*
- *Si, de plus, pour tout $a \in Y$, $\mu(f^{-1}(a)) = \nu$, on a alors $\mu(X) = \nu\mu(Y)$.*

Démonstration. Soit F un corps fini et $\psi(x, y, z) \in \mathcal{F}_{\mathbb{Z}}(x, y, z)$ une relation fonctionnelle en y. On note $\varphi(x, z)$ son domaine et $\theta(y, z)$ son codomaine. Soit $a \in F^z$ tel que $F \vDash \theta^{d,\mu}(a)$.

- Supposons que, pour tout $b \in \theta(F, a)$, $F \vDash \bigvee_i \psi^{n,\nu_i}(b, a)$. Pour tout i, soit $\xi_i(y, z) := \psi^{n,\nu_i}(y, z)$ et soit r_i, ρ_i tels que $F \vDash \xi_i^{r_i,\rho_i}(a)$. On remarque que $d = \max_i r_i$. Si $|F| \gg 0$, on a alors $|\varphi(F, a)| = \sum_{b\in\theta(F,a)} |\psi(F, b, a)| \sim \sum_i \rho_i\nu_i|F|^{r_i+n} \sim \zeta|F|^{d+n}$. On conclut, comme précédemment, que $d(X) = n + d(Y)$.
- Supposons maintenant que, pour tout $b \in \theta(F, a)$, $F \vDash \bigvee_i \psi^{n,\nu}(b, a)$. Si $|F| \gg 0$, on a alors $|\varphi(F, a)| = \sum_{b\in\theta(F,a)} |\psi(F, b, a)| \sim \nu\mu|F|^{n+d}$. On en conclut que $\mu(X) = \nu\mu(Y)$. □

Nous voudrions maintenant expliciter le lien entre $d(\varphi(x))$ et la dimension des variétés algébriques :

Proposition 4.22 : *Soit X un ensemble K-définissable et V la K-clôture de Zariski de $X(K)$. On a alors :*

$$d(X) = \dim(V) = \max\{\mathrm{trdeg}(c/K) : c \in X(N), N \succcurlyeq K\}.$$

Démonstration. Soit $\varphi(x, y)\mathcal{F}_{\mathbb{Z}}(x, y)$. Pour tout corps fini F et $a \in F^y$ tel que $\varphi(x, a)$ est une F-variété géométriquement intègre définies sur F, par le théorème de Lang-Weil — Théorème **(3.30)**, on a $F \vDash \varphi^{\dim(V),1}(a)$. On a donc $T_\mathrm{f} \vDash \forall y$ « $\varphi(x, a)$ définit une F-variété géométriquement intègres définie sur le corps » $\to \varphi^{\dim(V),1}(y)$. Pour toute K-variété géométriquement intègre définie sur K, $d(W) = \dim(W)$.

Assertion 4.23 : *$F \leqslant K$ des corps et V une F-variété. Si $X \subseteq V(K)$ est F-Zariski dense dans V, alors X est F-Zariski dense dans toute composante F-intègres de V.*

Démonstration. Soit $V = \bigcup_{i<n} W_i$ la décomposition de V en composantes F-intègres. Soit $U \subset W_{i_0}$ une sous-F-variété. Si $W_{i_0} \subseteq V \subseteq U \cup \bigcup_{i\neq i_0} W_i$, comme W_{i_0} est irréductible, on a soit $W_{i_0} \subseteq U$, ce qui contredit $U \subset W_{i_0}$, soit $W_{i_0} \subseteq W_i$, pour $i \neq i_0$, ce qui contredit que les W_i sont les composantes F-intègres (distinctes) de V. On a donc $U \cup \bigcup_{i\neq i_0} W_i \subset V$ et donc, par F-Zariski densité, il existe $x \in X \cap V \smallsetminus (U \cup \bigcup_{i\neq i_0} W_i)$; en particulier, $x \in X \cap W_{i_0} \smallsetminus U$. ◊

Assertion 4.24 : *Soit F un parfait corps, $X \subseteq F^x$ et V sa F-clôture de Zariski. Alors toute composante F-intègre de V est géométriquement intègres définie sur F.*

Démonstration. Par la Proposition **(4.11)**, il existe des F-variétés $(W_i)_{i<n}$ géométriquement intègres définies sur F, incluses dans V, telles que $V(F) = \bigcup_i W_i(F)$, on peut supposer qu'il n'y a pas de relations d'inclusion non triviales entre les W_i. Comme $\bigcup_i W_i \subseteq V$ est un F-fermé de Zariski qui contient $X \subseteq V(F)$ et que X est F-Zariski dense dans V, $V = \bigcup_i W_i$. Par la Proposition **(2.15)**, les W_i sont exactement les composantes F-intègres de V. ◊

Soient $(W_i)_{i<n}$ les composantes K-intègres de V. Par le Lemme **(4.20)**, il existe i tel que $d(V) = d(W_i)$. Par compacité, comme $X(K)$ est K-Zariski dense dans W_i, il existe $N \succcurlyeq K$ et $c \in X(N)$ qui est K-générique dans W_i.

D'après le Théorème **(3.63)** et la Proposition **(4.11)**, il existe aussi des K-variétés $(Y_j)_{j<m}$ géométriquement intègres définies sur K et des fonctions définissables (en l'occurence des projections) $f_j : Y_j \to X$ à fibres finies, telles que $X := \bigcup_{j<m} f_j(Y_j)$. Soient $j < m$ et $b \in Y_j(N)$ tel que $f_j(b) = c$. On a alors $\operatorname{trdeg}(c/K) = \operatorname{trdeg}(b/K) \leqslant \dim(Y_j) = d(Y_j) = d(X) \leqslant d(V) = d(W_i) = \dim(W_i) = \operatorname{trdeg}(c/K)$. La première égalité suit du fait que, comme les f_j sont à fibres finies, $K(c) \leqslant K(c,b)$ est une extension finie. La deuxième égalité suit de la définition de $\dim(Y_j)$. La quatrième égalité suit du Lemme **(4.21)** — on peut aussi le voir directement dans la preuve du Théorème **(4.16)**. La cinquième égalité suit du fait que $X \subseteq V$ et du Lemme **(4.19)**. Par ailleurs, $\operatorname{trdeg}(c/K) \leqslant \max\{\operatorname{trdeg}(c/K) : c \in X(N), N \geqslant K\} \leqslant \max\{\operatorname{trdeg}(c/K) : c \in V(N), N \geqslant K\} = \max_i(\dim(W_i)) = \max_i(d(W_i)) = \operatorname{trdeg}(c/K)$. Tous ces entiers sont dont égaux. □

On notera dorénavant tous ces entiers égaux $\dim(X)$.

Remarque 4.25 : Si V est une K-variété géométriquement intègre définie sur K, $V(K)$ est dense dans V, par le Lemme **(3.5)**, et donc les deux définitions de $\dim(X)$ — en tant qu'ensemble K-définissable et en tant que K-variété — coincident.

Décrivons maintenant les propriétés de μ :

Définition 4.26 : *Soit X un ensemble K-définissable. Pour tout ensemble K-définissable $Y \subseteq X$, on note $\mu_X(Y) := 0$ si $\dim(Y) < \dim(X)$ et $\mu_X(Y) := \mu(Y)/\mu(X)$ sinon.*

Proposition 4.27 : *La fonction μ_X définit une mesure de probabilité finiment additive sur les sous-ensembles K-définissables de X.*

Démonstration. Par définition $\mu_X(X) = 1$. Comme, pour tout $\varphi \in \mathcal{F}_{\mathbb{Z}}(x,y)$, tout corps fini F suffisamment grand et tout $a \in F^y$, $\varphi(F,a) = \varnothing$ implique $F \models \varphi^{(}0,0)(a)$, $\dim(\varnothing) = -\infty$ et $\mu_X(\varnothing) = 0$. Enfin, par induction à partir du Lemme **(4.20)**, on montre que si les $(Y_i)_{i<n} \subseteq X$ sont K-définissables disjoints, $\mu_X(\bigcup_i Y_i) = \sum_i \mu(Y_i)$. □

5 Théorie géométrique des modèles des corps PAC bornés

5.1 Quelques notions de classification

Une des notions fondamentales de la théorie des modèle contemporaine, introduite par Shelah, est celle de ligne de partage (*dividing line*). L'idée est d'organiser l'espace des théories en identifiant certaines dichotomies parmi les théories qui séparent celle qui ont de « bonnes propriétés » (on parle aussi de théorèmes de structure) et celles qui non seulement n'ont pas ces « bonnes propriétés » mais ont même de « mauvaise propriétés » (on parle aussi de théorèmes de non-structure). Parmi les « bonnes propriétés », on recherche, par exemple, le fait de pouvoir distinguer les modèles par des invariants cardinaux — c'est historiquement ce qui a motivé le travail de Shelah ; ou encore la finitude de certains rangs, les propriétés des types, des suites indiscernables ou bien celles de la déviation[1] (*forking*). Parmi les « mauvaise propriétés », on peut citer le fait d'avoir beaucoup de modèles à isomorphisme près, beaucoup de types, ou le

1. *cf.* Définition **(5.19)**. Dans les corps PAC bornés c'est la disjonction algébrique.

fait d'encoder certaines configurations combinatoires comme un ordre ou un graphe aléatoire bipartite (c'est-à-dire les parties d'un ensemble)[2].

La ligne de partage la plus emblématique est sans aucun doute la stabilité :

Théorème 5.1 : *Soit T une A-théorie, sont équivalents :*

1. *pour tout $M \vDash T$ et $A \subseteq M$, tout $p \in \mathcal{S}(A)$ est définissable ;*
2. *pour tout $M \vDash T$ et $p \in \mathcal{S}(M)$, les héritiers et les cohéritiers de p coincident ;*
3. *toute suite indiscernable est un ensemble indiscernable ;*
4. *le rang de Morley local de toute formule est bien défini ;*
5. *la déviation a un caractère local et pour tout $M \vDash T$, tout $p \in \mathcal{S}(M)$ est stationnaire ;*
6. *aucune formule $\varphi \in \mathcal{F}_A(x, y)$ n'a la propriété de l'ordre dans aucun modèle de T ;*
7. *il existe un cardinal λ tel que pour tout $M \vDash T$ avec $|M| \leqslant \lambda$, $|\mathcal{S}(M)| \leqslant \lambda$;*

On dit que T est stable quand ces conditions équivalentes sont vérifiées. On remarque que les propriétés 1 à 5 sont de « bonnes propriétés » alors que 6 et 7 sont la négations de « mauvaise propriétés ». Nous allons maintenant donner certaines de ces définitions, puis les illustrer dans ACF :

Définition 5.2 (Types définissables, héritiers, cohéritier) **:** *Soit T une A-théorie, $B \leqslant M \vDash T$ et $p \in \mathcal{S}^M_x(B)$. On dit que :*

- *p est A-définissable si, pour toute formule $\varphi \in \mathcal{F}_A(x, y)$, il existe $\theta \in \mathcal{F}_A(y)$ telle que, pour tout $b \in B^y$,*
$$\varphi(x, b) \in p \text{ si et seulement si } M \vDash \theta(b).$$
On note souvent $\mathrm{d}_p x\, \varphi(x, y) := \theta(y)$.
- *p est un héritier (*heir*) de $p|_A$ si, pour toute formule $\varphi \in \mathcal{F}_A(x, y)$ et $b \in B^y$ tel que $\varphi(x, b) \in p$, il existe $a \in A^y$ tel que $\varphi(x, a) \in p$.*
- *p est finiment satisfiable dans A (on dit aussi que p est un cohéritier (*coheir*) de $p|_A$) si, pour toute formule $\varphi(x) \in p$, il existe $a \in A^x$ tel que $M \vDash \varphi(a)$.*

Remarque 5.3 : $\mathrm{tp}(b/A[c])$ est un héritier de $\mathrm{tp}(b/A)$ si et seulement si $\mathrm{tp}(c/A[b])$ est un cohéritier de $\mathrm{tp}(c/A)$.

