Théorie des modèles des corps pseudo-finis et application à l'intégration motivique

Arthur Forey et Arthur-César Le Bras
Ecole Normale Supérieure
Juin 2011

Table des matières

Introduction

Cet exposé a pour objet l'étude des corps pseudo-finis, qui sont les modèles infinis de la théorie élémentaire des corps finis. On voit facilement qu'il en existe, par le théorème de compacité. Le résultat principal de cet exposé est le théorème d'Ax ([1, Ax]), qui montre que les corps pseudo-finis possèdent une axiomatisation particulièrement simple. Celui-ci prouve que les corps pseudo-finis sont définis par trois propriétés qui s'énoncent au premier ordre : être parfait, admettre une unique extension de tout degré fini, et être pseudo-algébriquement clos. On montrera que les énoncés de la théorie des corps pseudo-finis sont ceux vrais dans tout corps fini suffisamment grand. Les deux premières parties suivent essentiellement la preuve donnée par Chatzidakis du théorème d'Ax dans [3, Chatzidakis]. La première partie met en place les notions de théorie des modèles et de géométrie algébrique nécessaires, à l'exception de la cinquième section qui montre des résultats de bornes sur les idéaux de polynômes. La deuxième partie est essentiellement consacrée à la démonstration du théorème d'Ax, et montre aussi que la théorie des corps finis est décidable. Enfin, comme l'on sait compter les éléments dans un corps fini, on peut construire relativement naturellement des théories de la mesure pour les ensembles définissables dans les corps finis : c'est l'objet de la dernière section de la deuxième partie. La troisième partie de cet exposé présente un vaste prolongement de ce type d'idées, la théorie de l'intégration motivique arithmétique. Il ne s'agit pas d'une présentation détaillée ; l'accent est mis sur le lien avec la théorie des corps pseudo-finis, via les stratifications galoisiennes, et sur les aspects modèle-théoriques de la construction.

Remerciements.

Nous tenons à remercier chaleureusement Martin Hils, pour son enthousiasme, l'envie qu'il nous a donnée d'étudier la logique, le temps qu'il nous a consacré, et les multiples généralisations qu'il nous a fait entrevoir.

Première partie
Préliminaires logiques et algébriques

1 Rappels de théorie des modèles

Cette section préliminaire fixe le vocabulaire et les notions essentielles utilisées dans la suite. Le lecteur au fait de la théorie des modèles élémentaires peut donc la laisser de côté, à l'exception peut-être du résultat de préservation 1.10, qui nous sera très utile dans la suite. Dans cette section, $\mathcal{L}$ est un langage (du premier ordre).

1.1 Définitions et résultats fondamentaux

Rappelons pour commencer le théorème de complétude de Gödel et son très utile corollaire, le théorème de compacité.

Théorème 1.1 (Théorème de complétude de Gödel)**.** *Soit T une théorie, φ un énoncé. Alors $T \vDash \varphi$ si et seulement si $T \vdash \varphi$. En d'autres termes, une théorie a un modèle si et seulement si elle est cohérente.*

Théorème 1.2 (Théorème de compacité)**.** *Soit T une théorie dont toute partie finie a un modèle. Alors T a un modèle.*

Définition 1.3. Soient A et B deux $\mathcal{L}$-structures. On dit que A et B sont *élémentairement équivalentes*, et on note $A \equiv B$, si elles satisfont les mêmes énoncés. Si $A \subseteq B$ (cette notation signifie que A est une sous-structure de B), et si pour toute formule $\varphi(\bar{x})$ et tout uplet $\bar{a}$ de A, on a $A \vDash \varphi(\bar{a})$ si et seulement si $B \vDash \varphi(\bar{a})$, on dit que A est une *sous-structure élémentaire* de B, et on note $A \prec B$.

En particulier, si $A \prec B$, $A \equiv B$. Le test de Tarski-Vaught (cf. [17, Marker]) est très utile pour vérifier que deux structures sont élémentairement équivalentes. Voici une autre méthode, dite du va-et-vient, très utile aussi.

Proposition 1.4. *Soient A et B des $\mathcal{L}$-structures. Supposons qu'il existe une famille non vide I d'isomorphismes partiels, dont le domaine est contenu dans A et l'image dans B, et satisfaisant aux conditions suivantes :*

- *Pour tout $a \in A$ et tout $F \in I$, il existe $F' \in I$ étendant F et ayant a dans son domaine ;*
- *Pour tout $b \in B$ et tout $F \in I$, il existe $F' \in I$ étendant F et ayant b dans son image.*

Alors $A \equiv B$.

Démonstration. On prouve par induction sur le nombre de quantificateurs dans la formule $\varphi(\bar{x})$ écrite sous forme prénexe que si $\bar{a}$ est un uplet de A dans le domaine d'un élément F de I, alors

$$A \vDash \varphi(\bar{a}) \iff B \vDash \varphi(F(\bar{a})).$$

Pour les formules sans quantificateur, c'est la définition d'un isomorphisme partiel de $\mathcal{L}$-structures. Considérons la formule $\varphi(\bar{x}) = \exists y \psi(\bar{x}, y)$, en supposant connu le résultat pour la formule $\psi(\bar{x}, y)$. Soit $\bar{a}$ dans le domaine de $F \in I$ et supposons que $A \vDash \exists y \psi(\bar{a}, y)$. Soit $b \in A$ tel que $A \vDash \psi(\bar{a}, b)$. Il existe par hypothèse $F' \in I$ prolongeant F et ayant b dans son domaine. Par hypothèse d'induction, $B \vDash \psi(F'(\bar{a}), F'(b))$. Donc $B \vDash \varphi(F(\bar{a}))$. On fait un raisonnement semblable pour montrer l'autre direction. □

Décrivons enfin la notion de type et de modèle saturé. Soit B une $\mathcal{L}$-structure et $A \subseteq B$ un ensemble. On note $\mathcal{L}_A$ le langage obtenu en ajoutant à $\mathcal{L}$ des symboles de constantes pour tout $a \in A$. On peut naturellement voir B comme une $\mathcal{L}_A$-structure, et on note $Th_A(B)$ l'ensemble des $\mathcal{L}_A$-formules vraies dans B.

Définition 1.5. Soit p un ensemble de $\mathcal{L}_A$-formules en les variables libres $x_1, \ldots, x_n$. On dit que p est un *n-type* si $p \cup Th_A(B)$ est satisfiable. On dit que p est un *n-type complet* si $\varphi \in p$ ou $\neg\varphi \in p$, pour toute $\mathcal{L}_A$-formule φ en les variables libres $x_1, \ldots, x_n$. On note $S_n^B(A)$ l'ensemble des n-types complets.

Définition 1.6. Si p est un n-type sur A, on dit que $\bar{a} \in B^n$ *réalise* p si $B \vDash \varphi(\bar{a})$, pour tout $\varphi \in p$.

Par exemple, si $B = (\mathbb{Q}, <)$ et $A = \mathbb{N}$, $p(v) = \{\varphi(v) \in \mathcal{L}_A, B \vDash \varphi(1/2)\}$ est un 1-type complet, et le lecteur pourra prouver que les éléments de B qui réalisent p sont exactement les rationnels de l'intervalle $]0,1[$. Comme autre exemple, soit K un corps algébriquement clos, et k un sous-corps de K. on peut démontrer que l'application $p \to I_p := \{f(\bar{X}) \in k[X_1, \ldots, X_n], f(\bar{v}) = 0 \in p\}$ réalise une bijection (continue si l'on munit les espaces considérés de topologies convenables) de $S_n^K(k)$ sur $\mathrm{Spec}(k[X_1, \ldots, X_n])$.

Dans la suite de ce court paragraphe, T désigne une théorie complète possédant des modèles infinis, sur un langage $\mathcal{L}$ dénombrable.

Définition 1.7. Soit κ un cardinal infini. On dit qu'un modèle B de T est *κ-saturé*, si, pour tout sous-ensemble $A \subseteq B$, avec $|A| < \kappa$ et tout $p \in S_n^B(A)$, p est réalisé dans B.

Proposition 1.8. *Pour tout modèle B de T, il existe un modèle C κ^+-saturé de T avec $B \prec C$ et $|C| \leq |B|^\kappa$.*

Démonstration. Fait : Pour tout B, il existe $B \prec B'$ tel que $|B'| \leq |B|^\kappa$ tel que si $A \subseteq B$, et $p \in S_n^B(A)$ $(n < \omega)$, p est réalisé dans B'.

Preuve : On note pour commencer que

$$|\{A \subseteq B, |A| \leq \kappa\}| \leq |B|^\kappa.$$

(on peut toujours surjecter κ sur un tel A). Pour un tel A, on a aussi : $|S_n^B(A)| \leq 2^\kappa$. Soit $(p_\alpha, \alpha \leq |B|^\kappa)$ une énumération de tous les types de $S_n^B(A)$, pour $n < \omega$, $A \subseteq B$, $|A| \leq \kappa$. On construit alors une chaîne élémentaire par induction. On pose $B_0 = B$; si α est un ordinal limite, $B_\alpha = \cup_{\beta<\alpha} B_\beta$, et on choisit enfin pour $B_{\alpha+1}$ une extension élémentaire de B_α ayant même cardinal et réalisant p_α (l'existence d'une telle extension se déduit des théorèmes de compacité et de Löwenheim-Skolem descendant ; voir [17, Marker]). On voit par induction que pour tout α, $B_\alpha \leq |B|^\kappa$. En posant $B' = \cup_{\alpha<|B|^\kappa} B_\alpha$, on obtient le modèle recherché.

On construit alors une chaîne élémentaire $(C_\alpha, \alpha < \kappa^+)$ avec $|C_\alpha| \leq |B|^\kappa$ en posant $C_0 = B$; si α est un ordinal limite, $C_\alpha = \cup_{\beta<\alpha} C_\beta$. Si C_α est construit, $|C_\alpha| \leq |B|^\kappa$ et l'on peut trouver, en vertu du fait précédent, un modèle $C_{\alpha+1}$ tel que, si l'on se donne un sous-ensemble $A \subset C_\alpha$, $|A| \leq \kappa$, et $p \in S_n^{C_\alpha}(A)$, p est réalisé dans $C_{\alpha+1}$. De plus, le fait cité nous assure que $|C_{\alpha+1}| \leq |C_\alpha|^\kappa \leq (|B|^\kappa)^\kappa = |B|^\kappa$. Posons alors $C = \cup_{\alpha<\kappa^+} C_\alpha$. Comme $\kappa^+ \leq |B|^\kappa$, $|C| \leq |B|^\kappa$. Soient $A \subseteq C$, $|A| \leq \kappa$, $p \in S_n^C(A)$. Comme le cardinal κ^+ est régulier, il existe $\alpha < \kappa^+$ tel que $A \subseteq C_\alpha$ et p est réalisé dans $C_{\alpha+1} \prec C$. Ainsi, C est bien κ^+-saturé. □

Dans la suite de ce texte, nous utiliserons ce résultat dans le cas $\kappa = \aleph_0$.

1.2 Un résultat de préservation

Définition 1.9. Soit T une théorie du premier ordre.
- T est *complète* si elle est consistante et si pour tout énoncé φ, $T \vDash \varphi$ ou $T \vDash \neg\varphi$.
- T est *modèle complète* si, pour tous modèles A et B de T, si $A \subseteq B$, alors $A \prec B$.
- T admet l'*élimination des quantificateurs* si pour toute formule $\varphi(\bar{x})$, il existe une formule $\psi(\bar{x})$ sans quantificateurs, telle que

$$T \vdash \forall \bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})).$$

Notons que si T admet l'élimination des quantificateurs, T est modèle-complète, et que si T est modèle complète et s'il existe un modèle A de T qui se plonge dans tout modèle de T, alors T est complète.

On admettra qu'une théorie T est modèle complète si et seulement si toute formule $\varphi(\bar{x})$ est équivalente modulo T à une formule existentielle.

Proposition 1.10. *Soient T_1 et T_2 des théories. On suppose $T_1 \cup T_2$ consistante. Soit Δ un ensemble d'énoncés clos par disjonction finie. Les conditions suivantes sont équivalentes :*

(i) *Il existe $\Gamma \subseteq \Delta$ tel que $T_1 \cup \Gamma$ axiomatise $T_1 \cup T_2$;*

(ii) *Pour tous modèles A et B de T_1, si $A \vDash T_2$ et B satisfait tous les énoncés de Δ satisfaits par A, alors $B \vDash T_2$.*

Démonstration. Le fait que (i) implique (ii) est évident. Réciproquement, supposons la condition (ii) vérifiée. On pose $\Gamma = \{\psi \in \Delta, T_1 \cup T_2 \vDash \psi\}$. Evidemment, $T_1 \cup T_2 \vDash \Gamma$ et il suffit pour conclure de montrer que tout modèle B de $T_1 \cup \Gamma$ est aussi un modèle de T_2. On considère l'ensemble $\Sigma = \{\neg\psi, \psi \in \Delta, B \vDash \neg\psi\}$. Supposons la théorie $T_1 \cup T_2 \cup \Sigma$ inconsistante. Le théorème de compacité assure alors l'existence de $\neg\psi_1, \ldots, \neg\psi_n \in \Sigma$ et de $\varphi \in T_2$ tels que $T_1 \cup \{\neg\psi_1, \ldots, \neg\psi_n, \varphi\}$ est inconsistante. Mais alors $T_1 \cup \{\varphi\} \vdash (\psi_1 \vee \cdots \vee \psi_n)$, et donc, Δ étant clos par disjonction finie, $(\psi_1 \vee \cdots \vee \psi_n) \in \Gamma$. C'est une contradiction. On en déduit que la théorie $T_1 \cup T_2 \cup \Sigma$ est consistante. Soit A un modèle cette théorie. Soit $\psi \in \Delta$ satisfaite dans A. On ne peut donc avoir $\neg\psi \in \Sigma$. On en déduit que $B \vDash \psi$. On peut donc appliquer la propriété (ii), qui montre que B est modèle de T_2, comme voulu. □

Corollaire 1.11. *Soit T une théorie, $\varphi(\bar{x})$ une formule telle que la théorie $T \cup \exists\bar{x}\varphi(\bar{x})$ est consistante. Soit Δ un ensemble de formules dans les variables $\bar{x}$, clos par disjonction. Les conditions suivantes sont équivalentes :*

(i) Il existe des formules $\psi_1(\bar{x}), \ldots, \psi_m(\bar{x}) \in \Delta$ telles que

$$T \vdash \forall \bar{x}\ \varphi(\bar{x}) \leftrightarrow (\psi_1(\bar{x}) \wedge \cdots \wedge \psi_m(\bar{x}));$$

(ii) Pour tous modèles A et B de T, pour tous n-uplets $\bar{a}$ et $\bar{b}$ de A et B respectivement, si $A \vDash \varphi(\bar{a})$, et si toute formule $\psi(\bar{x})$ de Δ satisfaite par $\bar{a}$ dans A est satisfaite par $\bar{b}$ dans B, alors $B \vDash \varphi(\bar{b})$.

Démonstration. On agrandit le langage en ajoutant des nouveaux symboles de constantes $c_1, \ldots, c_n$. On applique le théorème précédent pour obtenir des formules $\psi_1, \ldots, \psi_m \in \Delta$ telles que

$$T \vdash \varphi(\bar{c}) \leftrightarrow (\psi_1(\bar{c}) \wedge \cdots \wedge \psi_m(\bar{c})),$$

ce qui entraîne, puisque les symboles de constantes $\bar{c}$ n'apparaissent pas dans T, que

$$T \vdash \forall \bar{x}\ \varphi(\bar{x}) \leftrightarrow (\psi_1(\bar{x}) \wedge \cdots \wedge \psi_m(\bar{x})).$$

□

1.3 Ultraproduits

Soit I un ensemble, (A_i) une famille de $\mathcal{L}$-structures indexée par I. Soit $\mathcal{F}$ un sous-ensemble de $\mathcal{P}(I)$. On dit que $\mathcal{F}$ est un filtre si $\emptyset \notin \mathcal{F}$, $I \in \mathcal{F}$, si $X \cap Y \in \mathcal{F}$ dès que $X, Y \in \mathcal{F}$ et si $Y \in \mathcal{F}$ dès qu'il existe $X \in \mathcal{F}$, $X \subseteq Y$. Si $\mathcal{F}$ est un filtre maximal (pour l'inclusion), on dit que $\mathcal{F}$ est un ultrafiltre. Cela revient dire que $\mathcal{F}$ est un filtre qui pour toute partie X de I, contient soit X soit son complémentaire. Un filtre $\mathcal{F}$ est dit principal s'il existe $i \in I$ tel que $\mathcal{F} = \{X \subseteq I, i \in X\}$. Dans le cas contraire, $\mathcal{F}$ est dit non principal.

On définit une $\mathcal{L}$-structure sur le produit cartésien des A_i de façon évidente. Donnons de plus un filtre $\mathcal{F}$ sur I. On définit le produit réduit des A_i suivant $\mathcal{F}$, noté $\Pi_{i\in I} A_i/\mathcal{F}$, comme étant la $\mathcal{L}$-structure suivante. L'univers de $\Pi_{i\in I} A_i/\mathcal{F}$ est le quotient de $\Pi_{i\in I} A_i$ par la relation d'équivalence :

$$a \equiv_{\mathcal{F}} b \iff \{i \in I, a(i) = b(i)\} \in \mathcal{F}.$$

La transitivité de $\equiv_{\mathcal{F}}$ découle des axiomes définissant les filtres. On note $[a]_{\mathcal{F}}$ la classe d'équivalence de $a \in \Pi_{i\in I} A_i$.

Si c est un symbole de constante, l'interprétation de c est donnée par $[(c(i))_{i\in I}]_{\mathcal{F}}$. Si f est un symbole de fonction n-aire, $f([a_1]_{\mathcal{F}}, \ldots, [a_n]_{\mathcal{F}}) = [f(a_1, \ldots, a_n)]_{\mathcal{F}}$, et si R est un symbole de relation n-aire, $\Pi_{i\in I} A_i/\mathcal{F} \vDash R([a_1]_{\mathcal{F}}, \ldots, [a_n]_{\mathcal{F}})$ si et seulement si $\{i \in I, A_i \vDash R(a_1(i), \ldots, a_n(i))\} \in \mathcal{F}$.

Si $\mathcal{F}$ est un ultrafiltre, le produit réduit des M_i est appelé *ultraproduit*.

Théorème 1.12 (Théorème de Loś)**.** *Soit I un ensemble, $\mathcal{F}$ un ultrafiltre sur I, (A_i) une famille de $\mathcal{L}$-structures, $A = \Pi_{i\in I} A_i/\mathcal{F}$ leur ultraproduit. Soit φ un $\mathcal{L}$-énoncé. Alors*

$$A \vDash \varphi \iff \{i \in I, A_i \vDash \varphi\} \in \mathcal{F}.$$

Démonstration. Montrons plus généralement que si $\varphi(\bar{x})$ est une formule quelconque, $\bar{a}$ un n-uplet de A, alors

$$A \vDash \varphi(\bar{a}) \iff \{i \in I, A_i \vDash \varphi(\bar{a}(i))\} \in \mathcal{F}.$$

La preuve se fait par induction sur la complexité de $\varphi(\bar{x})$. Une formule atomique est de la forme $R(t_1(\bar{x}), \ldots, t_n(\bar{x}))$ avec R une relation ou le symbole de l'égalité et $t_i(\bar{x})$ des termes du langage. Dans ce cas, l'équivalence résulte de la définition de la $\mathcal{L}$-structure de A. De même, si l'équivalence est vraie pour les formules $\varphi(\bar{x})$ et $\psi(\bar{x})$, elle l'est aussi pour $\varphi(\bar{x}) \wedge \psi(\bar{x})$. Si elle est vraie pour $\varphi(\bar{x}, y)$, elle l'est aussi pour $\exists y \varphi(\bar{x}, y)$. Tout cela utilise seulement le fait que $\mathcal{F}$ est un filtre. Il reste à montrer que si l'équivalence est vraie pour la formule $\varphi(\bar{x})$, elle l'est pour $\neg\varphi(\bar{x})$. C'est ici qu'intervient le fait que $\mathcal{F}$ est un ultrafiltre. Par hypothèse,

$$A \vDash \neg\varphi(\bar{a}) \iff \{i \in I, A_i \vDash \varphi(\bar{a}(i))\} \notin \mathcal{F}.$$

Mais comme $\mathcal{F}$ est un ultrafiltre,

$$\{i \in I, A_i \vDash \varphi(\bar{a}(i))\} \notin \mathcal{F} \iff \{i \in I, A_i \vDash \neg\varphi(\bar{a}(i))\} \in \mathcal{F}.$$

Cela donne l'équivalence pour $\neg\varphi(\bar{x})$. □

Corollaire 1.13. *Soit $\mathcal{F}$ un ultrafiltre sur un ensemble I, A une $\mathcal{L}$-structure. L'inclusion diagonale de A dans l'ultrapuissance A^I/D est élémentaire.*

Démonstration. Immédiat avec le théorème. □

Les ultraproduits joueront un rôle important dans la suite de ce texte. En guise d'exercice et de première application, le lecteur peut s'amuser à redémontrer le théorème de compacité à l'aide du théorème de Loś.

2 Corps algébriquement clos

2.1 Elimination des quantificateurs

On considère dans cette partie (et dans le reste de l'exposé) le langage des anneaux, $\mathcal{L} = \{+, -, \cdot, 0, 1\}$.

On considère la $\mathcal{L}$-théorie, notée ACF, composée des axiomes des corps avec zéro 0 et unité 1, et pour tout $n \geq 1$, de l'énoncé $\forall x_0, ..., x_{n-1} \exists y\, y^n + x_{n-1}y^{n-1} + ... + x_1 y + x_0 = 0$. Les modèles de ACF sont les corps algébriquement clos. On pose de plus pour p premier,

$$ACF_p = ACF \cup \{p = 0\} \text{ et } ACF_0 = ACF \cup \{n \neq 0 | \forall n \in \mathbb{N}\backslash\{0\}\}.$$

Lemme 2.1. *Soient K et L des corps algébriquement clos, et soit $f : A \to B$ un isomorphisme entre des sous-structures respectives de K et L. Soit $a \in K$ algébrique sur A. Alors il existe un isomorphisme f' étendant f et ayant a dans son domaine.*

Démonstration. Quitte à passer aux corps des quotients, on peut supposer que A et B sont des corps. Soit P le polynôme minimal de a au-dessus de A, et $f(P) \in B[X]$ le polynôme obtenu en appliquant f aux coefficients de P. Comme L est algébriquement clos, $f(P)$ admet une racine $b \in L$. On a alors

$$A(a) \simeq_A A[X]/f(X) \text{ et } B(b) \simeq_B B[X]/P(f)(X).$$

Donc f s'étend en un isomorphisme f' entre $A(a)$ et $B(b)$ qui envoie a sur b. □

Théorème 2.2. *La théorie ACF admet l'élimination des quantificateurs, et donc est modèle complète. Les théories ACF_p et ACF_0 sont complètes.*

Démonstration. Soient K et L des corps algébriquements clos, non dénombrables, de même caractéristique, et soit C une sous-structure dénombrable commune à K et L. On considère la famille I d'isomorphismes f entre des sous-structures dénombrables de K et L contenant C. On va montrer qu'elle satisfait la condition du va-et-vient : Soit $a \in K$, $f \in I$, A le domaine de f, $B = f(A)$. Si a est algébrique sur A, le lemme donne un isomorphisme partiel $f' \in I$ ayant a dans son domaine. Supposons que a n'est pas algébrique sur A : comme L est de cardinalité plus grande que celle de B, il existe $b \in L$ qui n'est pas algébrique sur B. On pose $f'(a) = b$ et cela étend f en un isomorphisme $f' : A[a] \to B[b]$.

Si $b \in L$, on raisonne de la même façon avec f^{-1} pour obtenir f' qui convient.

D'après le théorème du va-et-vient, la théorie obtenue en ajoutant à ACF les énoncés sans quantificateurs du langage $\mathcal{L}(C)$ (obtenu à partir de $\mathcal{L}$ en y ajoutant des symboles de constantes pour les éléments de C) est complète. Cela signifie que ACF élimine les quantificateurs.

En prenant $C = \emptyset$, on obtient que ACF_p et ACF_0 sont complètes.

□

Corollaire 2.3. *Tout ensemble définissable avec paramètres dans un corps algébriquement clos K est fini ou cofini.*

Démonstration. Toute formule atomique en une variable définit un ensemble fini ou tout (et donc cofini). Comme la propriété d'être fini ou cofini est stable par combinaisons booléennes, et que ACF élimine les quantificateurs, on a le résultat. □

2.2 Bases de transcendance, clôtures algébriques et définissables

Définition 2.4 (Bases de transcendance)**.** Soient $A \subseteq K$ des corps (ou anneaux intègres). Un élément $a \in K$ est *transcendant* sur A s'il n'est racine d'aucun polynôme à coefficients dans A.

Un sous-ensemble B de K est *algébriquement indépendant* sur A si pour tout uplet $\overline{b}$ dans B et tout polynôme $P(\overline{X})$ de $A[\overline{X}]$ non nul, $P(\overline{b}) \neq 0$.

Un sous-ensemble B de K algébriquement indépendant sur A et maximal avec cette propriété est appellé *base de transcendance* de K sur A.

Remarque 2.5. Si B est une base de transcendance de K sur A, K est algébrique sur $A(B)$, et on montre que la même façon que pour les espaces vectoriels que deux bases de transcendance ont le même cardinal, appelé degré de transcendance de K sur A.

Proposition 2.6. *Soit A un sous-corps du corps algébriquement clos K.*

(1) Si a et b sont algébriques sur A et ont le même polynôme minimal sur A, alors il existe un automorphisme de K qui préserve A et envoie a sur b.

(2) Si a et b sont transcendants sur A, alors il existe un automorphisme de K qui préserve A et envoie a sur b.

Démonstration. (1) D'après le lemme 2.1, il existe un A-isomorphisme f entre $A(a)$ et $A(b)$ qui envoie a sur b. Soit B une base de transcendance de K sur A. Les corps $A(a)(B)$ et $A(b)(B)$ sont isomorphes via g qui prolonge f et préserve B. Comme K est algébrique sur $A(a)(B)$, on étend g en un isomorphisme de K en utilisant le lemme de Zorn et le lemme 2.1.

(2) C'est similaire : on considère B et B' des bases de transcendance de K sur A contenant respectivement a et b. Elles sont de même cardinal, donc on a un isomorphisme entre $A(B)$ et $A(B')$ qui envoie c sur d, et on le prolonge à K comme pour (1). □

Définition 2.7. Soit M un modèle d'une théorie T (complète) dans un language $\mathcal{L}$, A un sous ensemble de M et $a \in M$.

On dit que a est *algébrique* sur A au sens de la théorie des modèles s'il existe une $\mathcal{L}(A)$-formule $\varphi(x)$ satisfaite par a dans M et n'ayant qu'un nombre fini de réalisations dans M. L'ensemble des éléments algébriques sur A de M est la clôture algébrique de A, notée $acl(A)$.

On dit que a est *définissable* sur A s'il existe une $\mathcal{L}(A)$-formule $\varphi(x)$ dont l'unique réalisation dans M est a. L'ensemble des éléments définissables sur A de M est la clôture définissable de A, notée $dcl(A)$.

On montre que :

$$A \subseteq dcl(A) \subseteq acl(A)\,,\ acl(acl(A)) = acl(A)\,,\ dcl(dcl(A)) = dcl(A)$$

et si $A \subseteq B$, alors

$$acl(A) \subseteq acl(B)\,,\ dcl(A) \subseteq dcl(B).$$

Proposition 2.8. *Soit A un sous-ensemble du corps algébriquement clos K, F le sous-corps de K engendré par A, et $T = Th(K)$.*

Un élément de K est algébrique sur A au sens de la théorie des modèles si et seulement s'il est algébrique sur F au sens de la théorie des corps.

Un élément de K est définissable sur A au sens de la théorie des modèles si et seulement s'il est dans la clôture parfaite de F, si et seulement s'il est algébrique sur F et fixé par tout automorphisme de K qui préserve A.

On rappelle qu'un corps est parfait s'il est de caractéristique nulle, ou s'il est de caractéristique $p > 0$ et clos par racine p-ème. La clôture parfaite d'un corps F de caractéristique $p > 0$, notée F^{1/p^∞}, est l'ensemble des éléments de la clôture algébrique racines des polynômes $X^{p^n} - a$ avec $n \in \mathbb{N}$ et $a \in F$. C'est le plus petit corps parfait contenant F.

Démonstration. Soit $a \in acl(A)$ et $\varphi(x)$ une formule de $\mathcal{L}(A)$ satisfaite par a et n'ayant qu'un nombre fini de réalisations dans K. D'après la preuve de la proposition 2.2, il existe un polynôme non nul à coefficients dans A dont a est racine. La réciproque est claire.

On remarque que $dcl(A)$ est un corps, en effet, si a et b sont définis respectivement par $\varphi(x)$ et $\psi(x)$, alors $a-b$ est défini par $\exists y \exists z \varphi(y) \wedge \psi(z) \wedge x = y - z$, ab par $\exists y \exists z \varphi(y) \wedge \psi(z) \wedge x = yz$, et a^{-1} par $\exists y \varphi(y) \wedge 1 = xy$. Sans perte de généralité on peut donc supposer que A est un corps, *i.e.* $A = F$. Soit alors $a \in acl(A)$, $P(X)$ son polynôme minimal sur A. Si P est de degré 1, $a \in A$. On suppose dans la suite que $\deg(P) > 1$. Soit b une autre racine de P dans K. Par la proposition 2.6, il existe un A-automorphisme de K qui envoie a sur b. Cela entraîne que a et b satisfont les mêmes formules à paramètres dans A. En particulier, si a est définissable sur A, P a une unique racine, donc la caractéristique est $p > 0$ et $P = X^{p^n} - c$ pour un $n \in \mathbb{N}$ et $c \in A$, donc a est dans la clôture parfaite de A et fixé par tout A-automorphisme de K. Les réciproques sont claires. □

3 Ensembles algébriques, topologie de Zariski, variétés

Dans toute cette partie, on considère un corps F, contenu dans un corps algébriquement clos K de cardinal strictement plus grand. On note $\widetilde{F}$ la clôture algébrique de F dans K, et F_s la clôture séparable de F dans K.

Soit $S \subseteq K^n$. On définit un idéal de $K[\overline{X}]$ par

$$I(S) = \{f(\overline{X}) \in K[\overline{X}] | f(\overline{a}) = 0 \, \forall \overline{a} \in S\}.$$

Réciproquement, si $I \subseteq K[\overline{X}]$, on définit

$$V(I) = \{\overline{a} \in K^n | f(\overline{a}) = 0 \, \forall f \in I\}.$$

On remarque que pour $I, J \subseteq K[\overline{X}]$ et $S, T \subseteq K^n$ on a :

$$V((0)) = K^n \, , \, V(K[\overline{X}]) = \emptyset \, , \, I(K^n) = (0) \, , \, I(\emptyset) = K[\overline{X}]$$

$$I \subseteq J \text{ implique } V(J) \subseteq V(I) \, , \, I \subseteq I(V(I)),$$

$$S \subseteq T \text{ implique } I(T) \subseteq I(S) \, , \, S \subseteq V(I(S)),$$

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

3.1 Topologie de Zariski

On définit une topologie sur K^n, la topologie de Zariski, dont les fermés, appelés ensembles algébriques, sont de la forme $V(I)$. Si $S \subseteq K^n$, on définit la clôture de Zariski de S par $\widetilde{S} = V(I(S))$. C'est le plus petit fermé contenant S, donc l'adhérence de S.

Montrons que l'on a bien défini une topologie sur K^n et qu'elle est noethérienne, c'est à dire que toute chaîne décroissante de fermés est stationnaire (*i.e.* est constante à partir d'un certain rang). Soient (S_i) une famille de fermés. On note $I_i = I(S_i)$. On a alors $\bigcap_i S_i = V(\sum_i I_i)$, en effet,

$$\overline{a} \in \bigcap_i S_i \iff \forall i \, \forall f \in I_i \, f(\overline{a}) = 0 \iff \overline{a} \in V(\sum_i I_i),$$

donc $\bigcap_i S_i$ est fermé.

Si S et T sont fermés, on note $I = I(S)$ et $J = I(T)$. Montrons que $S \cup T = V(I \cap J)$. Comme $I \cup J \subseteq I$, $S \subseteq V(I \cap J)$ par la remarque précédente et donc $S \cup T \subseteq V(I \cap J)$. Réciproquement, si $\overline{a} \notin S \cup T$, alors il existe $f \in I$ et $g \in J$ tels que $f(\overline{a}) \neq 0$ et $g(\overline{a}) \neq 0$, donc $fg(\overline{a}) \neq 0$ or $fg \in I \cap J$ donc $\overline{a} \notin V(I \cap J)$. Donc $I \cup J$ est fermé.

On rappelle qu'un anneau est noethérien si toute chaîne croissante d'idéaux est stationnaire. En particulier, un corps est noethérien (ses seuls idéaux sont (0) et lui-même) et le théorème de Hilbert montre que si R est noethérien, $R[X]$ l'est aussi. En particulier, $K[\overline{X}]$ est noethérien. Par passage aux idéaux, la noethérianité de la topologie de Zariski découle immédiatement de celle de $K[\overline{X}]$.

Cela montre notamment que toute intersection de fermés est l'intersection d'un nombre finis d'entre eux, et que si une intersection est vide, alors une sous-intersection finie est aussi vide.

Montrons maintenant une application élégante de l'élimination des quantificateurs de ACF.

Théorème 3.1 (Nullstellensatz de Hilbert)**.** *Soit I un idéal propre de $K[\overline{X}]$. Alors $V(I)$ est non vide.*

Démonstration. Soit M un idéal maximal contenant I. Le corps $K[X]/M$ contient K comme sous corps, et sa clôture algébrique L est une extension élémentaire de K (ACF élimine les quantificateurs, donc est modèle complète). Soient $f_1(\overline{X}), ..., f_l(\overline{X})$ des générateurs de I. Puisque $I \subseteq M$, les classes $\overline{x}$ de $\overline{X}$ modulo M sont zéros de $f_1, ..., f_l$. Donc $L \models \exists \overline{x} f_1(\overline{x}) = ... = f_l(\overline{x}) = 0$ et comme K est une sous-structure élémentaire de L, $K \models \exists \overline{x} f_1(\overline{x}) = ... = f_l(\overline{x}) = 0$, *i.e.* $V(I) \neq \emptyset$. □

Définition 3.2. Soit V un fermé de K^n. On dit que V est *défini* sur F si l'idéal $I(V)$ est engendré par $I(V) \cap F[\overline{X}]$. On dit que F est un *corps de définition* de V.

Théorème 3.3. *Soit $V \subseteq K^n$ un fermé de Zariski. Alors V a un plus petit corps de définition.*

Démonstration. Soit $I = I(V)$, et $R = K[\bar{X}]/I$. Soit M l'ensemble des monômes de $K[\bar{X}]$, c'est une base du K-espace vectoriel $K[\bar{X}]$. Soit $B \subseteq M$ une base du K-espace vectoriel R. Pour tout monôme m de M, on associe une (unique) combinaison linéaire A_m d'éléments de B telle que $m - A_m \in I$. Montrons que I est engendré par les $m - A_m$ où m parcourt M : soit $f \in I$, f s'écrit $f = \sum_{m \in M} a_m m$. Alors

$$f = \sum_{m \in M} a_m (m - A_m) + \sum_{m \in M} a_m A_m.$$

Donc $\sum_{m\in M} a_m A_m$ est une combinaison linéaire d'éléments de B qui est dans I (car f et les $m - A_m$ le sont), comme B est une K-base de R, elle est nulle, donc f est dans l'idéal engendré par les $m - A_m$.