Proposition 5.4 : *Soit $F \leqslant K$ des corps, avec $F \vDash \mathrm{ACF}$ et $p \in \mathcal{S}^{K^{\mathrm{a}}}_x(K)$. Sont équivalents :*

1. *p est F-définissable ;*
2. *p est un héritier de $p|_F$;*
3. *p est finiment satisfiable dans F ;*
4. *pour tout $a \vDash p$ (dans $L \vDash \mathrm{ACF}_K$), $F(a) \downarrow^{\mathrm{lin}}_F K$;*
5. *il existe $a \vDash p$ (dans $L \vDash \mathrm{ACF}_K$) tel que $F(a) \downarrow^{\mathrm{lin}}_F K$;*
6. *$\mathcal{I}_K(p) := \{f \in K[X] : f \simeq 0 \in p\}$ est défini sur F.*

Démonstration.

1 ⇒ 2 Soit $\varphi \in \mathcal{F}_{\mathbb{Z}}(xy)$ une formule et $b \in K^y$ tel que $\varphi(x, b) \in p$. On a alors $F \succcurlyeq K^{\mathrm{a}} \vDash \exists y\, \mathrm{d}_p x\, \varphi(x, y)$ et donc il existe $a \in F$ tel que $F \vDash \mathrm{d}_p x \varphi(x, a)$ et donc $\varphi(x, a) \in p$.

2 ⇒ 4 Soit $(\lambda_I)_{|I| \leqslant d} \in K$ non tous nuls tels que $\sum_I \lambda_I a^I = 0$. On a donc $\bigvee_I \lambda_I \neq 0 \wedge \sum_I \lambda_I x^I = 0 \in p$ et il existe donc $\mu_i \in F$ non tous nuls tels que $\sum_I \mu_I a^I = 0$. Toute sous-famille

2. Je recommande [Con] qui donne un panorama essentiellement exhaustif et interactif de ces lignes de partages.

F-linéairement indépendante de la famille $(a^I)_I \in F[a]$ reste donc K-linéairement indépendante.

4 ⇒ 5 C'est évident puisque p est consistent.

5 ⇒ 6 C'est une conséquence immédiate de Proposition **(2.39)** puisque $\mathcal{I}_K(p) = \mathcal{I}_K(a)$.

6 ⇒ 1 Soient $(P_i)_{i<n} \in F[x]$ des générateurs de $\mathcal{I}_K(p)$. Pour tout $Q \in \mathbb{Z}[x,y]$, et $b \in K^y$, $Q(x,b) \simeq 0 \in p$ si et seulement si $K^{\mathrm{a}} \vDash \forall x \bigwedge_i P_i(x) \simeq 0 \to Q(x,b) \simeq 0$. On a donc prouvé l'existence de $\mathrm{d}_p x P(x,y) \simeq 0$. L'existence de $\mathrm{d}_p x\varphi(x,y)$ suit par induction sur φ.

2 ⇔ 3 Soit $b \in K$ tel que $K = F(b)$. Le type $p := \mathrm{tp}(a/F(b))$ hérite de $\mathrm{tp}(a/F)$ si et seulement si $F(a) \downarrow^{\mathrm{lin}}_F F(b)$ si et seulement si $F(b) \downarrow^{\mathrm{lin}}_F F(a)$ si et seulement si $\mathrm{tp}(b/F(a))$ hérite de $\mathrm{tp}(b/F)$, c'est à dire que $\mathrm{tp}(a/F(b))$ cohérite de $\mathrm{tp}(a/F)$. □

Une autre avatar de la stabilité de ACF est l'unicité des extensions algébriquement indépendantes régulières :

Lemme 5.5 : *Soit $f : K_1 \to K_2$ et $g : L_1 \to L_2$ des isomorphismes de F-corps avec tels que $K_1 \downarrow^{\mathrm{alg}}_F L_1$, $K_2 \downarrow^{\mathrm{alg}}_F L_2$ — en particulier, on suppose que les K_i et L_i sont des sous F corps d'un même corps Ω_i — et $F \leqslant K_1$ est régulière. Il existe alors un isomorphisme de L-corps $h : K_1L_1 \to K_2L_2$ qui étend f et g.*

Démonstration. Comme $F \leqslant K_1$, et donc $F \leqslant K_2$, sont régulières, $K_1 \downarrow^{\mathrm{lin}}_F L_1$ et $K_2 \downarrow^{\mathrm{lin}}_F L_2$. On a alors $f \otimes_F g : K_1L_1 \cong K_1 \otimes_F L_1 \cong K_2 \otimes_F L_2 \cong K_2L_2$. □

Malheureusement, les corps PAC stables sont plutôt rares :

Théorème 5.6 (Duret, 1980) **:** *Un corps* PAC *stable est séparablement clos.*

La mesure pseudo-finie permet cependant de voir que les corps pseudo finis ne sont pas non plus trop loin dans la hiérarchie de la classification :

Proposition 5.7 (La propriété de l'ordre strict) **:** *Soit $\varphi \in \mathcal{F}_{\mathbb{Z}}(x,y)$. Il existe $N \in \mathbb{Z}_{\geqslant 0}$ tel que pour tout $K \vDash$ PSF et $(a_i)_{i\leqslant n} \in K^y$, si $\varphi(K,a_i) \subset \varphi(K,a_j)$, pour tous $i < j$, alors $n \leqslant N$.*

Démonstration. Soit $K \vDash$ PSF. On va montrer, par induction sur $\max_i \dim(\varphi(x,a_i))$, que toute suite $\varphi(K,a_i)$ croissante pour l'inclusion est stationnaire. Si $\max_i \dim(\varphi(x,a_i)) = -\infty$, $\varphi(K,a_i) = \varnothing$ est constante. En général, comme $\varphi(K,a_i) \subset \varphi(K,a_{i+1})$, la suite des paires $(d(\varphi(x,a_i)), \mu(\varphi(x,a_i)))$ est croissante, pour l'ordre lexicographique. Comme elle est bornée par le Théorème **(4.16)**, elle est stationnaire. Soit i_0 tel qu'elle soit contante au delà de i_0. On a $\mu_{\varphi(x,a_i)}(\varphi(x,a_{i_0})) + \mu_{\varphi(x,a_i)}(\varphi(x,a_i) \wedge \neg\varphi(x,a_{i_0})) = 1 = \mu_{\varphi(x,a_i)}(\varphi(x,a_{i_0}))$ et donc $\mu_{\varphi(x,a_i)}(\varphi(x,a_i) \wedge \neg\varphi(x,a_{i_0})) = 0$, c'est à dire $\dim(\varphi(x,a_i) \wedge \neg(\varphi(x,a_{i_0}))) < \dim(\varphi(x,a_{i_0}))$. Par induction cette suite est stationnaire, c'est donc aussi le cas de la suite originale.
La proposition suit alors par compacité. □

On verra que, plus généralement, les corps PAC bornés sont simples. La mesure pseudo-finie nous permet déjà de montrer la propriété suivante, plus forte que la propriété de l'ordre strict et qui implique la simplicité :

Proposition 5.8 (La propriété S1) **:** *Soit $\varphi \in \mathcal{F}_{\mathbb{Z}}(x,y)$ et $\psi \in \mathcal{F}_{\mathbb{Z}}(x,z)$. Il existe $N \in \mathbb{Z}_{\geqslant 0}$ tel que pour tout $K \vDash$ PSF, $(a_i)_{i\leqslant n} \in K^y$ et $c \in K^z$, si $\dim(\varphi(K,a_i) \cap \varphi(K,a_j)) < \dim(\varphi(K,a_i) \cap \psi(K,c)) = \dim(\psi(K,c))$, pour tout $i \neq j$, alors $n \leqslant N$.*

Démonstration. Supposons, au contraire qu'il existe $K \models \mathrm{PSF}$, $c \in K^z$ et $(a_i)_{i \geqslant 0} \in K^y$ tels que pour tout $i \neq j$, $\dim(\varphi(x,a_i) \cap \varphi(x,a_j)) < \dim(\varphi(x,a_i) \cap \psi(x,c)) = \dim(\psi(x,c))$. Par finitude, $\varepsilon := \min_i \mu(\varphi(x,a_i)) > 0$. On a alors $1 \geqslant \mu_{\psi(x,c)}(\bigvee_{i<n} \psi(x,a_i) \wedge \psi(x,c)) \geqslant n\varepsilon$, ce qui est une contradiction. La proposition suit alors par compacité. $\square$

5.2 Amalgamation et théories simples

Soit $K \models \mathrm{PPAC}_{\mathfrak{d}}$. On note F l'image de $C_{\mathfrak{d}}$ dans K. Soit de plus W un ensemble de sous-ensembles de $\underline{n} := \{0, \ldots, n-1\}$ clos par sous-ensemble.

Définition 5.9 : *Un W-système d'amalgamation dans K est un système cohérent de morphismes $f_{v,w} : A_v \to A_w$ de sous-F-algèbres de K, pour tous $v \subset w \in W$, avec $A_w = F(A_w)^{\mathrm{a}} \cap K$. On suppose de plus que pour tout $w \in W$ non vide, les $(f_{\{i\},w}(A_{\{i\}}))_{i \in w} \subseteq A_w$ sont algébriquement indépendants sur $f_{\varnothing,w}(A_\varnothing)$ et $A_w \subseteq F(f_{\{i\},w}(A_{\{i\}}) : i \in w)^{\mathrm{a}}$.*

Par la Proposition **(3.61)**, les morphismes $f_{v,w} : A_v \to K$ sont K-élémentaires. En particulier, l'extension $f_{v,w}(A_v) \leqslant A_w \leqslant K$ est régulière. On note $\mathfrak{P}^-(\underline{n}) = \mathfrak{P}(\underline{n}) \smallsetminus \{\underline{n}\}$.