Soit K_0 le sous corps de K engendré par les coefficients apparaissant dans les combinaisons linéaires $A_m, m \in M$. Nous avons montré que V est définie sur K_0. Montrons maintenant que K_0 est un plus petit corps de définition de V.

On suppose V définie sur K_1 et soient $f_1, ..., f_r \in K_1[\bar{X}]$ des générateurs de I. Il s'agit de montrer que $K_0 \subseteq K_1$. Soit $m_0 \in M\backslash B$. Comme $m_0 - A_{m_0} \in I$, il existe $g_1, ..., g_r \in K[\bar{X}]$ tels que $m_0 - A_{m_0} = f_1 g_1 + ... + f_r g_r$. On peut écrire $f_i = \sum_{m\in M} a_{im} m, a_{im} \in K_1$ et $g_i = \sum_{m\in M} b_{im} m, b_{im} \in K$. Le coefficient du monôme m dans $f_i g_i$ est alors $\sum_{m_1 m_2 = m} a_{im_1} b_{im_2}$.

Soit $S = \{m \in M |$ il existe i tel que $b_{im} \neq 0\}$. Le coefficient de m dans $f_1 g_1 + ... + f_r g_r$ est donc de la forme $c_m(\bar{b})$ où $\bar{b} = (b_{im})_{m\in S, i=1,...,r}$ et $c_m(\bar{Y}) \in K_1[\bar{Y}]$ est une K_1-combinaison linéaire des variables $\bar{Y}_{im}$. On considère le système d'équations linéaires :

$$\begin{cases} c_{m_0}(\bar{Y}) = 1 \\ c_m(\bar{Y}) = 0 \quad \text{pour } m \in M\backslash B, m \neq m_0. \end{cases}$$

Ce système a une solution dans K, les (b_{im}), donc il a aussi une solution (d_{im}) dans K_1. Soit $h_i = \sum_{m\in S} d_{im} m \in K_1[\bar{X}]$. On a alors

$$f_1 h_1 + ... + f_r = m_0 + \sum_{m\in B} e_m m \text{ pour des } e_m \in K_1.$$

Comme B est une base modulo I, $A_{m_0} = -\sum_{m\in B} e_m m$, donc $m_0 - A_{m_0} \in K_1[\bar{X}]$. Cela montre que $K_1[\bar{X}]$ contient tous les $m - A_m$, et donc K_1 contient K_0. □

Remarque 3.4. (1) On a montré que tout élément de $I(V)$ est une combinaison K-linéaire de polynômes $m - A_m, m \in M\backslash B$.

(2) On a aussi montré que si V est un fermé de $K^n, I = I(V), K_0$ le corps de définition de V, et σ un automorphisme de K. Alors,

$$\sigma(V) = V \Longleftrightarrow \sigma(I) = I \Longleftrightarrow \sigma \text{ fixe } K_0.$$

En effet, si $f_1, ..., f_r$ sont des générateurs de I, alors $\sigma(V) = V(\sigma(f_1), ..., \sigma(f_r))$.

3.2 Composantes irréductibles

Définition 3.5. On dit qu'un fermé de K^n est une *variété*, ou est irréductible, s'il n'est pas réunion de deux sous-ensembles propres fermés.

On dit qu'il est *F-irréductible* s'il est défini sur F et n'est pas réunion de deux sous-ensembles propres fermés définis sur F.

Remarque 3.6. 1. Comme la topologie est noethérienne, toute fermé se décompose de façon unique, à permutation près, comme union finie $V_1 \cup ... \cup V_l$ de variétés où aucune des V_i n'est contenue dans l'union des autres.

2. De plus, si V est un fermé défini sur F, alors V est une variété si et seulement si $I(V)$ est premier et V est F-irréductible si et seulement si $I(V) \cap F[\bar{X}]$ est premier.

3. Si V est défini sur F, soient $V_1, ..., V_s$ ses composantes irréductibles. Les V_i ne sont pas nécessairement définies sur F, mais on va montrer dans le théorème 3.12 qu'elles le sont sur une extension finie E de F, et que les conjugés $\sigma(V_i), \sigma \in \mathrm{Aut}(\tilde{F}/F)$ sont encore dans $\{V_1, ..., V_s\}$. Pour tout $i = 1, ..., s$ posons $W_i = \cap_\sigma \sigma(V_i)$, un fermé défini sur F (par la remarque 3.4(2)) qui vérifie $V_i \cap F^n = W_i \cap F^n$. On pose $V' = W_1 \cup ... \cup W_s$. Alors V' est un sous-ensemble fermé de V défini sur F vérifiant $V \cap F^n = V' \cap F^n$. On peut itérer le processus, on obtient une suite décroissante de fermés, qui va donc stationner, et on note V^* le résultat (éventuellement vide).

   On appelle le fermé V^* noyau F-absolu de V. Il est défini sur F et vérifie $V \cap F^n = V^* \cap F^n$, ses composantes irréductibles sont définies sur F, et il contient tous les composantes irréductibles de V définies sur F.

Définition 3.7. Soit V un fermé de K^n. On définit l'anneau affine de V par $K[V] = K[\overline{X}]/I(V)$. Si V est défini sur F, on définit aussi $F[V] = F[\overline{X}]/(I(V) \cap F[\overline{X}])$. Si V est irréductible, $K[V]$ est un anneau intègre, on note alors $K(V)$ son corps des fractions. De même si V est F-irréductible, on définit $F(V)$ corps de fractions de $F(V)$.

Si V est une variété, on définit la dimension de V, $\dim(V)$ comme le degré de transcendance de $K(V)$ sur K. Si Vest un fermé quelconque, alors $\dim(V)$ est la dimension maximale de ses composantes irréductibles.

Définition 3.8 (Point générique)**.** Soit V un fermé F-irréductible défini sur F, et $\overline{a} \in K^n$. On dit que $\overline{a}$ est un *point générique* de V sur F si $\overline{a} \in V$ et le F-homomorphisme : $F[V] \to F[\overline{a}]$ qui envoie la classe de $\overline{X}$ modulo $I(V) \cap F[\overline{X}]$ sur $\overline{a}$ est un isomorphisme. Si $\overline{a}$ et $\overline{b}$ sont des génériques, il existe alors un F-isomorphisme qui envoie $\overline{a}$ sur $\overline{b}$.

On définit de plus pour $\overline{a} \in K^n$, $I(\overline{a}/F) = \{f(\overline{X}) \in F[\overline{X}] | f(\overline{a}) = 0\}$.

Remarque 3.9. On vérifie alors que $I(\overline{a}/F)$ est un idéal premier, et que $F[\overline{a}] \simeq_F F[\overline{X}]/I(\overline{a}/F)$. On a que $\overline{a}$ est un générique de V sur F si et seulement si $I(\overline{a}/F) = I(V) \cap F[\overline{X}]$. De plus, si $\overline{a}$ est un générique de V sur F et $\overline{b} \in V$, alors il existe un F-homomorphisme : $F[\overline{a}] \to F[\overline{b}]$ qui envoie $\overline{a}$ sur $\overline{b}$.

Définition 3.10. Soient A et B deux F-algèbres contenues dans une F-algèbre commune. On dit que A et B sont *linéairement disjointes* au-dessus de F si tout ensemble d'éléments de A linéairement indépendants au-dessus de F (au sens des espaces vectoriels), le reste au dessus de B.

On va montrer que cette définition est symétrique.

Démonstration. On raisonne par contraposée. Soient $a_1, ..., a_n \in A$ linéairement indépendants au-dessus de F qui ne le restent pas au-dessus de B. Il existe alors $b_1, ..., b_n \in B$ non tous nuls tels que $a_1 b_1 + ... + a_n b_n = 0$. Quitte à réindicer, on peut supposer $b_1, ..., b_m$ libres sur F et $b_{m+1}, ..., b_n$ dans le F-espace vectoriel engendré par $b_1, ..., b_m$. On a alors $b_j = \sum_{i=1}^m c_{i,j} b_i$ avec $c_{i,j} \in F$ et $j = m+1, ..., n$. Alors

$$\begin{aligned} 0 &= a_1 b_1 + ... + a_n b_n \\ &= a_1 b_1 + ... + a_m b_m + a_{m+1}(\textstyle\sum_{i=1}^m c_{i,m+1} b_i) + ... + a_n(\sum_{i=1}^m c_{i,n} b_i) \\ &= (a_1 + \textstyle\sum_{j=m+1}^n a_j c_{1,j}) b_1 + ... + (a_m + \sum_{j=m+1}^n a_j c_{m,j}) b_m. \end{aligned}$$

A droite on a une combinaison linéaire à coefficients dans A non nuls car les a_i sont indépendants sur F, ce qui achève la démonstration. □

Remarque 3.11. 1. Si A est une extension algébrique de F, et t transcendant sur A, alors A et $F(t)$ sont linéairement disjoints au-dessus de F.

2. Soient A et B deux F-algèbres. Alors A et B sont linéairement disjointes au-dessus de F, si et seulement si pour toutes sous-algèbres A_0 de A et B_0 de B qui sont de type fini, A_0 et B_0 sont linéairement disjointes au-dessus de F.
3. Supposons que A est une extension Galoisienne de F, et que B est un corps (contenant F). Alors A et B sont linéairement disjoints au-dessus de F si et seulement si $A \cap B = F$. Le sens direct est clair. Réciproquement, par ce qui précède, on peut supposer que A est une extension Galoisienne finie de F. Soit $\alpha \in A$ tel que $A = F(\alpha)$ (un tel α existe par le théorème de l'élément primitif), et P son polynôme minimal sur F, Q son polynôme minimal sur B, $\alpha_1 = \alpha, ..., \alpha_m$ les racines de P. Le polynôme Q divise P, donc $Q = \prod_{i \in J}(X - \alpha_i)$ pour un sous-ensemble J de $\{1, ...m\}$. Les coefficients de Q sont dans A, puisqu'il contient tous les α_i, ils sont aussi dans B par définition de Q, donc dans $A \cap B = F$. Comme P est irréductible sur F, cela entraîne $Q = P$, donc A et B sont linéairement disjointes au-dessus de F, puisque $[A : F] = [B(\alpha) : B]$.
4. Soient L et $E_1 \subseteq E_2$ des corps contenant F. Alors L et E_2 sont linéairement disjoints au-dessus de F si et seulement si L et E_1 sont linéairement disjoints au-dessus de F et LE_1 et E_2 le sont au-dessus de E_1.

Théorème 3.12 (Décomposition d'un fermé F-irréductible)**.** *Soient V un fermé défini sur F et F-irréductible et $V_1, ..., V_m$ ses composantes irréductibles. Alors les V_i sont définies sur une extension normale finie E de F et le groupe de Galois $G = \mathrm{Gal}(E/F)$ des F-automorphismes de E agit transitivement sur les composantes V_i, i.e. pour tout i et j il existe $\sigma \in G$ tel que $\sigma(V_i) = V_j$. En particulier,* $\dim(V_i) = \dim(V)$ *pour tout i.*

Démonstration. On commence par montrer que les variétés V_i sont définies sur une extension algébrique de F. Soit $\sigma \in \mathrm{Aut}(K/F)$, par la remarque 3.4 (2) (V défini sur F), $\sigma(V) = V$, donc comme l'image d'une variété par un automorphisme de K reste une variété, σ permute les V_i. Comme le groupe des permutations de m éléments est de cardinal $m!$, $\sigma^{m!}(V_i) = V_i$ pour tout i. Donc toujours par le même corollaire $\sigma^{m!}$ est l'identité sur les corps de définitions E_i des V_i, donc sur E, le corps engendré par les E_i. De plus, $\sigma(E_i)$ est le corps de définition de la variété $\sigma(V_i)$, donc E est stable par tout les F-automorphismes de K donc E est une extension normale de F.

Montrons maintenant que les V_i sont toutes de dimension $\dim(V)$. Comme $V_i \subseteq V$, on a $\dim(V_i) \leq \dim(V)$. Soit $\overline{a} \in K^n$ un générique de V sur F et $\overline{b} \in K^n$ un générique de V_i sur $\widetilde{F}$. Par la remarque 3.9, il existe un F-homomorphisme $\varphi : F[\overline{a}] \to F[\overline{b}]$ qui envoie $\overline{a}$ sur $\overline{b}$. Par le lemme 2.1 et le lemme de Zorn, on peut étendre φ en un F-homomorphisme $\widetilde{\varphi} : \widetilde{F}[\overline{a}] \to \widetilde{F}[\overline{b}]$. La restriction de $\widetilde{\varphi}$ à $\widetilde{F}$ est un F-automorphisme de $\widetilde{F}$, qu'on note ψ (ψ est surjectif car son image est une extension de F algébriquement close contenue dans $\widetilde{F}$, donc égale à $\widetilde{F}$). Comme K est algébriquement clos de degré de transcendance infini sur F (car K est de cardinal strictement plus grand que F), il existe $\overline{c} \in K^n$ tel qu'on puisse étendre ψ en un isomorphisme $\theta : \widetilde{F}[\overline{a}] \to \widetilde{F}[\overline{c}]$ qui envoie $\overline{a}$ sur $\overline{c}$. Alors $\widetilde{\varphi} \circ \theta^{-1} : \widetilde{F}[\overline{c}] \to \widetilde{F}[\overline{b}]$ est un $\widetilde{F}$-homomorphisme qui envoie $\overline{c}$ sur $\overline{b}$.

Comme θ est un F-isomorphisme, $\overline{c}$ est un générique de V sur F. Soit j tel que $\overline{c} \in V_j$, comme $\overline{c}$ est générique de V sur F, il est générique de V_j sur $\widetilde{F}$ (car $\dim(V_j) \leq \dim(V)$). On a donc

$$I(V_j) \cap \widetilde{F}[\overline{X}] = I(\overline{c}/\widetilde{F}) \subseteq I(\overline{b}/\widetilde{F}) = I(V_i) \cap \widetilde{F}[\overline{X}]$$

(les égalités par la remarque sur les points génériques et l'inclusion par le $\widetilde{F}$-homomorphisme $\widetilde{\varphi} \circ \theta^{-1}$). On a donc $I(V_j) \subseteq I(V_i)$ (car V_i et V_j sont définies sur $\widetilde{F}$) et donc par définition de la décomposition en composantes irréductibles, $V_i = V_j$. Donc $\widetilde{\varphi} \circ \theta^{-1}$ est un isomorphisme, donc $\widetilde{\varphi}$ aussi.

Toutes les composantes de V ont donc la même dimension que V. Un générique de V_i sur $\widetilde{F}$ est donc aussi un générique de V sur F. Or si $\overline{a}$ et $\overline{b}$ sont des génériques quelconques de V sur F, il existe un automorphisme $\sigma \in \mathrm{Aut}(K/F)$ qui envoie $\overline{a}$ sur $\overline{b}$, ce qui montre que $\mathrm{Aut}(K/F)$, donc $\mathrm{Aut}(E/F)$ permute transitivement les V_i. □

Théorème 3.13. *Soit $\overline{a} \in K^n$, et E un sous corps de K contenant F. Alors l'idéal $I(\overline{a}/E)$ est engendré par des polynômes de $F[\overline{X}]$ si et seulement si $F(\overline{a})$ et E sont linéairement disjoints au-dessus de F.*

Démonstration. Supposons que $F(\overline{a})$ et E sont linéairement disjoints au-dessus de F. Soit C une base du F-espace vectoriel E et $f(\overline{X}) \in I(\overline{a}/E)$. On peut écrire $f(\overline{X}) = \sum_i c_i f_i(\overline{X})$ avec $c_i \in C$ et $f_i(\overline{X}) \in F[\overline{X}]$. On a alors $0 = f(\overline{a}) = \sum_i c_i f_i(\overline{a})$, donc par hypothèse de disjonction, $f_i(\overline{a}) = 0$ pour tout i, donc les f_i sont dans $I(\overline{a}/F)$, ce qui montre que $I(\overline{a}/E)$ est engendré par des polynômes de $F[\overline{X}]$.

Réciproquement, on suppose que $I(\overline{a}/E)$ est engendré par des polynômes de $F[\overline{X}]$. Il suffit de montrer que $F[\overline{a}]$ et E sont linéairement disjoints au-dessus de F. On note M l'ensemble des monômes de $F[\overline{X}]$ et $B \subseteq M$ une base du F-espace vectoriel $F[\overline{X}]/I(\overline{a}/F)$, de sorte que $\{b(\overline{a}) | b \in B\}$ est une base de $F[\overline{a}]$. Il n'y a plus qu'à montrer que cette base reste indépendante dans $E[\overline{a}]$. Soient $b_1, ..., b_r \in B$, $c_1, ..., c_r \in E$ tels que $b_1(\overline{a})c_1 + ... + b_r(\overline{a})c_r = 0$. Alors $b_1c_1 + ... + b_rc_r \in I(\overline{a}/E)$, et comme $I(\overline{a}/E)$ est engendré par $I(\overline{a}/F)$, par la remarque 3.4 il existe des $e_m \in E$ pour $m \in M \backslash B$ tels que

$$b_1c_1 + ... + b_rc_r = \sum_{m \in M \backslash B} e_m(m - A_m).$$

Donc

$$b_1c_1 + ... + b_rc_r + \sum_{m \in M \backslash B} e_m A_m = \sum_{m \in M \backslash B} e_m m,$$

or M est une base du E-espace vectoriel $E[\overline{X}]$, et la somme de gauche est combinaison linéaire d'éléments de B, donc $e_m = 0$ pour tout $m \in M \backslash B$, donc $b_1c_1 + ... + b_rc_r = 0$ donc les c_i sont tous nuls. □

Corollaire 3.14. *Soit V un fermé F-irréductible défini par des polynômes de $F[\overline{X}]$. Alors V est une variété si et seulement si $F(V) \cap F_s = F$ (F_s est la clôture séparable de F).*

Démonstration. Les conditions suivantes sont équivalentes :

(1) V est une variété ;
(2) Si $\bar{a}$ et $\bar{b}$ sont deux génériques de V sur F, alors il existe $\sigma \in \mathrm{Aut}(K/\widetilde{F})$ tel que $\sigma(\bar{a}) = \bar{b}$ (V n'a qu'une composante irréductible) ;
(3) Si $\bar{a}$ est un générique de V sur F, alors $I(\bar{a}/F^{1/p^\infty})$ engendre $I(\bar{a}/\widetilde{F})$ (car $I(\bar{a}/F^{1/p^\infty}) = I(V) \cap F^{1/p^\infty}[\bar{X}]$) ;
(4) Si $\bar{a}$ est un générique de V sur F, alors $F^{1/p^\infty}(\bar{a})$ et $\widetilde{F}$ sont linéairement disjoints au-dessus de F^{1/p^∞} (par le théorème 3.13) ;
(5) $F^{1/p^\infty}(V)$ et $\widetilde{F}$ sont linéairement disjoints au-dessus de F^{1/p^∞} (car $F(\bar{a}) \simeq_F F(V)$).

Si V est une variété, par (5), $F(V) \cap F_s = F$. Réciproquement, par la remarque 3.11.(3), on sait que $F(V) \cap F_s = F$ entraîne que $F(V)$ et F_s sont linéairement disjoints au-dessus de F. Par le théorème 3.13, si $\bar{a}$ est un générique de V sur F, alors $I(\bar{a}/F)$ engendre $I(\bar{a}/F_s)$. Soit $\bar{b}$ un autre générique de V sur F. Comme $I(\bar{a}/F_s) = I(\bar{b}/F_s)$, il existe un automorphisme de K laissant F_s fixe et envoyant $\bar{a}$ sur $\bar{b}$. Un tel automorphisme laisse $\widetilde{F}$ fixé (car $\widetilde{F}$ est une extension purement inséparable de F_s), donc V a une seule composante irréductible, c'est une variété. □

Corollaire 3.15. *Soit $\overline{a} \in K^n$. On a :*

Le fermé associé à $I(\overline{a}/F)$ est défini sur F si et seulement si $F[\overline{a}]$ et F^{1/p^∞} sont linéairements disjoints au-dessus de F.

Le fermé associé à $I(\overline{a}/F)$ est une variété si et seulement si $F[\overline{a}] \cap F_s = F$.

Le fermé associé à $I(\overline{a}/F)$ est une variété définie sur F si et seulement si $F[\overline{a}]$ et $\widetilde{F}$ sont linéairement disjoints au-dessus de F.

Définition 3.16. Soit L un corps contenu dans K et contenant F. On dit que L est une *extension régulière* de F si L et $\widetilde{F}$ sont linéairement disjoints au-dessus de F.

Théorème 3.17. *Soient $\overline{a}$ et $\overline{b} \in K^n$ tels que $I(\overline{a}/F) \subseteq I(\overline{b}/F)$. Alors*

$$deg.tr((\overline{b}/F) \leq deg.tr((\overline{a}/F).$$

Si ces degrés sont égaux, alors $I(\overline{a}/F) = I(\overline{b}/F)$.

Démonstration. Comme $I(\bar{a}/F) \subseteq I(\bar{b}/F)$, nous avons un F-homomorphisme $\varphi : F[\bar{a}] \to F[\bar{b}]$ qui envoie $\bar{a}$ sur $\bar{b}$. Supposons que $f(a_1, ..., a_r) = 0$, où $f \in F[X_1, ..., X_r]$, alors $\varphi(f(a_1, ..., a_r)) = 0 = f(b_1, ..., b_r)$, ce qui prouve l'inégalité.

On suppose maintenant que $deg.tr(\bar{a}/F) = deg.tr(\bar{b}/F)$. Il faut montrer que φ est un isomorphisme. Quitte à réindicer, on peut supposer que $(b_1, ..., b_d)$ est une base de transcendance de $F(\bar{b})$ sur F. Alors $a_1, ..., a_d$ sont algébriquement indépendants au-dessus de F, donc forment une base de transcendance de $F(\bar{a})$ sur F. En particulier, $\ker(\varphi) \cap F[a_1, ..., a_d] = (0)$.

Soit $c \in F[\bar{a}]$, $c \neq 0$, et $f \in F(a_1, ..., a_d)[X]$ son polynôme minimal sur $F(a_1, ..., a_d)$, quitte à multiplier par une constante non nulle, on peut supposer $f \in F[a_1, ..., a_d][X]$. Les coefficients de $\varphi(f)$ sont alors non tous nuls, et $\varphi(c)$ en est une racine. Comme le coefficient constant de $\varphi(f)$ est non nul, 0 n'est pas racine de $\varphi(f)$, donc $\varphi(c) \neq 0$. □

Corollaire 3.18. *Soient $V \subseteq W$ des fermés F-irréductibles. Alors* $\dim(V) \leq \dim(W)$ *et si* $\dim(V) = \dim(W)$*, alors $V = W$.*

Proposition 3.19. *Soit F un sous-corps des corps L et M.*

(1) Si L et M sont linéairement disjoints au-dessus de F, alors ils sont algébriquement indépendants au-dessus de F ;

(2) si F est algébriquement clos, la réciproque de (1) *est vraie ;*

(3) supposons que L est une extension régulière de F, algébriquement indépendante avec M au-dessus de F. Alors L et M sont linéairement disjoints au-dessus de F.

Démonstration. (1) Supposons que L et M sont linéairement disjoints au-dessus de F, et soit $f \in M[\bar{X}], \bar{X} = (X_1, ..., X_n)$, $\bar{a} \in L^n$, et supposons que $f(\bar{a}) = 0$. On peut écrire $f(\bar{a})$ comme une combinaison M-linéaire de monômes en $a_1, ..., a_n$, et la disjonction linéaire de L et M au-dessus de F entraîne l'existence d'un polynôme $g \in F$ tel que $g(\bar{a}) = 0$.

(2) Supposons que L et M sont algébriquement indépendants au-dessus de F algébriquement clos, et soit $\bar{a} \in L^n$. On va montrer que $I(\bar{a}/F)$ engendre $I(\bar{a}/M)$. Comme F est algébriquement clos, $I(\bar{a}/F)$ est l'idéal d'une variété V, et $\bar{a}$ est un générique de V sur F. Par hypothèse, $deg.tr(\bar{a}/F) = deg.tr(\bar{a}/M)$, donc par le théorème 3.17, $\bar{a}$ est un générique de V sur M, donc $I(\bar{a}/F)$ engendre $I(\bar{a}/M)$. Par le théorème 3.13, $F(\bar{a})$ et M sont linéairement disjoints au-dessus de F. Ceci étant vrai pour tout uplet fini $\bar{a}$ de L, on a le résultat.

(3) On sait que L et $\widetilde{F}$ sont linéairement disjoints au-dessus de F, comme M et L sont algébriquement indépendants au-dessus de F, $\widetilde{F}M$ et $\widetilde{F}L$ le sont aussi. Donc par (2) et la remarque 3.11.(4), L et $\widetilde{F}M$ sont linéairement disjoints au-dessus de F. □

4 Théorie des corps finis

4.1 Propriétés élémentaires

On donne dans cette partie quelques résultats très classiques sur les corps finis. On dit qu'un corps F est fini s'il n'a qu'un nombre fini d'éléments. Sa caractéristique est un nombre premier p et son sous corps premier est $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. L'extension $F/\mathbb{F}_p$ est donc une extension de corps de degré fini n, de sorte que le cardinal de F est p^n.

Théorème 4.1. *Pour tout p premier, $n \geq 1$, il existe un corps fini de cardinal p^n.*

Tout corps fini à p^n éléments est un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. Deux tels corps sont donc isomorphes.

Cela justifie que l'on parle du corps $\mathbb{F}_{p^n}$ à p^n éléments.

Démonstration. Soit K un corps de décomposition de $P(X) = X^{p^n} - X$ sur $\mathbb{F}_p$, et K' l'ensemble des racines de P dans K. La formule $(a+b)^p = a^p + b^p$, vraie dans tout corps de caractéristique p, montre que K' est un sous corps de K, il lui est donc égal. Les racines de P sont toutes distinctes car la dérivée de P est -1, donc P est séparable, donc le cardinal de K est p^n.

Soit K un corps fini à p^n éléments. Le groupe $(K^*, \times)$ est d'ordre $p^n - 1$, donc un élément non nul x vérifie $x^{p^n-1} = 1$, donc les éléments de K sont exactement les racines de P, qui est donc scindé dans K. Le corps K est donc un corps de décomposition de P sur $\mathbb{F}_p$. □

Proposition 4.2. *La clôture algébrique de $\mathbb{F}_p$ est*

$$\tilde{\mathbb{F}_p} = \bigcup_{m \in \mathbb{N}} \mathbb{F}_{p^m}$$

avec les inclusions $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ si et seulement si n divise m.

Démonstration. On remarque que pour m et n des entiers, $d = pgcd(n, m)$ et $M = ppcm(n, m)$ alors :

$$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \Longleftrightarrow n|m,\ \mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^d} \text{ et } \mathbb{F}_{p^n}\mathbb{F}_{p^m} = \mathbb{F}_{p^M}.$$

De plus, les extensions algébriques finies de $\mathbb{F}_p$ sont toutes des corps finis, et réciproquement tout corps fini de caractéristique p est une extension algébrique de $\mathbb{F}_p$. Cela montre bien le résultat. □

Proposition 4.3. *Le groupe de Galois de l'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ est cyclique d'ordre n engendré par l'automorphisme de Frobenius* $\mathrm{Fr} : x \mapsto x^p$.

Démonstration. Le corps $\mathbb{F}_{p^n}$ est l'ensemble des solutions de l'équation $X^{p^n} - X$, donc c'est une extension galoisienne (de degré n) de $\mathbb{F}_p$, donc $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ est d'ordre n. L'application Fr appartient à $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. En effet, la formule $(a+b)^p = a^p + b^p$ montre que c'est un morphisme de corps, il est donc injectif donc surjectif (le corps est fini).

Soit m son ordre (qui divise n). On alors $\mathrm{Fr}^m = \mathrm{Id}$, donc tout les éléments de $\mathbb{F}_{p^n}$ sont racines de $X^{p^m} - X$, donc $\sharp(\mathbb{F}_{p^n}) \leq p^m$, donc $m = n$. Comme $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ est d'ordre n, il est bien engendré par Fr. □

Remarque 4.4. Ce résultat s'étend en : le groupe de Galois de l'extension $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ est cyclique d'ordre m/n engendré par Fr^n.

Proposition 4.5. *Un corps fini est parfait.*

Démonstration. L'automorphisme de Frobenius montre que $\mathbb{F}_{p^n}$ est stable par racines p-èmes, donc parfait. □

4.2 Groupe de Galois absolu

Les puissances entières de Fr sont donc des automorphismes de $\tilde{\mathbb{F}_p}$, mais il y en a d'autres. Nous allons chercher à les décrire.

Soit $G := \prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z}$. On munit chaque $\mathbb{Z}/n\mathbb{Z}$ de la topologie discrète, et on munit G de la topologie produit. Par le théorème de Tychonoff, G est compact, de plus il admet une base d'ouvert-fermés. On remarque que c'est un groupe topologique.

Pour m qui divise n, on note π_{mn} la projection canonique $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Soit H l'ensemble des suites $(a_n)_{n\in\mathbb{N}} \in G$ vérifiant $\pi_{mn}(a_n) = a_m$ pour tout m, n avec $m|n$. H est la limite projective des $\mathbb{Z}/n\mathbb{Z}$ par rapport aux π_{mn}. L'ensemble H est un sous-groupe de G. De plus, on vérifie qu'il est fermé, donc compact : si $(b_n) \notin H$, il existe des entiers m, n avec $m|n$ tels que $\pi_{mn}(b_n) \neq b_m$, alors l'ouvert $\prod_{k\neq n, k\neq m} \mathbb{Z}/k\mathbb{Z} \times \{b_m\} \times \{b_n\}$ est disjoint de H et contient (b_n).

On peut aussi plonger $\mathbb{Z}$ dans H via l'application qui a un entier associe ses classes modulo n pour $n \geq 1$. L'image de $\mathbb{Z}$ dans H est dense dans H, c'est a dire intersecte tout ouvert qui intersecte H. Cela découle du fait que tout système fini de congruences consistantes a une solution dans $\mathbb{Z}$.

Soit $G(\mathbb{F}_p) := \mathrm{Gal}(\tilde{\mathbb{F}_p}/\mathbb{F}_p)$ le groupe des automorphismes de $\tilde{\mathbb{F}_p}$. On l'appelle groupe de Galois absolu de $\mathbb{F}_p$. Pour tout élément $\psi \in G(\mathbb{F}_p)$ on associe un élément $(a_n) \in G$ tel que pour tout n, les restrictions de ψ et Fr^{a_n} à $\mathbb{F}_{p^n}$ soient égales. On vérifie que c'est bien un morphisme injectif de groupes, dont l'image est dans H. On va maintenant montrer que c'est en fait un isomorphisme entre $G(\mathbb{F}_p)$ et H. Soit $(a_n) \in H$. On définit $\psi(b) := b^{p^{a_m}}$ pour $b \in \mathbb{F}_{p^m}$. Montrons que cela ne dépend pas de l'entier m choisi. Soit n tel que $m|n$. On a $a_n = a_m + km$ pour un entier k par définition de H, et comme $\mathrm{Fr}^m = Id$ dans $\mathbb{F}_{p^m}$, on a pour tout $b \in \mathbb{F}_{p^m}$, $b^{p^{a_n}} = b^{p^{a_m} p^{km}} = \mathrm{Fr}^m(b^{p^{a_n m}}) = b^{p^{a_n m}}$. Le morphisme ψ est donc un automorphisme sur chaque $\mathbb{F}_{p^n}$, donc c'est un automorphisme de $\tilde{\mathbb{F}_p}$.

Le groupe H est souvent noté $\hat{\mathbb{Z}}$, où encore

$$\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}.$$

On a donc montré :

Théorème 4.6. *Le groupe de Galois absolu $G(\mathbb{F}_p) = \mathrm{Gal}(\tilde{\mathbb{F}_p}/\mathbb{F}_p)$ de $\mathbb{F}_p$ est isomorphe à $\hat{\mathbb{Z}}$.*

On veut maintenant étendre la correspondance de Galois à $G(\mathbb{F}_p)$. Elle reste vraie, à la nuance près que les sous-groupes qui interviennent sont fermés.

Théorème 4.7. *Les applications qui à un sous groupe fermé de $G(\mathbb{F}_p)$ associent le sous corps de $\tilde{\mathbb{F}}_p$ fixé par les éléments de G, et qui à un sous corps E de $\tilde{\mathbb{F}}_p$ associent le sous-groupe (fermé) de $G(\mathbb{F}_p)$ des automorphismes laissant E invariant, qu'on note $G(E)$, sont des bijections réciproques.*

Démonstration. Montrons tout d'abord que le sous-groupe de $G(\mathbb{F}_p)$ qui laisse fixé E, pour un sous corps E de $\tilde{\mathbb{F}}_p$, est fermé. Soit $\sigma \in G(\mathbb{F}_p)$. Comme $E = \cup_n E \cap \mathbb{F}_{p^n}$, on a $\sigma \in G(E)$ si et seulement si les restictions de σ sont l'identité sur tous les $E \cap \mathbb{F}_{p^n}$. Pour tout n, $\mathrm{Gal}(\mathbb{F}_{p^n}/E \cap \mathbb{F}_{p^n})$ est (isomorphe à) un sous groupe de $\mathbb{Z}/n\mathbb{Z}$, de sorte que $G(E) = G(\mathbb{F}_p) \cap \prod_n \mathrm{Gal}(\mathbb{F}_{p^n}/E \cap \mathbb{F}_{p^n})$, or une intersection de fermés est fermée, donc $G(E)$ est fermé.

Soit H un sous groupe quelconque de $G(\mathbb{F}_p)$, E le sous corps de $\tilde{\mathbb{F}}_p$ fixé par H. Nous allons montrer que l'adhérence de $\bar{H}$ de H est le sous groupe qui fixe E, $G(E)$. Cela achèvera la démonstration du théorème. Pour n entier, soit res_n la restriction de $G(\mathbb{F}_p)$ à $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, donc $H_n = res_n(H)$ est (isomorphe à) un sous groupe de $\mathbb{Z}/n\mathbb{Z}$. On vérifie que $G(\mathbb{F}_p) \cap \prod_n H_n$ est le plus petit fermé de $\prod_n \mathbb{Z}/n\mathbb{Z}$ qui contient H, donc c'est $\bar{H}$. Comme $res_n(\bar{H}) = H_n$, le sous corps de $\tilde{\mathbb{F}}_p$ fixé par $\bar{H}$ est E. □

5 Bornes pour les idéaux de polynômes

Le but de cette section est de montrer l'existence d'une formule qui définit les coefficients de polynômes de degrés bornés qui engendrent l'idéal d'une variété.

Nous devons d'abord démontrer le théorème suivant :

Théorème 5.1. *Soient n, e entiers et $\overline{X} = (X_1, ..., X_n)$.*

(1) Il existe une constante $A = A(n, e)$ telle que pour tous corps K, et polynômes $f_1(\overline{X}), ..., f_m(\overline{X}), g(\overline{X}) \in K[\overline{X}]$ de degrés $\leq e$, si $g(\overline{X}) \in (f_1(\overline{X}), ..., f_m(\overline{X}))$, alors

$$g(\overline{X}) = h_1(\overline{X})f_1(\overline{X}) + ... + h_m(\overline{X})f_m(\overline{X})$$

pour des polynômes $h_1(\overline{X}), ..., h_m(\overline{X}) \in K[\overline{X}]$ de degré $\leq A$.

(2) Il existe une constante $B = B(n, e)$ telle que pour tous corps K, et I idéal de $K[\overline{X}]$ engendré par des polynômes de degré $\leq e$, on a que si pour tous polynômes $g(\overline{X}), h(\overline{X})$ de degrés $\leq D$, $g(\overline{X})h(\overline{X}) \in I$ entraine $g(\overline{X}) \in I$ ou $h(\overline{X}) \in I$, alors I est premier.

(3) Il existe une constante $C = C(n, e)$ telle que pour tout corps K, tout idéal I de $K[\overline{X}]$ engendré par des polynômes de degrés inférieurs à e, alors il y a au plus C idéaux minimaux contenant I et chacun est engendré par des polynômes de degrés inférieurs à C.

(4) Il existe une constante E=(n,e) telle que pour tout corps K, tous idéaux I, J de $K[\overline{X}]$ engendrés par des polynômes de degrés $\leq e$, l'idéal $I \cap J$ est engendré par des polynômes de degrés $\leq e$.

Pour montrer l'existence de ces bornes, nous allons utiliser une méthode non-constructive utilisant les ultraproduits (voir [24, van den Dries-Schmidt]). On peut en fait montrer que ces bornes sont des combinaisons de fonctions polynomiales et exponentielles des variables, donc sont récursives (voir [22, Seidenberg], 57 pour (1), 65 pour (2) et (3), et 56 pour (4)).

5.1 Modules plats

Dans toute la section, nous allons considérer l'ultraproduit $K = \prod_{i\in I} K_i/\mathcal{U}$ où les K_i sont des corps et $\mathcal{U}$ un ultrafiltre non principal sur I. On définit aussi l'*anneau des polynômes internes* de K comme l'ultraproduit d'anneaux $K[\overline{X}]_{int} = \prod_{i\in I} K_i[\overline{X}]/\mathcal{U}$. Remarquons qu'il contient des "ultra-polynômes" de degrés infini. On note $K(\overline{X})_{int}$ le corps des fractions de cet anneau intègre, qui est isomorphe à l'ultraproduit $\prod_{i\in I} K_i(\overline{X})/\mathcal{U}$. L'ultraproduit K est un corps, donc on peut définir l'anneau de polynômes $K[\overline{X}]$, qui se plonge canoniquement dans $K[\overline{X}]_{int}$. On notera pour un polynôme f, $\deg(f)$ le degré total de f, et $\deg_{X_i}(f)$ le degré par rapport à X_i.

Nous commençons par quelques résultats sans démonstration sur les modules plats. On peut trouver les démonstrations dans [2, Bourbaki]. La définition de module plat que nous donnons est inhabituelle, mais c'est la seule qui sera utile ici (elle est équivalente à celle usuelle).

Définition 5.2. Soit $R \subseteq S$ une extension d'anneaux. On dit que S est un R-module *plat* s'il vérifie l'une des deux propriétés équivalentes qui suivent :

(i)pour toute équation homogène

$$f_1Y_1 + ... + f_lY_l = 0, f_i \in R,$$

les solutions dans S^l sont combinaisons S-linéaires de solutions dans R^l ;

(ii) pour tout système linéaire homogène à coefficients dans R

$$\begin{cases} f_{11}Y_1 + ... + f_{1l}Y_l &= 0 \\ \vdots & \vdots \\ f_{k1}Y_1 + ... + f_{kl}Y_l &= 0, \end{cases}$$

les solutions dans S^l sont combinaison S-linéaires de solutions dans R^l.

Proposition 5.3. *La notion de module plat est stable par extension des scalaires et transitivité.*

Définition-Proposition 5.4. *Soit $R \subseteq S$ une extension d'anneaux. Les trois propositions ci-dessous sont équivalentes :*

(i) S est un R-module fidèlement plat.

(ii) S est un R-module plat et pour tout idéal maximal $\mathfrak{m}$ de R, $\mathfrak{m}S. \neq S$

(iii) S est un R-module plat et tout système

$$\begin{cases} f_{11}Y_1 + ... + f_{1l}Y_l &= f_1 \\ \vdots & \vdots \\ f_{k1}Y_1 + ... + f_{kl}Y_l &= f_k \end{cases} \qquad f_{ij}, f_i \in R$$

avec une solution dans S^l a une solution dans R^l.

Nous sommes maintenant en mesure d'énoncer et de démontrer des propriétés sur les ultraproduits qui nous intéressent.

Proposition 5.5. *L'ultraproduit $K[\overline{X}]_{int}$ est un $K[\overline{X}]$-module plat.*

Démonstration. On raisonne par récurrence sur le nombre de variables n. Si $n = 1$ c'est clair. Soit $n > 1$, $f_1Y_1 + ... + f_lY_l = 0, f_i \in K[\overline{X}]$, une équation homogène, et $g = (g_1, ..., g_l)$ une solution dans $K[\overline{X}]^l_{int}$. Il faut montrer que g est combinaison linéaires de solutions dans $K[\overline{X}]^l$. Quitte à faire un changement de variable (linéaire), on peut supposer que f_1 est non nul et unitaire en X_n. Soit $d = \deg_{X_n} f_1$. On a $g_2 = [(g_2(i))_{i\in I}]\mathcal{U}$, $f_1 = [(f_1(i))_{i\in I}]\mathcal{U}$ avec $g_2(i)$ et $f_1(i) \in K_i[\overline{X}]$, de plus, comme f_1 est unitaire de degré d en X_n, pour presque tout i, $f_1(i)$ est unitaire de degré d en X_n, donc on peut faire une division euclidienne et il existe $q(i), r(i) \in K_i[\overline{X}]$ avec $\deg_{X_n}(r(i)) < d$ tels que $g_2(i) = q(i)f_1(i) + r(i)$. Donc si on pose $q = [(q(i))_{i\in I}]\mathcal{U}$ et $r = [(r(i))_{i\in I}]\mathcal{U}$, on a $g_2 = qf_1 + r$ avec $\deg_{X_n}(r) < d$. Comme $(-f_2, f_1, 0, ..., 0)$ est solution de l'équation, on a une solution $\widetilde{g}$ combinaison linéaire de g et d'une solution dans $K[\overline{X}]$ telle que $\deg_{X_n}(\widetilde{g_2}) < d$. En itérant le procédé, on obtient une solution g' telle que $\deg_{X_n}(g'_k) < d$ pour $k = 2, ..., l$. Comme $f_1g'_1 + ... + f_lg'_l = 0$, $\deg_{X_n}(g'_1)$ est fini aussi, donc g' est solution dans $K[X_1, ..., X_{n-1}]_{int}[X_n]$. Par hypothèse de récurrence, $K[X_1, ..., X_{n-1}]_{int}$ est un $K[X_1, ..., X_{n-1}]$-module plat, donc par extension des scalaires, $K[X_1, ..., X_{n-1}]_{int}[X_n]$ est un $K[\overline{X}]$-module plat, donc g' est combinaison linéaire de solutions dans $K[\overline{X}]^l$, donc g aussi, ce qui achève la récurrence. □

On peut déjà prouver l'assertion (4) du théorème 5.1.

Démonstration. Remarquons déjà que si l'on arrive à trouver une borne qui dépend du nombre l de générateurs de I et J, on en aura une pour tout l car si E est une borne pour $l = \dim\{f \in K[\overline{X}] | \deg(f) \leq e\}$, E est une borne pour tout l (à n et e fixés). On fixe donc l, et on va raisonner par l'absurde. On suppose donc qu'il existe pour tout i entier un corps K_i et deux idéaux de I_i et J_i de $K[\overline{X}]$ engendrés respectivement par $f_1(i), ..., f_l(i)$ et $g_1(i), ..., g_l(i)$, tous de degrés $\leq e$, tels que $I_i \cap J_i$ ne soit pas engendré par des polynômes de degrés inférieurs à i.

Soit $K = \prod_{i\in\mathbb{N}} K_i(\overline{X})/\mathcal{U}$ un ultraproduit sur un ultrafiltre non principal. On considère le système linéaire homogène suivant :

$$\begin{cases} f_1Y_1 + ... + f_lY_l &= Y \\ \vdots & \vdots \\ g_1Y_1 + ... + g_lY_l &= Y, \end{cases}$$

où $f_k = [(f_k(i))_{i\in\mathbb{N}}]\mathcal{U}$ et $g_k = [(g_k(i))_{i\in\mathbb{N}}]\mathcal{U}$. Comme les $f_k(i)$ et $g_k(i)$ sont de degrés bornés par e, les f_k et g_k sont aussi de degrés bornés, donc en particulier ils sont dans $K[\overline{X}]$. On a donc un système linéaire homogène à coefficients dans $K[\overline{X}]$. Comme $K[\overline{X}]_{int}$ est un $K[\overline{X}]$-module plat, les solutions dans $K[\overline{X}]_{int}$ sont combinaisons linéaire de solutions dans $K[\overline{X}]$. Or l'hypothèse sur les $I_i \cap J_i$ montre qu'il y a une solution du système qui n'est pas combinaisons linaire de solutions dans $K[\overline{X}]$, contradiction. □

Proposition 5.6. *L'ultraproduit $K[\overline{X}]_{int}$ est un $K[\overline{X}]$-module fidèlement plat.*

Démonstration. On va utiliser la caractérisation (ii). On sait déjà qu'il est plat. Soit $\mathfrak{m}$ un idéal maximal de $K[\overline{X}]$. Par le Nullstellensatz, $\mathfrak{m}$ a un zéro dans une extension finie L de K. Il faut montrer que L est un ultraproduit, car alors on aura que $\mathfrak{m}K[\overline{X}]_{int}$ a un zéro dans l'extension $L[\overline{X}]_{int}$ de $K[\overline{X}]_{int}$, donc $\mathfrak{m}K[\overline{X}]_{int} \neq K[\overline{X}]_{int}$.

Comme L/K est une extension finie, elle a un nombre finis de générateurs, donc il suffit de montrer que pour x algébrique sur K, $K[x]$ est un ultraproduit. Soit P le polynôme minimal de x sur K. Comme P est irréductible, pour presque tout i (c'est à dire pour un ensemble de i

dans $\mathcal{U}$), $P(i)$ est irréductible, puisqu'être irréductible s'exprime au premier ordre. Donc pour presque tout i, soit x_i une racine de P_i dans le corps de rupture de P_i. Alors $K_i(x_i)$ est un corps pour presque tout i, et $[(x_i)_{i\in I}]_{\mathcal{U}}$ est racine de P dans l'ultraproduit $\prod_i K_i(x_i)/\mathcal{U}$, et engendre ce corps sur K. Cela montre que $K(x)$ et l'ultraproduit $\prod_i K_i(x_i)/\mathcal{U}$ sont isomorphes.

□

On est maintenant en mesure de prouver la partie (1) du théorème 5.1 :

Théorème. *Il existe une constante $A = A(n, e)$ telle que pour tout corps K, et polynômes $f_1(\overline{X}), ..., f_m(\overline{X}), g(\overline{X}) \in K[\overline{X}]$ de degré $\leq e$, si $g(\overline{X}) \in (f_1(\overline{X}), ..., f_m(\overline{X}))$, alors*

$$g(\overline{X}) = h_1(\overline{X})f_1(\overline{X}) + ... + h_m(\overline{X})f_m(\overline{X})$$

pour des polynômes $h_1(\overline{X}), ..., h_m(\overline{X}) \in K[\overline{X}]$ de degré $\leq A$.

Démonstration. Remarquons déjà que si l'on arrive à trouver une borne qui dépend de m, on en aura une pour tout m car si A est une borne pour $m = \dim\{f \in K[\overline{X}] | \deg(f) \leq e\}$, A est une borne pour tout m (à n et e fixés).

On raisonne par l'absurde : on fixe m, n, e et on suppose qu'il n'existe pas de telle borne, c'est à dire que pour tout entier i, il existe un corps K_i et une équation comme dans l'énoncé qui a une solution dans K_i^m mais pas de solution de degré inférieur à i. On considère alors l'ultraproduit $K = \prod_{i\in\mathbb{N}} K_i/\mathcal{U}$, avec $\mathcal{U}$ ultrafiltre non principal sur $\mathbb{N}$. Les équations précédentes nous donnent alors une équation linéaire à coefficients dans $K[\overline{X}]$ (car ils sont tous de degrés bornés par e) mais qui a une solution dans $K[\overline{X}]_{int}$, mais pas dans $K[\overline{X}]$. Cela contredit le fait que $K[\overline{X}]_{int}$ est un $K[\overline{X}]$-module fidèlement plat, par la caractérisation (iii). □

5.2 Idéaux premiers

Pour obtenir la borne pour les idéaux premiers, nous avons besoin de deux lemmes.

Lemme 5.7. *Si K est un ultraproduit, alors $K(\overline{X})_{int}$ est une extension régulière de $K(\overline{X})$, i.e. l'extension est relativement algébriquement close et séparable.*

Démonstration. Montrons tout d'abord que l'extension est relativement algébriquement close. Soit $z \in K(\overline{X})_{int}$ algébrique sur $K(\overline{X})$, montrons que $z \in K(\overline{X})$. Il suffit de montrer que c'est vrai pour z entier sur $K[\overline{X}]$ et $z \neq 0$. Or $K[\overline{X}]_{int}$ est intégralement clos car les anneaux de polynômes le sont et que cela s'énonce au premier ordre dans le langage des anneaux, donc la propriété est vraie dans l'ultraproduit d'anneaux de polynômes, donc $z \in K[\overline{X}]_{int}$. On a z^{-1} qui est dans $K(\overline{X})_{int}$ et aussi algébrique sur $K[\overline{X}]$, donc ils existe un $h \in K[\overline{X}]$ tel que $z^{-1}h$ soit entier sur $K[\overline{X}]$, donc $z^{-1}h \in K[\overline{X}]_{int}$, donc $h = zg$, avec $z, g \in K[\overline{X}]_{int}$. Alors $\deg(h) = \deg(z) + \deg(g)$, et comme $\deg(h)$ est fini, $\deg(z)$ doit être fini, donc $z \in K[\overline{X}]$.

Pour le second point, supposons que $car(K) = p > 0$. Il suffit de voir que si $a_1, ..., a_m \in K$ sont p-indépendants dans K, alors $a_1, ..., a_m, X_1, ..., X_n$ sont p-indépendants dans $K(\overline{X})_{int}$. □

Lemme 5.8. *Soit K un ultraproduit et $f \in K[X_1]_{int}$ irréductible de degré infini, et soit I un idéal de $K[\overline{X}]$, $n > 0$. Alors l'image de f dans $K[\overline{X}]_{int}/IK[\overline{X}]_{int}$ n'est pas un diviseur de 0.*

Démonstration. Soit $g \in K[\overline{X}]_{int}$ tel que

$$(1)\ fg = \sum_{i=0}^{m} h_i f_i, f_i \in I, h_i \in K[\overline{X}]_{int}.$$

Il s'agit de montrer que $g \in IK[\overline{X}]_{int}$. Comme f est de degré infini, le morphisme canonique

$$K[X_1]_{int} \to L := K[X_1]_{int}/(f)$$

plonge $K[X_1]$ dans le corps L, donc $K(X_1)$ est plongé dans L via un plongement ϕ (L est un corps car passage au quotient et ultraproduit commutent, de sorte que L est aussi un ultraproduit). Le morphisme ϕ nous permet de considérer L comme une $K(X_1)$-algèbre, cela entraine que L est un $K(X_1)$-module plat, et donc $L[X_2, ..., X_n]$ est un $K(X_1)[X_2, ..., X_n]$-module plat. Or par la proposition 5.5, $L[X_2, ..., X_n]_{int}$ est un $L[X_2, ..., X_n]$-module plat, donc par transitivité des modules plats, on a $L[X_2, ..., X_n]_{int}$ est un $K(X_1)[X_2, ..., X_n]$-module plat. On a que (1) implique que dans $L[X_2, ..., X_n]_{int}$ on a

$$(2) \sum_i h_i(\phi(X_1), X_2, ..., X_n) f_i(\phi(X_1), X_2, ..., X_n) = 0.$$

On considère les solutions $(y_1, ..., y_m)$ dans $K(X_1)[X_2, ..., X_n]^m$ de

$$(3)\ Y_1 f_1 + ... + Y_m f_m = 0.$$

Le $K(X_1)[X_2, ..., X_n]$-module de ces solutions est engendré par $(h_{11}, ..., h_{1m}), ..., (h_{k1}, ..., h_{km}), h_{ij} \in K(X_1)[X_2, ..., X_n]$, quitte à multiplier par un dénominateur commun, on peut les supposer dans $K[\overline{X}]$. Par (2), $(h_1, ..., h_m)$ est solution de (3), donc comme $L[X_2, ..., X_n]_{int}$ est un $K(X_1)[X_2, ..., X_n]$-module plat,

$$h_j(\phi(X_1), X_2, ..., X_n) = \sum_{i=1}^{k} \lambda_i h_{ij}(\phi(X_1), X_2, ..., X_n), \lambda_i \in L[X_2, ..., X_n]_{int}.$$

Or $\lambda_i = \mu_i(\phi(X_1), X_2, ..., X_n)$, $\mu_i \in K[\overline{X}]_{int}$. Alors :

$$(4)\ h_j = (\sum_{i=1}^{k} \mu_i h_{ij}) + f q_j, j = 1, ..., m, q_j \in K[\overline{X}]_{int}.$$

On substitue (4) dans (1), en se rapelant que les $(h_{i1}, ..., h_{im})$ sont solution de (3), et on obtient

$$fg = \sum_{j=1}^{m} f q_j f_j,$$

donc $g \in IK[\overline{X}]_{int}$. □

Corollaire 5.9. *Soit K un ultraproduit, et I un idéal de $K[X]$. Si $I : (f) = I$ pour tout $f \in K[X_1]$ irréductible, alors*

$$IK[\overline{X}]_{int} : (fK[\overline{X}]_{int}) = IK[\overline{X}]_{int} \text{ pour tout } f \in K[X_1]_{int} \backslash \{0\}$$

Démonstration. On raisonne par l'absurde. Soit f de degré minimal contredisant la propriété. Alors il existe $g \in K[\overline{X}]_{int}$ avec $gf \in IK[\overline{X}]_{int}$ mais $g \notin IK[\overline{X}]_{int}$. Comme f est de degré minimal, f est irréductible dans $K[X_1]_{int}$, donc par le lemme il ne peut pas être de degré infini, donc $f \in K[X_1]$, mais alors par l'hypothèse $I : (f) = I$ et en utilisant la propriété de module plat on a $g \in IK[\overline{X}]_{int}$, contradiction. □

Proposition 5.10. *Soit K un ultraproduit et I un idéal de $K[\overline{X}]$. Alors I est premier si et seulement si $IK[\overline{X}]_{int}$ est premier dans $K[\overline{X}]_{int}$.*

Démonstration. En utilisant la propriété 5.4 (*iii*) des modules fidèlement plats, on a que $IK[\overline{X}]_{int} \cap K[\overline{X}] = I$, donc la réciproque est claire. Pour le sens direct, on raisonne par récurrence sur n, le nombre de variables. Si $n = 1$, alors $I = (0)$ ou $I = (f)$ pour un f irréductible dans $K[X_1]$, et comme f reste irréductible dans $K[X_1]_{int}$, le résultat est vrai dans ce cas. On suppose donc $n > 1$. Il y a deux cas à distinguer :

(1) Soit $I \cap K[X_i] \neq 0$ pour tout $i = 1, ..., n$. Dans ce cas, soit $f_i \in I \cap K[X_i]$ avec $\deg(f_i) = d_i > 0$. Alors l'image x_i de X_i dans $K[\overline{X}]/I$ est algébrique de degré $\leq d_i$ sur K, donc $K[\overline{X}]/I = K[x_1, ..., x_n]$ est une extension de corps (finie) de K. Pour les mêmes raisons, la K-algèbre $K[\overline{X}]_{int}/IK[\overline{X}]_{int}$ est engendrée sur K par les images des X_i, donc le morphisme canonique $K[\overline{X}]/I \to K[\overline{X}]_{int}/IK[\overline{X}]_{int}$ est surjectif, et comme $K[\overline{X}]/I$ est un corps ce morphisme est un isomorphisme, donc $IK[\overline{X}]_{int}$ est premier.

(2) Sinon il existe un i tel que $I \cap K[X_i] = 0$, et on peut supposer quitte à réindicer que $I \cap K[X_1] = 0$. Alors $IK(X_1)[X_2, ..., X_n]$ est un idéal premier, donc par le lemme, l'idéal $IK(X_1)_{int}[X_2, ..., X_n]$ est premier dans $K(X_1)_{int}[X_2, ..., X_n]$. On rappelle que $K(X_1)_{int}$ est un ultraproduit, donc par l'hypothèse de récurrence, $IK(X_1)_{int}[X_2, ..., X_n]_{int}$ est un idéal premier de $K(X_1)_{int}[X_2, ..., X_n]_{int}$, donc $IK(X_1)_{int}[X_2, ..., X_n]_{int} \cap K[\overline{X}]_{int}$ est un idéal premier de $K[\overline{X}]_{int}$. Il reste à montrer que $IK(X_1)_{int}[X_2, ..., X_n]_{int} \cap K[\overline{X}]_{int} = IK[\overline{X}]_{int}$. Soit $g \in IK(X_1)_{int}[X_2, ..., X_n]_{int} \cap K[\overline{X}]_{int}$ et $f_1, ..., f_m$ des générateurs de I. Alors $g = \sum(h_i/f)f_i$ pour des $h_i \in K[\overline{X}]_{int}$ et un $f \in K[X_1]_{int}$. Alors $fg \in IK[\overline{X}]_{int}$, *i.e.* $g \in IK[\overline{X}]_{int} : (fK[\overline{X}]_{int})$. Par le corollaire 5.9, on en déduit que $g \in IK[\overline{X}]_{int}$. □

On peut en déduire la deuxième assertion du théorème 5.1 :

Théorème. *Il existe une constante $B = B(n, e)$ telle que pour tout corps K, et I idéal de $K[\overline{X}]$ engendré par des polynômes de degré $\leq e$, on a que si pour tout polynômes $g(\overline{X}), h(\overline{X})$ de degrés $\leq D$, $g(\overline{X})h(\overline{X}) \in I$ entraine $g(\overline{X}) \in I$ ou $h(\overline{X}) \in I$, alors I est premier.*

Démonstration. On fait comme pour l'autre borne : si c'était faux on pourrait construire un ultraproduit K et un idéal I de $K[\overline{X}]$ tel que I n'est pas premier mais $IK[\overline{X}]_{int}$ est premier dans $K[\overline{X}]_{int}$. □

Pour démontrer la troisième partie, on a besoin de deux résultats sur les idéaux associés et les modules plats, qu'on ne démontrera pas, mais qui sont démontrés dans [2, Bourbaki]. Un idéal premier $\mathfrak{p}$ d'un anneau R est dit associé à un R-module M s'il existe un $x \in M$ non nul tel que $\mathfrak{p} = \{a \in R | ax = 0\}$. On note $\mathrm{Ass}_R(M)$ l'ensemble des idéaux premiers de R associés à M.

Proposition 5.11. *(1)Soit $A \subseteq B$ deux anneaux, A noethérien. Soient E un A-module, F un B-module tel que quand on voit F comme un A-module grâce à l'inclusion $A \subseteq B$, F soit un A-module plat. On a :*

$$\mathrm{Ass}_B(E \otimes_A F) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_A(E)} \mathrm{Ass}_B(F/\mathfrak{p}F).$$

(2) Soit A un anneau noethérien, I un idéal de A. L'ensemble des idéaux premiers minimaux contenant l'idéal I est $\mathrm{Ass}_A(A/IA)$.

Proposition 5.12. *Soit K un ultraproduit de corps et I un idéal de $K[\overline{X}]$. Alors :*

$$\mathrm{Ass}_{K[\overline{X}]_{int}}(K[\overline{X}]_{int}/IK[\overline{X}]_{int}) = \{\mathfrak{p}K[\overline{X}]_{int} | \mathfrak{p} \in \mathrm{Ass}_{K[\overline{X}]}(K[\overline{X}]/IK[\overline{X}])\}.$$

Démonstration. On applique la proposition 5.11 (1) avec $A = K[\overline{X}]$, $B = F = K[\overline{X}]_{int}$, $E = K[\overline{X}]/IK[\overline{X}]$. Cela montre

$$\mathrm{Ass}_{K[\overline{X}]_{int}}(K[\overline{X}]_{int}/IK[\overline{X}]_{int}) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_{K[\overline{X}]}(K[\overline{X}]/IK[\overline{X}])} \mathrm{Ass}_{K[\overline{X}]_{int}}(K[\overline{X}]_{int}/\mathfrak{p}K[\overline{X}]_{int}).$$

Il reste à voir que

$$\bigcup_{\mathfrak{p} \in \mathrm{Ass}_{K[\overline{X}]}(K[\overline{X}]/IK[\overline{X}])} \mathrm{Ass}_{K[\overline{X}]_{int}}(K[\overline{X}]_{int}/\mathfrak{p}K[\overline{X}]_{int}) = \{\mathfrak{p}K[\overline{X}]_{int} | \mathfrak{p} \in \mathrm{Ass}_{K[\overline{X}]}(K[\overline{X}]/IK[\overline{X}])\}.$$

L'inclusion réciproque est claire si on se souvient que $\mathfrak{p}K[\overline{X}]_{int}) \cap K[\overline{X}] = \mathfrak{p}$ pour un $\mathfrak{p}$ premier. Pour le sens direct, si $\mathfrak{p} \in \mathrm{Ass}_{K[\overline{X}]}(K[\overline{X}]/IK[\overline{X}])$, par la proposition 5.10, $\mathfrak{p}K[\overline{X}]_{int}$ est premier, donc $K[\overline{X}]_{int}/\mathfrak{p}K[\overline{X}]_{int}$ est intègre, donc $\mathrm{Ass}_{K[\overline{X}]}(K[\overline{X}]/IK[\overline{X}]) = \{\mathfrak{p}\}$, ce qui achève la démonstration. □

On peut maintenant prouver la dernière partie du théorème 5.1 :

Théorème. *Il existe une constante $C = C(n, e)$ telle que pour tout corps K, tout idéal I de $K[\overline{X}]$ engendré par des polynômes de degrés inférieurs à e, alors il y a au plus C idéaux minimaux contenant I et chacun est engendré par des polynômes de degrés inférieurs à C.*

Démonstration. C'est encore le même type de raisonnement. Par la proposition 5.11, il s'agit en fait de compter les idéaux premiers associés à un idéal I. On raisonne par l'absurde. Pour tout entier i, il existe alors un corps K_i et un idéal I_i de $K_i[\overline{X}]$ engendré par des polynômes de degrés $\leq e$ tel que :

-(a) soit I_i possède plus de i idéaux premiers associés ;

-(b) soit l'un des idéaux premiers associés à I_i, disons J_i n'est pas engendré par des polynômes de degrés inférieurs à i.

On considère alors K un ultraproduit sur un ultrafiltre $\mathcal{U}$ non principal des K_i. Alors soit l'ensemble des i tels qu'on ait (a) est dans $\mathcal{U}$, soit l'ensemble des i tels qu'on ait (b) est dans $\mathcal{U}$. Si on est dans le cas (a), $\mathrm{Ass}_{K[\overline{X}]_{int}}(K[\overline{X}]_{int}/IK[\overline{X}]_{int})$ est infini, ce qui est absurde par la proposition précédente. Si on est dans le cas (b), on a un idéal dans $\mathrm{Ass}_{K[\overline{X}]_{int}}(K[\overline{X}]_{int}/IK[\overline{X}]_{int})$ qui n'est pas un $\mathfrak{p}K[\overline{X}]_{int}$, ce qui est tout aussi absurde. □

5.3 Formules pour les variétés

Soient K un corps (quelconque), r, n, e des entiers positifs, et $M(n, e)$ l'ensemble des monômes de degré $\leq e$ en les variables $\overline{X} = (X_1, ..., X_n)$. Un idéal de $K[\overline{X}]$ engendré par des polynômes de degrés $\leq e$ est en fait engendré par au plus $\sharp(M(n, e)$ polynômes.

Proposition 5.13. *Soient r, n, e entiers fixés.*

(1) Il existe une formule $\alpha_{n,e,r}(\bar{x}_1, ..., \bar{x}_{r+1})$, où $\bar{x}_i = (x_{im})_{m \in M(n,e)}$, telle que pour tout corps K, si $f_i = \sum_{m \in M(n,e)} a_{im} m \in K[\bar{X}]$, alors

$$f_{r+1} \in (f_1, ..., f_r) \Longleftrightarrow K \models \alpha_{n,e,r}(\bar{a}_1, ..., \bar{a}_{r+1}).$$

(2) Il existe une formule $\beta_{n,e,r}(\bar{x}_1, ..., \bar{x}_r)$, où $\bar{x}_i = (x_{im})_{m \in M(n,e)}$, telle que pour tout corps K, si $f_i = \sum_{m \in M(n,e)} a_{im} m \in K[\bar{X}]$, alors

$$(f_1, ..., f_r) \text{ est premier} \iff K \models \beta_{n,e,r}(\bar{a}_1, ..., \bar{a}_r).$$

Démonstration. (1) On a par le théorème 5.1(1) $f_{r+1} \in (f_1, ..., f_r)$ si et seulement si il existe des polynômes $h_1, ..., h_r$ de degré $\leq A$ tels que $f_{r+1} = f_1 h_1 + ... + f_r h_r$. Les monômes qui apparaissent dans les produits $f_i h_i$ sont de degré $\leq e + A$, et leurs coefficients sont des termes du langage en fonction du uplet des coefficients de f_i et h_i. Il existe donc une formule $\psi(\bar{x}_1, ..., \bar{x}_{r+1}, \bar{y}_1, ..., \bar{y}_r)$, conjonction d'équations telle que pour tout corps K, et uplets $\bar{a}_1, ..., \bar{a}_{r+1}, \bar{b}_1, ..., \bar{b}_r$ de K avec $\bar{a}_i = (a_{im})_{m \in M(n,e)}$ et $\bar{b}_i = (x_{im})_{m \in M(n,A)}$, on a, pour $f_i = \sum_{m \in M(n,e)} a_{im} m$ et $h_i = \sum_{m \in M(n,A)} b_{im} m$,

$$f_{r+1} = f_1 h_1 + ... + f_r h_r \iff K \models \psi(\bar{a}_1, ..., \bar{a}_{r+1}, \bar{b}_1, ..., \bar{b}_r).$$

La formule $\exists (\bar{y}_{im})_{1 \leq i \leq r, m \in M(n,A)} \psi(\bar{x}_1, ..., \bar{x}_{r+1}, \bar{y}_1, ..., \bar{y}_r)$ convient pour $\alpha_{n,e,r}$.

(2) On prend pour $\beta_{n,e,r}$ la traduction en une formule du premier ordre de ceci : pour tout $\bar{y} = (y_m)_{m \in M(n,B)}$, pour tout $\bar{z} = (z_m)_{m \in M(n,B)}$, si $\bar{t} = (t_m)_{m \in M(n,2B)}$ est la suite des coefficients du polynôme $(\sum_{m \in M(n,B)} y_m m)(\sum_{m \in M(n,B)} z_m m)$, alors $\alpha_{n,2D,r}(\bar{x}_1, ..., \bar{x}_r, \bar{t}) \to \alpha_{n,D,r}(\bar{x}_1, ..., \bar{x}_r, \bar{y}) \vee \alpha_{n,D,r}(\bar{x}_1, ..., \bar{x}_r, \bar{z})$.

Le théorème 5.1(2) montre que $\beta_{n,e,r}$ convient. □

Nous touchons enfin au but de cette partie :

Théorème 5.14. *Pour n, e, r entiers fixés, il existe une formule sans quantificateurs qui définit dans tout corps F les coefficients de polynômes $f_1, ..., f_r$ de degré $\leq e$ qui engendrent l'idéal d'une variété.*

Démonstration. Comme la théorie des corps algébriquement clos admet l'élimination des quantificateurs, il existe une formule $\beta_0(\bar{x}_1, ..., \bar{x}_r)$ sans quantificateurs, équivalente à $\beta_{n,e,r}$ modulo ACF.

Soient F un corps, K un corps algébriquement clos contenant F, et $f_1, ..., f_r \in F[\bar{X}]$ de degré $\leq e$. Les f_i s'écrivent $f_i = \sum_{m \in M(n,e)} a_{im} m$. Soit I l'idéal de $K[\bar{X}]$engendré par $f_1, ..., f_r$. Alors

$$I \text{ est premier } \iff K \models \beta_0(\bar{a}_1, ..., \bar{a}_r) \iff F \models \beta_0(\bar{a}_1, ..., \bar{a}_r).$$

On a utilisé l'équivalence de β_0 et $\beta_{n,e,r}$ et le fait que β_0 est sans quantificateurs. □

Voici une dernière proposition qui sera utile lorsque nous définirons une mesure sur les ensembles définissables dans les corps pseudo-finis.

Proposition 5.15. *Soient n, e des entiers. Il existe une constante $D = D(n, e)$ telle que pour tout corps $F \subseteq K = \tilde{K}$, et I idéal de $F[\bar{X}]$ engendré par des polynômes de degrés $\leq e$, le noyau F-absolu (voir remarque 3.6 3) $V(I)^*$ possède moins de C composantes irréductibles, et leurs idéaux associés sont engendrés par des polynômes de degrés $\leq e$.*

De plus, soit tous $f = (f_1, ..., f_r) \in \mathbb{Z}[\bar{X}, \bar{Y}], d, \mu$ entiers, il existe une $\mathcal{L}$-formule $S_{f,d,\mu}(\bar{x})$ qui définit dans tout corps F l'ensemble des $\bar{y} \in F^m$ tels que $V(f(\bar{X}, y))^*$ est de dimension d et possède exactement μ composantes F-irréductibles définies sur F.

Démonstration. En observant la construction de $V(I)^*$, on voit que tant qu'il y a des composantes irréductibles non définies sur F, la suite de la dimension maximale de ces composantes est strictement décroissante. Cela montre donc que la suite s'arrête en moins de n étapes. A chaque étape on ne fait que des intersections finies (il n'y a qu'un nombre fini de composantes irréductibles). On a alors que $V(I)^*$ est une union finie d'intersections finies. A chaque étape, on peut grâce aux points (3) et (4) du théorème 5.1 trouver une borne qui ne dépend que de (n, e) sur le nombre d'idéaux qui interviennent et le degré des polynômes qui les engendrent. Finalement, au bout de n étapes, on a une borne qui ne dépend que de (n, e) sur le nombre de composantes irréductibles de $V(I)^*$ et le degrés des polynômes qui les engendrent.

De plus, on voit qu'on peut trouver une formule $S_{f,d,\mu}(\bar{x})$ en suivant le processus définissant $V(I)^*$. □

Deuxième partie

Théorie des modèles des corps finis et pseudo-finis

6 Les corps pseudo-finis

Nous avons désormais sous la main tous les outils nécessaires pour introduire et étudier l'objet central de cet exposé : la théorie du premier ordre Psf, dont les modèles seront appelés les corps pseudo-finis. Le résultat fondamental, démontré par Ax (voir [1, Ax]) affirme que les corps pseudo-finis sont exactement les modèles infinis de la théorie T_f des corps finis.