$\mathfrak{P}(\cdot)$ dénote l'ensemble des parties.

Théorème 5.10 (Amalgamation supérieure, Hrushovski, 1991) **:** *Tout $\mathfrak{P}^-(\underline{n})$-système d'amalgamation f se prolonge en un $\mathfrak{P}(\underline{n})$-système d'amalgamation g, dans $K^\bullet \succcurlyeq K$; c'est à dire, pour tout $v \subset w \in \mathfrak{P}^-(\underline{n})$, $g_{v,w} = f_{v,w}$.*

Démonstration. On procède par induction sur n. Le cas $n = 1$ est trivial. Soit f un $\mathfrak{P}^-(\underline{n+1})$-système d'amalgamation. Par induction, le $\mathfrak{P}^-(\underline{n})$-système d'amalgamation $g_{v,w} : C_v \to C_w$, où $g_{v,w} := f_{v\cup\{n\},w\cup\{n\}}$ et $C_w := A_{w\cup\{n\}}$, peut se prolonger en un $\mathfrak{P}(\underline{n})$-système que l'on note aussi g. On remarque que g n'induit pas un $\mathfrak{P}(\underline{n+1})$-système qui prolonge f : il nous manque la fonction $A_{\underline{n}} \to C_{\underline{n}}$.
Pour tout $w \subset \underline{n}$, on note $B_{w\cup\{n\}} := g_{w,\underline{n}}(A_{w\cup\{n\}}) \leqslant C_{\underline{n}}$. Soit $B_n := \prod_{w \subset \underline{n}} B_{w\cup\{n\}} \leqslant C_{\underline{n}}$. Pour tout $w \subset \underline{n}$, on note $B_w := g_{w,\underline{n}}(f_{w,w\cup\{n\}}(A_w)) \leqslant C_{\underline{n}}$ et $B^- := \prod_{w \subset \underline{n}} B_w \leqslant B_n$. On note aussi $A^- := \prod_{w \subset \underline{n}} f_{w,\underline{n}}(A_w) \leqslant A_{\underline{n}}$.
Comme $A_{\{i\}} \downarrow^{\mathrm{alg}}_{A_\varnothing} \prod_{j<i} A_{\{j\}}$ et $B_{\{i\}} \downarrow^{\mathrm{alg}}_{B_\varnothing} \prod_{j<i} B_{\{j\}}$, on peut étendre par induction sur i le l'isomorphisme, $g_0 : A_\varnothing \to B_\varnothing$ en un isomorphisme $g_i : \prod_{j<i} A_{\{j\}} \to \prod_{j<i} B_{\{j\}}$ (*cf.* lemma Lemme **(5.5)**). Par la Proposition **(3.58)**, on étend g_n en un isomorphisme $g^- : A^- \to B^-$ qui s'étend lui mème à $g^- : (A^-)^{\mathrm{a}} \supseteq A_{\underline{n}}$ et on note $B_{\underline{n}} := g^-(A_{\underline{n}})$.

Assertion 5.11 : $B_n \downarrow^{\mathrm{lin}}_{B_\varnothing} B_\varnothing^{\mathrm{a}}$.

Démonstration. Les extensions $B_\varnothing \leqslant B_{\{n\}} \leqslant C_{\underline{n}}$ sont régulières, *i.e.* $C_{\underline{n}} \downarrow^{\mathrm{lin}}_{B_\varnothing} B_\varnothing^{\mathrm{a}}$. Puisque $B_n \leqslant C_{\underline{n}}$, l'assertion en découle. $\lozenge$

Assertion 5.12 : $B_{\underline{n}} \downarrow^{\mathrm{lin}}_{B^-} B_\varnothing^{\mathrm{a}} B^-$.

Démonstration. L'extension $B_\varnothing \leqslant B_{\underline{n}}$ est régulière et donc $B_{\underline{n}} \downarrow^{\mathrm{lin}}_{B^-} B_\varnothing^{\mathrm{a}} B^-$. $\lozenge$

Assertion 5.13 : $B_\varnothing^{\mathrm{a}} B_{\underline{n}} \downarrow^{\mathrm{lin}}_{B_\varnothing^{\mathrm{a}} B^-} B_\varnothing^{\mathrm{a}} B_n$.

Démonstration(Assertion **(5.13)**). On veut montrer que $B_\varnothing B_{\underline{n}}^{\mathrm{a}} \downarrow^{\mathrm{lin}}_{B_\varnothing^{\mathrm{a}}} B_\varnothing^{\mathrm{a}} B_n$. Il suffit donc de le faire pour sous algèbres de type fini de $B_\varnothing B_{\underline{n}}^{\mathrm{a}} \leqslant (B_\varnothing^{\mathrm{a}} B^-)^{\mathrm{a}}$. Comme tous les corps considérés sont parfait, une telle extension est engendrée par un unique $c \in (B_\varnothing^{\mathrm{a}} B^-)^{\mathrm{a}}$. Il suffit alors de vérifier que les puissances de c qui sont linéairement indépendantes sur $B^{\mathrm{a}}_{\varnothing}B^-$ le restent sur $B^{\mathrm{a}}_{\varnothing}B_n$ — autrement dit le polynôme minimal P de c sur $B^{\mathrm{a}}_{\varnothing}B^-$ est irréductible sur $B^{\mathrm{a}}_{\varnothing}B_n$. Soient $Q, R \in B^{\mathrm{a}}_{\varnothing}[x, \overline{y}]$, un uplet $b_n \in B_{\{n\}}$ et $d_w \in B_w(b_n)^{\mathrm{a}}$, tel que $P(x) = Q(x, \overline{d})R(x, \overline{d})$. Comme $B^{\mathrm{a}}_{\varnothing}B_n \downarrow^{\mathrm{lin}}_{B^{\mathrm{a}}_{\varnothing}} B^{\mathrm{a}}_{\varnothing}B^-$, par la Proposition **(5.4)**, $\mathrm{tp}(b_n/B^-)$ est finiment satisfiable dans $B^{\mathrm{a}}_{\varnothing}$ et donc il existe $a \in B^{\mathrm{a}}_{\varnothing}$ et $e_w \in (B_w a)^{\mathrm{a}} \leqslant B^{\mathrm{a}}_w \leqslant B^{\mathrm{a}}_{\varnothing}B^-$ tel que $\deg(Q(x, \overline{e})) = \deg(Q(x, \overline{d}))$ et $P(x, \overline{b}) = Q(x, \overline{e})R(x, \overline{e})$. Comme P est irréductible sur $B^{\mathrm{a}}_{\varnothing}B^-$, $\deg(Q(x, \overline{e}))$ est soit égal à $\deg(P(x, \overline{b}))$ soit nul, ce qui conclut la preuve. ◊

Assertion 5.14 : *L'extension $B_{\varnothing} \leqslant B_n B_{\underline{n}}$ est régulière.*

Démonstration. On a $B_{\underline{n}} \downarrow^{\mathrm{lin}}_{B^-} B^{\mathrm{a}}_{\varnothing}B^-$ et $B^{\mathrm{a}}_{\varnothing}B_{\underline{n}} \downarrow^{\mathrm{lin}}_{B^{\mathrm{a}}_{\varnothing}B^-} B^{\mathrm{a}}_{\varnothing}B_n$; d'où $B_{\underline{n}} \downarrow^{\mathrm{lin}}_{B^-} B^{\mathrm{a}}_{\varnothing}B_n$. En particulier, $B_{\underline{n}}B_n \downarrow^{\mathrm{lin}}_{B_n} B^{\mathrm{a}}_{\varnothing}B_n$. De plus, $B_n \downarrow^{\mathrm{lin}}_{B_{\varnothing}} B^{\mathrm{a}}_{\varnothing}$ et donc $B_{\underline{n}}B_n \downarrow^{\mathrm{lin}}_{B_{\varnothing}} B^{\mathrm{a}}_{\varnothing}$. ◊

Par le Lemme **(2.52)**, on trouve un corps algébriquement clos $\mathfrak{C}$ contenant K et un morphisme de $A_{\varnothing}$-algèbre $f : B_n B_{\underline{n}} \to \mathfrak{C}$ tel que $f(B_n B_{\underline{n}}) \downarrow^{\mathrm{alg}}_{A_{\varnothing}} K$ — la structure de $A_{\varnothing}$-algèbre de $B_n B_{\underline{n}}$ est donnée par l'isomorphisme $A_{\varnothing} \to B_{\varnothing}$.

Assertion 5.15 : *L'extension $K \leqslant K f(B_n B_{\underline{n}})$ est régulière.*

Démonstration. On a $f(B_n B_{\underline{n}}) \downarrow^{\mathrm{alg}}_{A_{\varnothing}} K^{\mathrm{a}}$ et donc, comme $B_{\varnothing} \leqslant B_n B_{\underline{n}}$, $f(B_n B_{\underline{n}}) \downarrow^{\mathrm{lin}}_{A_{\varnothing}} K^{\mathrm{a}}$; d'où $K f(B_n B_{\underline{n}}) \downarrow^{\mathrm{lin}}_{K} K^{\mathrm{a}}$. ◊

Il existe donc un morphisme $h : K f(B_n B_{\underline{n}}) \to K^{\bullet}$ tel que $h|_K$ est élémentaire. On prolonge alors f à $\mathfrak{P}(\underline{n+1})$ en posant $A_{\underline{n+1}} := f(B_n B_{\underline{n}})^{\mathrm{a}} \cap K^{\bullet}$. □

Corollaire 5.16 (Théorème d'indépendance) **:** *Soit $K \vDash \mathrm{PPAC}_{\mathfrak{d}}$, $A = A^{\mathrm{a}} \cap K \leqslant K$ une sous-$C_{\mathfrak{d}}$-algèbre, $a_1 \in K^x$, $a_2 \in K^y$ avec $A(a_1) \downarrow^{\mathrm{alg}}_{A} A(a_2)$ et $c_1, c_2 \in K^z$ tel que $c_1 \equiv_A c_2$ et $A(c_i) \downarrow^{\mathrm{alg}}_{A} A(a_i)$, pour $i = 1, 2$. Il existe alors $c \in K^{\bullet} \succcurlyeq K$ tel que $c \equiv_{A(a_i)} c_i$, pour $i = 1, 2$, et $A(c) \downarrow^{\mathrm{alg}}_{A} A(a_1 a_2)$.*

Démonstration. Soit $A_{\varnothing} := A$, $A_{\{i\}} := A(a_i)^{\mathrm{a}} \cap K$ pour $i = 1, 2$ et $A_{\{0\}} := A(c_1)^{\mathrm{a}} \cap K \cong A(c_2)^{\mathrm{a}} \cap K$. On pose aussi $A_{\{1,2\}} := A(a_1 a_2)^{\mathrm{a}} \cap K$ et $A_{\{0,i\}} := A(a_i c_i)^{\mathrm{a}} \cap K$. Les fonctions f_{vw} sont toutes des inclusions sauf $f_{\{0\},\{0,2\}}$ qui est induit par l'isomorphisme $A(c_1)^{\mathrm{a}} \cap K \cong A(c_2)^{\mathrm{a}} \cap K$. On a alors un $\mathfrak{P}^-(3)$-système d'amalgamation dans K qui, par le Théorème **(5.10)**, se prolonge en un $\mathfrak{P}(3)$-système d'amalgamation dans $K^{\bullet} \succcurlyeq K$. On trouve alors, dans $A_{\{0.1,2\}}$, a'_i et c' algébriquement indépendants sur A tels que $c' a'_i \equiv_A c_i a_i$ et $a'_1 a'_2 \equiv_A a_1 a_2$. Quitte à agrandir $K^{\bullet}$ on trouve c tel que $c a_1 a_2 \equiv A c' a'_1 a'_2$ qui a donc toutes les propriétés voulues. □

Définition 5.17 (Division) **:** *Soit M une A-algèbre, $\varphi \in \mathcal{F}_A(x, y)$ et $b \in M^y$. On dit que $\varphi(x, b)$ divise (*divides*) sur A s'il existe $k \in \mathbb{Z}_{>0}$ et $(b_i)_{i \geqslant 0} \in M^{\bullet} \succcurlyeq M$ tel que $b_i \equiv_A b$ et tout sous-ensemble de taille k de $\{\varphi(x, b_i) : i \geqslant 0\}$ est inconsistant.*

La définition de la division peut être simplifiée un peu en utilisant une suite indiscernable :

Remarque 5.18 : La formule $\varphi(x, b)$ divise sur A si et seulement s'il existe une suite indiscernable $(b_i)_{i \geqslant 0} \in M^{\bullet} \succcurlyeq M$ tel que $b_0 = b$ et $\{\varphi(x, b_i) : i \geqslant 0\}$ est inconsistant.

Définition 5.19 (Déviation) **:** *Soit M une A-algèbre. Un type partiel $p(x)$ sur M dévie (*forks*) sur A s'il implique une disjonction finie de formules $\psi_i \in \mathcal{F}_{M^{\bullet}}(x)$, où $M^{\bullet} \succcurlyeq M$, telles que chaque ψ_i divise sur A.*

Notation 5.20 ($\downarrow^{\mathrm{f}}$) **:** Pour toutes A-algèbres $B, C, E \leqslant M$, on note $B \downarrow^{\mathrm{f}}_E C$ si $\mathrm{tp}(B/C)$ ne dévie pas sur E.

Définition 5.21 (Théorie simple) **:** *Une A-théorie T est simple si $\downarrow^{\mathrm{f}}$ a un caractère local : pour toutes sous-A-algèbres $B, C \leqslant M \vDash T$, avec B de type fini, il existe une sous-A-algèbre $E \leqslant C$ telle que $|E| \leqslant |A| + \aleph_0$ et $B \downarrow^{\mathrm{f}}_E C$;*

Théorème 5.22 (Kim-Pillay, 1997) **:** *Soit T une A-théorie et $B \downarrow_E C$ une relation sur les triplets de sous-A-algèbres $B, C, E \leqslant M \vDash T$. Sont équivalents :*

1. *T est simple et $\downarrow = \downarrow^{\mathrm{f}}$;*
2. *$\downarrow$ vérifie, pour tous $M, M' \vDash T$, tous uples $b, c, e, a_1, a_1, c_1, c_2 \in M$ et $b', c', e' \in M'$ et sous-A-algèbres $B, E, C, D \leqslant M$:*
   - *(Invariance)* $\mathrm{tp}^M_A(bce) = \mathrm{tp}^M_A(b'c'e')$ *et* $A[b] \downarrow_{A[e]} A[c]$ *implique* $A[b'] \downarrow_{A[e']} A[c']$ *;*
   - *(Monotonicité)* $B \downarrow_E CD$ *implique* $B \downarrow_E C$ *et* $B \downarrow_{EC} D$ *;*
   - *(Transitivité)* $B \downarrow_E C$ *et* $B \downarrow_{EC} D$ *impliquent* $B \downarrow_E CD$ *;*
   - *(Symétrie)* $B \downarrow_E C$ *implique* $C \downarrow_E B$ *;*
   - *(Caractère fini)* $B \downarrow_E C_0$ *pour toute A-algèbre $C_0 \leqslant C$ de type fini implique* $B \downarrow_E C$ *;*
   - *(Existence) il existe* $b' \in M^\bullet \succcurlyeq M$ *tel que* $b' \equiv_E b$ *et* $A[b] \downarrow^{\mathrm{alg}}_E C$ *;*
   - *(Caractère local) il existe* $C_0 \leqslant C$ *tel que* $|C_0| \leqslant |A| + |B| + \aleph_0$ *et* $B \downarrow_{C_0} C$ *;*
   - *(Indépendance) il existe* $c \in N^\bullet \succcurlyeq N$ *tel que* $c \equiv_{MA_i} c_i$ *et* $c \downarrow_M A[a_1 a_2]$.

Remarque 5.23 : Il existe une caractérisation similaire de la stabilité. Il faut remplacer l'indépendance par la propriété plus forte de stationarité sur les modèles : soit $M \vDash T$, B, C_1 et C_2 des sous-A-algèbres de modèles de T telles que $C_1 \equiv_M C_2$ et $C_i \downarrow_M B$, pour $i = 1, 2$, on a alors $C_1 \equiv_B C_2$.

Proposition 5.24 : *La théorie* $\mathrm{PPAC}_{\mathfrak{d}}$ *est simple et* $\downarrow^{\mathrm{f}} = \downarrow^{\mathrm{alg}}$.

Démonstration. Il suffit de vérifier que $\downarrow^{\mathrm{alg}}$ vérifie les propriétés du Théorème **(5.22)**. L'invariance est évidente puisque qu'il suffit que $BCE \cong B'C'E'$ pour que $\downarrow^{\mathrm{alg}}$ soit préservé. La monotonicité et la transitivité suivent de l'additivité du degré de transcendance dans les tours d'extensions. La symétrie aussi (*cf.* Lemme **(2.48)**). Le caractère fini provient du fait que pour tout corps algébriquement clos est l'union des clôtures algébriques de ses sous-corps de type fini.
L'existence suit du théorème d'amalgamation pour $n = 2$. Mais c'est un cas facile à voir : soient $B, C, E \leqslant K \vDash \mathrm{PPAC}_{\mathfrak{d}}$ des $C_{\mathfrak{d}}$-algèbres. Soit $\overline{B} := B^{\mathrm{a}} \cap K$. Par le Lemme **(2.52)**, il existe $\Omega \succcurlyeq K$ et $\overline{B}' \leqslant \Omega$ tel que $\overline{B} \cong_E \overline{B}'$ et $\overline{B}' \downarrow^{\mathrm{alg}}_E K$. En particulier $\overline{B}' \downarrow^{\mathrm{alg}}_E C$. De plus, $\overline{B}' \downarrow^{\mathrm{alg}}_{E^{\mathrm{a}} \cap K} K^{\mathrm{a}}$ et donc $\overline{B}' \downarrow^{\mathrm{lin}}_{E^{\mathrm{a}} \cap K} K^{\mathrm{a}}$. Il s'ensuit que $K\overline{B}' \downarrow^{\mathrm{lin}}_K K^{\mathrm{a}}$, c'est-à-dire $K \leqslant KB'$ et donc B' se plonge (au dessus de E) dans $K^\bullet \succcurlyeq K$. Par la Proposition **(3.61)** $\overline{B} \equiv_E \overline{B}'$.
Pour ce qui est du caractère local, soit $b \in B^x$ qui engendre B (en tant qu'anneau). Soit V la C-clôture de Zariski de b et E le corps de définition de B. Par noethérianité de $C[x]$, $|E| \leqslant \aleph_0$. Par la Proposition **(2.39)**, $E[b] \downarrow^{\mathrm{lin}}_E C$, en particulier $B \downarrow^{\mathrm{alg}}_E C$.
L'indépendance, enfin, a été démontrée au Corollaire **(5.16)**. □

5.3 Les imaginaires

On a vu dans la Proposition **(4.8)**, que toute F-variété V a un plus petit corps de définition et que ce corps est laissé fixe point par point par les automorphismes qui stabilisent V globalement. Le but de cette section est d'étendre ce résultats à tous les ensembles définissables dans un corps $\mathrm{PPAC}_{\mathfrak{d}}$.

Pour des raisons qui deviendront apparentes plus tard (*cf.* Définition **(5.36)**), nous allons sortir du cadre du langage des anneaux et commencer à travailler dans le cadre général de la logique du premier ordre avec des sortes.

Définition 5.25 (Language) **:** *Un language $\mathfrak{L}$ est la donnée de :*

- *un ensemble $\mathfrak{X}$ — ce sont les sortes de $\mathfrak{L}$;*
- *pour tout uple fini $X \in \mathfrak{X}$, un ensemble $\mathfrak{R}_X$ — ce sont les relations sur $\prod_i X_i$;*
- *pour tout uple fini $X \in \mathfrak{X}$ et singleton $Y \in \mathfrak{X}$, un ensemble $\mathfrak{f}_{X,Y}$ — ce sont les fonctions $\prod_i X_i \to Y$.*

On fixe $\mathfrak{L}$ un language.

Définition 5.26 (Structure) **:** *Une $\mathfrak{L}$-structure et la donnée de :*

- *pour tout $X \in \mathfrak{X}$ un ensemble $X(M)$;*
- *pour tout $R \in \mathfrak{R}_X$ un sous-ensemble $R(M) \subseteq \prod_i X_i(M)$;*
- *pour tout $f \in \mathfrak{f}_{X,Y}$ une fonction $f^M : \prod_i X_i(M) \to Y(M)$.*

On fixe des ensembles dénombrables disjoints $(V_X)_{X\in\mathfrak{X}}$ — les variables de sorte X.

Définition 5.27 (Syntaxe) **:** *Pour tout uple $x := (x_i)_i$ de variables et singleton $Y \in \mathfrak{X}$, on définit l'ensemble des termes par induction :*

- *$x_i \in \mathfrak{T}(x, X_i)$ où $x_i \in V_{X_i}$;*
- *si $f \in \mathfrak{f}_{X,Y}$ et pour tout i, $t_i \in \mathfrak{T}(z, X_i)$, alors $f(t) \in \mathfrak{T}(z, Y)$.*

On définit aussi l'ensemble des formules $\mathfrak{F}(x)$ par induction :

- *si $R \in \mathfrak{R}_{X,Y}$ et pour tout i, $t_i \in \mathfrak{T}(z, X_i)$, alors $R(t) \in \mathfrak{F}(z)$;*
- *si $t_1, t_2 \in \mathfrak{T}(x, X)$, $t_1 \simeq t_2 \in \mathfrak{F}(x)$;*
- *$\perp \in \mathfrak{F}(x)$;*
- *si $\varphi, \psi \in \mathfrak{F}(x)$, alors $\varphi \to \psi \in \mathfrak{F}(x)$;*
- *si $\varphi \in \mathfrak{F}(yx)$, alors $\exists y\, \varphi \in \mathfrak{F}(x)$.*

On définit alors de manière évidente l'interprétation d'un terme et d'une formule et on peut refaire toutes la théorie des modèles dans ce nouveau cadre. Pour toute $\mathfrak{L}$-structure M et tout $A \subseteq M$, on note $\mathfrak{L}(A)$ le language $\mathfrak{L}$ enrichi d'une constante par élément de A. On munit M de sa $\mathfrak{L}(A)$-structure naturelle.