6.1 Définitions et premières propriétés

Définition 6.1. Un corps F est *pseudo-fini* s'il vérifie les propriétés suivantes :

P1 F est un corps parfait ;

P2 Pour tout entier $n > 1$, F a exactement une extension algébrique de degré n ;

P3 Toute variété V définie sur F a un point F-rationnel.

Un corps vérifiant la propriété P3 est dit PAC.

Remarque. Les corps algébriquement clos sont PAC, la réciproque n'est pas vraie (car, vu notre définition des variétés, un polynôme de $F[X]$ ne définit une variété que s'il est irréductible dans $\tilde{F}[X]$, c'est-à-dire de degré 1 !). Les corps finis vérifient P1 et P2, mais pas P3 : soit $\mathbb{F}_q$ un corps fini ; considérons la variété $V \subseteq \tilde{\mathbb{F}}_q^{q+2}$ définie par l'équation

$$X_0 \prod_{1 \leq i < j \leq q+1} (X_i - X_j) = 1.$$

V n'a aucun point $\mathbb{F}_q$-rationnel.

La première chose à faire est de s'assurer que la théorie Psf s'exprime au premier ordre. Les axiomes pour P1 sont clairs : on donne les axiomes de la théorie des corps, en ajoutant pour chaque nombre premier p un axiome disant que si la caractéristique est p, tout élément a une racine p-ème. Les axiomes pour P3 se déduisent de 5.14. En effet, on a vu que pour tout triplet (n, r, m) d'entiers, on peut exprimer au premier ordre :

Pour tout $f_1(\bar{X}), \ldots, f_m(\bar{X}) \in F[\bar{X}]$ de degré $\leq e$, où $\bar{X} = (X_1, \ldots, X_n)$, si "l'idéal engendré par $f_1(\bar{X}), \ldots, f_m(\bar{X}) \in F[\bar{X}]$ est premier", alors $\exists \bar{x}, f_1(\bar{x}) = \cdots = f_m(\bar{x}) = 0$.

Pour la propriété P2, fixons un entier $n > 1$. Il existe une formule $Irr(\bar{x})$ ($\bar{x} = (x_1, \ldots, x_n)$), qui dans tout corps F définit les n-uplets $\bar{a}$ tels que le polynôme $X^n + a_1 X^{n-1} + \cdots + a_n$ soit irréductible dans F (utiliser le fait que si $f(X) = g(X)h(X)$, les degrés de g et h sont bornés par n). Or, à toute formule $\theta(\bar{y})$ ($\bar{y} = (y_1, \ldots, y_m)$), on peut associer une formule $\theta^*(\bar{x}, \bar{y})$ ($\bar{x} = (x_1, \ldots, x_n)$), telle que, pour tout corps F, tout n-uplet $\bar{a}$ de F, si le polynôme $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$ est irréductible sur F et $\bar{b} \in F^m$, alors

$$F(X/(f(X))) \vDash \theta(\bar{b}) \iff F \vDash \theta^*(\bar{a}, \bar{b}).$$

(En effet, il suffit pour cela de savoir interpréter dans F un corps isomorphe à $F(\alpha)$, où α est une racine de f dans une extension de F : pour cela, on voit $F(\alpha)$ comme un F-espace vectoriel de base $(1, \alpha, \ldots, \alpha^{n-1})$; l'addition se définit coordonnée par coordonnée et la multiplication via la matrice compagnon de f, et se définit donc uniformément en les paramères de f).

Soit alors

$$\theta(\bar{y}) = \exists z_1, \ldots, z_n(\wedge_{i=1}^n z_i^n + y_1 z_i^{n-1} + \cdots + y_n = 0 \wedge \forall x(x^n + y_1 x^{n-1} + \cdots + y_n = 0 \to \vee_{i=1}^n x = z_i)),$$

où $\bar{y} = (y_1, \ldots, y_n)$ et considérons l'énoncé suivant, avec $\bar{x}$ et $\bar{y}$ comme ci-dessus :

$$\exists \bar{x}, Irr(\bar{x}) \wedge \forall \bar{y} Irr(\bar{y}) \to \theta^*(\bar{x}, \bar{y}).$$

Cet énoncé traduit au premier ordre le fait que F a une extension de degré n et que tout polynôme irréductible sur F s'y scinde. Un tel corps F a donc exactement une extension de degré n. Ceci achève la vérification.

Rappelons le résultat cité en tête de cette section : les corps pseudo-finis sont exactement les modèles infinis de la théorie T_f des corps finis. Nous démontrons ici que les modèles infinis de la théorie des corps finis sont effectivement des corps pseudo-finis. La preuve de ce résultat fait appel au théorème suivant :

Théorème 6.2 (Lang-Weil)**.** *Soient m, n, e des entiers positifs. Il existe une constante positive C ne dépendant que du triplet (m, n, e), telle que pour tout corps fini $F = \mathbb{F}_q$, pour tous polynômes $f_1(\bar{Y}), \ldots, f_m(\bar{Y}) \in F[\bar{Y}]$ (avec $\bar{Y} = (Y_1, \ldots, Y_n)$) de degré $\leq e$, si les polynômes $f_1(\bar{Y}), \ldots, f_m(\bar{Y})$ engendrent l'idéal d'une variété V de dimension d,*

$$|\sharp(V \cap F^n) - q^d| < Cq^{d-1/2}.$$

Démonstration. Voir l'annexe 1. La preuve de ce théorème est au-delà du niveau de cet exposé. C'est une conséquence presque immédiate des conjectures de Weil, dont la démonstration (en toute généralité) nécessite le recours à des théories géométriques et cohomologiques sophistiquées. Cela dit, dans le cas des estimées de Lang-Weil, c'est le cas $d = 1$ qui est difficile ; le cas $d > 1$ s'en déduit par une récurrence que nous indiquons en annexe par souci de complétude. On renvoit à l'excellent texte [20, Raskin] pour une démonstration de l'hypothèse de Riemann dans le cas des courbes, qui ne fait pas appel au formalisme de la cohomologie étale (seulement à la théorie de l'intersection, telle qu'exposée par exemple dans [14, Hartshorne]). □

Notons en particulier qu'avec les notations du théorème, si $q > C^2$, alors l'encadrement obtenu assure que $V \cap F^n$ est non vide. Le résultat cherché est alors immédiat :

Théorème 6.3 (Ax)**.** *Les modèles infinis de la théorie T_f des corps finis sont des corps pseudo-finis.*

Démonstration. On a déjà signalé que les corps finis satisfont P1 et P2, et donc aussi tout modèle (infini) de la théorie des corps finis. Quant à P3, le théorème de Lang-Weil implique (avec les mêmes notations) que, pour tout corps fini F, si les polynômes $f_1(\bar{Y}), \ldots, f_m(\bar{Y})$ engendrent l'idéal d'une variété, et si F a au moins $C^2 + 1$ éléments, il existe $\bar{x}$ un uplet de F tel que $f_1(\bar{x}) = \cdots = f_m(\bar{x}) = 0$. En particulier un modèle infini de T_f est PAC. □

6.2 Exemples de corps pseudo-finis

Il est temps de donner des exemples. Cette section en développe quelques-uns. On se rend assez vite compte qu'il est difficile d'exhiber des exemples "naturels" de corps pseudo-finis... Toutefois, nous donnons en fin de paragraphe un résultat qui montre qu'il en existe relativement beaucoup !

(1) L'exemple le plus immédiat (pour le logicien) de corps pseudo-fini consiste évidemment à se donner un ultrafiltre $\mathcal{F}$ non principal sur l'ensemble des puissances de nombres premiers, et à considérer $F = \Pi_q \mathbb{F}_q/\mathcal{F}$. C'est en vertu du théorème de Loś rappelé en introduction un modèle infini de la théorie des corps finis, donc un corps pseudo-fini !

(2) Voici un exemple de corps pseudo-fini algébrique sur le corps premier $\mathbb{F}_p$. On choisit une fonction f définie sur l'ensemble des nombres premiers et à valeurs dans $\mathbb{N}$, et telle que $f(l) > 0$ pour une infinité de nombres premiers l. Soit F le corps engendré par tous les $\mathbb{F}_{p^{lf(l)}}$, quand l décrit l'ensemble des nombres premiers. F est infini et contenu dans $\tilde{\mathbb{F}}_p$, donc vérifie P3. Comme tout corps fini est parfait, tout sous-corps de $\tilde{\mathbb{F}}_p$ est parfait, et donc F vérifie P1. Il nous reste donc à vérifier que F a exactement une extension algébrique de degré n pour tout n. Si (l_m) désigne la suite des nombres premiers rangés par ordre croissant, on notera F_m le corps engendré par les $\mathbb{F}_{p^{lf(l)}}$, pour l premier, $l \leq l_m$. Soit $n \in \mathbb{N}$ et choisissons m suffisamment grand pour que tout nombre premier supérieur ou égal à l_m est premier avec n, et E l'extension de F_m de degré n. On a $[EF_{m'} : F_{m'}] = n$ pour tout $m' \leq m$, car n divise $[EF_{m'} : F_{m'}][F_{m'} : F_m] = [EF_{m'} : F_m]$ et est premier avec $[F_{m'} : F_m]$. F a donc une extension de degré n, à savoir EF. S'il en avait deux, elles donneraient deux extensions distinctes de même degré d'un corps fini, ce qui est impossible. En termes de groupes de Galois, la construction précédente revient à déterminer un sous-groupe de $\hat{\mathbb{Z}}$ d'indice infini et isomorphe à $\hat{\mathbb{Z}}$.

(3) Nous montrons ici que les corps pseudo-finis abondent.

Soit K un corps. Le groupe topologique $\mathrm{Gal}(K)$ est compact, donc munie d'une mesure de Haar finie, invariante à gauche et à droite. On la normalise pour en faire une mesure de probabilité, notée μ. Jarden a obtenu les résultats suivants. Pour la démonstration (et la définition d'un corps hilbertien), on renvoie à [7, Fried-Jarden].

Proposition 6.4. *Soit K un corps hilbertien, e un entier positif. Alors $\langle \sigma_1, \ldots, \sigma_e \rangle \simeq \hat{F}_e$, pour presque tout $\bar{\sigma} \in \mathrm{Gal}(K)^e$.*

Proposition 6.5. *Soit K un corps dénombrable hilbertien, e un entier positif. Alors $K_s(\bar{\sigma})$ (corps fixé par $\bar{\sigma}$) est un corps PAC pour presque tout $\bar{\sigma} \in \mathrm{Gal}(K)^e$.*

En combinant les théorèmes précédents, on obtient en particulier :

Théorème 6.6. *Soit K un corps dénombrable hilbertien de caractéristique nulle (par exemple : $K = \mathbb{Q}$). Alors $K(\sigma)$ est un corps pseudo-fini pour presque tout $\sigma \in \mathrm{Gal}(K)$.*

7 Equivalence élémentaire pour les corps pseudo-finis

Cette section est la plus technique de cette première partie de l'exposé. L'objectif est le théorème 7.5. La preuve est longue et relativement abstraite, mais, une fois le résultat en main, nous pourrons en déduire de nombreux corollaires.

Lemme 7.1. *Soit K un corps parfait.*

- *Supposons que K a au plus une extension de degré n pour tout entier n. Alors toutes les extensions finies de K sont galoisiennes, de groupe de Galois cyclique.*
- *Les conditions suivantes s'équivalent :*
  (i) *Pour tout entier n, K a exactement une extension de degré n ;*
  (ii) $\mathrm{Gal}(\tilde{K}/K) = \hat{\mathbb{Z}}$.

Démonstration. Soit E une extension galoisienne finie de K. On va montrer que E/K est une extension cyclique. Comme tous les sous-groupes de $\mathrm{Gal}(E/K)$ sont alors distingués, cela entraînera que toutes les extensions finies de K contenues dans E sont galoisiennes cycliques. Comme toute extension finie de K est contenue dans une extension galoisienne (K est parfait), cela donnera le premier point.

On est en fait ramené à montrer que si G est un groupe fini, tel que pour tout diviseur m de $|G|$, il existe au plus un sous-groupe de G d'ordre m, alors G est cyclique. On le fait par récurrence sur l'ordre n de G. Si n est premier, c'est clair. L'hypothèse assure que tous les sous-groupes de G sont distingués. Soit p premier divisant n, $a \in G$ d'ordre p (lemme de Cauchy). L'hypothèse de récurrence implique que $G/\langle a\rangle$ est cyclique, engendré par un certain élément b. Comme a est d'ordre premier, soit $\langle a\rangle \subseteq \langle b\rangle$, soit $\langle a\rangle \cap \langle b\rangle = \{1\}$. Comme ces sous-groupes sont distingués, cela donne $a^{-1}b^{-1}ab = 1$. Donc $G = \langle a\rangle \times \langle b\rangle$. G n'ayant qu'un seul sous-groupe d'ordre p, p ne divise pas l'ordre de $\langle b\rangle$, donc G est cyclique.

Montrons le second point. On suppose (i). Soit L une extension galoisienne finie de K de degré n. Le groupe $\mathrm{Gal}(L/K)$ est cyclique par ce qui précède. De plus, pour tout n, K a une extension de degré n. Cela entraîne (par définition) $\mathrm{Gal}(\tilde{K}/K) = \hat{\mathbb{Z}}$. Réciproquement, supposons (ii). Les extensions de K de degré n correspondent, par la correspondance de Galois, aux sous-groupes H fermés de $\hat{\mathbb{Z}}$ d'indice n. Un sous-groupe H fermé d'indice fini est aussi ouvert. Il contient donc un groupe isomorphe à $m!\mathbb{Z}$ pour m suffisamment grand. En quotientant par ce sous-groupe, on voit que $H/m!\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}/m!\mathbb{Z}$ d'indice n, ce qui laisse une seule possibilité. Le sous-groupe H est donc uniquement déterminé (c'est l'ensemble des éléments de la forme $(a_m)_m$, avec pour tout m, a_m divisible par n dans $\mathbb{Z}/m\mathbb{Z}$). □

Lemme 7.2. *On suppose que K est un corps ayant pour tout entier n exactement une extension de degré n. On suppose que E est une extension de K, telle que K est algébriquement clos dans E. Si σ est un générateur topologique de $\mathrm{Gal}(\tilde{K}/K)$, et τ un prolongement de σ à $\tilde{E}$, fixant un sous-corps M de E, alors τ est un générateur topologique de $\mathrm{Gal}(\tilde{E}/M)$. Réciproquement, si τ est un générateur topologique de $\mathrm{Gal}(\tilde{L}/L)$, sa restriction σ à $\tilde{K}$ est un générateur topologique de $\mathrm{Gal}(\tilde{K}/K)$.*

Démonstration. Dans les deux cas, remarquons que comme τ prolonge σ, $\tilde{K} \cap M = K$ (avec la convention $M = K$ dans le second cas). Donc, si K_n est l'extension de degré n de K, $n = [K_n : K] = [K_nM : M]$. Donc M a au moins une extension de degré n, et au plus une car c'est le corps fixé par τ. Donc la restriction $\mathrm{Gal}(\tilde{E}/M) \to \mathrm{Gal}(\tilde{K}/K)$ est (dans les deux cas) un isomorphisme, ce qui donne le résultat. □

Lemme 7.3. *Soit F un corps parfait PAC, contenu dans un corps K, $\bar{a}$ un uplet de K, A un sous-ensemble dénombrable de K. Si F est relativement algébriquement clos dans $F(\bar{a})$, il existe un F-morphisme : $F[\bar{a}] \to F$. Si F est relativement algébriquement clos dans $F(A)$ et $\aleph_1$-saturé, il existe un F-morphisme : $F[A] \to F$.*

Démonstration. Montrons la première assertion. Considérons l'idéal $I(\bar{a}/F)$. Comme F est parfait et relativement algébriquement clos dans $F(\bar{a})$, $F(\bar{a})$ et $\tilde{F}$ sont linéairement disjoints au-dessus de F. Par 3.15, $I(\bar{a}/F)$ engendre l'idéal d'une variété V. Comme F est PAC, $V(F)$ contient un point $\bar{b}$, d'où l'existence d'un morphisme $F[\bar{a}] \to F$ envoyant $\bar{a}$ sur $\bar{b}$ (puisque $\bar{a}$ est un point générique de V).

Passons à la seconde assertion. Notons $A = \{a_i, i \in \mathbb{N}\}$. Se donner un F-morphisme $F[A] \to F$ revient a trouver une réalisation d'un certain type sur F (en les variables $(x_i)_{i\in\mathbb{N}}$). En effet, si $I = I(A/F)$ est l'idéal de A dans $F[X_1, X_2, ...]$, et $B = (b_1, b_2, ...)$ un uplet de longueur ω (dans une extension de F), il faut et il suffit que $I(B/F)$ contienne I pour que $a_i \to b_i$ définisse un F-morphisme. Ainsi, comme on cherche un morphisme à valeurs dans F, il faut et il suffit que l'uplet B en question soit un zéro de I, autrement dit un zéro commun d'un ensemble de générateurs de I. Or, comme A est dénombrable, il existe un sous-corps dénombrabale F_0 de F tel que $I(A/F_0)$ engendre I. Donc I possède une famille dénombrable de générateurs, et le type en question est finiment satisfiable dans F par la premiere partie du lemme (autrement dit : il est consistant). Par $\aleph_1$-saturation, on peut realiser toutes les conditions à la fois. □

Soient $K \subseteq E$ des corps parfaits, $\tilde{F}$ un corps algébriquement clos qui contient K, et supposons donné un $\tilde{K}$-isomorphisme $\psi : \tilde{E} \to \tilde{F}$. Soit $F = \psi(E)$. Alors l'application $\Psi : \mathrm{Gal}(\tilde{E}/E) \to \mathrm{Gal}(\tilde{F}/F)$ définie par : $\Psi(\sigma) = \psi \circ \sigma \circ \psi^{-1}$, est un isomorphisme, vérifiant $\Psi(\sigma)(a) = \sigma(a)$ pour tous $a \in \tilde{K}$ et $\sigma \in \mathrm{Gal}(\tilde{E}/E)$.

Lemme 7.4. *Soit K un sous-corps des corps E et F. On suppose K, E et F parfaits, K relativement algébriquement clos dans E et F, E dénombrable, et F pseudo-fini $\aleph_1$-saturé. On suppose de plus qu'existe un isomorphisme continu $\Phi : \mathrm{Gal}(\tilde{F}/F) \to \mathrm{Gal}(\tilde{E}/E) \simeq \widehat{\mathbb{Z}}$, tel que $\Phi(\sigma)(a) = \sigma(a)$ pour tous $\bar{a} \in \tilde{K}$ et $\sigma \in \mathrm{Gal}(\tilde{F}/F)$. Alors il existe un plongement $\varphi : \tilde{E} \to \tilde{F}$ qui est l'identité sur $\tilde{K}$, et satisfait, pour tout $a \in \tilde{E}$, pour tout $\sigma \in \mathrm{Gal}(\tilde{F}/F)$,*

$$\varphi(\Phi(\sigma)(a)) = \sigma(\varphi(a)).$$

En outre, F est une extension régulière de $\varphi(E)$.

Démonstration. Montrons tout d'abord que l'on peut supposer $\tilde{E}$ et $\tilde{F}$ linéairement disjoints au-dessus de $\tilde{K}$. Soit $(t_i)_{i\in I}$ une base de transcendance de E sur K et choisissons des éléments $(u_i)_{i\in I}$ algébriquement indépendants au-dessus de F, dans un grand corps algébriquement clos contenant tous les corps considérés. L'application qui envoie t_i sur u_i pour $i \in I$ se prolonge en un $\tilde{K}$-isomorphisme ψ de $\tilde{E}$ sur la clôture algébrique de $\tilde{K}(u_i)_{i\in I}$. On note $E' = \psi(E)$. Comme $\tilde{E}'$ et $\tilde{F}$ sont algébriquement indépendants au-dessus de $\tilde{K}$, ils sont linéairement disjoints au-dessus de $\tilde{K}$ par 3.19. De plus, en utilisant l'isomorphisme donné par la remarque précédant le lemme, on voit que l'on peut se ramener à traiter le problème pour F et E'. En d'autres termes, on peut donc bien supposer $\tilde{E}$ et $\tilde{F}$ linéairement disjoints au-dessus de $\tilde{K}$.

Cela entraîne que le corps $\tilde{E}\tilde{F}$ est isomorphe au corps des fractions de $\tilde{E} \otimes_{\tilde{K}} \tilde{F}$. Soit σ_0 un générateur topologique de $\mathrm{Gal}(\tilde{F}/F)$, et définissons $\tau_0 \in \mathrm{Gal}(\tilde{E}\tilde{F}/EF)$ ainsi :

$$\tau_0(a \otimes b) = \Phi(\sigma_0)(a) \otimes \sigma_0(b),$$

pour $a \in E$, $b \in F$. On note que τ_0 prolonge σ_0 et $\Phi(\sigma_0)$; en outre, comme l'action de ces deux éléments sur $\tilde{K}$ est la même, et comme $\tilde{E}$ et $\tilde{F}$ sont linéairement disjoints sur $\tilde{K}$, τ_0 est bien défini. On prolonge τ_0 en un élément de $\mathrm{Gal}(\tilde{EF}/EF)$ et on note M le sous-corps de $\tilde{EF}$ fixé

par τ_0. Comme σ_0 et $\Phi(\sigma_0)$ engendrent topologiquement $\mathrm{Gal}(\tilde{F}/F)$ et $\mathrm{Gal}(\tilde{E}/E)$, E et F sont relativement algébriquement clos dans M. Enfin, $\tilde{M} = E\tilde{F} = \tilde{E}M = \tilde{F}M$.

Comme $\tilde{M}$ est algébrique sur M, le corps $\tilde{F}M$ est égal à $M[\tilde{F}]$. Tout $a \in \tilde{E}$ s'écrit donc $\Sigma_{i\in I(a)}\ b_{a,i}y_{a,i}$, avec $b_{a,i} \in M$, $y_{a,i} \in \tilde{F}$. L'ensemble $M_0 := E \cup \{b_{a,i}, a \in \tilde{E}, i \in I(a)\}$ est dénombrable, et $\tilde{E} \subseteq \tilde{F}[M_0]$.

Comme $\tilde{F}[M_0] \subseteq M$, F est relativement algébriquement clos dans $\tilde{F}[M_0]$. Comme F est $\aleph_1$-saturé, il existe d'après le lemme 7.3 un F-morphisme $\varphi_0 : F[M_0] \to F$, prolongeable en un $\tilde{F}$-morphisme $\varphi : \tilde{F}[M_0] \to \tilde{F}$ car $I(M_0/\tilde{F})$ est engendré par $I(M_0/F)$. La restriction de φ à $\tilde{E}$ est un $\tilde{K}$-isomorphisme sur son image : c'est un $\tilde{K}$-morphisme car $\tilde{K} \subseteq \tilde{F}$. Son noyau est un idéal propre de $\tilde{E}$, c'est-à-dire (0).

Soit $a \in \tilde{E}$. On calcule

$$\varphi(a) = \sum_{i\in I(a)} \varphi(b_{a,i})y_{a,i} \quad ; \quad \tau(\varphi(a)) = \sigma_0(\varphi(a)) = \sum_{i\in I(a)} \varphi(b_{a,i})\sigma_0(y_{a,i}),$$

car τ est l'identité sur $\varphi(M_0) \subseteq F$. On a aussi

$$\Phi(\sigma_0)(a) = \tau(a) = \sigma_0(\varphi(a)) = \sum_{i\in I(a)} b_{a,i}\sigma_0(y_{a,i}).$$

Donc

$$\varphi(\Phi(\sigma_0)(a)) = \sigma_0(\varphi(a)),$$

car φ est un $\tilde{F}$-morphisme. Cette relation reste valable en remplaçant σ_0 par un élément quelconque σ de $\mathrm{Gal}(\tilde{F}/F)$. En effet soient $a \in \tilde{E}$, $\sigma \in \mathrm{Gal}(\tilde{F}/F)$. Alors a est dans une extension finie L de E, donc $\Phi(\sigma)|_L = \Phi(\sigma_0)^m|_L$, pour un certain entier m, puisque σ_0 est un générateur topologique de $\mathrm{Gal}(\tilde{F}/F)$. La relation voulue s'en déduit immédiatement.

Il reste à vérifier que $\varphi(E)$ est algébriquement clos dans F (puisqu'on sait déjà que $\varphi(E) \subseteq F$), i.e. que $\varphi(\tilde{E}) \cap F = \varphi(E)$. Or, pour $a \in \tilde{E}$ l'on a $\varphi(a) \in F$ ssi $\sigma_0(\varphi(a)) = \varphi(a)$ (car σ_0 est un générateur topologique de $\mathrm{Gal}(\tilde{F}/F)$) ssi $\varphi(\Phi(\sigma_0)(a)) = \varphi(a)$ (d'après les calculs précédents) ssi $\Phi(\sigma_0)(a) = a$ (car φ est un plongement) ssi $a \in E$ (car σ_0 est un générateur topologique de $\mathrm{Gal}(\tilde{F}/F)$). □

Le résultat s'étend bien sûr au cas où E et F n'ont pas de sous-corps commun K, mais contiennent des corps notés respectivement K_1 et K_2, isomorphes via φ_0 satisfaisant : pour tout $a \in K_1$, pour tout $\sigma \in \mathrm{Gal}(\tilde{F}/F)$, $\varphi_0(\Phi(\sigma)(a)) = \sigma(\varphi_0(a))$.

Théorème 7.5. *Soient E et F des corps pseudo-finis, K un sous-corps. Alors*

$$E \equiv_K F \iff E \cap \tilde{K} \simeq_K F \cap \tilde{K}.$$

Démonstration. Supposons $E \equiv_K F$. On sait alors que, pour tout $f(X) \in K[X]$,

$$E \vDash \exists x f(x) = 0 \iff F \vDash \exists x f(x) = 0.$$

Soit L une extension normale finie de K, et $S_L = \{\sigma \in \mathrm{Aut}(\tilde{K}/K), \sigma(L \cap E) = L \cap F\}$. L'ensemble S_L est réunion finie de cosets du sous-groupe $\mathrm{Aut}(\tilde{K}/L)$ et est donc fermé. Supposons dans un premier temps L séparable sur K, et soit α tel que $L \cap E = K(\alpha)$. Soit $f(X)$ le polynôme minimal de α sur K, et $\beta \in F$ une racine de f (qui existe par hypothèse). On a aussi $\beta \in L$ car l'extension est L de K est normale. On a alors : $[E \cap L : k] = [K(\beta) : K] \leq [F \cap L : K]$, et par

symétrie ces degrés sont égaux. Si $\sigma \in \mathrm{Gal}(L/K)$ est tel que $\sigma(\alpha) = \beta$, $\sigma(L \cap E) = L(\beta) = L \cap F$ et donc $\sigma \in S_L$. Donc S_L est non vide.

Supposons maintenant L non séparable. K n'est alors pas parfait et donc infini. Soient $L_1, \ldots, L_n$ les images par les éléments de $\mathrm{Aut}(L/K)$ du corps $L \cap F$. Soit $a \in L \cap E$. Par hypothèse, il existe $b \in L \cap F$ de même polynôme minimal que a sur K. Il existe donc $\sigma \in \mathrm{Aut}(L/K)$ envoyant a sur b. Ainsi $L \cap E \subseteq L_1 \cup \cdots \cup L_n$. Un fait classique d'algèbre linéaire assure l'existence de i tel que $L \cap E \subseteq L_i$, car K est infini. On conclut alors comme dans le cas précédent que S_L est non vide.

Ainsi, S_L est non vide pour toute extension galoisienne finie de K. On a vu que cet ensemble est aussi fermé. Si $L_1, \ldots, L_m$ sont des extensions galoisiennes finies de K, et $M = L_1 \ldots L_m$, alors $S_M \subseteq S_{L_1} \cap \cdots \cap S_{L_m}$. Par compacité de $\mathrm{Gal}(\tilde{K}/K)$, l'intersection des fermés S_L est non vide, et donc : $E \cap \tilde{K} \simeq_K F \cap \tilde{K}$.

Montrons l'autre implication. On peut bien sûr supposer K relativement algébriquement clos dans E et F. En appliquant le théorème de Löwenheim-Skolem au triplet (E, F, K), on se ramène au cas où ces corps sont tous dénombrables. Passant à des extensions élémentaires, on peut ensuite supposer E et F $\aleph_1$-saturés (cf. la proposition 1.8). Il nous reste alors à construire l'isomorphisme Φ entre les groupes de Galois pour pouvoir appliquer le lemme de plongement.

Soit σ_1 un générateur topologique de $\mathrm{Gal}(\tilde{E}/E)$, σ_0 sa restriction à $\tilde{K}$. Par 7.2, σ_0 est un générateur topologique de $\mathrm{Gal}(\tilde{K}/K)$. On cherche à le prolonger en un générateur topologique σ_2 de $\mathrm{Gal}(\tilde{F}/F)$. Pour chaque extension galoisienne finie L de F, soit S_L l'ensemble des éléments de $\mathrm{Gal}(\tilde{F}/F)$ dont la restriction à L engendre $\mathrm{Gal}(L/F)$ et qui prolonge σ_0 sur $\tilde{K} \cap L$. Par définition S_L est une réunion de cosets de $\mathrm{Gal}(\tilde{F}/L)$ donc fermé. Montrons qu'il est non vide. Les groupes $\mathrm{Gal}(L/F)$ et $\mathrm{Gal}(\tilde{K} \cap L/K)$ sont cycliques, et l'application restriction est un morphisme surjectif. Il suffit alors de vérifier qu'étant donné un morphisme surjectif entre groupes cycliques finis, tout générateur du groupe à l'arrivée se relève par ce morphisme en un générateur du groupe de départ : ce petit exercice de théorie des groupes est laissé au lecteur.

Chaque S_L est donc un fermé non vide de $\mathrm{Gal}(\tilde{F}/F)$. Si $L_1, \ldots, L_m$ sont des extensions galoisiennes finies de F, et $M = L_1 \ldots L_m$, $S_M \subseteq S_{L_1} \cap \cdots \cap S_{L_m}$. On conclut en utilisant la compacité de $\mathrm{Gal}(\tilde{F}/F)$ et 7.2, à l'existence d'un générateur topologique σ_2 de $\mathrm{Gal}(\tilde{F}/F)$ prolongeant σ_0.

Ainsi, comme $\mathrm{Gal}(\tilde{E}/E)$ et $\mathrm{Gal}(\tilde{F}/F)$ sont isomorphes à $\hat{\mathbb{Z}}$, l'application $\sigma_1 \to \sigma_2$ se prolonge de manière unique en un isomorphisme $\Phi : \mathrm{Gal}(\tilde{E}/E) \to \mathrm{Gal}(\tilde{F}/F)$, qui satisfait $\Phi(\sigma(a)) = \sigma(a)$ pour tous $a \in \tilde{K}$, $\sigma \in \mathrm{Gal}(\tilde{E}/E)$. Soit E_0 une sous-structure élémentaire dénombrable de E contenant K (dont on a vu qu'on pouvait le supposer dénombrable). Alors E_0 est relativement algébriquement clos dans E, et $\tilde{E}_0 E = \tilde{E}$, car E_0 a exactement une extension de degré n pour tout n. Donc le morphisme de restriction $\mathrm{Gal}(\tilde{E}/E) \to \mathrm{Gal}(\tilde{E}_0/E_0)$ est un isomorphisme, et on dispose donc d'un isomorphisme $\Phi_0 : \mathrm{Gal}(\tilde{E}_0/E_0) \to \mathrm{Gal}(\tilde{F}/F)$. On est maintenant exactement en mesure d'appliquer le lemme 7.4, puisque E_0 est dénombrable et F $\aleph_1$-saturé. Il existe un $\tilde{K}$-isomorphisme $\varphi_0 : \tilde{E}_0 \to \tilde{F}$, avec $\varphi_0(E_0) \subseteq F$, F extension régulière de $\varphi_0(E_0)$ et, pour tous $a \in E_0$ et $\sigma \in \mathrm{Gal}(\tilde{F}/F)$, $\varphi_0(\Phi_0^{-1}(\sigma)(a)) = \sigma(\varphi_0(a))$.

Soit F_0 une sous-structure élémentaire de F contenant $\varphi_0(E_0)$. On a un isomorphisme $\Psi_0 : \mathrm{Gal}(\tilde{E}/E) \to \mathrm{Gal}(\tilde{F}_0/F_0)$. Toujours par 7.4, on peut donc trouver un $\tilde{K}$-isomorphisme $\psi_0 : \tilde{F}_0 \to \tilde{E}$, prologeant φ_0^{-1}, avec $\psi_0(F_0) \subseteq E$, E extension régulière de $\psi_0(F_0)$ et, pour tous $a \in F_0$ et $\sigma \in \mathrm{Gal}(\tilde{E}/E)$, $\psi_0(\Psi_0^{-1}(\sigma)(a)) = \sigma(\psi_0(a))$.

Répétant le procédé, on construit deux familles d'isomorphismes partiels φ_i et ψ_i, satisfaisant

– Le domaine de φ_i est la clôture algébrique d'une sous-structure élémentaire E_i de E contenant $\psi_{i-1}(F_{i-1})$.
– Le domaine de ψ_i est la clôture algébrique d'une sous-structure élémentaire F_i de F contenant $\psi_i(F_i)$.
– φ_i prolonge ψ_{i-1}^{-1} et ψ_i prolonge φ_i^{-1}.
– les φ_i et ψ_i se comportent comme vu plus haut ... !

Soient $E_\omega = \cup_{i\in\mathbb{N}} E_i$, $F_\omega = \cup_{i\in\mathbb{N}} F_i$. Alors $E_\omega \prec E$ et $F_\omega \prec F$. De plus l'application $\varphi_\omega = \cup_{i\in\mathbb{N}}\varphi_i$ définit un isomorphisme de $\tilde{E}_\omega$ sur $\tilde{F}_\omega$, d'inverse $\psi_\omega = \cup_{i\in\mathbb{N}}\psi_i$. Donc $\varphi_\omega(E_\omega) = F_\omega$ et donc $E \equiv_K F$. □

Nous pouvons maintenant récolter les fruits de notre travail. Comme corollaire immédiat du théorème et de 1.11, nous obtenons déjà :

Corollaire 7.6. *Soient E et F des corps pseudo-finis de même caractéristique, k leur sous-corps premier.*

$$E \equiv F \iff E \cap \tilde{k} \simeq F \cap \tilde{k}$$

La théorie Psf $\cup\{\exists x f(x) = 0, f(x) \in \mathbb{Z}[X], E \vDash \exists x f(x) = 0\} \cup \{\forall x f(x) \neq 0, f(x) \in \mathbb{Z}[X], E \vDash \forall x f(x) \neq 0\}$ *est complète. De plus si φ est un énoncé du langage des anneaux, il existe un énoncé ψ, combinaison booléenne d'énoncés de la forme $\exists x f(x) = 0$, où $f(x) \in \mathbb{Z}[X]$, tel que*

$$\text{Psf} \vdash (\varphi \leftrightarrow \psi).$$

En appliquant le théorème 7.5 à $K = E$, on obtient aussi :

Corollaire 7.7. *Soient $E \subseteq F$ des corps pseudo-finis. Alors*

$$E \prec F \iff \tilde{E} \cap F \simeq E.$$

Pour chaque $n \in \mathbb{N}$, $n > 1$, donnons-nous des nouveaux symboles de constantes $c_{i,n}$, $i = 1, \ldots, n$. Soit $\mathcal{L}_c$ le langage $\mathcal{L} \cup \{c_{i,n}, n > 1, i = 1, \ldots, n\}$ ($\mathcal{L}$ désignant le langage des anneaux), et soit Psf_c la théorie obtenue en ajoutant à Psf, pour tout $n > 1$, l'énoncé exprimant que le polynôme $x^n + c_{1,n}x^{n-1} + \cdots + c_{n,n}$ est irréductible.