Revenons maintenant à la question des plus petits ensembles de définition. On fixe M une $\mathfrak{L}$-structure et X un ensemble $\mathfrak{L}(M)$-définissable, en les variables x — c'est à dire $X \subseteq \prod_i X_i$ où $x_i \in V_{X_i}$.

Définition 5.28 : *Soit $\varphi \in \mathfrak{F}(xy)$ une formule. On dit que $a \in M^y$ est un paramètre canonique de X via φ si pour tout $c \in M^y$,*

$$\varphi(M, c) = X(M) \text{ si et seulement si } c = a.$$

On autorise y a être le uple vide. Le uple vide est un paramètre canonique de X si et seulement si X est $\mathfrak{L}$-définissable.

Soit $A \subseteq M$ — c'est à dire $A \subseteq \bigcup_{X \in \mathfrak{X}} X(M)$. On dit que $a \in M$ est $\mathcal{L}(A)$-définissable si $\{a\}$ est $\mathcal{L}(A)$-définissable. On note $\operatorname{dcl}(A) := \{a \in M : a \text{ est } \mathcal{L}(A)\text{-définissable}\}$.

En écrivant les preuves, je me suis rendu compte que je ne faisais pas assez attention aux ensembles $\mathfrak{L}$-définissables. J'autorise explicitement le uple vide comme paramètre canonique pour ne pas casser bêtement les équivalences plus tard.

Lemme 5.29 : *Soit a un paramètres canonique de X (via une formule φ). Pour tout $A \subseteq M$, sont équivalents :*

1. *X est $\mathcal{L}(A)$-définissable ;*
2. *$a \in \operatorname{dcl}(A)$;*
3. *$\operatorname{dcl}(a) \subseteq \operatorname{dcl}(A)$.*

Démonstration.

1 ⇒ 2 Soit $\psi \in \mathfrak{F}_A(x)$ qui définit X. On a alors, pour tout $c \in M^y$, $M \vDash \forall x\, \varphi(x, c) \leftrightarrow \psi(x)$ si et seulement si $c = a$ ce qui prouve que $a \in \operatorname{dcl}(A)$.

2 ⇒ 1 Soit $\psi \in \mathfrak{F}_A(y)$ qui définit a et $\theta(x) := \exists y\, \psi(y) \wedge \varphi(xy) \in \mathfrak{F}_A(x)$. On a $\theta(M) = X(M)$ qui est donc bien $\mathfrak{L}(A)$-définissable.

2 ⇒ 3 On peut vérifier que $\operatorname{dcl}(\operatorname{dcl}(C)) = C$ et si $C \subseteq A$, on a $\operatorname{dcl}(C) \leqslant \operatorname{dcl}(B)$. Il s'ensuit que $\operatorname{dcl}(a) \subseteq \operatorname{dcl}(\operatorname{dcl}(A)) = \operatorname{dcl}(A)$.

3 ⇒ 2 On a $a \in \operatorname{dcl}(a) \subseteq \operatorname{dcl}(A)$. □

On a donc que $\operatorname{dcl}(a)$ est le plus petit ensemble dcl-clos de définition de X.

Remarque 5.30 : On a aussi, pour tout $\sigma \in \operatorname{Aut}(M)$, $\sigma(X) = X$ si et seulement si $\sigma|_{\operatorname{dcl}(a)} = \operatorname{id}$.

On fixe maintenant T une $\mathfrak{L}$-théorie. Le principal problème pour appliquer les résultats ci-dessus, c'est que les paramètres canoniques n'existent pas toujours…

Définition 5.31 (Élimination des imaginaires, Poizat, 1983) **:** *On dit que*

- *T élimine les imaginaires si pour tout ensemble $\mathfrak{L}(M)$-définissable, où $M \vDash T$, il existe $\varphi \in \mathfrak{F}(xy)$ et $b \in M^z$ un paramètre canonique de X via φ.*
- *T élimine uniformément les imaginaires si pour tout $Y \subseteq X \times V$ $\mathfrak{L}$-définissables, il existe $Z \subseteq X \times W$ $\mathfrak{L}$-définissables tel que pour tout $M \vDash T$ et $a \in V(M)$, il existe un unique $b \in W(M)$ tel que $Y_a(M) := \{c \in X(M) : ca \in Y\} = Z_b(M)$.*

Un reformulation syntaxique de l'élimination uniforme est la suivante : pour toute formule $\varphi \in \mathfrak{F}(xv)$, il existe des formules $\psi \in \mathfrak{F}(xw)$ et $\theta \in \mathfrak{F}(w)$ telles que :

$$T \vDash \forall v \exists w_0\ (\theta(w_0) \wedge \forall w\, \theta(w) \to ((\forall x\, \varphi(x, v) \leftrightarrow \psi(x, w)) \leftrightarrow w = w_0))\,.$$

La définition de l'élimination uniforme des imaginaires est plus compliquée que la définition naïve la plus naturelle — en particulier, θ est nécessaire pour obtenir la Proposition **(5.34)**.

La terminologie semble probablement un peu obscure, mais elle fait référence au fait que, lors du développement de la théorie de stabilité, Shelah nomme les classes d'équivalences de relations d'équivalence définissables des « imaginaires » ; et comme l'on verra plus loin — *cf.* Proposition **(5.34)** — l'élimination (uniforme) des imaginaires a trait au fait de pouvoir remplacer ces éléments « imaginaires » par des éléments « réels ».

Définition 5.32 (Quotient représenté) **:** *Soit M $\mathfrak{L}$-structure, $A \subseteq M$, X et $E \subseteq X^2$ des ensembles $\mathfrak{L}(A)$-définissables tels que $E(M)$ est une relation d'équivalence sur $X(M)$. On dit que E est* *représentée sur A dans M s'il existe une fonction $\mathfrak{L}(A)$-définissable $f : X \to Y$ telle que, pour tous $c_1, c_2 \in X(M)$:*

$$M \vDash c_1 E c_2 \leftrightarrow f(c_1) = f(c_2).$$

La fonction f induit alors une bijection $X(M)/E(M) \cong f(X(M))$ et l'ensemble « $\mathfrak{L}(M)$-interprétable » X/E peut être identifié avec l'ensemble $\mathfrak{L}(M)$-définissable $f(X)$.

Définition 5.33 : *On dit que les unions disjointes sont représentées dans T si pour tout uples finis $X, Y \in \mathfrak{X}$, il existe un uple $Z \in \mathfrak{X}$ et des fonctions $\mathfrak{L}$-définissables injectives , $\iota_X : X \to Z$ et $\iota_Y : Y \to Z$ dont les images sont disjointes (modulo T).*

C'est à dire qu'il existe des formules $\varphi \in \mathfrak{F}(xz)$ et $\psi \in \mathfrak{F}(yz)$ avec $x \in V_X := \prod_i V_{X_i}$, $y \in V_Y$ et $z \in V_Z$ telles que :

$$\begin{aligned} T \vDash & \forall x\, (\exists z\, \varphi(xz) \wedge \forall z_1 \forall z_1\, \varphi(xz_1) \wedge \varphi(xz_2) \to z_1 = z_2) \wedge \\ & \forall y\, (\exists z\, \psi(yz) \wedge \forall z_1 \forall z_1\, \psi(yz_1) \wedge \psi(yz_2) \to z_1 = z_2) \wedge \\ & \forall x \forall y \forall z\, \neg(\varphi(xz) \wedge \varphi(yz)). \end{aligned}$$

On identifie ici un uple de sortes X avec l'ensemble $\mathfrak{L}$-définissable $\prod_i X_i$. On autorise de nouveau le uple vide dont le seul point est le uple vide. En particulier, quitte à prendre pour X et Y le uple vide, on voit qu'il existe une sorte S qui contient deux éléments de $\mathrm{dcl}(\varnothing)$.

Nous pouvons maintenant décrire les liens entre l'élimination, l'élimination uniforme des imaginaires et la représentation des quotients :

Proposition 5.34 : *On suppose que les unions disjointes sont représentées dans T. Sont équivalents :*

1. *T élimine uniformément les imaginaires ;*
2. *toute relation d'équivalence $\mathfrak{L}(A)$-définissable, où $A \subseteq M \vDash T$, est représentée sur A ;*
3. *T élimine les imaginaires.*

J'ai réorganisé les équivalences après m'être rendu compte qu'aucun de ces trois énoncés n'implique la représentation des unions disjointes... J'avais oublié deux structures pénibles : la structure vide et la structure singleton. Mon plan initial était de modifier la syntaxe pour incorporer les unions disjointes de produits de sortes, mais ça rendait la syntaxe encore un peu plus incompréhensible.

Démonstration.

$1 \Rightarrow 2$ Soient $\varphi \in \mathfrak{F}(xy)$ et $\psi \in \mathfrak{F}(x_1x_2y)$ et $a_0 \in A^y$ tels que $\psi(M, M, a_0)$ soit une relation d'équivalence sur $\varphi(M, a_0)$. Soit $Z \subseteq X \times W$ tels que pour tout $ca \in \varphi(M, M)$, il existe un unique $b \in W(M)$ tel que $Z_b = \psi(M, c, a)$. On note f la fonction $\mathfrak{L}(a_0)$-définissable qui à tout $c \in \varphi(M, a_0)$ associe l'unique b tel que ci-dessus. Comme $\psi(M, c, a_0)$ est la classe de $c \in \varphi(M, a_0)$, on a $f(c_1) = f(c_2)$ si et seulement si $\psi(M, c_1, a_0) = Z_{f(c_1)} = Z_{f(c_2)} = \psi(M, c_2, a_0)$, *i.e.* $M \vDash \psi(c_1, c_2, a_0)$.

$2 \Rightarrow 3$ Soit $\varphi \in \mathfrak{F}(xy)$. On considère $\psi(y_1, y_2) := \forall x\, \varphi(xy_1) \leftrightarrow \varphi(xy_2) \in \mathfrak{F}(y_1y_2)$ qui définit une relation d'équivalence E $\mathfrak{L}$-définissable sur le produit de sortes Y de y. Soit $f : Y \to W$ $\mathfrak{L}$-définissable qui représente E. Soit $a_0 \in M^y$ tel que $\varphi(M, a_0) \neq \varnothing$. On définit alors $\theta := \exists y\, f(y) = w \wedge \varphi(x, y) \in \mathfrak{F}(xw)$. Pour tout $c \in M^w$, soit $c \in f(Y(M))$ et $\theta(M, c) = \varphi(M, a)$, pour tout $a \in M^y$ tel que $f(a) = c$. Si $c \notin f(Y(M))$, $\theta(M, c) = \varnothing$. On a donc bien $\theta(M, c) = \varphi(M, a_0)$ si et seulement si $c = f(a_0)$. Si $\varphi(M, a_0) = \varnothing$, on peut choisir $\theta := \bot \in \mathfrak{F}(x)$ et le uple vide[3] est alors un paramètre canonique de $\varphi(M, a_0)$ via θ.

3. Aux grand maux, les grands remèdes !

$3 \Rightarrow 1$ Soient $Y \subset X \times V$ des ensembles $\mathfrak{L}$-définissables. Pour tout $M \models T$ et $a \in V(M)$, il existe $\varphi \in \mathfrak{F}(xw)$ et $c \in M^w$ un paramètre canonique de Y_a via φ. L'ensemble $\pi(v) := \{\neg\exists w \forall w' \, (\forall x, \varphi(xw') \leftrightarrow xv \in Y) \leftrightarrow w = w' : \varphi \in \mathfrak{F}\}$ est donc inconsistant avec T. Il existe donc $\varphi_i \in \mathfrak{F}(xw_i)$, pour $i < n$, tels que pour tout $M \models T$ et $a \in V(M)$, il existe $i < n$ et $c \in M^{w_i}$ qui est un paramètre canonique de Y_a via φ_i. Soient $\iota_i : W_i \to W$ qui représentent l'union disjointe des W_i, (uple de) sortes de w_i. On définit $\theta(w) := \bigvee_{i<n} \exists w_i \, \iota_i(w_i) = w \wedge \bigwedge_{j \leqslant i} \forall w_j (\forall v_j (\forall x \, \varphi_j(xv_j) \leftrightarrow \varphi_i(xw_i)) \leftrightarrow v_j = w_j) \leftrightarrow \iota_j(w_j) = \iota_i(w_i)$ et $\psi(xw) := \bigvee_{i<n} \exists w_i \, \iota_i(w_i) = w \wedge \varphi_i(xw_i)$. Pour tout $a \in V(M)$ il existe un unique $c \in \theta(M)$ tel que $Y_a = \psi(M, c)$. $\square$

Remarque 5.35 :

- les implications $1 \Rightarrow 2$ et $2 \Rightarrow 3$ n'utilisent pas la représentabilité des unions disjointes dans T.
- Les énoncés 1,2 et 3 sont valables dans la théorie (à une sorte) de la structure vide (resp. du singleton), mais les unions disjointes ne sont pas représentées.
- Supposons qu'il existe une sorte $X \in \mathfrak{X}$ telle que T implique que X contient au moins deux éléments. Sont équivalents :
  1. T élimine uniformément les imaginaires ;
  2. Les quotients sont représentés dans T (l'énoncé 2) ;
  3. T élimine les imaginaires et les unions disjointes sont représentés dans T.
- Supposons que $\mathfrak{L}$ n'ait qu'une seule sorte et que T $|\mathrm{dcl}(\varnothing)| \geqslant 2$. Les unions disjointes sont alors représentées dans T. Si T élimine les imaginaires, la réciproque est vérifiée.

Quitte à rajouter des sortes pour les points « imaginaires », on peut toujours supposer qu'une théorie élimine les imaginaires : 31/03

Définition 5.36 (La construction eq, Shelah) **:** *On dénote* $\mathfrak{L}^{\mathrm{eq}}$ *le language augmenté d'une sorte* $X_{\varphi,x}$ *et d'une fonction* $f_{\varphi,x} : \prod_i V_{Y_i} \to X_{\varphi,x}$ *où* $y_i \in V_{Y_i}$*, pour tout* $\varphi \in \mathfrak{F}(xy)$*. On note* T^{eq} *la* $\mathfrak{L}^{\mathrm{eq}}$*-théorie :*

On est en train de construire la théorie dont la catégorie syntaxique est le prétopos associé à la catégorie syntaxique de T.

$$T \cup \{\forall z \exists y\, f_{\varphi,x}(y) \simeq z \wedge \\ \forall y_1 y_2\ (f_{\varphi,x}(y_1) = f_{\varphi,x}(y_2) \leftrightarrow (\forall x\, \varphi(xy_1) \leftrightarrow \varphi(xy_2))) : \varphi \in \mathfrak{F}(xy)\}.$$

Lemme 5.37 :

- *Pour tout* $M \vDash T$*, il existe un unique* $M^{\mathrm{eq}} \vDash T^{\mathrm{eq}}$ *(à unique* $\mathfrak{L}^{\mathrm{eq}}(M)$*-isomorphisme près) tel que pour tout* $X \in \mathfrak{F}^{\mathfrak{L}}$*,* $X(M^{\mathrm{eq}}) = M$*, pour tout* $R \in \mathfrak{R}^{\mathfrak{L}}$*,* $R(M^{\mathrm{eq}}) = R(M)$ *et, pour tout* $f \in \mathfrak{f}^{\mathfrak{L}}$*,* $f^{M^{\mathrm{eq}}} = f^M$ *— on dit que* M^{eq} *est un* $\mathfrak{L}^{\mathrm{eq}}$*-enrichissement de* M*.*
- *Si* $N \vDash T^{\mathrm{eq}}$*, alors la restriction* $M := N|_{\mathfrak{L}}$ *de* N *à* $\mathfrak{L}$ *est un modèle de* T*. En particulier, il existe un unique* $\mathfrak{L}^{\mathrm{eq}}(M)$*-isomorphisme* $M^{\mathrm{eq}} \cong_M N$*.*
- *Pour tout* $\varphi \in \mathfrak{F}^{\mathfrak{L}^{\mathrm{eq}}}(y)$*, il existe* $\psi \in \mathfrak{F}^{\mathfrak{L}}(z)$ *telle que* $T^{\mathrm{eq}} \vDash \forall z \varphi(f(z)) \Leftrightarrow \psi(z)$*, où* $f_i(z_i) = f_{\theta,x}(z_i)$ *si* $y_i \in V_{X_{\theta,x}}$ *et* $f_i(z_i) = z_i = y_i$ *sinon.*
- T^{eq} *élimine uniformément les imaginaires.*

Démonstration.

- Soit M^{eq} le $\mathfrak{L}^{\mathrm{eq}}$-enrichissement de M tel que $X_{\varphi,x}(M^{\mathrm{eq}}) = Y(M)/E_{\varphi,x}$ où $y_1 E_{\varphi,x} y_2$ si $\varphi(M, y_1) = \varphi(M, y_2)$. On interprète $f_{\varphi,x}^{M^{\mathrm{eq}}} : Y(M) \to X_{\varphi,x}(M)$ comme la projection canonique. On vérifie aisément que $M^{\mathrm{eq}} \vDash T^{\mathrm{eq}}$. Soit $N \vDash T^{\mathrm{eq}}$ un autre $\mathfrak{L}^{\mathrm{eq}}$-enrichissement de M. Pour tout $a \in X_{\varphi,x}(N)$, il existe $c \in Y(M)$ tel que $f_{\varphi,x}^N(c) = a$. On définit $\sigma(a) = c/E_{\varphi,x}$. Si $a \in M$, on définit $\sigma(a) = a$. On peut alors vérifier que σ est bien défini et que c'est un $\mathfrak{L}^{\mathrm{eq}}(M)$-isomorphisme. De plus comme tout élément de N et de M^{eq} est l'image par un terme d'un élément de M, cet isomorphisme est uniquement déterminé par sa restriction à M — ici l'identité.
- Comme $T \subseteq T^{\mathrm{eq}}$, il est évident que $M = N|_{\mathfrak{L}} \vDash T$. Le reste suit du point précédent.
- On procède par induction sur φ. Pour les formules atomiques de la forme $\varphi := R(t)$ où $R \in \mathfrak{R}^{\mathfrak{L}}$, puisque des variables de sortes $X_{\theta,x}$ ne peuvent pas apparaître dans un terme de codomaine dans $\mathfrak{X}^{\mathfrak{L}}$, on a donc $\varphi(f(z)) = \varphi(y) \in \mathfrak{F}^{\mathfrak{L}}$ et le résultat suit. Si $\varphi := t_1 \simeq t_2$ où t_j est de codomaine dans $\mathfrak{X}^{\mathfrak{L}}$, le même raisonnement s'applique. Si t_j est de codomaine $X_{\theta,x}$, soit $t_j := f_{\theta,x}(s_j)$ où s_j est un uple de $\mathfrak{L}$-termes — avec possiblement des variables inutiles des nouvelles sortes. On pose $\psi := \forall x\, \theta(x, s_1) \leftrightarrow \theta(x, s_2)$ et le résultat suit. Sinon t_j est la projection sur une variable x_{i_j} et on peut prendre $\psi := \forall x\, \theta(x, y_{i_1}) \leftrightarrow \theta(x, y_{i_2})$. Ceci conclut le cas des formulas atomiques.
  Les combinaisons booléennes sont évidentes et si $\varphi := \exists t \theta(yt)$, soit χ (et fg) obtenus par induction : $T^{\mathrm{eq}} \vDash \forall zs\, \theta(f(z)g(s)) \leftrightarrow \chi(zs)$. Comme g est surjective, on a alors $T^{\mathrm{eq}} \vDash \forall z\, (\exists t\, \theta(f(z)t) \leftrightarrow \exists s\, \chi(zs))$.
- Soient $\varphi \in \mathfrak{F}^{\mathfrak{L}^{\mathrm{eq}}}(xy)$ et $\psi \in \mathfrak{F}^{\mathfrak{L}}(vz)$ et gf tels qu'au dessus : $T^{\mathrm{eq}} \vDash \forall vz\, \varphi(g(v)f(z)) \leftrightarrow \psi(vz)$. On a alors, puisque g est surjective, $T^{\mathrm{eq}} \vDash (\forall x\, \varphi(xf(z_1)) \leftrightarrow \varphi(xf(z_2))) \leftrightarrow (\forall v\, \psi(vz_1) \leftrightarrow \psi(vz_2))$. Soit $\theta(xt) := \exists z\, f_{\psi,v}(z) = t \wedge \varphi(xf(z))$.