Proposition 7.8. *La théorie* Psf_c *est modèle complète.*

Démonstration. Soient $(E, \bar{c}) \subseteq (F, \bar{c})$ deux modèles de Psf_c. E est relativement algébriquement clos dans F puisque pour chaque n le polynôme définissant l'extension de E de degré n reste irréductible sur F. On applique le théorème précédent pour conclure. □

Proposition 7.9. *Soit $\varphi(\bar{x})$, $\bar{x} = (x_1, \ldots, x_n)$, une formule existentielle du langage des corps. Alors il existe une formule $\psi(\bar{x})$, conjonction de formules de la forme $\exists t f(\bar{x}, t) = 0$, où $f(\bar{X}, T) \in \mathbb{Z}[\bar{X}, T]$, qui est équivalente à $\varphi(\bar{x})$ modulo la théorie des corps parfaits PAC.*

Démonstration. On peut supposer $\varphi(\bar{x})$ positive (toute formule $g(\bar{x}) \neq 0$ est équivalente modulo la théorie des corps à $\exists t g(\bar{x}, t) - 1 = 0$). On se réduit donc à une formule $\varphi(\bar{x})$ du type

$$\exists \bar{y}\theta(\bar{x}, \bar{y}),$$

avec $\bar{y} = (y_1, \ldots, y_m)$ et $\theta(\bar{x}, \bar{y})$ conjonction d'équations.

Soit Δ l'ensemble des disjonctions finies de formules de la forme $\exists t f(\bar{x}, t) = 0$, où $f(\bar{X}, T) \in \mathbb{Z}[\bar{X}, T]$. Soient F_1, F_2 deux corps PAC parfaits, $\bar{\in} F_1^n$, $\bar{b} \in F_2^n$. Supposons que $F_1 \vDash \exists \bar{y}\theta(\bar{a}, \bar{y})$,

et que $\bar{b}$ satisfait toutes les formules de Δ satisfaites par $\bar{a}$ dans F_1. On en déduit que F_1 et F_2 ont même caractéristique, et que si k est leur sous-corps premier, $k(\bar{a})$ et $k(\bar{b})$ sont isomorphes. Soit K un grand corps algébriquement clos contenant F_1 et F_2. Soit $\bar{c} \in F_1^m$ tel que $F_1 \models \theta(\bar{a}, \bar{c})$, et considérons le corps $k(\bar{a}, \bar{c}) \cap k(\bar{a})_s$. C'est une extension séparable finie de $k(\bar{a})$, donc de la forme $k(\bar{a}, \alpha)$, pour un α séparable sur $k(\bar{a})$. En outre, l'ensemble algébrique V des zéros dans K^m de $I(\bar{c}/k(\bar{a}, \alpha))$ est une variété d'après 3.15, définie sur la clôture parfaite de $k(\bar{a}, \alpha)$.

Soit $p(\bar{X}, T) \in \mathbb{Z}[\bar{X}, T]$ tel que $p(\bar{a}, T)$ est irréductible au dessus de $k(\bar{a})$ et a α pour racine. Par hypothèse, il existe $\beta \in F_2$ tel que $p(\bar{b}, \beta) = 0$. On en déduit l'existence d'un isomorphisme $\psi : k(\bar{a}, \alpha) \to k(\bar{b}, \beta)$, envoyant $(\bar{a}, \alpha)$ sur $(\bar{b}, \beta)$. Prolongeons ψ^{-1} en un automorphisme de K. On peut alors remplacer F_2 par une copie isomorphe, et supposer $(\bar{a}, \alpha) = (\bar{b}, \beta)$. Comme F_2 est parfait, la variété V est définie sur F_2 ; comme F_2 est PAC, on peut trouver $\bar{d} \in V(F_2)$. Puisque $\bar{c}$ est un point générique de V, il existe un $k(\bar{a}, \alpha)$-morphisme : $k(\bar{a}, \alpha)[\bar{c}] \to k(\bar{a}, \alpha)[\bar{d}]$. La formule $\theta(\bar{x}, \bar{y})$ est positive, sans quantificateurs, satisfaite par $(\bar{a}, \bar{c})$. Elle est donc aussi satisfaite par $(\bar{a}, \bar{d}) = (\bar{b}, \bar{d})$. Cela montre que $F_2 \models \exists \bar{y} \theta(\bar{b}, \bar{y})$.

Le résultat de préservation 1.10 assure alors que $\varphi(\bar{x})$ est équivalente à une conjonction de formules de Δ modulo la théorie des corps parfaits PAC. Mais modulo la théorie des corps, toute formule de Δ est équivalente à une formule de la forme $\exists t f(\bar{x}, t) = 0$. Le résultat suit. □

Proposition 7.10. *Soit $\varphi(\bar{x})$ une formule de $\mathcal{L}_c$, $\bar{x} = (x_1, \ldots, x_n)$. Il existe des formules $\psi_I(\bar{x})$, de la forme $\exists t_1, \ldots, t_m \theta_I(\bar{x}, \bar{t})$, où $\theta(\bar{x}, \bar{t})$ est une conjonction d'équations, telles que*

- $\mathrm{Psf}_c \vdash \varphi(\bar{x}) \leftrightarrow \vee_I \psi_I(\bar{x})$;
- *Pour chaque I, il existe une constante N_I telle que si $(F, \bar{c})$ est un modèle de Psf_c, et $\bar{a} \in F^n$ satisfait $\psi_I(\bar{x})$, alors l'ensemble $\{\bar{t} \in F^m, F \models \theta_I(\bar{a}, \bar{t})\}$ a au plus N_I éléments.*

Démonstration. En combinant les deux propositions précédentes, on obtient que $\varphi(\bar{x})$ est équivalente modulo Psf_c à une formule de la forme $\exists t_1, \ldots, t_m \wedge_{i=1}^s f_i(\bar{x}, \bar{c}, t_i) = 0$, avec $f_i(\bar{X}, \bar{C}, T_i) \in \mathbb{Z}[\bar{X}, \bar{C}, \bar{T_i}]$. Soit $(F, \bar{c}) \models Psf_c$, et $\bar{a} \in F^n$ qui satisfait $\varphi(\bar{x})$. Pour chaque sous-ensemble I de $\{1, \ldots, s\}$, considérons la formule $\overset{\psi}{I}(\bar{x})$ exprimant les propriétés qui suivent :

(i) Si $i \notin I$, les coefficients de $f_i(\bar{x}, \bar{c}, T_i)$ sont tous nuls ;

(ii) Si $i \in I$, un des coefficients de $f_i(\bar{x}, \bar{c}, T_i)$ est non nul ;

(iii) $\wedge_{i \in I} \exists t_i f_i(\bar{x}, \bar{c}, t_i) = 0$.

Modulo Psf_c, $\varphi(\bar{x})$ est équivalente à la disjonction de $\psi_I(\bar{x})$ quand I décrit $\mathcal{P}(\{1, \ldots, s\})$. La condition (i) est positive sans quantificateurs. Si (ii) est vérifiée, et $i \in I$, l'ensemble des t_i vérifiant $f_i(\bar{x}, \bar{c}, t_i) = 0$ est bien sûr fini. Reste à montrer que la condition (ii) de façon positive. Or, modulo la théorie des corps, la disjonction $\vee y_i \neq 0$ équivaut à $\exists u \Pi(y_i u - 1) = 0$. On en déduit pour chaque $i \in I$, l'existence d'une formule $\exists u_i p_i(\bar{x}, \bar{c}, u_i) = 0$, exprimant que le polynôme $f_i(\bar{x}, \bar{c}, T_i)$ n'est pas nul. La borne N_I est alors simplement le produit des degrés des polynômes $f_i(\bar{x}, \bar{c}, T_i)$ et $p_i(\bar{x}, \bar{c}, U_i)$ pour $i \in I$. □

Corollaire 7.11. *Soit F un corps pseudo-fini, et $S \subseteq F^m$ un ensemble définissable. Alors il existe un ensemble algébrique $V \subset F^{m+n}$ tel que si $\pi : F^{m+n} \to F^m$ est la projection sur les m premières coordonnées, alors $\pi(V(F)) = S$, et pour tout $\bar{a} \in S$, $\pi^{-1}(\bar{a})$ est fini.*

Démonstration. Plaçons-nous dans le langage $\mathcal{L}_c$, et trouvons des interprétations pour les constantes $c_{i,n}$ telles que $(F, \bar{c}) \models \mathrm{Psf}_c$. Soit $\varphi(\bar{x}, \bar{y})$ et $\bar{a}$ un n-uplet de F tel que S est défni par $\varphi(\bar{x}, \bar{a})$.

Soient $\psi_I(\bar{x}, \bar{y})$ les formules obtenues en appliquant à $\varphi(\bar{x}, \bar{y})$ la proposition précédente. Pour chaque I, l'ensemble défini par la formule $\psi_I(\bar{x}, \bar{a})$ est la projection de l'ensemble algébrique

défini par la formule $\theta_I(\bar{x}, \bar{a}, \bar{t})$, et au-dessus d'un point $(\bar{b}, \bar{a})$ satisfaisant $\psi(\bar{x}, \bar{a})$, il y a au plus N_I uplets $\bar{t}$. D'où le résultat, en prenant l'union de tous ces ensembles algébriques. □

8 Théorie des corps finis, décidabilité

Ce théorème (difficile) nous va nous servir à la démonstration de la réciproque du théorème d'Ax. Nous ne donnons ici aucune démonstration. On peut la trouver dans [7, Fried-Jarden].

Soient $K \subseteq L$ des corps de nombres. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Comme l'anneau $\mathcal{O}_L$ est un anneau de Dedekind, l'idéal $\mathfrak{p}\mathcal{O}_L$ se décompose en produit d'idéaux premiers. Si $\mathfrak{q}$ est un idéal premier de $\mathcal{O}_L$ apparaissant dans cette décomposition, on dira que $\mathfrak{q}$ divise $\mathfrak{p}$. Fixons de tels idéaux $\mathfrak{p}$ et $\mathfrak{q}$. On dit que l'extension L/K est non ramifiée en $\mathfrak{q}$ si l'exposant de $\mathfrak{q}$ dans la décomposition de $\mathfrak{p}$ est 1. Supposons de plus l'extension L/K galoisienne. On montre alors que le groupe de Galois agit transitivement sur les idéaux premiers au-dessus de $\mathfrak{p}$ et la condition précédente ne dépend donc pas du choix de $\mathfrak{q}$: on peut donc dire que l'extension est non ramifiée en $\mathfrak{p}$ (dans le cas $K = \mathbb{Q}$, on peut montrer que seul un ensemble fini de nombres premiers se ramifient). Le sous-groupe $D_\mathfrak{q}$ de $\mathrm{Gal}(L/K)$ formé des éléments σ tels que $\sigma(\mathfrak{q}) = \mathfrak{q}$ est appelé groupe de décomposition de $\mathfrak{q}$ dans L/K. On montre que la condition de non-ramification équivaut à dire que l'application naturelle de $D_\mathfrak{q}$ dans $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{q}/\mathcal{O}_K/\mathfrak{p})$ est un isomorphisme. Or le groupe à l'arrivée est un groupe cyclique, engendré par un élément de Frobenius. Soit $s_\mathfrak{q}$ l'élément de $D_\mathfrak{q}$ correspondant à ce générateur. On le note $\mathrm{Fr}_{L/K}(\mathfrak{q})$, ou simplement $\mathrm{Fr}(\mathfrak{q})$. Si l'on avait choisi un autre idéal premier divisant $\mathfrak{p}$, on aurait obtenu un élément conjugué au précédent. L'élément $\mathrm{Fr}(\mathfrak{p})$ est donc bien défini comme classe de conjugaison dans $\mathrm{Gal}(L/K)$. Le théorème de Chebotarev (une version affaiblie) affirme alors :

Théorème 8.1. *On garde les hypothèses et notations précédentes, en prenant $K = \mathbb{Q}$. Si X est un sous-ensemble de* $\mathrm{Gal}(L/\mathbb{Q})$ *stable par conjugaison, et P_X l'ensemble des nombres premiers non ramifiés dans L tels que la classe du Frobenius* $\mathrm{Fr}(p)$ *est contenue dans X, alors P_X est infini.*

Théorème 8.2 (Ax)**.** *Tout corps pseudo-fini est un modèle de la théorie T_f des corps finis. De plus, tout corps pseudo-fini de caractéristique nulle est élémentairement équivalent à un ultraproduit de corps premiers finis.*

Démonstration. Le cas le plus simple est celui de la caractéristique p. Soit F un corps pseudo-fini de caractéristique p. Le théorème 7.6 nous ramène à chercher un ultraproduit F^* de corps finis, tel que $\tilde{\mathbb{F}}_p \cap F \simeq \tilde{\mathbb{F}}_p \cap F^*$. Supposons pour commencer $\tilde{\mathbb{F}}_p \cap F$ infini. On peut donc écrire $\tilde{\mathbb{F}}_p \cap F = \cup_n F_n$, avec F_n une suite croissante de sous-corps finis de F. Soit $\mathcal{F}$ un ultrafiltre non principal sur $\mathbb{N}$, et

$$F^* = \prod F_n/\mathcal{F}.$$

Alors $\tilde{\mathbb{F}}_p \cap F^* = \cup_n F_n$.

Si, au contraire, le corps $F_0 := \tilde{\mathbb{F}}_p \cap F$ est fini, notons Q l'ensemble des nombres premiers ne divisant pas le degré de F_0 sur $\mathbb{F}_p$, et pour $q \in Q$, F_q l'extension de F_0 de degré q. Soit $\mathcal{F}$ un ultrafiltre non principal sur Q, et $F^* = \prod_q F_q/\mathcal{F}$. Alors $F^* \cap \tilde{\mathbb{F}}_p = F_0$.

Le cas de la caractéristique nulle est plus difficile. Nous aurons besoin du théorème de Chebotarev 8.1.

Soit donc F un corps pseudo-fini de caractéristique nulle. On note $K = F \cap \tilde{\mathbb{Q}}$. Pour $f \in \mathbb{Z}[X]$ ayant une racine dans K, on note $A(f) = \{p, \mathbb{F}_p \vDash \exists x, f(x) = 0\}$, et pour $g \in \mathbb{Z}[X]$, tel que g

n'a pas de racine dans K, on note $B(g) = \{p, \mathbb{F}_p \vDash \forall x, g(x) \neq 0\}$. Choisissons sur l'ensemble des nombres premiers un ultrafiltre non principal $\mathcal{F}$ tel que $A(f) \in \mathcal{F}$ pour tout $f \in \mathbb{Z}[X]$ ayant une racine dans K, et tel que $B(g) \in \mathcal{F}$ pour tout $g \in \mathbb{Z}[X]$ sans racine dans K. Il faut encore s'assurer qu'un tel ultrafiltre existe. Cela fait, le corps $F^* = \prod \mathbb{F}_p/\mathcal{F}$ vérifiera $\tilde{\mathbb{Q}} \cap F = \tilde{\mathbb{Q}} \cap F^*$, comme voulu. Pour s'assurer de l'existence de $\mathcal{F}$, il suffit de vérifier que l'intersection d'une famille finie d'éléments de $V = \{A(f), f \in \mathbb{Z}[X]$ ayant une racine dans $K\} \cup \{B(g), g \in \mathbb{Z}[X]$ sans racine dans $K\} \cup C$, où C désigne l'ensemble des parties cofinies de l'ensemble des nombres premiers, est non vide.

Soient $f_1, f_2 \in \mathbb{Z}[X]$ ayant chacun une racine dans K, notées respectivement a_1 et a_2. Soit $a \in K$ un élément primitif de l'extension $\mathbb{Q}(a_1, a_2)$, et f unitaire irréductible à coefficients entiers annulant a. Il existe un ensemble fini T de nombres premiers, tel que, pour tout $p \notin T$, p ne divise pas le discriminant de f, et a s'écrit comme combinaison de a_1 et a_2 à coefficients rationnels de dénominateurs premiers à p. Soit N une extension finie galoisienne de $\mathbb{Q}$ contenant $\mathbb{Q}(a)$. Il s'ensuit que si $p \notin T$, et si H est le corps de décomposition d'un idéal premier $\mathfrak{p}$ de N au-dessus de p (c'est-à-dire le corps fixé par le groupe de décomposition de $\mathfrak{p}$), alors $\mathbb{Q}(a) \subseteq H$. En considérant les classes résiduelles modulo $\mathfrak{p}$, on obtient une racine $\bar{a}_i \in \mathbb{F}_p$ de f_i $(i = 1, 2)$. Donc $A(f) - T \subseteq A(f_1) \cap A(f_2)$; en particulier, $A(f_1) \cap A(f_2)$ est infini.

Si $g_1, g_2 \in \mathbb{Z}[X]$ sont sans racine dans K, $g_1 g_2$ aussi, et $B(g_1) \cap B(g_2) = B(g_1 g_2)$ est infini. Il ne nous reste donc plus qu'à vérifier que si $f \in \mathbb{Z}[X]$ a une racine dans K, et $g \in \mathbb{Z}[X]$ n'en a aucune, alors $A(f) \cap B(g)$ est infini. On considère une extension finie H galoisienne de $\mathbb{Q}$ contenant toutes les racines de g. Comme F est pseudo-fini, K a au plus une extension de tout degré. Donc l'extension KH/K est cyclique (cf. 7.1). Il existe donc un sous-corps L de K, fini sur $\mathbb{Q}$, contenant une racine de f, et tel que l'extension LH/L est cyclique (choisir L contenant les coefficients du polynôme minimal d'un élément primitif de H). Soit N une extension galoisienne de LH, et τ un automorphisme de N prologeant un générateur de $\mathrm{Gal}(LH/L)$. Si M est le corps fixe de τ, l'extension N/M est cyclique, et $LH \cap M = L$. Si g avait une racine dans M, comme toutes ses racines sont dans LH, g aurait une racine dans $LH \cap M = L \subseteq K$, ce qui n'est pas. Par conséquent, g n'a pas de racine dans M. Soit A l'ensemble des nombres premiers p tels que M soit le corps de décomposition sur N d'un idéal premier de N au-dessus de p. Comme l'extension N/M est cyclique, le théorème de Chebotarev garantit que A est infini. Comme M contient L, et comme L contient une racine de f, $A - A(f)$ est fini, par un raisonnement semblable au précédent. Comme g n'a pas de racine dans M, $A - B(g)$ est fini. Donc $A - (A(f) \cap B(g))$ est fini, et par conséquent $A(f) \cap B(g)$ est infini. Ceci achève la preuve. □

On prouve maintenant que les théories Psf, Psf_0 (la théorie des corps pseudo-finis de caractéristique nulle) et T_f sont décidables. On sait déjà, au vu de ce qui précède que $\mathrm{Psf} = T_f \cup \{$il existe une infinité d'élements$\}$, et $\mathrm{Psf}_0 = Th(\mathbb{F}_p, p) \cup \{$il existe une infinité d'élements$\}$.

Soit φ un énoncé. On veut décider si $T_f \vdash \varphi$. Enumérons les énoncés ψ combinaisons booléennes d'énoncés de la forme $\exists t, f(t) = 0$, pour $f(T) \in \mathbb{Z}[T]$. On sait que φ est équivalent à un tel énoncé modulo Psf. On sait qu'on peut montrer que les constantes A et B du théorème 5.1 sont récursives (voir [22, Seidenberg]), de sorte que la théorie Psf est récursive, on peut donc se donner aussi une énumération des preuves à partir de Psf. A l'étape n, nous regardons si l'une des n premières preuves prouve que l'un des n premiers énoncés ψ est équivalent à φ. Un tel n existe nécessairement par la proposition 7.9.

La preuve que $\mathrm{Psf} \vdash (\varphi \leftrightarrow \psi)$ est finie, donc n'utilise qu'un nombre fini d'énoncés exprimant que le corps est PAC. Le théorème de Lang-Weil permet donc de choisir une constante C telle

que si $q > C$, $\mathbb{F}_q \vDash \varphi \leftrightarrow \psi$ (voir la preuve du théorème 6.3). Il nous suffit donc de savoir décider la validité de l'énoncé ψ dans tous les corps pseudo-finis, et celle de l'énoncé φ dans tous les corps finis de cardinal inférieur ou égal à C. La deuxième partie est récursive, car l'on peut contrôler de façon récusive la constante apparaissant dans le théorème de Lang-Weil (voir la remarque à la fin de l'annexe 1). Occupons-nous donc de la première.

Il s'agit de décider si ψ est vrai dans tout corps pseudo-fini. Vu la forme de ψ, ψ est vraie dans un corps pseudo-fini F si et seulement si elle l'est dans E, défini comme l'intersection de F avec la clôture algébrique du corps premier de F. Quels sont les corps qui peuvent s'écrire comme intersection d'un corps pseudo-fini avec la clôture algébrique du corps premier k de ce corps pseudo-fini ? Un tel corps E vérifie nécessairement que $\mathrm{Gal}(\tilde{k}/E)$ est procyclique (i.e. E a au plus une extension de degré n pour tout n). Réciproquement, on a vu dans la preuve du théorème 8.2 qu'un corps ayant cette propriété peut s'écrire comme intersection d'un corps pseudo-fini de corps premier k avec $\tilde{k}$ (conséquence du théorème de Chebotarev dans le cas de la caractéristique 0). La combinaison des deux remarques précédentes montre qu'il nous faut décider si tout sous-corps E de la clôture algébrique du corps premier k, avec $\mathrm{Gal}(\tilde{k}/E)$ procyclique, satisfait ψ. Ecrivons

$$\psi = P((\exists x_1, f(x_1) = 0, \ldots, \exists x_m, f(x_m) = 0)),$$

avec $P(X_1, \ldots, X_m)$ un polynôme booléen, $f_1, \ldots, f_m \in \mathbb{Z}[X]$.

Traitons en premier le cas de la caractéristique nulle. On note L le corps de décomposition sur $\mathbb{Q}$ du produit des polynômes apparaissant dans ψ. Comme le groupe de Galois de E sur $\mathbb{Q}$ est procyclique, l'extension EL/E est cyclique (cf. 7.1), engendré par un élément σ, que l'on peut prolonger en $\tau \in \mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q})$. Considérons alors K le sous-corps de L fixé par τ, de sorte que $E \cap L = K$. Donc pout chaque i, f_i a une solution dans E si et seulement si f_i a une solution dans K. On est donc ramené à : calculer effectivement le groupe de Galois de L sur $\mathbb{Q}$, tester si les sous-corps de L fixés par un élément de ce groupe statisfont tous ψ. On peut donc décider si $\mathrm{Psf}_0 \vdash \psi$. On en déduit que la théorie Psf_0 est décidable.

Montrons maintenant comment décider si $\mathrm{Psf} \vDash \psi$. Supposons que $\mathrm{Psf}_0 \vdash \psi$. Il existe alors une preuve de l'énoncé φ à partir de Psf_0. Cette preuve n'utilise qu'un nombre fini d'énoncés exprimant que la caractéristique est différente de p, et on peut donc trouver une constante C' telle que tous les corps pseudo-finis de caractéristique $> C'$ satisfont φ. Il reste à voir ce qui se passe pour les corps pseudo-finis de caractéristique inférieure ou égale à C' ; pour cela il suffit comme précédemment de considérer un corps de décomposition des f_i sur $\mathbb{F}_p$, pour tout $p \leq C'$ et de répéter le même raisonnement.

9 Mesure des ensembles définissables

On peut se poser la question de savoir s'il existe une formule du langage des anneaux qui définit dans tout corps fini $\mathbb{F}_{q^2}$ le sous corps $\mathbb{F}_q$.

On sait déjà que c'est impossible par la preuve de la réciproque du théorème d'Ax. En effet, supposons qu'on a une telle formule ϕ. On considère alors un ultraproduit F sur un ultrafiltre non principal des $\mathbb{F}_{q^2}$. C'est un corps pseudo-fini de caractéristique nulle, or on a montré dans la réciproque du théorème d'Ax qu'un corps pseudo-fini de caractéristique nulle est élémentairement équivalent à un ultraproduit de corps premiers $\mathbb{F}_p$. Or ϕ définit pour tout q un sous-corps strict de $\mathbb{F}_{q^2}$, donc ϕ définit un sous-corps strict de F, donc pour une infinité de p premiers, ϕ définit un sous-corps strict de $\mathbb{F}_p$, ce qui est absurde.

Cependant, on peut généraliser le résultat et montrer que pour toute formule ϕ du langage des anneaux, il existe au plus un nombre fini de q tels que ϕ définisse $\mathbb{F}_q$ dans $\mathbb{F}_{q^2}$. Pour cela, on a besoin du résultat suivant, qui généralise le théorème de Lang-Weil et permet de définir une mesure sur les ensembles définissables dans les corps pseudo-finis. On suit la démonstration donnée dans [4, Chatzidakis-van den Dries-Macintyre].

Théorème 9.1. *Soit $\phi(\bar{x}, \bar{y}), \bar{x} = (x_1, ..., x_m), \bar{y} = (x_1, ..., x_n)$ une formule du langage des anneaux $\mathcal{L}$. Alors il existe un ensemble fini D de paires $(d, \mu) \in \{0, ..., n\} \times \mathbb{Q}^{>0}$ et une constante $C > 0$ tels que pour tous corps fini $k = \mathbb{F}_q$, et m-uplet $\bar{x}$ de k, si l'ensemble $\phi(\bar{x}, k^n) := \{\bar{b} \in k^n | k \models \phi(\bar{x}, \bar{b})\}$ est non vide, alors*

$$|\sharp\phi(\bar{x}, k^n) - \mu q^d| \leq C q^{d-1/2},$$

pour un certain $(d, \mu) \in D$.

La preuve du théorème va essentiellement consister à généraliser le théorème de Lang-Weil pour des formules de plus en plus complexes. En effet, dans le cas où $\phi(\bar{x}, \bar{a})$ définit une variété V, c'est le théorème de Lang-Weil avec $d = \dim(V)$ et $\mu = 1$. Nous procéderons par étapes. On fixe dans toute la partie un corps fini $k = \mathbb{F}_q$, des entiers n, m, e, r, $\bar{X} = (X_1, ..., X_m)$, $\bar{Y} = (Y_1, ..., Y_n)$.

Proposition 9.2. *Soit I un idéal engendré par r polynômes de $k[\bar{x}]$ de degrés inférieurs à e. Il existe alors un $C > 0$ et un entier M ne dépendant que de (e, n, r) tels que si $V(k) := V(I) \cap k \neq \emptyset$ alors*

$$|\sharp V(k) - \mu q^d| \leq C q^{d-1/2}$$

pour un $(d, \mu) \in \{0, ..., \dim(V)\} \times \{1, ..., M\}$.

Démonstration. On raisonne par récurrence sur $\dim(V)$. Il n'y a pas besoin d'initialiser comme on le verra dans la suite de la preuve. On suppose $V(k) \neq \emptyset$. Comme $V(I)$ est définie sur k, soit V^* le noyau k-absolu de V (voire remarque 3.6(3)) et soient $V_1, ..., V_s$ les composantes irréductibles de V^*, de sorte que $V(k) = V_1(k) \cup ... \cup V_s(k)$. Par la proposition 5.15, s est bornée par D qui ne dépend que de (e, n, r). Quitte à réordonner, on peut supposer que $V_1, ..., V_\mu$ sont de dimension maximale $d \leq dim(V)$ et que $\dim(V_j) < d$ pour $\mu < j \leq s$.

On va maintenant montrer que pour ces valeurs de d et μ, on a

$$|\sharp V(k) - \mu q^d| \leq C q^{d-1/2} \text{ pour un } C > 0 \text{ qui ne dépend que de } (e, n, r).$$

Cela achèvera la démonstration de la proposition. Toujours par la proposition 5.15, les V_j sont de la forme $V(h_1, ..., h_D)$ pour des $h_i \in k[\bar{X}]$ de degrés $\leq D$ (D qui ne dépend que de (e, n, r)). Le théorème de Lang-Weil fournit alors les estimations suivantes :

(1)$|\sharp V_j(k) - q^d| \leq C_1 q^{d-1/2}$ pour $j \in \{1, ..., \mu\}$ et un $C_1 > 0$ qui ne dépend que de (D, n) donc que de (e, n, r).

(2)$|\sharp V_j(k)| \leq C_2 q^{d-1}$ pour $\mu < j \leq s$ et un $C_2 > 0$ qui ne dépend que de (D, n) donc que de (e, n, r).

Soient $1 \leq i < j \leq s$. Alors V_i et V_j sont des variétés définies sur k, donc leur intersection est un fermé défini sur F de dimension $< d$, défini par $2D$ polynômes sur k de degrés $\leq e$. S'il est non vide, par hypothèse de récurrence :

(3)$|\sharp(V_i(k) \cap V_j(k))| \leq C_3 q^{d-1}$ pour un $C_3 > 0$ qui ne dépend que de (D, n) donc que de (e, n, r).

Le résultat du théorème découle alors de la combinaison de (1), (2), et (3). □

Remarque 9.3. Soit $f = (f_1, ..., f_r) \in \mathbb{Z}[\bar{X}, \bar{Y}]^r$ avec les f_i de degrés $\leq e$ en $\bar{Y}$. La proposition s'applique à $f(\bar{x}, \bar{Y}) \in k[Y]^r$, pour tout corps fini k et $\bar{x} \in k^m$. Soit $V_{\bar{x}}(k) := \{\bar{y} \in k^n | f(\bar{x}, \bar{y}) = 0\}$.

On a alors le résultat suivant : soient C et M les constantes de la proposition, $d \in \{0, ..., n\}$ et $\mu \in \{1, ..., M\}$. Alors l'ensemble des $\bar{x} \in k^m$ tels que $|\sharp V(k) - \mu q^d| \leq C q^{d-1/2}$ est défini dans le corps k par une $\mathcal{L}$-formule $S_{f,d,\mu}(\bar{x})$ qui est indépendante de k. Cela découle de la proposition 5.15.

On remarque aussi que si $q = \sharp k$ est suffisamment grand par rapport à C, pour tout $\bar{x} \in k^n$ tel que $V_{\bar{x}}(k) \neq \emptyset$, il existe exactement une paire $(d, \mu) \in \{0, ..., n\} \times \{1, ..., M\}$ telle que $k \models S_{f,d,\mu}(\bar{x})$, tandis que si $V_{\bar{x}}(k) = \emptyset$, il n'y en a aucune.

Lemme 9.4. *Soit ϕ une $\mathcal{L}$-formule sans quantificateurs. Alors il existe une constante $C > 0$ et un entier M, ne dépendant que de ϕ (et pas de k), tels que si $\bar{a} \in k^m$ et $\phi(\bar{a}, k^n) \neq \emptyset$, alors $|\sharp\phi(\bar{a}, k^n)) - \mu q^d| \leq C q^{d-1/2}$ pour un $(d, \mu) \in \{0, ..., n\} \times \{1, ..., M\}$.*

Démonstration. La formule ϕ est équivalente une disjonction $\bigvee_{i=1}^N \phi_i$ où les ϕ_i sont des conjonctions de formules atomiques :

$$\phi_i(\bar{x}, \bar{y}) : \bigwedge_{j=1}^{r_i} f_{ij}(\bar{x}, \bar{y}) = 0 \wedge \bigwedge_{j=1}^{r_i} g_{ij}(\bar{x}, \bar{y}) \neq 0, \text{ avec } f_{ij}, g_{ij} \in \mathbb{Z}[\bar{X}, \bar{Y}]$$

telles que les ensembles définis par deux ϕ_i distincts soient disjoints dans tous corps. On considère alors $\bar{y}' = (y_{n+1}, ..., y_{n+N})$ des nouvelles variables et on définit

$$\phi_i'(\bar{x}, \bar{y}, \bar{y}') : \bigwedge_{j=1}^{r_i} f_{ij}(\bar{x}, \bar{y}) = 0 \wedge \bigwedge_{j=1}^{r_i} g_{ij}(\bar{x}, \bar{y}) y_{n+i} = 1 \wedge \bigwedge_{l \neq i} y_{n+l} = 0$$

et $\phi'(\bar{x}, \bar{y}, \bar{y}') : \bigvee_{i=1}^N \phi_i'(\bar{x}, \bar{y}, \bar{y}')$. La formule ϕ' est alors positive sans quantificateur, donc équivalente modulo la théorie des corps à une conjonction d'équations polynomiales en $(\bar{x}, \bar{y}, \bar{y}')$. On peut donc appliquer la proposition 9.2 aux ensembles $\phi'(\bar{x}, k^{n+N})$. Il existe $C > 0$ et un entier M ne dépendant que de ϕ' donc que de ϕ tels que pour tout $\bar{x} \in k^m$ et $\phi'(\bar{x}, k^{n+N}) \neq \emptyset$, alors

$$|\sharp\phi'(\bar{x}, k^{n+N}) - \mu q^d| \leq C q^{d-1/2} \text{ pour un } (d, \mu) \in \{0, ..., n+N\} \times \{1, ..., M\}.$$

Mais la dimension de $\phi'(\bar{x}, k^{n+N})$ est visiblement inférieure ou égale à n, donc d est dans $\{0, ..., n\}$. Puisque deux formules de la disjonction ci-dessus sont disjointes, on a pour tout $\bar{x} \in k^m$ une bijection $\phi'(\bar{x}, k^{n+N}) \to \phi'(\bar{x}, k^n) : (\bar{y}, \bar{y}') \mapsto \bar{y}$, ce qui achève la démonstration. □

Remarque 9.5. Soient C et M les constantes du lemme, et $(d, \mu) \in \{0, ..., n\} \times \{1, ..., M\}$. Alors l'ensemble des $\bar{x} \in k^m$ tels que $|\sharp\phi'(\bar{x}, k^{n+N}) - \mu q^d| \leq C q^{d-1/2}$ est défini dans le corps k par une $\mathcal{L}$-formule $\phi_{d,\mu}(\bar{x})$ indépendante de k. Cela découle de la remarque précédente et du lemme.

On peut maintenant prouver le théorème 9.1 :

Théorème. *Soit $\phi(\bar{x}, \bar{y}), \bar{x} = (x_1, ..., x_m), \bar{y} = (x_1, ..., x_n)$ une formule du langage des anneaux $\mathcal{L}$. Alors il existe un ensemble fini D de paires $(d, \mu) \in \{0, ..., n\} \times \mathbb{Q}^{>0}$ et une constante $C > 0$ tels que pour tout corps fini $k = \mathbb{F}_q$, et m-uplet $\bar{a}$ de k, si l'ensemble $\phi(\bar{a}, k^n) := \{\bar{b} \in k^n | k \models \phi(\bar{a}, \bar{b})$ est non vide, alors*

$$|\sharp\phi(\bar{a}, k^n) - \mu q^d| \leq C q^{d-1/2},$$

pour un certain $(d, \mu) \in D$.