Pour tout $a_0 \in (M^{\mathrm{eq}})^y$, soit $b_0 \in M^z$ tel que $f(b_0) = a_0$ et $c_0 := f_{\psi,v}(b_0)$. Pour tout $c \in X_{\psi,v}(M^{\mathrm{eq}})$, on a $\theta(M, c) = \varphi(M, a_0)$ si et seulement s'il existe $b \in M^z$ tel que $f_{\psi,v}(b) = c$ et $\psi(M, b) = \varphi(M^{\mathrm{eq}}, f(b)) = \varphi(M^{\mathrm{eq}}, a_0) = \varphi(M^{\mathrm{eq}}, f(b_0)) = \psi(M, b_0)$, ce qui est équivalent à $c = f_{\psi,v}(b) = f_{\psi,v}(b_0) = c_0$. □

On est alors en droit de se demander quelle est l'intérêt de la question de l'élimination des imaginaires. Si on étudie une théorie précise — au hasard, ACF — rendre une propriété (syntaxique) vraie en changeant le language, que ce soit la morleyisation pour l'élimination des quantificateurs ou la construction eq pour l'élimination des imaginaires, est profondément inutile. Ce dont il faut se rendre compte c'est qu'obtenir un résultat d'élimination à tout prix, n'est pas, en soit, intéressant. C'est leur contenu descriptif qui nous importe. Autrement dit, un résultat d'élimination des quantificateurs n'est pas simplement une formalité syntaxique, c'est un résultat de description des ensembles définissables. La description donnée par l'élimination des quantificateurs dans le language morleyisé étant : « les ensembles définissables sont les ensembles définissables » cela ne nous avance pas à grand chose. De même, l'élimination (uniforme) des imaginaires dans T^{eq} nous décrit les ensembles interprétables comme étant les ensembles interprétables. Ce résultat nous dit aussi : « quitte à rajouter des paramètres canoniques, on a des paramètres canoniques » ; énoncé dont l'utilité est toute relative.
Ceci étant, vous pourriez vous demander pourquoi alors est-ce qu'on s'intéresse à la construction eq. La principale raison est que c'est un outil fondamental pour pouvoir raisonner sur les imaginaires : en en faisant des points « réels », on peut leur appliquer tous les résultats de théorie des modèles qu'on a déjà prouvé. En particulier, cela peut aider à prouver un résultat d'élimination des imaginaires et décrire ces points imaginaires que l'on vient de rajouter.
On note $\mathrm{dcl}^{\mathrm{eq}}$ la clôture définissable dans $M^{\mathrm{eq}} \vDash T^{\mathrm{eq}}$.

Définition 5.38 (Code) **:** *Soit M une $\mathfrak{L}$-structure et X un ensemble $\mathfrak{L}(M)$-définissable. On note* $\ulcorner X \urcorner := \mathrm{dcl}^{\mathrm{eq}}(a)$ *où $a \in M^{\mathrm{eq}}$ est un paramètre canonique de X.*

Remarque 5.39 : C'est le plus petit ensemble $\mathrm{dcl}^{\mathrm{eq}}$-clos de définition de X, qui ne dépend donc pas du choix de a.

Lemme 5.40 : *Soient M une $\mathfrak{L}$-structure et X un ensemble $\mathfrak{L}(M)$-définissable. Sont équivalents :*
1. *X admet un paramètre canonique — via une formule $\varphi \in \mathfrak{F}^{\mathfrak{L}}$;*
2. *X est $\mathfrak{L}(A)$-définissable où $A := \ulcorner X \urcorner \cap M$.*

Démonstration.
1 ⇒ 2 Soit $a \in M$ un paramètre canonique de X via $\varphi(xy) \in \mathfrak{F}^{\mathfrak{L}}$. Par définition, on a $\ulcorner X \urcorner = \mathrm{dcl}^{\mathrm{eq}}(a)$ et donc $a \in A$. Comme X est $\mathfrak{L}(a)$-définissable, il est aussi $\mathfrak{L}(A)$-définissable.
2 ⇒ 1 Soit $e_0 \in (M^{\mathrm{eq}})^y$ un paramètre canonique de X via $\varphi \in \mathfrak{F}^{L^{\mathrm{eq}}}(xy)$. Soient $\psi \in \mathfrak{F}^{\mathfrak{L}}(xz)$ et $a_0 \in M^z$ tels que $\psi(M, a_0) = X(M)$. Par définition de A, il existe $\theta \in \mathfrak{F}^{\mathfrak{L}^{\mathrm{eq}}}(yz)$ tel que $\theta(e_0, M) = \{a_0\}$. Soit $\chi(xz) := \exists y\, \theta(yz) \wedge (\forall x\, \varphi(xy) \leftrightarrow \psi(xz)) \wedge \psi(xz)$. Par le Lemme **(5.37)**, on peut supposer que $\chi \in \mathfrak{F}^{\mathfrak{L}}(xz)$.
On a $\chi(M, a_0) = \psi(M, a_0) = X(M)$. Soit $a \in M^z$ tel que $\chi(M, a) = X(M)$. On a donc e tel que $M^{\mathrm{eq}} \vDash \theta(ea)$ et $\varphi(M, e) = \varphi(M, a) = \chi(M, a) = X(M) = \varphi(M, e_0)$ et donc $e = e_0$. D'où $a \in \theta(M, e_0) = \{a_0\}$ et $a = a_0$. □

Corollaire 5.41 : *Sont équivalents :*

1. *T élimine les imaginaires ;*
2. *Pour tout $M \vDash T$ et $e \in M^{\mathrm{eq}}$, on a $e \in \mathrm{dcl}^{\mathrm{eq}}(\mathrm{dcl}^{\mathrm{eq}}(e) \cap M)$.*

Démonstration.

$1 \Rightarrow 2$ Si $e \in M$, l'énoncé 2 est évident. Si $e \in X_{\varphi,x}(M^{\mathrm{eq}})$, soit $a \in M$ un paramètre canonique de $f_{\varphi,x}^{-1}(e)$. Comme $f_{\varphi,x}^{-1}(e)$ est $\mathfrak{L}^{\mathrm{eq}}(e)$-définissable, $a \in \mathrm{dcl}^{\mathrm{eq}}(e) \cap M$. Comme $f_{\varphi,x}(f_{\varphi,x}^{-1}(e)) = \{e\}$, $e \in \mathrm{dcl}^{\mathrm{eq}}(a)$.

$2 \Rightarrow 1$ Soit $\varphi \in \mathfrak{F}^{\mathfrak{L}}(xy)$, $M \vDash T$ et $a \in M^y$. Comme $e := f_{\varphi,x}(a) \in \mathrm{dcl}^{\mathrm{eq}}(\mathrm{dcl}^{\mathrm{eq}}(e) \cap M) = \mathrm{dcl}^{\mathrm{eq}}(\ulcorner \varphi(x,a) \urcorner \cap M)$, l'ensemble $\varphi(x,a)$ est donc $\mathfrak{L}(\ulcorner \varphi(x,a) \urcorner \cap M)$-définissable et donc, par le Lemme **(5.40)**, $\varphi(x,a)$ admet un paramètre canonique dans M. □

Il y a une classe d'imaginaires qui jouent un rôle un peu particulier : les paramètres canoniques d'ensembles finis. Essentiellement parce que la distinction entre ensembles finis et infinis est plus notable que celle des singletons parmi les les ensembles finis, la clôture algébrique joue un rôle beaucoup plus important en théorie des modèles que la clôture définissable. En contrepartie, il est, en général, plus facile de trouver des paramètres canoniques à ensemble fini près.

Soit $A \subseteq M$. On dit que $a \in M$ est $\mathcal{L}(A)$-algébrique — ou plus simplement algébrique sur A — s'il existe X $\mathcal{L}(A)$-définissable fini tel que $a \in X(M)$. On note $\mathrm{acl}(A) := \{a \in M : a \text{ est } \mathcal{L}(A)\text{-algébrique}\}$.

Définition 5.42 (Élimination faible des imaginaires, Poizat, 1983) **:** *On dit que T élimine faiblement les imaginaires si pour tout $M \vDash T$ et $e \in M^{\mathrm{eq}}$, on a $e \in \mathrm{dcl}^{\mathrm{eq}}(\mathrm{acl}^{\mathrm{eq}}(e) \cap M)$.*

Remarque 5.43 : On pourrait aussi donner une définition syntaxique de l'élimination faible (uniforme) des imaginaires en terme de « paramètre presque canonique ».

Décrivons maintenant la différence entre l'élimination faible et l'élimination des imaginaires :

Proposition 5.44 : *Les énoncés suivants sont équivalents :*

1. *T élimine les imaginaires ;*
2. *T élimine faiblement les imaginaires et tout sous-ensemble fini de M^x, où $M \vDash T$ et x est un uple de variables, admet un paramètre canonique.*

Démonstration.

$1 \Rightarrow 2$ C'est évident par le Corollaire **(5.41)** et le fait que $\mathrm{dcl}^{\mathrm{eq}} \subseteq \mathrm{acl}^{\mathrm{eq}}$.

$2 \Rightarrow 1$ Soit $e \in M^{\mathrm{eq}}$. Par élimination faible, il existe un uple $d \in \mathrm{acl}^{\mathrm{eq}}(e) \cap M$ tel que $e \in \mathrm{dcl}^{\mathrm{eq}}(d)$. Soit $\varphi \in \mathfrak{F}^{\mathfrak{L}^{\mathrm{eq}}}(yx)$ tel que $\varphi(M^{\mathrm{eq}}, e)$ est fini minimal qui contient d. Soit f $\mathfrak{L}^{\mathrm{eq}}$-définissable tel que $f(d) = e$. On a alors $f(y) = e \cap \varphi(y,e)$ équivalent à $\varphi(y,e)$ par minimalité et donc $f(\varphi(M^{\mathrm{eq}}, e)) = \{e\}$. Soit b un paramètre canonique de $\varphi(x,e)$. On a alors $e \in \mathrm{dcl}^{\mathrm{eq}}(b)$ et $b \in \mathrm{dcl}^{\mathrm{eq}}(e)$. □

Comme on l'a vu, les paramètres canoniques ont un lien avec les automorphismes qui laissent globalement X invariant. On peut affiner ses résultats si l'on dispose de suffisamment d'automorphismes :

Définition 5.45 : *Soit κ un cardinal infini. La $\mathfrak{L}$-structure M est :*

- *κ-saturée si tout $p \in \mathcal{S}_x(A)$ avec $A \leqslant M$, $|A| < \kappa$ et $|x| < \kappa$ est réalisé dans M ;*
- *fortement κ-homogène si tout $f : A \to M$ avec $A \leqslant M$, $|A| < \kappa$, s'étend en $\sigma \in \mathrm{Aut}(M/A)$.*

Proposition 5.46 : *Pour tout cardinal infini κ et toute $\mathfrak{L}$-structure M, il existe $N \succcurlyeq M$ κ-saturée et fortement κ-homogène.*

Soit M $\aleph_0$-saturé et fortement $\aleph_0$-homogène. On peut alors caractériser $\ulcorner X \urcorner$ en terme d'automorphismes qui laissent globalement X invariant :