Démonstration. D'après la proposition 7.10, il existe un sous-uplet fini $\bar{c}$ des constantes de $\mathcal{L}_c$ et une $\mathcal{L}$-formule existentielle

$$\phi'(\bar{x},\bar{y},\bar{c}) = \exists \bar{t}\psi(\bar{x},\bar{y},\bar{c},\bar{t}) \text{ avec } \psi \text{ sans quantificateurs}$$

telle que $\mathrm{Psf}_c \vdash \forall\bar{x}\forall\bar{y}(\phi(\bar{x},\bar{y}) \leftrightarrow \phi'(\bar{x},\bar{y},\bar{c}))$ et qu'il existe un entier e (ne dépendant que de ϕ) tel que pour tout modèle $(F,\vec{c}')$ de Psf_c, et $\bar{a},\bar{b}$ des uplets de F, l'ensemble $\{\bar{t} \in F^r | F \models \psi(\bar{a},\bar{b},\bar{c},\bar{t})\}$ a au plus e éléments. Par compacité, il existe une formule $\theta(\bar{c})$ telle que $Psf \vdash \forall\bar{z}\theta(\bar{z}) \to (\phi(\bar{x},\bar{y}) \leftrightarrow \phi'(\bar{x},\bar{y},\bar{z}))$. La même chose est donc vraie dans tout corps fini suffisamment grand. Il suffit donc de montrer le théorème pour les formules du même type que ϕ', où l'on considère $\bar{x},\bar{z}$ comme le paramètre.

Soit donc $\phi(\bar{x},\bar{y}) = \exists\bar{t}\psi(\bar{x},\bar{y},\bar{t})$ avec ψ sans quantificateurs et qui vérifie qu'il existe e ne dépendant que de ϕ tel que pour tout corps fini k, et $\bar{a},\bar{b}$ des uplets de k, l'ensemble $\{\bar{t} \in k^r | k \models \psi(\bar{a},\bar{b},\bar{t})\}$ a au plus e éléments.

Par le lemme 9.4, il existe $A > 0$ et un entier N (ne dépendant que de ϕ), tels que pour tout $\bar{x} \in k^m$ et $\psi(\bar{x},k^{n+r}) \neq \emptyset$, on a

$$|\sharp\psi(\bar{x},k^{n+k}) - \mu q^d| \leq Aq^{d-1/2} \text{ pour un } (d,\mu) \in \{0,...,n+r\} \times \{1,...,M\}.$$

On fixe $\bar{x} \in k^m$ avec $\psi(\bar{x},k^{n+r}) \neq \emptyset$, et soient $(d,\mu) \in \{0,...,n+r\} \times \{1,...,M\}$ pour que l'estimée soit vraie. On définit

$$\mathcal{F} := \phi(\bar{x},k^n),\ \mathcal{F}_j := \{\bar{y} \in k^n | \sharp\psi(\bar{x},\bar{y},k^r) = j\} \text{ et } \mathcal{G} := \psi(\bar{x},k^{n+r}).$$

On a alors

$$\sharp\mathcal{F} = \sharp\mathcal{F}_1 + ... + \sharp\mathcal{F}_e,$$

$$\sharp\mathcal{G} = \sharp\mathcal{F}_1 + 2\cdot\sharp\mathcal{F}_2 + ... + e\cdot\sharp\mathcal{F}_e,$$

$$(1)\ |\sharp\mathcal{G} - \mu q^d| \leq Aq^{d-1/2} \text{ et } \sharp\mathcal{F} \geq \sharp\mathcal{G}/e,$$

de sorte que

$$(2)\ q^n \geq \sharp\mathcal{F} \geq \mu/eq^d - A/eq^{d-1/2}.$$

Donc quitte à supposer q assez grand, on a $d \leq n$.

On va maintenant chercher à estimer les $\sharp\mathcal{F}_j$. Pour cela, on considère les formules sans quantificateurs

$$\psi_j(\bar{x},\bar{y},\bar{z}^1,....,\bar{z}^j) := \bigwedge_{1\leq i\leq j} \psi(\bar{x},\bar{y},\bar{z}^i) \wedge \bigwedge_{l\neq m} \bar{z}^l \neq \bar{z}^m \text{ pour } 1 \leq j \leq e,$$

où les $\bar{z}^i$ sont des r-uplets de nouvelles variables, et $\bar{z}^l \neq \bar{z}^m$ la disjonction exprimant les deux uplets different au moins par une coordonnée. Soit $\mathcal{H}_j := \psi_j(\bar{x},k^{n+jr})$. Chaque point $\bar{y} \in \mathcal{F}_j$ donne $j!$ points dans $\mathcal{H}_j$, et plus généralement pour $0 \leq t \leq e-j$, chaque $\bar{y} \in \mathcal{F}_{j+t}$ donne $j![(j+t)!/!jt!] = (j+t)!/t!$ points dans $\mathcal{H}_j$. On a donc

$$\sharp\mathcal{H}_j = j!/0!\sharp\mathcal{F}_j + (j+1)!/1!\sharp\mathcal{F}_{j+1} + ... + e!/(e-j)!\sharp\mathcal{F}_e.$$

On peut inverser ce système triangulaire, pour obtenir les $\sharp\mathcal{F}_i$ en fonction des $\sharp\mathcal{H}_i$, et on utilise $\sharp\mathcal{F} = \sharp\mathcal{F}_1 + ... + \sharp\mathcal{F}_e$ pour obtenir

$$(3)\ \sharp\mathcal{F} = r_1\sharp\mathcal{H}_1 + ... + r_e\sharp\mathcal{H}_e,$$

où les r_i sont des rationnels ne dépendant que de e. On remarque que $\sharp\mathcal{H}_j \leq$ constante $\sharp\mathcal{G}$, et on applique le lemme 9.4 à la formule sans quantificateur ψ_j :

$$(4)\ |\sharp\mathcal{H}_j - \mu_j q^d| \leq A_j q^{d-1/2}$$

pour un $\mu_j \in \{0, ..., M_j\}$ avec M_j entier et $A_j > 0$. L'exposant est bien d par la remarque précédente, et notons qu'on autorise ici $\mu_j = 0$. On a M_j et A_j qui ne dépendent que de ψ_i donc que de ϕ, alors que μ_j dépend de k et $\bar{x} \in k^n$. On combine alors (3) et (4) pour obtenir

$$|\sharp\mathcal{F} - (r_1\mu_1 + ... + r_e\mu_e)q^d| \leq Cq^{d-1/2},$$

avec $C = |r_1 A_1| + ... + |r_e A_e|$.

On déduit alors de (2) que $r_1\mu_1 + ... + r_e\mu_e \geq \mu/e > 0$, pour k de cardinal assez grand. Comme les r_i sont uniquement déterminés par e, il n'y a qu'un nombre fini de possibilités pour les $\mu_1, ..., \mu_e$, ce qui termine la preuve. □

Proposition 9.6. *Soient C et D comme dans le théorème, et $(d, \mu) \in D$. Alors l'ensemble des $\bar{x} \in k^m$ tels que $|\sharp\phi(\bar{x}, k^n) - \mu q^d| \leq Cq^{d-1/2}$ est défini dans le corps k par une $\mathcal{L}$-formule $\phi_{d,\mu}(\bar{x})$ indépendante de k.*

Démonstration. Cela découle par la remarque précédant le théorème de l'existence de telles formules pour les ψ_j. Le fait d'avoir remplacé des constantes $\bar{c}$ par des nouvelles variables ne pose pas de problème. □

Remarque 9.7. On fixe une formule $\phi(\bar{x}, \bar{y})$. Soit D l'ensemble de paires associées. Pour tout corps $\mathbb{F}_q$ assez grand, pour tout m-uplet $\bar{a}$ de $\mathbb{F}_q$, il existe une unique paire $(d, \mu) \in D$ telle que $\mathbb{F}_q \models \phi_{d,\mu}(\bar{a})$. Pour tout corps pseudo-fini F, si $S \subseteq F^n$ est défini par la formule $\phi(\bar{a}, \bar{y})$ pour un $\bar{a} \in F^m$, on peut donc définir$(\dim(S), \mu(S))$ comme l'unique paire $(d, \mu) \in D$ telle que $F \models \phi_{d,\mu}(\bar{a})$.

On peut vérifier les propriétés suivantes, pour $S, T \in F^n$ définissables et disjoints :

– si V est une variété définie sur F, alors $\dim(V(F)) = \dim(V)$ et $\mu(V(F)) = 1$;

– la dimension algébrique de la clôture de Zariski de S est $\dim(S)$;

–

$$\mu(S \cup T) \begin{cases} \mu(S) + \mu(T) & \text{si } \dim(S) = \dim(T), \\ \mu(S) & \text{si } \dim(S) > \dim(T), \\ \mu(T) & \text{si } \dim(S) < \dim(T). \end{cases}$$

On peut maintenant prouver le résultat présenté en motivation de cette partie.

Proposition 9.8. *Soit ϕ une formule du langage des anneaux. Alors il existe au plus un nombre fini de q tels que ϕ définisse $\mathbb{F}_q$ dans $\mathbb{F}_{q^2}$.*

Démonstration. D'après le théorème 9.1, il existe des constantes A et C et des rationnels $0 < \mu_1 < ... < \mu_k \leq 1$ tels que pour tout q puissance d'un p premier, soit $\sharp\phi(\mathbb{F}_{q^2}) \leq A$, soit $|\sharp\phi(\mathbb{F}_{q^2}) - \mu_i q^2| \leq Bq$ pour un certain i. En particulier, il existe des constantes A et C telles que soit $\sharp\phi(\mathbb{F}_{q^2}) \leq A$, soit $\sharp\phi(\mathbb{F}_{q^2}) \geq C\sharp\mathbb{F}_q$, ce qui montre bien ce que l'on veut. □

Troisième partie

Introduction à l'intégration motivique arithmétique

Cette dernière partie utilise librement le langage des variétés et des schémas, tel que développé dans [14, Hartshorne] ou [19, Perrin]. En particulier, le mot variété a son sens usuel (en termes abstraits, une variété sur un corps k est un schéma intègre séparé de type fini sur k), distinct du sens naïf que nous lui avions donné dans la partie qui précède.

10 Stratifications et formules galoisiennes

Cette section définit les notions de stratification et de formules galoisiennes. Le résultat principal de cette partie est un résultat d'élimination des quantificateurs pour les formules galoisiennes, sur les corps pseudo-finis (théorème 10.5). Cet énoncé possède son intérêt propre ; surtout, il sert à élaborer la théorie de l'intégration motivique arithmétique que nous présentons dans la section suivante. Il fait donc le lien entre cette théorie et celle des corps pseudo-finis. C'est pourquoi nous avons choisi de le développer en détail.

Il existe différentes preuves de ce résultat. [16, Fried-Haran-Jarden] et [7, Fried-Jarden] en donnent une preuve algébrique dans le cadre plus général des corps de Frobenius. [18, Nicaise] le démontre dans un contexte relatif, à l'aide d'outils élaborés de géométrie algébrique. La preuve que nous avons choisie est celle de [8, Fried-Sacerdote]. Ce n'est sûrement pas la plus directe, ni la plus limpide. Mais elle a l'avantage de faire appel à des raisonnements géométriques, tout en évitant les arguments sophistiqués.

L'observation de départ est la suivante. Il est faux que la théorie Psf élimine les quantificateurs dans le langage des anneaux. Pour s'en convaincre, considérons la formule

$$\varphi(x) = (\exists x, f(x) = 0),$$

avec $f \in \mathbb{Z}[X]$ irréductible unitaire de degré au moins 2. Si l'on pouvait éliminer les quantificateurs, on en déduirait soit que f a une racine modulo p pour presque tout nombre premier p, soit l'inverse. Or le théorème de Chebotarev nous dit justement qu'il existe une infinité de p tels que f a une racine modulo p, et une infinité de p tels que f n'a pas de racine modulo p... Au vu de la proposition 7.9, on devine toutefois que les obstructions de cette nature sont à peu près les seules. C'est cette idée que la notion de stratification galoisienne va permettre de formaliser.

10.1 Notations, définitions et position du problème

10.1.1 Conventions

Le concept essentiel de cette section est celui de revêtement fini étale galoisien. Les propriétés de base de ces morphismes sont rappelés dans l'annexe 2. Dans toute la suite, le terme *revêtement signifiera toujours revêtement fini étale galoisien.* Voici une situations simple où apparaissent ces revêtements. On se donne A un sous-schéma localement fermé de $\mathbb{A}^n_{\mathcal{O}_K}$, avec K un corps de nombres, et L une extension finie galoisienne du corps des fonctions $K(A)$. Le

théorème de l'élément primitif permet d'écrire $L \simeq K(A)[X]/(f(X))$, avec $f \in \mathcal{O}_K[A][X]$ un polynôme à coefficients réguliers sur A. D'où un morphisme

$$\mathrm{Spec}(\mathcal{O}_K[A][X]/(f(X))) \to A.$$

Ce n'est pas un revêtement, car ce n'est pas un morphisme étale. Mais on dispose d'un ouvert de Zariski de A sur lequel le discriminant $D(f)$ de f est inversible (c'est simplement $\mathrm{Spec}(\mathcal{O}_K[A, 1/D(f)])$). On note V ce sous-schéma, et on note $C(V)$ le pull-back de $\mathrm{Spec}(\mathcal{O}_K[A][X]/(f(X)))$ au-dessus de V. On a ainsi associé à l'extension galoisienne L/K un revêtement $C(V) \to V$.

10.1.2 Le procédé d'union-intersection

Soient k un corps fini, et W un sous-schéma localement fermé de $\mathbb{A}^n_k$. On notera $IU(W,k) := \{X, X \text{ sous-schéma absolument irréductible de } W \text{ défini sur } k\}$. Soit $C(W) \to W$ un revêtement connexe. Si $X \in IU(W,k)$, on considère le pull-back $C(W)|_X \to X$. Comme X est un sous-schéma localement fermé de $\mathbb{A}^n_k$, on peut définir son adhérence $\bar{X}$. On définit $\deg(\bar{X} - X)$ comme la famille des degrés des composantes k-irréductibles de $\bar{X} - X$. On définit de même $\dim(\bar{X} - X)$. Les composantes connexes C de $C(W)|_X$ sont toutes isomorphes, et leurs groupes de Galois $H(C,X)$ (comme revêtement de X) sont conjugués, chacun étant isomorphe à un sous-groupe de $\mathrm{Gal}(C(W)/W)$. Si $k(C)$ est le corps des fonctions rationnelles de C, on note $\tilde{k}$ la clôture algébrique de k dans $k(C)$, et $\tilde{H}(C,X)$ l'ensemble des éléments de $H(C,X)$ qui induisent l'élément de Frobenius en restriction à $\tilde{k}$.

Définition 10.1. Le type de $IU(W,k)$ est la famille finie d'uplets

$$\{(\deg X, \dim X, \deg(\bar{X} - X), \dim(\bar{X} - X), H(C,X), \tilde{H}(C,X))\},$$

pour $X \in IU(W,k)$.

On peut généraliser cette construction au cas où k est seulement un corps parfait. Pour bien le distinguer du précédent, notons T un corps parfait, W un sous-schéma localement fermé de $\mathbb{A}^n_T$. On nomme $IU(W,T)$ la famille de paires (U,σ) calculés par l'algorithme suivant. On commence par écrire $W = W_1 \cup \cdots \cup W_l$ comme union de variétés absolument irréductibles définis sur $T(1)$, avec $T(1)$ une extension galoisienne de T (première étape). Pour tout $\sigma(1) \in \mathrm{Gal}(T(1)/T)$, on écrit

$$\bigcap_{r=0}^{|\sigma(1)|-1} {}^{\sigma(1)^r}W_i = W_{\sigma(1),i_1} \cup \cdots \cup W_{\sigma(1),i_{l(i)}}$$

comme union de variétés absolument irréductibles. Les variétés du membre de droite sont définies sur $T(1) \subseteq T(2)$, extension galoisienne de T (deuxième étape). Pour chaque paire $(\sigma(1),\sigma(2))$, avec $\sigma(2) \in \mathrm{Gal}(T(2)/T)$ prolongeant $\sigma(1)$, on écrit

$$\bigcap_{r=0}^{|\sigma(2)|-1} {}^{\sigma(2)^r}W_{\sigma(1),i_j} = W_{\sigma(1),i_j,1} \cup \cdots \cup W_{\sigma(1),i_j,l(i_j)}$$

comme union de variétés absolument irréductibles, définies sur $T(3)$ (troisième étape), etc. On répète le procédé. L'algorithme s'arrête, c'est-à-dire redonne la même variété, au plus tard à

la $(\dim W + 1)$-ème étape (et s'il termine avant, convenons de le faire continuer jusque là). On note $T^* = T^*(IU(W,T))$ le corps obtenu à la dernière étape. Pour tout $\sigma \in \mathrm{Gal}(T^*/T)$, on dispose des variétés obtenues à la dernière étape de l'algorithme correspondant à la chaîne des restrictions de σ aux $T(i)$. On note $IU(W,T,\sigma)$ la famille de ces variétés. Elles sont absolument irréductibles.

Soit $C(W) \to W$ un revêtement connexe, défini sur T. On note $H(C(W),X)$ le sous-groupe de $\mathrm{Gal}(C(W)/W)$ obtenu à partir d'une composante connexe de $C(W)|_X \to X$, comme plus haut.

Définition 10.2. Le type de $IU(W,T)$ est la famille des types

$$\{(\deg X, \dim X, \deg(\bar{X} - X), \dim(\bar{X} - X), H(C(W),X)\},$$

indexée par les paires (σ, X), avec $\sigma \in \mathrm{Gal}(T^*/T)$, $X \in IU(W,T,\sigma)$.

10.1.3 Stratifications et formules galoisiennes

Soit $S = \mathrm{Spec}(R)$ un schéma affine intègre, X une variété sur S. Supposons données les structures suivantes :

- une stratification de X, notée $\mathfrak{S}(X)$, c'est-à-dire une partition de X en une famille de sous-schémas intègres localement fermés ;
- pour chaque $Y_i \in \mathfrak{S}(A)$, un revêtement $C(Y_i) \to Y_i$;
- pour chaque $Y_i \in \mathfrak{S}(A)$, une famille $\mathrm{Con}(A_i)$ de sous-groupes de $\mathrm{Gal}(C(Y_i)/Y_i)$ stable par conjugaison par les éléments de $\mathrm{Gal}(C(Y_i)/Y_i)$.

Une telle donnée est ce que l'on appelle une stratification galoisienne de X. Si l'on ôte la dernière condition, on dira qu'il s'agit seulement d'une stratification galoisienne incolore ; choisir un coloriage d'une stratification galoisienne incolore signifiera que l'on se donne une famille de sous-groupes comme dans le troisème point précédent.

Si x est un point fermé de S, on note $\mathbb{F}_x$ le corps résiduel de S en x, et X_x la fibre de X au-dessus de x. Plus généralement si le corps F contient $\mathbb{F}_x$, on note $X_{x,F}$ le produit fibré de X et $\mathrm{Spec}(F)$ au-dessus de x. On suppose en outre que l'on dispose d'une stratification galoisienne $\mathfrak{A}$ de X. Soit a un F-point de X_x, appartenant à $Y_{i,x}$. On note $Ar(C(Y_i)/Y_i, x, a)$ la classe de conjugaison formée des sous-groupes de $\mathrm{Gal}(C(Y_i)/Y_i)$ correspondant aux groupes de décomposition en a, ainsi définis : le groupe de Galois $\mathrm{Gal}(C(Y_i)/Y_i)$ agit sur $C(Y_i) \times_{Y_i} a$; à chaque composante connexe Z de $C(Y_i) \times_{Y_i} a$, on associe le sous-groupe de décomposition de Z, formé des éléments de $\mathrm{Gal}(C(Y_i)/Y_i)$ qui stabilisent Z (si η_Z est le point générique de Z, ce groupe n'est autre que $\mathrm{Gal}(\eta_Z/a)$). Si l'on choisit une autre composante connexe Z', le groupe de décomposition de Z' est conjugué à celui de Z, et $Ar(C(Y_i)/Y_i, x, a)$ n'est autre que l'union des sous-groupes de $\mathrm{Gal}(C(Y_i)/Y_i)$ ainsi obtenus. On notera

$$Ar(a) \subseteq \mathrm{Con}(\mathfrak{A}))$$

pour

$$Ar(C(Y_i)/Y_i, x, a) \subseteq \mathrm{Con}(\mathfrak{A}).$$

Soit $\mathfrak{A}$ une stratification galoisienne de $\mathbb{A}_S^{m+n}$, $Q_1, \ldots, Q_m$ des quantificateurs. On note $\theta(Y)$ l'expression formelle

$$(Q_1 X_1) \ldots (Q_m X_m)[Ar(X,Y) \subseteq \mathrm{Con}(\mathfrak{A})],$$

avec $X = (X_1, \ldots, X_m)$, $Y = (Y_1, \ldots, Y_n)$. On dit que $\theta(Y)$ est une formule galoisienne sur R en les variables libres Y. On note enfin, toujours pour x point fermé de S, et F corps contenant $\mathbb{F}_x$,

$$Z(\mathfrak{A}, x, F) := \{a \in X(F), Ar(a) \subseteq \mathrm{Con}(\mathfrak{A})\}.$$

Reprenons ce qui précède pour mieux comprendre dans le cas $S = \mathrm{Spec}(\mathcal{O}_K)$. Soit $C(V) \to V \to \mathcal{O}_K$ un revêtement connexe, et notons $\varphi : C(V) \to V$. Soient $w \in C(V)$, $v \in V$ des points fermés, avec $\varphi(w) = v$, et $\mathfrak{p}$ l'idéal premier de $\mathcal{O}_K$ au-dessus duquel vit v. Soient B et A les anneaux des fonctions régulières sur $C(V)$ et V respectivement, et $\mathfrak{p}(w)$ et $\mathfrak{p}(v)$ les idéaux premiers de B et A correspondant à w et v. Alors $B/\mathfrak{p}(w)$ est une extension finie du corps $A/\mathfrak{p}(v)$, lui-même extension finie du corps résiduel $\mathcal{O}_K/\mathfrak{p}$. Le groupe $\mathrm{Gal}(B/\mathfrak{p}(w)/A/\mathfrak{p}(v))$ a un générateur, l'élément de Frobenius Fr. On définit alors l'élément de Frobenius associé à w, et on note $\mathrm{Fr}(w)$ l'unique élément de $\mathrm{Gal}(C(V)/V)$ tel que $\mathrm{Fr}(w)^*$ induise Fr sur $\mathrm{Gal}(B/\mathfrak{p}(w)/A/\mathfrak{p}(v))$. Cet élément est unique, car le revêtement est étale (dans le cas $V = \mathrm{Spec}(\mathcal{O}_K[1/a])$, penser à une extension non ramifiée de corps de nombres). Si l'on avait choisi un autre élément w' au-dessus de v, on sait, par la théorie algébrique des nombres, que $\mathrm{Fr}(w')$ est conjugué dans $\mathrm{Gal}(C(V)/V)$ à $\mathrm{Fr}(w)$. On note donc à bon droit $\mathrm{Fr}(v)$ la classe de conjugaison de $\mathrm{Fr}(w)$. On retrouve donc ici formulé un peu différemment ce que l'on disait au-dessus. En particulier, on peut réécrire la formule galoisienne $\theta(Y)$:

$$(Q_1X_1)\ldots(Q_mX_m)[\mathrm{Fr}(X,Y) \in \bigcup_{Z \in \mathfrak{S}(\mathfrak{A})} \mathrm{Con}(Z)].$$

Remarque. Si T est un corps parfait, A un sous-schéma localement fermé au-dessus de T, équipé d'une stratification galoisienne $\mathfrak{A}$, on définit le type de $IU(W,T)$ comme l'union des types des $IU(Y,T)$, pour $Y \in \mathfrak{S}(A)$.

Remarque. Soit $\varphi(Y_1, \ldots, Y_n)$ une formule du premier ordre dans le langage des anneaux à coefficients dans l'anneau R, en les variables libres $Y_1, \ldots, Y_n$. Pour tout point fermé x de S, et tout corps F contenant $\mathbb{F}_x$, on note $Z(\varphi, x, F)$ le sous-ensemble de F^n défini par (l'image sur $\mathbb{F}_x$ de) la formule φ. On peut supposer φ sous forme normale prénexe, c'est-à-dire de la forme

$$(Q_1X_1)\ldots(Q_mX_m)[\vee_{i=1}^{k} \wedge_{j=1}^{l} f_{i,j}(X,Y) = 0 \wedge g_{i,j}(X,Y) \neq 0],$$

avec $f_{i,j}, g_{i,j} \in R[X,Y]$. La formule entre crochets définit un ensemble constructible W, et on peut trouver une stratification de $\mathbb{A}_S^{n+m}$ en sous-schémas localement fermés, telle que chaque strate Y_i est contenue ou dans W, ou dans son complémentaire. On choisit alors comme revêtement $C(Y_i) \to Y_i$ l'identité, et pour $\mathrm{Con}(Y_i)$ le groupe trivial si Y_i est contenu dans W, l'ensemble vide sinon. On obtient ainsi une formule galoisienne θ telle que $Z(\theta, x, F) = Z(\varphi, x, F)$, pour tout point fermé x de S, et tout corps F contenant $\mathbb{F}_x$.

Réciproquement, on peut démontrer (cf. [18, Nicaise], paragraphe 3.3) que l'on peut associer à toute formule galoisienne θ sur S une formule du langage des anneaux φ, telle que $Z(\theta, x, F) = Z(\varphi, x, F)$, pour tout point fermé x de S, et tout corps F contenant $\mathbb{F}_x$.

Ainsi, on ne modifie pas la classe des ensembles définissables en considérant des formules galoisiennes à la place des formules du premier ordre dans le langage des anneaux. L'avantage de ce nouveau formalisme est qu'il vérifie une propriété d'élimination des quantificateurs, que l'on va maintenant expliquer.

10.2 Elimination des quantificateurs pour les formules galoisiennes

On garde les notations et les hypothèses du paragraphe précédent. Nous allons prouver, suivant Fried et Sacerdote, dans ce paragraphe et les suivants, le résultat annoncé d'élimination des quantificateurs. Soyons plus précis. Soit $\mathfrak{A}$ une stratification galoisienne de A, sous-schéma localement fermé de $\mathbb{A}^n$, $\mathfrak{A} \to \mathbb{A}^n_{\mathcal{O}_K}$. On considère une formule du type

$$(Q_1 x_1) \dots (Q_n x_n)[\mathrm{Fr}(x_1, \dots, x_n) \in \bigcup_{X \in \mathfrak{S}(A)} \mathrm{Con}(X)].$$

On peut évidemment, par récurrence, se ramener au cas où l'on a un seul quantificateur. Il nous faut donc trouver une stratification galoisienne notée $pr(\mathfrak{A})$, d'espace sous-jacent $\mathrm{pr}_{n-1}(A)$ (où pr_{n-1} désigne la projection sur les n premières coordonnées), telle que

$$Q_n x_n[\mathrm{Fr}(x_1, \dots, x_n) \in \bigcup_{X \in \mathfrak{S}(A)} \mathrm{Con}(X)] \iff [\mathrm{Fr}(x_1, \dots, x_{n-1}) \in \bigcup_{Y \in \mathfrak{S}(\mathrm{pr}_{n-1}(A))} \mathrm{Con}(Y)].$$

avec $(x_1, \dots, x_{n-1}) \in \mathbb{A}^n_{\mathcal{O}_K/\mathfrak{p}}$, pour tout $\mathfrak{p}$ idéal premier de $\mathcal{O}_K[1/\alpha(pr(\mathfrak{A}))]$, avec $\alpha(pr(\mathfrak{A}))$ à choisir ultérieurement.

Dans cette optique, le théorème clé est le suivant. Comme la preuve en est longue et technique, nous la reportons pour le moment au paragraphe suivant.

Théorème 10.3. *Soit $C(A) \to A$ un revêtement K-irréductible de A, avec A sous-schéma localement fermé de $\mathbb{A}^n_{\mathcal{O}_k}$. Il existe une stratification galoisienne incolore $\mathfrak{S}'(\mathrm{pr}_{n-1}(A))$, telle que, pour tout $Y \in \mathfrak{S}'(\mathrm{pr}_{n-1}(A))$, et tout point $y \in Y$ de degré 1 (i.e. y vit au-dessus de l'idéal maximal $\mathfrak{m}$ de $\mathcal{O}_K$ et est un $\mathcal{O}_K/\mathfrak{m}$-point de $Y_{\mathfrak{m}}$), le type de $IU(A_y, \mathcal{O}_K/\mathfrak{m})$ ne dépend que de $\mathrm{Fr}(y)$ (où A_y est équipé de la restriction du revêtement $C(A)$ à A_y).*

Le lecteur aura sûrement deviné que la stratification galoisienne obtenue est celle recherchée. Toutefois, il s'agit seulement d'une stratification galoisienne incolore ; il faut donc encore choisir le coloriage. Ce choix dépendra évidemment de la nature du quantificateur Q_n.

Fixons quelques notations. Soit W un sous-schéma localement fermé et absolument irréductible de $\mathbb{A}^n_k$, avec k un corps fini. Soit $C(W) \to W$ un revêtement k-irréductible. On note $\hat{k}$ la clôture algébrique de k dans $k(C(W))$, et $\hat{G}$ le sous-ensemble de $G = \mathrm{Gal}((C(W)/W)$, formé des $\sigma \in G$ tels que l'action de σ^* sur $k(C(W))$, en restriction à $\hat{k}$, coïncide avec celle du Frobenius. Soient alors, avec les hypothèses et notations du théorème, $Y \in \mathfrak{S}'(\mathrm{pr}_{n-1}(A))$, et $\sigma \in \mathrm{Gal}(C(Y)/Y)$. Nous dirons que la classe de conjugaison $\mathrm{Con}(\sigma)$ de σ satisfait

- *le cas 1* si : pour tout point $y \in Y$ avec $\mathrm{Fr}(y) = \mathrm{Con}(\sigma)$, $IU(A_y, \mathcal{O}_K/\mathfrak{m})$ est non vide et $\mathrm{Con}(M) \cap \hat{G}(C(M)/M)$ est non vide pour un certain élément M de la stratification induite sur $IU(A_y, \mathcal{O}_K/\mathfrak{m})$.
- *le cas 2* si : pour tout point $y \in Y$ avec $\mathrm{Fr}(y) = \mathrm{Con}(\sigma)$, $IU(A_y, \mathcal{O}_K/\mathfrak{m})$ a pour espace sous-jacent la fibre tout entière de $\mathbb{A}^n \to \mathbb{A}^{n-1}$ au-dessus de y), et $\mathrm{Con}(M)$ contient $\hat{G}(C(M)/M)$ pour tout élément M de la stratification galoisienne induite sur $IU(A_y, \mathcal{O}_K/\mathfrak{m})$.

D'après la proposition, l'une de ces conditions est satisfaite par tous les y de degré 1 tels que $\mathrm{Fr}(y) = \mathrm{Con}(\sigma)$ si elle l'est pour l'un d'entre eux.

Revenons alors au problème initial. On considère donc une formule du type

$$(Q_1 x_1) \dots (Q_n x_n)[\mathrm{Fr}(x_1, \dots, x_n) \in \bigcup_{X \in \mathfrak{S}(A)} \mathrm{Con}(X)].$$

Il nous faut donc trouver une stratification galoisienne notée $pr(\mathfrak{A})$, d'espace sous-jacent $\mathrm{pr}_{n-1}(A)$, telle que

$$Q_n x_n[\mathrm{Fr}(x_1,\dots,x_n) \in \bigcup_{X\in\mathfrak{S}(A)} \mathrm{Con}(X)] \iff [\mathrm{Fr}(x_1,\dots,x_{n-1}) \in \bigcup_{Y\in\mathfrak{S}(\mathrm{pr}_{n-1}(A))} \mathrm{Con}(Y)].$$

avec $(x_1,\dots,x_{n-1}) \in \mathbb{A}^n_{\mathcal{O}_K/\mathfrak{p}}$, pour tout $\mathfrak{p}$ idéal premier de $\mathcal{O}_K[1/\alpha(pr(\mathfrak{A}))]$. Comme on l'a déjà dit, la stratification galoisienne que l'on va considérer est celle procurée par le théorème 10.3. Il reste à définir le coloriage. On procède de la façon suivante :

- Si $Q_n = \exists$: pour $Y \in \mathfrak{S}'(\mathrm{pr}_{n-1}(A))$, on définit $\mathrm{Con}(Y)$ comme l'union des classes de conjugaison $\mathrm{Con}(\sigma)$, $\sigma \in \mathrm{Gal}(C(Y)/Y)$, avec $\mathrm{Con}(\sigma)$ satisfaisant le cas 1.
- Si $Q_n = \forall$: pour $Y \in \mathfrak{S}'(\mathrm{pr}_{n-1}(A))$, on définit $\mathrm{Con}(Y)$ comme l'union des classes de conjugaison $\mathrm{Con}(\sigma)$, $\sigma \in \mathrm{Gal}(C(Y)/Y)$, avec $\mathrm{Con}(\sigma)$ satisfaisant le cas 2.

On a donc sous la main une nouvelle stratification galoisienne, que l'on note $pr(\mathfrak{A})$. Voyons si elle convient.

Notons $y = (x_1,\dots,x_{n-1}) \in \mathrm{pr}_{n-1}(A)$ un point de degré 1 au-dessus de l'idéal premier $\mathfrak{p}$, avec $\mathfrak{p}$ idéal premier de $\mathcal{O}_K$. Il existe un unique $Y \in \mathfrak{S}(\mathrm{pr}_{n-1}(A))$. Traitons le cas du quantificateur existentiel. Dire qu'il existe x_n tel que $\mathrm{Fr}(x_1,\dots,x_n) \in \cup_{X\in\mathfrak{S}(A)}\mathrm{Con}(X)$ implique que si $\mathrm{Con}(\sigma) = \mathrm{Fr}(y)$, $\mathrm{Con}(\sigma)$ satisfait le cas 1. En effet, identifions x_n à un point de $IU(A_y, \mathcal{O}_K/\mathfrak{p})$, disons $x_n \in M$, et $\mathrm{Fr}(x_1,\dots,x_n)$ à une classe de conjugaison de $C(M)/M$ par restriction de $C(X)$ (pour X contenant $(x_1,\dots,x_n)$) à la fibre A_y. Via cette identification, la restriction de $\mathrm{Fr}(x_1,\dots,x_n)$ à $C(M) \to M$ est contenue dans l'intersection évoquée dans l'énoncé définissant le cas 1. Mais si l'on essaye de prouver que réciproquement, si dès que $\mathrm{Con}(\sigma) = \mathrm{Fr}(y)$, $\mathrm{Con}(\sigma)$ satisfait le cas 1, alors il existe x_n tel que $\mathrm{Fr}(x_1,\dots,x_n) \in \cup_{X\in\mathfrak{S}(A)}\mathrm{Con}(X)$, on est bloqué ! En effet, on sait qu'il existe $\mathrm{Con}(\tau)$ dans $\mathrm{Con}(M)\cap\hat{G}(C(M)/M)$, mais rien ne nous dit qu'il existe effectivement un élément $x_n \in M$ qui soit un $\mathcal{O}_K/\mathfrak{p}$-point et tel que $\mathrm{Fr}(x_1,\dots,x_n) = \mathrm{Con}(\tau)$, ne serait-ce que parce que la fibre A_y peut n'avoir aucun point $\mathcal{O}_K/\mathfrak{p}$-rationnel !

On voit bien que cette première approche était trop brutale : il n'y a pas de raison a priori pour que nos deux formules soient équivalentes pour *tout* idéal premier de $\mathcal{O}_K$... C'est ici qu'intervient un deuxième résultat crucial, énoncé par la proposition. Il va nous permettre de déterminer la constante $\alpha(pr(\mathfrak{A}))$ évoquée plus haut et d'éliminer un nombre fini d'idéaux premiers qui posent problème.