Lemme 5.47 : *Soit X un ensemble $\mathfrak{L}(M)$-définissable. On a :*

$$\ulcorner X \urcorner = \{a \in M^{\mathrm{eq}} : \forall \sigma \in \mathrm{Aut}(M^{\mathrm{eq}}), \sigma(X) = X \Rightarrow \sigma(a) = a\}.$$

Démonstration. Soit $a \in M^{\mathrm{eq}}$ un paramètre canonique de X via $\varphi(xy)$. Si $\varphi(M^{\mathrm{eq}}, a) = X(M) = \sigma(X(M)) = \varphi(M^{\mathrm{eq}}, \sigma(a))$, on a alors $a = \sigma(a)$ et donc $\sigma|_{\mathrm{dcl}^{\mathrm{eq}}(a)} = \mathrm{id}_{\mathrm{dcl}^{\mathrm{eq}}(a)}$. On a donc montré que $\ulcorner X \urcorner \subseteq \{a \in M^{\mathrm{eq}} : \forall \sigma \in \mathrm{Aut}(M^{\mathrm{eq}}), \sigma(X) = X \Rightarrow \sigma(a) = a\}$.
Réciproquement, soit $b \notin \ulcorner X \urcorner = \mathrm{dcl}^{\mathrm{eq}}(a)$. Il existe $c \in M^{\mathrm{eq}}$ tel que $c \equiv_{\ulcorner X \urcorner} b$ et $c \neq b$. Soit $\sigma \in \mathrm{Aut}(M/\ulcorner X \urcorner)$ tel que $\sigma(b) = c$. Comme X est $\mathfrak{L}^{\mathrm{eq}}(\ulcorner X \urcorner)$, on a $\sigma(X) = X$. Ce qui montre que $\ulcorner X \urcorner \supseteq \{a \in M^{\mathrm{eq}} : \forall \sigma \in \mathrm{Aut}(M^{\mathrm{eq}}), \sigma(X) = X \Rightarrow \sigma(a) = a\}$. □

Une autre utilité des modèles saturés et homogènes est qu'on peut détecter la définissabilité au dessus de paramètres avec des automorphismes :

Lemme 5.48 : *Soit M κ-saturé et fortement κ-homogène. $A \subseteq M$ avec $|A| < \kappa$ et X $\mathfrak{L}(M)$-définissable. Sont équivalents :*
1. *X est $\mathfrak{L}(A)$-définissable ;*
2. *pour tout $\sigma \in \mathrm{Aut}(M/A)$, $\sigma(X) = X$.*

On note $\mathfrak{F}_A$ l'ensemble des $\mathfrak{L}$-formules à paramètres dans A.

Démonstration.
1 ⇒ 2 C'est une conséquence de la (version pour $\mathfrak{L}$ quelconque de la) Proposition **(1.19)**.
2 ⇒ 1 Pour tout $a, b \in M^x$ tels que $a \equiv_A b$, il existe $\sigma \in \mathrm{Aut}(M/A)$ tel que $\sigma(a) = b$. On a donc $a \in X$ si et seulement si $b = \sigma(a) \in X$. Par la Proposition **(3.62)**, il existe $\varphi(x) \in \mathfrak{F}_A(x)$ telle que $X(M) = \varphi(M)$, c'est à dire X est $\mathfrak{L}(A)$-définissable. □

Revenons à l'élimination des imaginaires dans les corps $\mathrm{PPAC}_{\mathfrak{d}}$. On commence par les ensembles finis : 02/04

Proposition 5.49 : *Soit K un corps. Tout ensemble fini $C \subseteq K^x$ admet un paramètre canonique.*

Démonstration. Quitte à passer à une extension élémentaire, on peut supposer K $\aleph_0$-saturé et homogène. On note $\{c_1, \ldots, c_n\} := C$, $Q_i := X - \sum_j c_{i,j} Y_j$ et $P := \prod_i Q_i$. On remarque que les Q_i sont irréductibles. Soit a le uple des coefficients de P. Pour tout $\sigma \in \mathrm{Aut}(K)$, $\sigma(X) = X$ si et seulement si σ permute les Q_i, si et seulement si $\sigma(P) = P$, si et seulement si $\sigma(a) = a$. Il s'ensuit que $a \in \ulcorner C \urcorner \cap K$ et X est a-définissable. □

Proposition 5.50 : *Soit K un corps parfait et $X \neq \varnothing$ un ensemble K-définissable. On note $k := \mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner) \cap K$. Il alors existe une k-variété V géométriquement intègre telle que X soit consistant avec le type des K-génériques de V.*

Démonstration. Soit W la K-clôture de Zariski de X. Par la Proposition **(4.11)**, il existe $V_i \subseteq W$ des K-fermés de Zariski géométriquement intègres tels que $X \leqslant W(K) = \bigcup_i V_i(K)$. Il s'en suit que $W = \bigcup_i V_i$ et on peut donc supposer que les V_i sont exactement les composantes géométriquement intègres de W. Soit $V := V_0$. Pour tout $U \subset V$, K-fermé de Zariski, si $V(K) \cap X \subset U(K)$, alors $X \subseteq U \cup \bigcup_{i \neq 0} V_i \subset W$, une contradiction. Par compacité, X est donc consistant avec le K-générique de V.

Soit k_0 le corps de définition de W. Comme W est K-définissable, on a $k_0 \subseteq K$. De plus, pour tout $\sigma \in \mathrm{Aut}(K/\ulcorner X \urcorner)$, $X \leqslant \sigma(W) \cap W$ et donc $\sigma(W) = W$. Il s'en suit que $\sigma|_{k_0} = \mathrm{id}$. On a donc $k_0 \subseteq \ulcorner X \urcorner$ par le Lemme **(5.47)**. Comme V est k_0^{a}-définissable et K-définissable, elle est définie sur $k_0^{\mathrm{a}} \cap K \subseteq \mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner) \cap K = k$. □

Théorème 5.51 (Poizat, 1983) **:** *La théorie* ACF *élimine (uniformément) les imaginaires.*

Démonstration. Par les Propositions **(5.44)** et **(5.49)**, il suffit de monter l'élimination faible. Soit $K \models \mathrm{ACF}$ $\aleph_0$-saturé et fortement $\aleph_0$-homogène — en particulier, K^{eq} est aussi $\aleph_0$-saturé et fortement $\aleph_0$-homogène. Soit $e \in K^{\mathrm{eq}}$ et $k := \mathrm{acl}^{\mathrm{eq}}(e) \cap K$. Soit aussi $a \in K$ un uple et f $\varnothing$-définissable telle que $e = f(a)$. Par la Proposition **(5.50)**, il existe une k-variété géométriquement intègre définie sur k dont le type K-générique p est consistant avec $f^{-1}(e)$. Comme p est un K-type complet, $p(x) \models f(x) = e$. Pout tout $\sigma \in \mathrm{Aut}(K/k)$, $\sigma(p) = p$ et donc $p(x) \models \sigma(e) = f(x) = e$. On a donc, par le Lemme **(5.48)**, que $e \in \mathrm{dcl}^{\mathrm{eq}}(k)$. Ce qui conclut la preuve. □

Lemme 5.52 : *Soit K un corps parfait $A \subseteq K^{\mathrm{eq}}$ contenant $\mathrm{acl}^{\mathrm{eq}}(A) \cap K$, π un type partiel sur A et $k := A \cap K$. Il alors existe une k-variété V géométriquement intègre telle que π soit consistant avec le type des K-génériques de V.*

Démonstration. On suppose π clos par conjonction. Pour tout $X \in \pi$, on note V_X la variété obtenue dans la Proposition **(5.50)**. On remarque que $\ulcorner X \urcorner \subseteq \mathrm{dcl}^{\mathrm{eq}}(A)$ et donc V_X est k-définissable. Comme il n'existe pas de chaîne strictement décroissante de variétés, il existe V_X minimal pour l'inclusion. Comme π est clos par conjonction, ce minimum est en fait un plus petit élément, noté $V = V_X$.

Il reste à démontrer que π est consistant avec le K-générique de V. Soit $Y \in \pi$. On a $V_{X \cap Y} = V_X = V$ et par définition $X \cap Y$, et donc X, est consistant avec le K-générique de V. □

Théorème 5.53 (Hrushovski, 1991) **:** *La théorie* $\mathrm{PPAC}_{\mathfrak{d}}$ *élimine (uniformément) les imaginaires.*

Démonstration. Par les Propositions **(5.44)** et **(5.49)**, il suffit de monter l'élimination faible. Soit $e \in K^{\mathrm{eq}}$, $k = \mathrm{acl}^{\mathrm{eq}}(e) \cap K$. On veut montrer que $e \in \mathrm{dcl}^{\mathrm{eq}}(k)$. Soit f $\varnothing$-définissable et $a \in K$ tel que $e = f(a)$ et $X = f^{-1}(e)$. Par la Proposition **(5.50)**, il existe $c \mathop{\downarrow}_k^{\mathrm{alg}} a$ tel que $c \in X$, c'est-à-dire $f(c) = e = f(a)$. Soit maintenant $b \equiv_k a$. Par le Lemme **(5.52)**, on trouve b' tel que $b' \equiv_{\mathrm{acl}^{\mathrm{eq}}(e)} b$ et $b' \mathop{\downarrow}_k^{\mathrm{alg}} a$. Comme $b' \equiv_k a$, il existe d tel que $db' \equiv_k ca$. En particulier, $d \mathop{\downarrow}_k^{\mathrm{alg}} b'$, $c \equiv_k d$ et $f(d) = f(b')$. Par le théorème d'indépendance, on peut supposer $c = d$ et donc $e = f(a) = f(c) = f(d) = f(b')$. Comme $b \equiv_{\mathrm{acl}^{\mathrm{eq}}(e)} b'$, il s'en suit que $f(b) = e$. Par compacité, il existe $X \in \mathrm{tp}(a/k)$ tel que $f(X) = \{e\}$ et donc $e \in \mathrm{dcl}^{\mathrm{eq}}(k)$. □

Références

[Cha96] Z. Chatzidakis. Théorie des modèles des corps finis et pseudo-finis. Cours de M2. 1996.

[CDM92] Z. Chatzidakis, L. van den Dries et A. Macintyre. Definable sets over finite fields. *J. Reine Angew. Math.* 427 (1992), p. 107-135.

[Con] G. Conant. https://www.forkinganddividing.com.

[DS84] L. van den Dries et K. Schmidt. Bounds in the theory of polynomial rings over fields. A nonstandard approach. *Invent. Math.* 76.1 (1984), p. 77-91.

[FJ08] M. D. Fried et M. Jarden. *Field arithmetic*. Third. T. 11. Ergeb. Math. Grenzgeb. (3). Revised by Jarden. Springer-Verlag, Berlin, 2008, p. xxiv+792.

[Hru02] E. Hrushovski. Pseudo-finite fields and related structures. In : *Model theory and applications*. T. 11. Quad. Mat. Aracne, Rome, 2002, p. 151-212.