Soit W un sous-schéma localement fermé et absolument irréductible de $\mathbb{A}^n_k$, avec k un corps fini. Soit $C(W) \to W$ un revêtement k-irréductible. On note $B(\sigma)$, pour $\sigma \in \mathrm{Gal}((C(W)/W)$, l'ensemble des points $x \in W$ tels que $\mathrm{Con}(\sigma) = \mathrm{Fr}(x)$. On note enfin $\bar{W}$ l'adhérence de W dans $\mathbb{A}^n_k$.

Théorème 10.4. *Il existe une constante C, ne dépendant que du degré et de la dimension de W, de* $\deg(C(W)/W)$*, et du degré et de la dimension des composantes de $\bar{W} - W$, et telle que*

$$|B(\sigma) - \frac{|\mathrm{Con}(\sigma)|}{|\hat{G}|}.|k|^{\dim W}| < C.|k|^{\dim W - 1/2}.$$

Démonstration. Nous ne la donnons pas, et renvoyons à [8, Fried-Sacerdote]. Fried voit ce résultat comme un analogue non régulier du théorème de Chebotarev. □

C'est cette proposition qui justifie que l'on se soit ramené, par le procédé d'union-intersection, à considérer des schémas localement fermés *abolument irréductibles définis sur* $\mathcal{O}_K/\mathfrak{p}$.

Nous sommes désormais en mesure de démontrer l'existence de la constante $\alpha(pr(\mathfrak{A}))$. Pour cela, considérons M élément de la stratification induite sur $IU(A_y, \mathcal{O}_K/\mathfrak{m})$, comme dans les cas 1 et 2. La proposition 10.4 nous donne une constante $C(M,\sigma)$. Cette même proposition montre que la quantité $B(\sigma)$ est non nulle dès lors que

$$|k| \geq (\frac{C(M,\sigma).|\hat{H}(C,M)|}{|\mathrm{Con}(\sigma)|})^2 =: C'(M,\sigma).$$

Cette constante, d'après la proposition, ne dépend que du type de $IU(A_y, \mathcal{O}_K/\mathfrak{p})$, qui par 10.3, ne dépend lui-même que de $\mathrm{Fr}(y)$, élément du groupe fini $\mathrm{Gal}(C(Y)/Y)$, avec $C(Y) \to Y$ membre de la stratification galoisienne $\mathfrak{S}'(\mathrm{pr}_{n-1}(A))$. A τ dans $\mathrm{Gal}(T^{**}/K(Y))$ et $Y \in \mathfrak{S}'(\mathrm{pr}_{n-1}(A))$ fixés, on peut donc choisir $C''(Y,\tau)$ une constante supérieure ou égale à tous les $C'(M,\sigma)$, avec M dans la stratification galoisienne induite sur $IU(A_y, \mathcal{O}_K/\mathfrak{p})$. On choisit enfin D plus grand que $C''(Y,\tau)$, pour tout $Y \in \mathfrak{S}'(\mathrm{pr}_{n-1}(A))$ et tout $\tau \in \mathrm{Gal}(T^{**}/K(Y))$.

On choisit alors pour $\alpha(pr(\mathfrak{A}))$ un idéal divisible par tout idéal premier $\mathfrak{p}$ satisfaisant $|N_{K/\mathbb{Q}}(\mathfrak{p})| \leq D$, ou tel que $\mathfrak{p}$ n'est pas dans l'image de la flèche $Y \to \mathcal{O}_K$ (supposée dominante). Nous avons tous les éléments sous la main ; il ne reste donc plus qu'à vérifier que tout se recolle bien.

Reprenons la démonstration de l'équivalence dans le cas du quantificateur existentiel. On rappelle que $y = (x_1, \ldots, x_{n-1}) \in \mathrm{pr}_{n-1}(A)$ un point de degré 1 au-dessus de l'idéal premier $\mathfrak{p}$, avec $\mathfrak{p}$ idéal premier de $\mathcal{O}_K[1/\alpha(pr(\mathfrak{A}))]$. Il existe un unique $Y \in \mathfrak{S}(\mathrm{pr}_{n-1}(A))$. Dire qu'il existe x_n tel que $\mathrm{Fr}(x_1, \ldots, x_n) \in \cup_{X \in \mathfrak{S}(A)} \mathrm{Con}(X)$ équivaut à dire que si $\mathrm{Con}(\sigma) = \mathrm{Fr}(y)$, $\mathrm{Con}(\sigma)$ satisfait le cas 1. En effet, identifions x_n à un point de $IU(A_y, \mathcal{O}_K/\mathfrak{p})$, disons $x_n \in M$, et $\mathrm{Fr}(x_1, \ldots, x_n)$ à une classe de conjugaison de $C(M)/M$ par restriction de $C(X)$ (pour X contenant $(x_1, \ldots, x_n)$) à la fibre A_y. Via cette identification, la restriction de $\mathrm{Fr}(x_1, \ldots, x_n)$ à $C(M) \to M$ est contenue dans l'intersection évoquée dans l'énoncé définissant le cas 1. Réciproquement, vu le choix de $\alpha(pr(\mathfrak{A}))$, le théorème 10.4 nous assure, si l'on est dans le cas 1, qu'il existe $x_n \in M$ un $\mathcal{O}_K/\mathfrak{p}$-point, et tel que $\mathrm{Fr}(x_1, \ldots, x_n)$ se restreint en un élément de $\mathrm{Con}(M) \cap \hat{G}(C(M)/M)$.

Le cas du quantificateur universel se traite de façon tout à fait semblable. Modulo le théorème 10.3, le résultat est entièrement démontré. Nous le reformulons sous une forme différente, qui fait apparaître le lien avec les corps pseudo-finis.

Théorème 10.5. *Soient K un corps de nombres, $\mathfrak{A}$ une stratification galoisienne de $\mathbb{A}_k^{n+m}$, et θ une formule galoisienne*

$$(Q_1 X_1) \ldots (Q_m X_m)[Ar(X,Y) \subseteq \mathrm{Con}(\mathfrak{A})].$$

Alors il existe une stratification galoisienne $\mathfrak{B}$ de $\mathbb{A}_k^n$, telle que pour tout corps pseudo-fini F contenant k,

$$Z(\theta, \mathrm{Spec}(k), F) = Z(\mathfrak{B}, \mathrm{Spec}(k), F).$$

Démonstration. Nous allons exploiter le lien déjà vu entre formules du langage des anneaux et formules galoisiennes. Notons $\mathfrak{B}$ la stratification galoisienne de $\mathbb{A}_k^n$ que le travail effectué nous a permis de construire : pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K[1/a]$, pour un certain a, $Z(\theta, x, \mathcal{O}_K/\mathfrak{p}) = Z(\mathfrak{B}, x, F)$.

La remarque qui clôt le paragraphe 10.1.3 nous permet de trouver deux formules du premier ordre du langage des anneaux φ, ψ telles que pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, $Z(\theta, x, \mathcal{O}_K/\mathfrak{p}) =$

$Z(\varphi, x, \mathcal{O}_K/\mathfrak{p})$ et $Z(\mathfrak{B}, x, \mathcal{O}_K/\mathfrak{p}) = Z(\psi, x, \mathcal{O}_K/\mathfrak{p})$. Ainsi, pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K[1/a]$, $Z(\varphi, x, \mathcal{O}_K/\mathfrak{p}) = Z(\psi, x, \mathcal{O}_K/\mathfrak{p})$. Autrement dit, pour tout idéal premier de $\mathfrak{p}$ de $\mathcal{O}_K[1/a]$, $\mathcal{O}_K/\mathfrak{p} \vDash \forall \bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$. On note η la formule galoisienne associée à cette formule (remarque à la fin de 10.1.3), qui est donc sans variable libre. Soit ρ une formule galoisienne sans quantificateurs définissant les mêmes ensembles que η dans tout corps de la forme $\mathcal{O}_K/\mathfrak{p}$, $\mathfrak{p}$ idéal premier de $\mathcal{O}_K[1/a]$ (quitte à modifier a). L'intérêt de la formule ρ est qu'elle est *sans variable libre et sans quantificateur*. Soit $\mathfrak{A}$ la stratification galoisienne associée à ρ. Comme ρ est sans variable libre, $\mathfrak{A} \otimes k$ consiste simplement en un revêtement $\mathrm{Spec}(L) \to \mathrm{Spec}(k)$, avec L extension galoisienne de k.

Supposons qu'il existe un corps pseudo-fini F contenant k dans lequel ρ est fausse. Soit τ un générateur de $\mathrm{Gal}(\tilde{F}/F)$, σ sa restriction à L. Alors

$$Ar(\mathrm{Spec}(L)/\mathrm{Spec}(k), 0, F) = \{g\langle\sigma\rangle g^{-1}, g \in \mathrm{Gal}(L/k)\}.$$

Comme on a supposé ρ fausse dans F, on a $\langle\sigma\rangle \not\subseteq \mathrm{Con}(\mathfrak{A})$. Mais alors l'application du théorème de Chebotarev contredirait notre hypothèse... □

Corollaire 10.6. *Soit $\varphi(Y_1, \ldots, Y_n)$ une formule du premier ordre du langage des anneaux à coefficients dans un corps k, en les variables libres $Y_1, \ldots, Y_n$. Il existe une stratification galoisienne $\mathfrak{B}$ de $\mathbb{A}^n_k$, telle que pour tout corps pseudo-fini F contenant k,*

$$Z(\varphi, \mathrm{Spec}(k), F) = Z(\mathfrak{B}, \mathrm{Spec}(k), F).$$

Dans la suite de ce texte, nous *admettrons* que ces deux résultats restent valables quand K n'est plus seulement un corps de nombres, mais le corps des fractions d'un anneau intègre R de type fini sur $\mathbb{Z}$.

10.3 Une généralisation du théorème de Bertini-Noether

Ce dernier paragraphe est consacré à la démonstration du théorème 10.3, que nous avions admis.

Soit $\varphi : W \to V$ un morphisme de $\mathcal{O}_K$-schémas irréductibles comme K-schémas, tels que φ et $V \to \mathcal{O}_K$ soient dominants. Soit $\tilde{x}$ le point générique de V. Considérons la fibre générique $W_{\tilde{x}}$ du morphisme φ. Supposons $W_{\tilde{x}}$ absolument irréductible sur $K(\tilde{x})$. Par exemple, supposons que $V = \mathrm{Spec}(A)$, $W = \mathrm{Spec}(B)$ soient des variétés affines, avec B une A-algèbre, et $B = \mathcal{O}_K[X_1, \ldots, X_n]/I$, I idéal. Alors $K(\tilde{x})$ est le corps des fractions de B. Si Ω est une clôture algébrique du corps des fractions de B, notre hypothèse revient donc à dire que $\mathrm{Spec}(\Omega[X_1, \ldots, X_n]/I)$ est une Ω-variété irréductible.

Le théorème suivant est bien connu.

Théorème 10.7 (Bertini-Noether)**.** *Avec les mêmes notations et hypothèses, il existe un ouvert de Zariski non vide U de V tel que, pour tout point fermé $p \in U$, W_p est irréductible, vu comme variété sur le le spectre du corps résiduel en p,* $\mathrm{Spec}(k_p)$.

Démonstration. Contentons-nous de donner l'idée de la démonstration. On suppose pour simplifier (on pourrait se ramener à ce cas) que $W \to \mathbb{A}^{r+1} \times V$ est une famille d'hypersurfaces de $\mathbb{A}^{r+1}$. On peut aussi supposer $V = \mathrm{Spec}(R)$, avec $R = \mathcal{O}_K[Y_1, \ldots, Y_t]/J$, avec J un idéal de $\mathcal{O}_K[Y_1, \ldots, Y_t]$, et W définie par $g \in R[X_1, \ldots, X_{r+1}]$. Si p est un point fermé de V, notons g_p le polynôme obtenu en réduisant les coefficients de g modulo l'idéal premier de R correspondant

à p. On va montrer qu'il existe, pour tout l entre 1 et $\deg g - 1$, un ouvert non vide $U^{(l)}$ de V, tel que si p est un point fermé de $U^{(l)}$, g_p n'a pas de diviseur de degré l sur $\bar{k_p}$, une clôture algébrique de k_p. Une fois cela fait, il suffira de considérer l'ouvert $\cap_{l=1}^{\deg g-1} U^{(l)}$.

Soit f un polynôme sur un corps algébriquement clos Ω, en les variables $X_1, \ldots, X_{r+1}$, de même degré que g. Supposons que f se factorise $f = f_1 f_2$, avec $f_1 = \Sigma a_i Y^i$ de degré l, $f_2 = \Sigma b_i Y^i$. Si l'on fixe les b_i, les a_i sont solutions d'un système linéaire. L'algèbre linéaire élémentaire nous apprend alors que les b_i sont solutions d'un système d'équations polynomiales $\{P_1, \ldots, P_m\}$, dont les coefficients sont des polynômes en les coefficients de f. On déduit alors du Nulstellensatz qu'il existe une autre famille de polynômes, notée P', nuls une fois évalués en les coefficients des polynômes de P. Il existe donc une famille universelle P'' de polynômes en les coefficients de f qui sont nuls si et seulement si f a un facteur de degré l. Notons-la $P'' = \{Q_1, \ldots, Q_d\}$. Considérons le morphisme $\psi : V \to \mathbb{A}^d_R$, qui à $p \in V$ associe l'évaluation en les coefficients de g_p des Q_i. Par nos hypothèses, $\psi(\tilde{x}) \neq (0, \ldots, 0)$. Si V' est la fibre de V relativement à ψ au-dessus de l'origine de $\mathbb{A}^d_R$, $U^{(l)} = V - V'$ est l'ouvert cherché. Ceci achève la preuve du théorème. □

Le théorème 10.3 peut être vu comme une généralisation du théorème de Bertini-Noether. Nous le redonnons sous une forme plus commode : le premier point de l'énoncé qui suit servira simplement à prouver le second.

Théorème 10.8. (i) *Soit $A \to \mathcal{O}_K$ un sous-schéma constructible de $\mathbb{A}^n_{\mathcal{O}_K}$. Il existe une stratification galoisienne (incolore) $\mathfrak{S}(\mathrm{pr}_{n-1}(A))$ telle que pour tout $Y \in \mathfrak{S}(\mathrm{pr}_{n-1}(A))$, et tout point fermé y de Y de degré 1 (i.e. y vit au-dessus de l'idéal maximal $\mathfrak{m}$ de $\mathcal{O}_K$ et est un $\mathcal{O}_K/\mathfrak{m}$-point de $Y_{\mathfrak{m}}$), le type de $IU(A_y, \mathcal{O}_K/\mathfrak{p})$ ne dépend que de* $\mathrm{Fr}(y)$.

(ii) *Soit $C(A) \to A$ un revêtement K-irréductible de A, avec A sous-schéma localement fermé de $\mathbb{A}^n_{\mathcal{O}_k}$. Il existe une stratification galoisienne incolore $\mathfrak{S}'(\mathrm{pr}_{n-1}(A))$, telle que, pour tout $Y \in \mathfrak{S}'(\mathrm{pr}_{n-1}(A))$, et tout point $y \in Y$ de degré 1, le type de $IU(A_y, \mathcal{O}_K/\mathfrak{m})$ ne dépend que de* $\mathrm{Fr}(y)$ *(où A_y est équipé de la restriction du revêtement $C(A)$ à A_y).*

Démonstration. Montrons le premier point. On peut déjà, par hypothèse, partitionner A en sous-schémas localement fermés K-irréductibles. Si le théorème est démontré pour ces sous-schémas, il le sera pour A en recollant les stratifications obtenues. On peut donc supposer que A est un sous-schéma localement fermé de $\mathbb{A}^n_{\mathcal{O}_k}$.

Partitionnons $\mathrm{pr}_{n-1}(A)$ en sous-schémas localement fermés K-irréductibles (théorème de Chevalley). On note cette stratification $\mathfrak{S}_1$. Soit $Y \in \mathfrak{S}_1$, $K(Y) = K(y_{gen})$ le corps des fonctions de Y (avec y_{gen} un point générique de Y). Notons $A_{y_{gen}}$ la fibre de $A|_Y \to Y$ au-dessus du point générique de Y. Soit T^*_Y le corps $T^*(IU(A_{y_{gen}}, K(Y))$ obtenu par le procédé d'union-intersection décrit en 10.1.2. Alors T^*_Y est une extension galoisienne de $K(Y)$. Pour tout $\sigma \in \mathrm{Gal}(T^*_Y/K(Y))$, le procédé d'union intersection nous donne une famille de variétés absolument irréductibles, définies sur T^*_Y.

L'extension galoisienne $T^*_Y/K(Y)$ permet, comme expliqué dans le premier paragraphe de cette section, de construire un revêtement $C(Z) \to Z$ d'un ouvert de Zariski Z de Y défini sur K. Si $\sigma \in \mathrm{Gal}(C(Z)/Z)$, on peut considérer $C(Z) \to C^{(\sigma)}(Z) \to Z$, où $C(Z) \to C^{(\sigma)}(Z)$ est un revêtement de groupe de Galois engendré par σ (dernier théorème de l'annexe 2). Soit $A|_{C^{(\sigma)}(Z)} \to C^{(\sigma)}(Z)$ le pullback de A au-dessus de $C^{(\sigma)}(Z)$. Soient z un point fermé de Z de degré 1, z' un point de $C^{(\sigma)}(Z)$ au-dessus de z, et z'' un point de $C(Z)$ au-dessus de z'. On va montrer maintenant que quitte à remplacer Z par un ouvert de Z, encore noté Z, on a l'égalité,

pour $\sigma = \mathrm{Fr}(z'')$ et $\mathfrak{p}$ l'idéal premier de $\mathcal{O}_K$ en dessous de z :

$$(IU(A_{y_{gen}}, K(Y), \sigma))_{z''} = IU((A|_{C^{(\sigma)}(Z)})_{z'}, \mathcal{O}_K/\mathfrak{p}). \quad (*)$$

On verra plus bas que (*) montre que pour $z \in Z$ donné comme ci-dessus, le type du membre de droite de l'égalité ne dépend que de la classe de conjugaison de σ.

Avec un léger abus de notation, notons $W_{\sigma,y_{gen}}$ l'une des variétés apparaissant lors de l'éxécution de l'algorithme d'union-intersection pour construire $IU(A_{y_{gen}}, K(Y), \sigma)$. Les coefficients des polynômes définissant cette variété engendrent un corps M au-dessus de $K(C^{(\sigma)}(Z))$. D'où des flèches $C(Z) \to C' \to C^{(\sigma)}(Z)$, avec $K(C') = M$. On peut donc voir $W_{\sigma,y_{gen}}$ comme la fibre générique d'un morphisme $\varphi_\sigma : W_\sigma \to C'$. On va en fait construire Z en demandant un peu plus que la condition (*). Nous souhaitons que pour tout σ et tout W_σ comme ci-dessous :

(i) φ_σ ait des fibres de dimension constante ;

(ii) le degré des fibres géométriques de φ_σ soit constant ;

(iii) si $\tilde{z} \in C'$ vit au-dessus de $z' \in C^{(\sigma)}(Z)$, le corps engendré par les coefficients des polynômes définissant $(W_\sigma)_{\tilde{z}}$ (en tant qu'extension de $\mathcal{O}_K[C^{(\sigma)}(Z)]/\mathfrak{p}(z')$) soit $\mathcal{O}_K[C']/\mathfrak{p}(\tilde{z})$.

Supposons que pour chaque $Y \in \mathfrak{S}_1$, un tel ouvert non vide Z ait été choisi. La conclusion du premier point du théorème sera alors vérifiée pour un sous-ensemble constructible Y' de $\mathrm{pr}_{n-1}(A)$, avec $\mathrm{pr}_{n-1}(A) - Y'$ de dimension strictement inférieure à celle de $\mathrm{pr}_{n-1}(A)$. En procédant par récurrence sur la dimension des éléments de $\mathfrak{S}_1$, on pourra considérer la restriction de $A \to \mathrm{pr}_{n-1}(A)$ au complémentaire de Y dans $\mathrm{pr}_{n-1}(A)$ et former une stratification satisfaisant aux conditions du premier point du théorème, en appliquant l'hypothèse de récurrence.

Notons pour commencer qu'en vertu du théorème de platitude générique, il existe $f \in \mathcal{O}_K[Z]$, tel que si $Z^* = \mathrm{Spec}(\mathcal{O}_K[Z, 1/f])$, $\varphi_\sigma|_{Z^*} : W_\sigma|_{Z^*} \to C'|_{Z^*}$ est plat. En particulier, la dimension des fibres de ce morphisme est constante. On peut aussi montrer que dans ce cas le degré des fibres géométriques l'est aussi (admis). Quitte à remplacer Z par Z^*, on peut donc satisfaire à (i) et (ii).

Pour vérifier (iii), on commence par écrire $K(C') = K(C^{(\sigma)}(Z), a))$ pour un certain a (théorème de l'élément primitif). Alors, $\mathrm{Spec}(\mathcal{O}_K[C^{(\sigma)}(Z)][X]/(f(X)))$ (f polynôme minimal de a sur $\mathcal{O}_K[C^{(\sigma)}(Z)]$) est isomorphe à $\mathrm{Spec}(\mathcal{O}_K[C'])$ hors du lieu d'annulation du discriminant de f. Donc, quitte à remplacer à nouveau Z par un ouvert de Zariski, on peut aussi supposer qu'on a (iii).

Tout ceci nous permet d'affirmer que les dimensions et les degrés du membre de gauche (et donc du membre de droite) de (*) ne dépendent que de σ. Le théorème de Bertini-Noether permet de remplacer Z par un ouvert de Z encore noté Z, tel que $(W_\sigma)_{\tilde{z}}$ est absolument irréductible, vue comme variété sur $\mathcal{O}_K[C']/\mathfrak{p}(\tilde{z})$, pour $\tilde{z} \in C'$ au-dessus de $z \in Z$ de degré 1. Pour Z satisfaisant toutes ces propriétés, on est certain que $(W_\sigma)_{\tilde{z}}$ n'est pas définie sur un sous-corps propre de $\mathcal{O}_K[C']/\mathfrak{p}(\tilde{z})$. Cela clôt la preuve du premier point du théorème.

Montrons le deuxième point. On note $\mathfrak{S}(\mathrm{pr}_{n-1}(A))$ la stratification de A obtenue lors de la preuve du premier point. Pour $Y \in \mathfrak{S}(\mathrm{pr}_{n-1}(A))$, on va construire Y' sous-schéma ouvert de Y et un revêtement $C(Y') \to Y'$, tel que pour tout point fermé y de Y' de degré 1, le type de $IU(A_y, \mathcal{O}_K/\mathfrak{p})$ équipé du revêtement induit par la restriction à la fibre A_y de $C(A)$, ne dépende que de $\mathrm{Fr}(y)$. On pourra conclure alors par récurrence sur la dimension, puisque les Y construits dans la preuve qui précède sont des sous-schémas localement fermés K-irréductibles. On donne juste l'idée de la fin de la preuve, qui est assez similaire à celle du premier point. La seule chose de plus à faire est de s'assurer, avec le théorème de Bertini-Noether, que l'on peut aussi obtenir par spécialisation les composantes absolument irréductibles de la restriction

de $C(A)$ à l'élément de $IU(A_z, \mathcal{O}_K/\mathfrak{p})$ correspondant, par ce qu'on a fait avant, à $W_{\sigma,y_g en}$ (par cette même spécialisation). □

11 Vers l'intégration motivique arithmétique

L'intégration motivique a été introduite pour la première fois par Kontsevitch en 1995, qui cherchait à donner sens à des intégrales sur les $\mathbb{C}[[t]]$-points de variétés algébriques. Auparavant, Batyrev avait déjà obtenu des résultats pour des variétés complexes par des considérations d'intégration p-adique. Il y a là (a posteriori !) pour le théoricien des modèles autre chose qu'une coïncidence (que l'on pense par exemple au théorème d'Ax sur les applications polynomiales). Et l'on va voir qu'en effet, la théorie de l'intégration motivique fournit des résultats de "transfert" dans cet esprit.

Notre but ici n'est pas de présenter un panorama satisfaisant des diverses théories existantes rassemblées sous le nom générique "d'intégration motivique". Cela dépasserait le niveau de cet exposé et les connaissances de ses auteurs... Nous avons choisi d'exposer, souvent sans preuve, l'intégration motivique dite arithmétique, développée par J. Denef et F. Loeser dans [5, Denef-Loeser]. La théorie des corps pseudo-finis y tient une bonne place.

La rédaction s'inspire de [5, Denef-Loeser], ainsi que de [6, Denef-Loeser] et [13, Hales].

11.1 Des formules aux motifs

11.1.1 L'anneau de Grothendieck des motifs de Chow

Nous nous contenterons du strict minimum sur les motifs. Ces objets occupent une place majeure dans différentes théories très profondes.

Soit k un corps. On note $K_0(\mathrm{Sch}_k)$ l'anneau de Grothendieck des variétés algébriques sur k. C'est l'anneau engendré par les symboles $[X]$, pour X k-variété, avec les relations $[X] = [X']$ si X et X' sont isomorphes, $[X] = [X \backslash X'] + [X']$ si X' est fermé dans X, $[X \times X'] = [X].[X']$. On note $\mathbb{L} = \mathbb{A}^1_k$, et $K_0(\mathrm{Sch}_k)_{loc} = K_0(\mathrm{Sch}_k)[\mathbb{L}^{-1}]$. L'introduction de cet objet est assez naturel : lorsque l'on calcule des intégrales (au sens usuel) simples sur $\mathbb{F}_q[[t]]$ (par exemple), on se retrouve avec des sommes de puissances de q ou de q^{-1}. Le motif de Lefschetz $\mathbb{L}$ est le symbole par lequel on aimerait remplacer q dans les formules précédentes, dans le cas général.

On note Mot_k la catégorie semi-abélienne des motifs de Chow sur k, à coefficients dans $\mathbb{Q}$. On note $K_0(\mathrm{Mot}_k)$ son groupe de Grothendieck. On peut identifier les objets de Mot_k aux triplets (X, p, n), avec X une variété propre et lisse sur k, p une correspondance idempotente sur X à coefficients dans $\mathbb{Q}$, $n \in \mathbb{Z}$. Le produit tensoriel sur Mot_k induit un produit sur $K_0(\mathrm{Mot}_k)$, ce qui en fait un anneau. De même, on définit $\mathrm{Mot}_{k,\bar{\mathbb{Q}}}$ la catégorie des motifs de Chow sur k à coefficients dans $\bar{\mathbb{Q}}$ et $K_0(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})$ son groupe de Grothendieck.

11.1.2 Motifs et actions de groupes

Soit k un corps de caractéristique nulle. Soit G un groupe fini. Soit X une variété définie sur k munie d'une action de G. On dit que X est une G-variété si la G-orbite de tout point fermé de X est contenue dans un sous-schéma ouvert affine de X. On définit de façon usuelle immersions fermées et isomorphismes entre G-variétés, et on définit donc à bon droit $K_0(\mathrm{Sch}_k, G)$, l'anneau de Grothendieck des G-variétés sur k. Soit α le caractère d'une représentation de dimension finie de G définie sur $\bar{\mathbb{Q}}$. On note $R_{\bar{\mathbb{Q}}(G)}$ le groupe des caractères des représentations virtuelles de G

définies sur $\bar{\mathbb{Q}}$. Dans leurs travaux, Gillet, Soulé ([10, Gillet-Soulé]), Guillén et Navarro Aznar ([11, Guillén-Navarro Aznar]) ont construit, pour tout $\alpha \in R_{\bar{\mathbb{Q}}(G)}$, un morphisme d'anneaux $\chi_c(.,\alpha) : K_0(\mathrm{Sch}_k, G) \to K_0(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})$, tel que si X est une G-variété fixée, $\alpha \to \chi_c(X,\alpha)$ soit un morphisme de groupes, et uniquement déterminé par certaines propriétés "naturelles". On note

$$\chi_c(X) = \sum_\alpha n_\alpha \chi_c(X,\alpha)$$

où α décrit l'ensemble des caractères irréductibles de G, et n_α la dimension de la représentation associée à α. Nous ne détaillerons par les propriétés de χ_c ; notons seulement la propriété de compatibilité suivante : si H est un sous-groupe de G, α un caractère de H, X une G-variété,

$$\chi_c(X, \mathrm{Ind}_H^G \alpha) = \chi_c(X,\alpha),$$

où l'on voit X comme une H-variété dans le membre de droite. L'intérêt de ce résultat est le suivant. Notons $C(G,\bar{\mathbb{Q}})$ le $\bar{\mathbb{Q}}$-espace vectoriel des fonctions centrales sur G à valeurs dans $\bar{\mathbb{Q}}$, et $C(G,\mathbb{Q})$ le $\mathbb{Q}$-espace vectoriel des combinaisons linéaires rationnelles des caractères des représentations $\mathbb{Q}$-irréductibles de G définies sur $\mathbb{Q}$. On définit par linéarité, pour tout $W \in K_0(\mathrm{Sch}_k, G)$, une application linéaire $\alpha \to \chi_c(W,\alpha)$, de $C(G,\bar{\mathbb{Q}})$ dans $K_0(\mathrm{Mot}_{k,\bar{\mathbb{Q}}}) \otimes \bar{\mathbb{Q}}$ (écrire une fonction centrale comme combinaison linéaire de caractères irréductibles). Si maintenant $\alpha \in C(G,\mathbb{Q})$, un théorème d'Artin assure que α est combinaison linéaire à coefficients dans $\mathbb{Q}$ de caractères de la forme $\mathrm{Ind}_H^G 1_H$, H sous-groupe cyclique de G. C'est ici qu'intervient la propriété citée : elle nous dit que si X est une G-variété,

$$\chi_c(X, \mathrm{Ind}_H^G 1_H) = \chi_c(X, 1_H) = \chi_c(X/H).$$

Par conséquent, pour tout $\alpha \in C(G,\mathbb{Q})$, pour tout $W \in K_0(\mathrm{Sch}_k, G)$, $\chi_c(W,\alpha)$ appartient à l'image de l'application linéaire $K_0(\mathrm{Sch}_k) \otimes \mathbb{Q} \to K_0(\mathrm{Mot}_{k,\bar{\mathbb{Q}}}) \otimes \mathbb{Q}$ induite par χ_c, image que nous noterons $K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}$.

Résumons les résultats obtenus dans une proposition.

Proposition 11.1. *Soit G un groupe fini. Pour toute fonction centrale $\alpha \in C(G,\mathbb{Q})$, pour tout $W \in K_0(\mathrm{Sch}_k, G)$, le motif virtuel $\chi_c(W,\alpha)$ appartient à l'image de l'application linéaire $K_0(\mathrm{Sch}_k) \otimes \mathbb{Q} \to K_0(\mathrm{Mot}_{k,\bar{\mathbb{Q}}}) \otimes \mathbb{Q}$ induite par χ_c, notée $K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}$.*

11.1.3 Stratifications galoisiennes et motifs

Ceci va nous permettre d'associer un motif virtuel à une stratification galoisienne. Soit tout d'abord A un schéma sur k, $C \to A$ un revêtement (fini étale galoisien, comme toujours) de groupe de Galois G, et Con une famille stable par conjugaison de sous-groupes de G. On considère sur G la fonction centrale α_{Con} définie par : $\alpha_{\mathrm{Con}}(x) = 1$ si le sous-groupe engendré par x appartient à Con, 0 sinon. De toute évidence, $\alpha_{\mathrm{Con}} \in C(G,\mathbb{Q})$, et la proposition précédente permet de lui associer

$$\chi_c(C/A, \mathrm{Con}) := \chi_c(C, \alpha_{\mathrm{Con}}) \in K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}.$$

Si X est un schéma sur k, et $\mathfrak{A}$ une stratification galoisienne de X, on définit (avec les notations habituelles)

$$\chi_c(\mathfrak{A}) := \sum_i \chi_c(C_i/A_i, \mathrm{Con}(A_i)).$$

On vérifie que si $\mathfrak{A}$ et $\mathfrak{B}$ sont deux stratifications galoisiennes d'un schéma X sur $S = \mathrm{Spec}(R)$, telles qu'il existe $f \in R$ non nul, tel que pour tout point fermé de S_f, l'on ait $Z(\mathfrak{A}, x, \mathbb{F}_x) = Z(\mathfrak{B}, x, \mathbb{F}_x)$, alors

$$\chi_c(\mathfrak{A} \otimes k) = \chi_c(\mathfrak{B} \otimes k).$$

En effet, on se ramène facilement à montrer que si A est un schéma sur S, $C \to A$, $C' \to A$ deux revêtements de groupes de Galois G et G', avec des familles de sous-groupes respectifs stables par conjugaison Con et Con$'$, vérifiant : il existe $f \in R - \{0\}$, tel que pour tout point fermé x de S_f et tout point fermé y de A_x, $Ar(C/A, x, y) \subseteq \mathrm{Con}$ si et seulement si $Ar(C'/A, x, y) \subseteq \mathrm{Con}'$, alors

$$\chi_c(C \otimes k, \alpha_{\mathrm{Con}}) = \chi_c(C' \otimes k, \alpha_{\mathrm{Con}'}).$$

Mais cela signifie exactement qu'il existe $f \in R - \{0\}$, tel que pour tout point fermé x de S_f et tout point fermé y de A_x,

$$\alpha_{\mathrm{Con}}(\mathrm{Fr}(y)) = \alpha_{\mathrm{Con}'}(\mathrm{Fr}(y)),$$

et on conclut avec le théorème de Chebotarev.

11.1.4 Formules du langage des anneaux et motifs

Nous passons à la dernière étape de cette première construction. Nous sommes désormais en mesure d'associer un motif virtuel à une formule φ du premier ordre du langage des anneaux, à coefficients dans k, en les variables libres $X_1, \ldots, X_n$. Pour cela, on suppose dans un premier temps que k est le corps des fractions d'un anneau R intègre de type fini sur $\mathbb{Z}$ (k est toujours supposé de caractéristique nulle). Par le corollaire 10.6, on peut associer à φ une stratification galoisienne $\mathfrak{A}$ de $\mathbb{A}^n_{S_f}$ ($S = \mathrm{Spec}(R)$, $f \in R$ non nul), telle que pour tout point fermé de S_f,

$$Z(\varphi, x, \mathbb{F}_x) = Z(\mathfrak{A}, x, \mathbb{F}_x).$$

La stratification $\mathfrak{A} \otimes k$ n'est pas attachée canoniquement à φ. Mais ce qu'on a dit juste au-dessus assure que le choix de la stratification galoisienne satisfaisant à l'égalité ci-dessus n'a pas d'importance. On est donc autorisé à définir

$$\chi_c(\varphi) := \chi_c(\mathfrak{A} \otimes k) \in K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}.$$

On vérifie que si k' est une extension de k qui est encore de type fini sur $\mathbb{Q}$, et si $\varphi \otimes k'$ désigne la formule φ vue comme formule à coefficients dans k', on a simplement : $\chi_c(\varphi \otimes k') = \chi_c(\varphi) \otimes k'$.

Par conséquent, χ_c se comporte bien relativement aux extensions de corps. On peut donc maintenant donner une définition en toute généralité. Soit k un corps de caractéristique nulle, φ une formule du premier ordre du langage des anneaux, à coefficients dans k. On se donne un sous-corps k_0 de k de type fini sur $\mathbb{Q}$ tel que l'on puisse voir φ comme une formule φ_0 du premier ordre du langage des anneaux à coefficients dans k_0, et l'on pose

$$\chi_c(\varphi) = \chi_c(\varphi_0) \otimes k.$$

Ce qui précède garantit que le choix de k_0 est indifférent, et tout ceci a donc un sens.

Soient φ et φ' deux formules du langage des anneaux, à coefficients dans k, en les variables libres $X_1, \ldots, X_n$ et $X_1, \ldots, X_m$. On écrit $\varphi \equiv_{\mathrm{Psf}_k} \varphi'$, ou plus simplement $\varphi \equiv \varphi'$, s'il existe une formule ψ du langage des anneaux à coefficients dans k, en les variables libres $X_1, \ldots, X_{n+m}$,

telle que pour tout corps pseudo-fini F contenant k, $Z(\psi, \mathrm{Spec}(k), F)$ est le graphe d'une bijection entre $Z(\varphi, \mathrm{Spec}(k), F)$ et $Z(\varphi', \mathrm{Spec}(k), F)$. On peut démontrer que si $\varphi \equiv \varphi'$, $\chi_c(\varphi) = \chi_c(\varphi')$. Nous ne donnons pas la preuve car elle est assez longue. Remarquons simplement que si $\varphi \equiv_{\mathrm{Psf}_k} \varphi'$, alors $\varphi \equiv_{\mathrm{Psf}_{k_0}} \varphi'$, pour un certain sous-corps k_0 de k, de type fini sur $\mathbb{Q}$ (une fois que l'on sait cela, on se ramène à raisonner sur les stratifications, un peu comme on l'a fait à la fin du paragraphe précédent). Pour cela, on raisonne par l'absurde. On note Σ l'ensemble des corps de type fini sur $\mathbb{Q}$, sous-corps de k, et contenant les constantes de φ, φ' et ψ : $\Sigma = \{k_i, i \in I\}$. On suppose que pour tout $i \in I$, il existe F_i pseudo-fini contenant k_i tel que $Z(\psi, \mathrm{Spec}(k), F_i)$ n'est pas le graphe d'une bijection entre $Z(\varphi, \mathrm{Spec}(k), F_i)$ et $Z(\varphi', \mathrm{Spec}(k), F_i)$. On choisit $\mathcal{F}$ un ultrafiltre sur I contenant $S_i = \{j, k_i \subseteq k_j\}$ pour tout $i \in I$. On note F l'ultraproduit des F_i relativement à $\mathcal{F}$. Par le théorème de Los, F est un corps pseudo-fini tel que $Z(\psi, \mathrm{Spec}(k), F)$ n'est pas le graphe d'une bijection entre $Z(\varphi, \mathrm{Spec}(k), F)$ et $Z(\varphi', \mathrm{Spec}(k), F)$. L'application qui à $a \in k$ associe (a_i) modulo $\mathcal{F}$, avec $a_i = a$ si $a \in k_i$, $a_i = 0$ sinon, est un plongement de k dans F. En effet, si $a \in k$ s'envoie sur 0 (avec $a \neq 0$) l'ensemble $\{i \in I, a \notin k_i\} \in \mathcal{F}$ (par définition). Mais si l'on choisit $i \in I$ tel que $a \in k_i$ (c'est évidemment possible), alors on sait aussi que $S_i \in \mathcal{F}$ par choix de $\mathcal{F}$. Or ces deux ensembles sont disjoints, d'où la contradiction : nécessairement, $a = 0$. Cela contredit le fait que $\varphi \equiv_{\mathrm{Psf}_k} \varphi'$.

La proposition suivante n'est pas difficile.

Proposition 11.2. *L'application $\chi_c : \mathrm{Form}_k \to K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}$ (Form_k est l'ensemble des formules du langage des anneaux à coefficients dans k) vérifie les propriétés suivantes :*

– *Soient φ, φ' des formules. Alors*

$$\chi_c(\varphi \vee \varphi') = \chi_c(\varphi) + \chi_c(\varphi') - \chi_c(\varphi \wedge \varphi').$$

– *Soient φ, φ' des formules. On note $\varphi \times \varphi'$ la formule obtenue en donnant des noms différents aux variables libres de φ et de φ', et en prenant la conjonction des deux formules. Alors*

$$\chi_c(\varphi \times \varphi') = \chi_c(\varphi)\chi_c(\varphi').$$

– *Si φ a n variables libres,*

$$\chi_c(\neg\varphi) = \mathbb{L}^n - \chi_c(\varphi).$$

Si $\mathcal{L}$ est un langage du premier ordre, T une théorie du langage $\mathcal{L}$, nous noterons $K_0(T)$ le quotient du groupe abélien libre engendré par les symboles $[\varphi]$, pour φ formule de $\mathcal{L}$, par le sous-groupe engendré par les relations suivantes :

– Si φ et φ' sont des formules de $\mathcal{L}$, et si $\varphi \equiv_T \varphi'$, i.e. si

$$T \vDash [\forall x(\varphi(x) \to \exists! x' : (\varphi'(x') \wedge \psi(x, x')))] \wedge [\forall x'(\varphi'(x') \to \exists! x : (\varphi(x) \wedge \psi(x, x')))],$$

alors $[\varphi] = [\varphi']$.

– Si φ et φ' sont des formules de $\mathcal{L}$, $[\varphi \vee \varphi'] = [\varphi] + [\varphi'] - [\varphi \wedge \varphi']$.

On munit $K_0(T)$ d'une structure d'anneau en posant

$$[\varphi].[\varphi'] = [\varphi \times \varphi'],$$

pour φ et φ' formules de $\mathcal{L}$. L'introduction de cet objet permet de résumer en un seul énoncé les résultats obtenus.

Théorème 11.3. *Soit k un corps de caractéristique nulle. Soit $\mathcal{L}$ le langage des anneaux et* Psf_k *la théorie des corps pseudo-finis contenant k. Il existe un morphisme d'anneaux (canonique)*

$$\chi_c : K_0(\mathrm{Psf}_k) \to K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}$$

factorisant le morphisme

$$\chi_c : K_0(\mathrm{Sch}_k) \to K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}.$$

Le résultat est assez remarquable : on sait désormais associer à une formule tous les invariants cohomologiques associés à un motif : caractéristique d'Euler, etc. !

Encore faut-il s'assurer que la construction donne quelque chose de raisonnable et de conforme aux objectifs du début... Supposons ici que k soit le corps des fractions d'un anneau intègre de type fini R, et notons $S = \mathrm{Spec}(R)$. Denef et Loeser prouvent que si X une variété sur S, φ une formule du premier ordre du langage des anneaux, il existe $f \in R - \{0\}$ tel que pour tout point fermé de S_f, l'on ait

$$\mathrm{TrFrob}_x(\chi_c(\varphi)) = |Z(\varphi, x, \mathbb{F}_x)|.$$

Nous ne précisons ni le sens exact du membre de gauche ni sa preuve (qui repose sur la formule des traces de Grothendieck), mais on comprend que cette formule justifie en quelque sorte la construction précédente. En termes imagés, celle-ci permet donc de "compter le nombre d'éléments" d'un corps fini satisfaisant à une formule φ donnée du langage des anneaux, *de façon indépendante du corps fini considéré*. Un peu plus précisément, disons pour $R = \mathbb{Z}$: soit φ une formule du langage des anneaux en n variables libres, $\Sigma\ a_i[X_i]$ une écriture de $\chi_c(\varphi)$ comme combinaison formelle de variétés. Pour tout i, choisissons un modèle sur $\mathbb{Z}$ de chaque X_i. Alors, pour tout m et pour presque tout nombre premier p, le nombre d'éléments de $\mathbb{F}_{p^m}^n$ satisfaisant à φ est $\Sigma\ a_i|X_i(\mathbb{F}_{p^m})|$. Cependant, cette construction a ses limites. Dans la pratique, on aimerait disposer d'une théorie motivique de la mesure, non sur les corps finis, mais sur les corps localement compacts, qui interviennent fréquemment en géométrie arithmétique (corps p-adiques, etc.). C'est précisément à l'esquisse de cette construction qu'est consacré le paragraphe suivant.

11.2 Volume motivique arithmétique

Ce dernier paragraphe est bien plus allusif que les précédents. Nous ne donnons aucune démonstration. La présentation est inspirée de l'excellent texte [13, Hales].

Comme nous voulons passer des corps finis aux corps localement compacts, il va nous falloir considérer des formules dans un nouveau langage, plus riche. Le lecteur aura remarqué le rôle crucial joué par le théorème 10.5 d'élimination des quantificateurs dans la construction précédente. Nous énonçons ici sans démonstration d'autres résultats d'élimination des quantificateurs dans le nouveau langage considéré, qui seront utiles pour la suite.

Soit K un corps valué, muni d'une valuation $ord : K \to \Gamma \cup \{\infty\}$, avec Γ un groupe abélien ordonné. On note $\mathcal{O}_K$ l'anneau des entiers de K (l'ensemble des éléments de valuation positive), et κ le corps résiduel de K. La projection canonique $K \to \kappa$ est noté Res. Enfin, on suppose que K admet une application "composante angulaire", c'est-à-dire une application $\bar{ac} : K \to \kappa$, nulle en 0, de restriction à $K^\times$ multiplicative, et dont la restriction au groupe des unités de $\mathcal{O}_K$ coïncide avec Res. En outre, on fait les hypothèses suivantes : K est hensélien, κ est de caractéristique nulle, et Γ est élémentairement équivalent à $\mathbb{Z}$ dans le langage des groupes abéliens ordonnés (notée provisoirement hypothèse (H)).

On considère alors le langage à trois sortes suivant

$$\mathcal{L}_{Pas} = (\mathcal{L}_K, \mathcal{L}_\kappa, \mathcal{L}_{PR} \cup \{\infty\}, ord, \bar{ac}),$$

où $\mathcal{L}_K$ est le langage des anneaux, $\mathcal{L}_\kappa$ le langage des anneaux, $\mathcal{L}_{PR}$ le langage de Presburger : $\mathcal{L}_{PR} = \{+, 0, 1, \leq\} \cup \{\equiv_n, n \in \mathbb{N}, n > 1\}$.

Nous admettrons le théorème suivant, qui se déduit du résultat d'élimination des quantificateurs de Presburger et d'un théorème de Pas :

Théorème 11.4. *On fait l'hypothèse* (H). *Pour toute $\mathcal{L}_{Pas}$-formule φ, il existe une $\mathcal{L}_{Pas}$-formule φ' sans quantificateurs sur la sorte du corps valué, ni sur celle du groupe des valeurs, et telle que φ' est équivalente à φ dans K' pour toute $\mathcal{L}_{Pas}$-extension hensélienne K' de K de groupe des valeurs élémentairement équivalent à $\mathbb{Z}$.*

A partir de maintenant, on suppose $K = k((t))$, $\kappa = k$ (k est donc un corps de caractéristique nulle), et que *ord* et $\bar{ac}$ ont leur sens usuel dans les corps de séries formelles. Soit R un sous-anneau de k. Par le terme *$\mathcal{L}_{Pas}$-formule à coefficients dans R dans la sorte du corps valué et dans la sorte du corps résiduel*, nous entendrons une formule du langage $\mathcal{L}_{Pas}$, auquel on a ajouté, pour tout élément de R, un nouveau symbole pour désigner cet élément dans le corps valué et dans le corps résiduel. Le théorème précédent reste valable pour de telles formules. Enfin, on appelle formule sur $R[[t]]^m$ une $\mathcal{L}_{Pas}$-formule à coefficients dans R dans la sorte du corps valué et dans la sorte du corps résiduel, dont les m variables libres appartiennent à la sorte du corps valué (s'imaginer que les variables libres parcourent $R[[t]]^m$).

En combinant le théorème 11.4 et le théorème 10.5, on obtient alors

Théorème 11.5. *Soit R un anneau intègre de type fini sur $\mathbb{Z}$, de corps des fractions k. Soit σ un $\mathcal{L}_{Pas}$-énoncé à coefficients dans R dans la sorte du corps valué et dans la sorte du corps résiduel. Les assertions suivantes sont équivalentes :*

- *L'énoncé σ est vrai dans $F((t))$ pour tout corps pseudo-fini F contenant k ;*
- *Il existe $f \in R - \{0\}$ tel que, pour tout point fermé x de* $\mathrm{Spec}(R_f)$*, l'énoncé σ est vrai dans $\mathbb{F}_x((t))$.*

Donnons une idée de la suite de la construction. On va voir schématiquement que le corollaire 11.5 est exactement le résultat qu'il nous fallait. Comment attribuer une mesure à un ensemble ? Considérons pour commencer le cas familier de l'espace euclidien $\mathbb{R}^n$. Notons, pour m entier, C_m l'ensemble des cubes de $\mathbb{R}^n$, de côtés de longueur $1/2^m$, centrés en un point du réseau $1/2^m\mathbb{Z}$. Si A est un sous-ensemble de $\mathbb{R}^n$ assez régulier, une idée naturelle est de considérer l'ensemble $C_m(A)$ des cubes de C_m rencontrant A, et de définir le volume de A au niveau m par la formule $|C_m(A)|/2^{mn}$. Mimons ce procédé dans le cas des $\mathcal{L}_{Pas}$-formules. Qu'est-ce ici que le cube de niveau m centré en a de K^n (K comme ci-dessus) ? C'est l'ensemble

$$\{(x_1, \ldots, x_n) \in K^n, ord(x_i - a_i) \geq m, i = 1, \ldots, m\}.$$

Regardons le cas où $K = k((t))$. Un cube centré en a est alors l'ensemble des séries formelles ayant mêmes premiers termes dominants que a. On dispose dans ce cas d'une application de troncature :

$$k[[t]] \to k[[t]]/(t^m) \simeq k^m, \quad \sum_{i=0}^{+\infty} a_i t^i \to \sum_{i=0}^{m-1} a_i t^i \to (a_0, \ldots, a_{m-1}).$$

Réciproquement, à $b \in k^m$, on peut associer $p(b,t) = \sum_{i=0}^{m-1} b_i t^i \in k[[t]]$. On dira alors que la formule φ_m est une *approximation extérieure au niveau* m de la $\mathcal{L}_{Pas}$-formule φ si c'est une formule du langage des anneaux en nm variables libres $u_{i,j}$ telle que, pour tout corps k,

$$\{u \in k^{nm}, \phi_m(u)\} = \{u \in k^{nm}, \exists a_1 \dots \exists a_n \ \varphi(a_1, \dots, a_n) \wedge ord(a_i - p((u_{i,j})_j, t)) \geq m\}.$$

Ce dernier ensemble est exactement l'ensemble des centres des cubes de $k[[t]]$ contenant un élément satisfaisant à la formule φ. Le corollaire 11.5 se réécrit alors ainsi :

Proposition 11.6. *Pour toute formule φ sur $k[[t]]^m$, pour tout entier m, il existe des approximations extérieures de φ de niveau m.*

On va donc pouvoir imiter la construction euclidienne usuelle ! Il faut donner un sens dans le cas présent au numérateur et au dénominateur de l'expression qui définissait le volume de niveau m d'un ensemble euclidien. Le numérateur était le cardinal du nombre de cubes rencontrant A ; ici, vu le travail effectué auparavant, le choix s'impose de lui-même : c'est la quantité $\chi_c(\varphi_m)$ qu'il faut considérer. Le dénominateur était un facteur de normalisation. Pour le calculer, considérons la formule $\varphi(x_1, \dots, x_n) = \top$. Alors, pour tout m, on a $\varphi_m(u_{i,j}) = \top$, et donc $\chi_c(\varphi_m) = [\mathbb{A}^{nm}] = \mathbb{L}^{nm}$. La seule formule raisonnable pour la mesure motivique (ou volume motivique) de la $\mathcal{L}_{Pas}$-formule φ est donc

$$\lim_{m \to +\infty} \chi_c(\varphi_m) \mathbb{L}^{-nm} \quad (*) \quad ,$$

en un sens à préciser : a priori, $K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}$ n'est muni d'aucune topologie. On lui en donne une comme suit. Si $M \in K_0(\mathrm{Sch}_k)$, on dira que M est de dimension $\leq n$ si M s'écrit comme combinaison formelle de variétés algébriques de dimension $\leq n$. Pour $m \in \mathbb{Z}$, on note $F^m K_0(\mathrm{Sch}_k)_{loc}$ le sous-groupe engendré par les éléments de la forme $[S]\mathbb{L}^{-i}$, avec $i - \dim S \geq m$. Cela définit une filtration décroissante F^m sur $K_0(\mathrm{Sch}_k)_{loc}$. On note encore F^m l'image de cette filtration dans $K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}$. On note alors $\hat{K}_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}$ la complétion de $K_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}$ relativement à la filtration F^m. Denef et Loeser montrent que la limite précédente existe dans $\hat{K}_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}}$.

Résumons tout cela de façon plus précise. Un peu de vocabulaire est nécessaire. Soit X une variété algébrique définie sur un corps k de caractéristique nulle. On note $h_{\mathcal{L}(X)}$ le foncteur de la catégorie $Field_k$ des corps contenant dans la catégorie des ensembles, $F \to F(K[[t]])$. La donnée pour tout objet C de $\mathcal{C}$ d'un sous-ensemble $h(C)$ de $h_{\mathcal{L}(X)}(C)$ est ce qu'on appelle un sous-assignement du foncteur $h_{\mathcal{L}(X)}$. Si X est une sous-variété de l'espace affine, on dit qu'un sous-assignement h de $h_{\mathcal{L}(X)}$ est définissable s'il existe une formule φ sur $k[[t]]^m$, telle que pour tout $F \in Field_k$, $h(F) = Z(\varphi, F[[t]])$. Si X est une variété algébrique quelconque sur k, on dira que le sous-assignement h de $h_{\mathcal{L}(X)}$ est définissable s'il existe un recouvrement fini $(X_i)_{i \in I}$ de X par des sous-schémas ouverts affines et des sous-assignements définissables h_i de $h_{\mathcal{L}(X_i)}$, tels que $h = \cup_{i \in I} h_i$. (On a juste traduit dans le cas d'une variété générale l'idée de sous-ensemble défini par une formule). On note $\mathrm{Def}_k(\mathcal{L}(X))$ l'ensemble des sous-assignements définissables de $h_{\mathcal{L}(X)}$. Le résultat central de [5, Denef-Loeser] dit dans ce langage que, si $h \in \mathrm{Def}_k(\mathcal{L}(X))$, la formule (*), convenablement étendue au cadre des sous-assignements définissables, définit une application :

$$\nu : \mathrm{Def}_k(\mathcal{L}(X)) \to \hat{K}_0^v(\mathrm{Mot}_{k,\bar{\mathbb{Q}}})_{\mathbb{Q}},$$

appelée volume motivique arithmétique, entièrement caractérisée par certaines propriétés naturelles pour une mesure.

On peut alors généraliser ce que l'on a vu à la fin du paragraphe 11.1.4. Denef et Loeser obtiennent le merveilleux résultat suivant, que nous énonçons de façon informelle, et en nous cantonnant au cas $R = \mathbb{Z}$, comme le fait [12, Hales]. Soit φ une formule sur $\mathbb{Q}[[t]]^m$, en n variables libres. Ecrivons son volume motivique (ou plutôt celui du sous-assignement définissable de $\mathbb{A}^n$ associé) comme combinaison formelle (infinie) de variétés sur $\mathbb{Q}$, $\Sigma\ a_i[X_i]\mathbb{L}^{-n_i}$. Choisissons des modèles X_i pour les variétés, définis sur $\mathbb{Z}$. Alors, quitte à exclure un ensemble fini de nombres premiers, pour toute $\mathcal{L}_{Pas}$-structure localement compacte K, le volume de l'ensemble défini par φ dans K^n (au sens de la mesure de Haar) s'écrit comme somme de la série numérique convergente

$$\sum_i a_i |X(\mathbb{F}_q)| q^{-n_i},$$

où $\mathbb{F}_q$ est le corps résiduel de K. On sait donc exprimer par un procédé géométrique le volume des différentes réalisations, de façon indépendante du corps considéré.

Les applications de l'intégration motivique arithmétique sont nombreuses. Nous nous contenterons d'un exemple. Soit X une variété algébrique, définie sur $\mathbb{Z}$. On note $N_{p,n}$ le cardinal de la projection $X(\mathbb{Z}_p) \to X(\mathbb{Z}/p^{n+1}\mathbb{Z})$. Une conjecture de Serre et Oesterlé affirme que la série de Poincaré

$$P_p(T) = \sum_n N_{p,n} T^n$$

est rationnelle. Denef en a donné une preuve reposant sur l'intégration p-adique. Toutefois, cette méthode ne renseigne pas sur la dépendance en p. A l'aide de la théorie développée ci-dessus, Denef et Loeser ont abouti au résultat suivant.

Théorème 11.7. *Il existe, pour X comme ci-dessus, une série canonique $P_{ar}(T)$, à coefficients dans $K_0^v(\mathrm{Mot}_{\mathbb{Q},\bar{\mathbb{Q}}}) \otimes \mathbb{Q}$, qui est une fonction rationnelle de T, qui se spécialise (après avoir pris la trace du Frobenius d'une réalisation étale) en la série de Poincaré p-adique $P_p(T)$, pour presque tout nombre premier p.*

Annexe 1 : Estimées de Lang-Weil

La preuve est recopiée de [15, Katz]. On prend le terme variété dans son sens général (cf [19, Perrin]).

Théorème (Lang-Weil pour les hypersurfaces projectives)**.** *Soient d et e des entiers positifs, alors il existe une constante C ne dépendant que de d et e telle que pour tout corps fini $F = \mathbb{F}_q$ et toute hypersurface V de l'espace projectif $\mathbb{P}^{d+1}$ définie sur F de degré e, c'est à dire définie par un polynôme homogène $f \in F[\bar{X}]$ de degré e, on ait :*

$$|\sharp(V \cap F^n) - q^d| < Cq^{d-1/2}.$$

Démonstration. On suppose établie l'hypothèse de Riemann dans le cas des courbes ($d = 1$). On procède par récurrence. Si $d = 1$, $V \subseteq \mathbb{P}^2$ est une hypersurface de degré noté e. Notons V' la normalisation de V et $\pi : V' \to V$. La suite exacte courte de faisceaux

$$0 \to \mathcal{O}_V \to \pi_*\mathcal{O}_{V'} \to \pi_*\mathcal{O}_{V'}/\mathcal{O}_V \to 0,$$

donne en cohomologie

$$h^0(\pi_*\mathcal{O}_{V'}/\mathcal{O}_V) \leq h^1(\mathcal{O}_V) = \frac{(e-1)(e-2)}{2}.$$

Or

$$h^0(\pi_*\mathcal{O}_{V'}/\mathcal{O}_V) \geq \sum_{x \in V_{sing}(\mathbb{F}_q)} \pi^{-1}(x)(\mathbb{F}_q) - 1.$$

D'où

$$\sharp V'(\mathbb{F}_q) - \sharp V(\mathbb{F}_q) \leq \sum_{x \in V_{sing}(\mathbb{F}_q)} \pi^{-1}(x)(\mathbb{F}_q) - 1 \leq \frac{(e-1)(e-2)}{2}.$$

On a aussi

$$\sharp V'(\mathbb{F}_q) - \sharp V(\mathbb{F}_q) \geq -X_{sing}(\bar{\mathbb{F}}_q) \geq -\frac{(e-1)(e-2)}{2}.$$

Ces deux inégalités assurent que

$$|\sharp V'(\mathbb{F}_q) - \sharp V(\mathbb{F}_q)| \leq \frac{(e-1)(e-2)}{2}.$$

Appliquons alors l'hypothèse de Riemann à V' :

$$|\sharp V'(\mathbb{F}_q) - q - 1| \leq 2\text{genre}(V')\sqrt{q}.$$

Comme $2\text{genre}(V') \leq (e-1)(e-2)$, on a finalement

$$|\sharp V(\mathbb{F}_q) - q - 1| \leq (e-1)(e-2)\sqrt{q} + \frac{(e-1)(e-2)}{2}.$$

Passons au cas $d > 1$. On note $\mathbb{P}^{\check{}\,d+1}$ le dual projectif dont les éléments s'identifient aux hyperplans de $\mathbb{P}^{d+1}$. Définissons $Z = \{(x, H) \in V \times \mathbb{P}^{\check{}\,d+1}, x \in H\}$. La fibre en $x \in V$ de la première projection est l'espace projectif de dimension d des hyperplans de $\mathbb{P}^{d+1}$ passant par

x. La fibre en $H \in \mathbb{P}^{\check{}\, d+1}$ de la deuxième projection est $V \cap H$. On peut supposer $e > 1$ de sorte que V n'est inclus dans aucun hyperplan. On a

$$\sharp Z = \sharp V.\sharp\mathbb{P}^d = \sum_{H \in \mathbb{P}^{\check{}\, d+1}(\mathbb{F}_q)} \sharp V \cap H.$$

Nous utiliserons les faits suivants :

(1) Si $X \subseteq \mathbb{P}^{d+1}$ est une hypersurface (pas nécessairement irréductible) de degré e, $\sharp X \leq e.\sharp\mathbb{P}^d$ (projeter X sur $\mathbb{P}^d$) ;

(2) L'ensemble $\{H \in \mathbb{P}^{\check{}\, d+1}, H \cap V$ n'est pas géométriquement irréductible $\}$ est inclus dans une hypersurface de $\mathbb{P}^{\check{}\, d+1}$ dont le degré D ne dépend que de d et e. Il s'agit d'une version du théorème de Bertini, pour lequel nous renvoyons à [Hartshorne].

On a tous les ingrédients pour conclure. On dira qu'un hyperplan $H \in \mathbb{P}^{\check{}\, d+1}$ est g.i. s'il est géométriquement irréductible, g.r. sinon. Alors

$$|\sharp Z - \sum_{H \ g.i.} \sharp V \cap H| \leq \sum_{H \ g.r.} \sharp V \cap H \leq eD\sharp\mathbb{P}^d.\sharp\mathbb{P}^{d+1} = O(q^{2d-1}).$$

On a aussi $\sharp\mathbb{P}^{d+1} - \sharp\{H, H \ g.i.\} = O(q^d)$, et pour H g.i., par hypothèse de récurrence,

$$|\sharp V \cap H - q^{d-1}| \leq C(d-1, e)q^{d-1-1/2}.$$

En mettant bout à bout nos estimations, on obtient

$$|\sharp V - q^d| \leq C(d, e)q^{d-1/2}.$$

□

Pour traiter le cas d'une variété V absolument irréductible quelconque, on procède par récurrence sur la dimension d. Quitte à projeter, on peut supposer $V \subseteq \bar{V} \subseteq \mathbb{P}^{d+1}$, où $\bar{V}$ est la clôture projective de V (obtenue en homogénéisant les équations qui définissent la variété si elle est affine). L'hypothèse de récurrence permet de se ramener à montrer le résultat pour $\bar{V}$, qui découle du théorème précédent, et du fait qu'on contrôle le degré de $\bar{V}$. Cet argument peut être rendu rigoureux, ce qui permet d'obtenir le théorème suivant.

Théorème (Lang-Weil)**.** *Soient m, n, e des entiers positifs. Il existe une constante positive C ne dépendant que du triplet (m, n, e), telle que pour tout corps fini $F = \mathbb{F}_q$, pour tous polynômes $f_1(\bar{Y}), \ldots, f_m(\bar{Y}) \in F[\bar{Y}]$ (avec $\bar{Y} = (Y_1, \ldots, Y_n)$) de degré $\leq e$, si les polynômes $f_1(\bar{Y}), \ldots, f_m(\bar{Y})$ engendrent l'idéal d'une variété absolument irréductible V de dimension d,*

$$|\sharp(V \cap F^n) - q^d| < Cq^{d-1/2}.$$

On admet que la constante C du théorème précédent est une fonction primitive récursive de m, n et e (voir [9, Ghorpade-Lachaud]).

Annexe 2 : Revêtements étales finis galoisiens

Nous exposons ici les notions de base concernant les revêtements finis étales, nécessaires à la compréhension de la partie III. Nous utilisons librement le langage des schémas ; voir par exemple [14, Hartshorne]. L'exposition faite ici suit de très près l'excellente présentation qu'en donne [23, Szamuely].

1) Définitions et propriétés des morphismes étales

Si l'on se donne k fonctions différentiables (resp. analytiques) $f_1, \ldots, f_k$ au voisinage d'un point $x \in \mathbb{R}^{n+k}$ (resp. $\mathbb{C}^{n+k}$), nulles en x, et telles que

$$\det_{1 \leq i,j \leq k} \frac{\partial f_i}{\partial x_j}(x) \neq 0,$$

alors la restriction de la projection sur les n dernières coordonnées

$$\{y, f_1(y) = \cdots = f_k(y) = 0\} \to \mathbb{R}^n \text{ (resp.}\mathbb{C}^n)$$

$$(x_1, \ldots, x_{n+k}) \to (x_{k+1}, \ldots, x_{n+k}),$$

est localement un isomorphisme au voisinage de x, en vertu du théorème des fonctions implicites.

On ne dispose pas en géométrie algébrique d'analogue immédiat de ce théorème. Considérons en effet la situation simple suivante : on considère la projection sur la deuxième coordonnée de $\mathrm{Spec}(k[X_1, X_2]/(X_1^2 - X_2))$ dans $\mathbb{A}^1_k$ (k un corps de caractéristique différente de 2), $(x_1, x_2) \to x_2$. En $x = (1, 1)$,

$$\frac{\partial}{\partial x_1}(x_1^2 - x_2) \neq 0,$$

mais le morphisme considéré n'est bijectif dans aucun ouvert de Zariski U contenant x, puisque un tel U contient les points $(-\sqrt{a}, a)$ et $(\sqrt{a}, a)$ pour tout a hors d'un ensemble fini (pour k algébriquement clos). On voit bien sur cet exemple que comme les ouverts de Zariski sont très gros, dire qu'un morphisme de S-schémas $X \to Y$ est un isomorphisme local en $x \in X$ s'il réalise un isomorphisme de S-schémas d'un ouvert de X contenant x sur un ouvert V de Y est une condition bien trop forte (si X et Y sont des schémas intègres de type fini sur un corps k, cela implique que X et Y sont k-birationnels !).

Par contre, on aimerait généraliser la situation dans l'exemple, en considérant les morphismes qu'on obtiendrait localement sous la forme : $X = \mathrm{Spec}(R[X_1, \ldots, X_n]/(f_1, \ldots, f_n)) \to Y = \mathrm{Spec}(R)$, avec $\det \frac{\partial f_i}{\partial x_j}(x) \neq 0$ en $x \in X$. Une telle définition est évidemment imprécise et malcommode à formaliser. En travaillant, on arrive à la définition abstraite suivante :

Définition. Un morphisme de schémas $\varphi : X \to S$ fini, est dit localement libre si l'image directe $\varphi_* \mathcal{O}_X$ est localement libre (de rang fini). Si, de plus, chaque fibre X_P de φ est le spectre d'une $k(P)$-algèbre finie étale (i.e. produit fini d'extensions séparables de $k(P)$), on dit que φ est un morphisme fini étale. On parle de revêtement fini étale si en outre φ est surjectif.

Ce qui suit permettra d'éclairer un peu cette définition. Le lien avec ce qu'on a dit avant se comprend bien si l'on dispose du faisceau des différentielles, mais nous n'en parlerons pas ici. Voici pour commencer quelques remarques et exemples.

Remarques.

– Si A est un anneau local, dire qu'un A-module fini est libre revient à dire qu'il est plat. Donc un morphisme fini de schémas est localement libre si et seulement si $\varphi_*\mathcal{O}_X$ est un faisceau de $\mathcal{O}_S$-modules plats. On peut en fait définir la notion de morphisme étale pour des morphismes non nécessairement finis : un morphisme est dit étale s'il est plat, localement de présentation finie, et si la fibre au-dessus de chaque point P admet un recouvrement ouvert par des spectres de $k(P)$-algèbres étales finies. Nous ne considèrerons dans ce qui suit que des morphismes finis.
– L'image d'un morphisme fini et localement libre est à la fois ouverte et fermée (pourquoi ?).

Exemples.
– Une extension finie de corps est étale si et seulement si elle est séparable.
– Reprenons l'exemple du début. On note $X = \mathrm{Spec}(k[X_1, X_2]/(X_1^2 - X_2)$, $Y = \mathbb{A}^1_k$. Le morphisme considéré n'est pas étale en $(0,0)$ (la fibre en ce point est $\mathrm{Spec}(k[\epsilon])$), et étale en tous les autres points : si a n'est pas un carré dans k, la fibre au-dessus de a est le spectre d'un corps, et isomorphe à $\mathrm{Spec}(k \times k)$ sinon.
– *Le cas des courbes.* Soit $\varphi : X \to Y$ un morphisme fini étale entre courbes affines intègres sur un corps k, correspondant à une inclusion d'anneaux $A \to B$. Si P est un idéal premier de A, on dispose d'un isomorphisme $B/PB \simeq (\varphi_*\mathcal{O}_X)_P \otimes_{\mathcal{O}_{Y,P}} k(P)$, donc B/PB est une algèbre finie étale sur A/P. De même, $(\varphi_*\mathcal{O}_X)_{(0)}$ est une extension séparable de $(\mathcal{O}_Y)_0 = k(X)$. En particulier, si X et Y sont normales, A et B sont des anneaux de Dedekind, et dire que X_P est étale revient à dire que les facteurs premiers dans la décomposition de PB sont tous simples. Si de plus $K \subseteq L$ sont des corps de nombres, $A \subseteq B$ leurs anneaux d'entiers respectifs, dire que φ est étale revient à dire que l'extension L/K est non ramifiée au sens de la théorie algébrique des nombres.
– Le schéma $\mathrm{Spec}(\mathbb{Z})$ n'admet pas de revêtement fini étale non trivial (conséquence du point précédent et d'un théorème de Minkowski).
– Soient $Y = \mathrm{Spec}(A)$, $X = \mathrm{Spec}(B)$ des schémas affines, avec $B = A[X]/(f)$, $f \in A[X]$ unitaire de degré d. Comme B est un A-module libre de rang d, le morphisme $\varphi : X \to Y$ est fini et localement libre. Supposons en outre que f et f' soient premiers entre eux dans $A[X]$. Alors X_P est le spectre de $B \otimes_A k(P) \simeq k(P)[X]/(\tilde{f})$. Comme les racines de $\tilde{f}$ sont simples par hypothèse, X_P est le spectre d'une $k(P)$-algèbre finie étale.

La proposition suivante, qui est une conséquence assez directe du lemme de Hensel, fait le lien avec le préambule et montre que l'on dispose quand même d'un analogue affaibli du théorème des fonctions implicites (le résultat peut être amélioré, bien entendu). Elle est valable pour les morphismes étales non nécessairement finis, tels que définis dans les remarques ci-dessus. Le lecteur peut la prouver, ou consulter [14, Hartshorne].

Proposition. *Soient A un anneau local noethérien complet, d'idéal maximal $\mathfrak{m}$, de corps résiduel k, et $f : X \to \mathrm{Spec}(A)$ un morphisme de type fini. Soit $x \in X$ au-dessus de $\mathfrak{m}$, tel que $K(x) \simeq k$. Alors, si f est étale en x, f est un isomorphisme local au voisinage de x.*

Voici une autre proposition, conceptuellement satisfaisante car elle éclaire la terminologie.

Proposition. *Soit S un schéma connexe, $\phi : X \to S$ un morphisme affine surjectif. Alors φ est un revêtement fini étale si et seulement s'il existe un morphisme fini, localement libre et surjectif $\psi : Y \to S$, tel que le changement de base $X \times_S Y \to Y$ soit un revêtement trivial de Y.*

Démonstration. Voir [23, Szamuely, proposition 5.2.9, p. 155-156]. □

En topologie générale, les revêtements sont caractérisés par le fait d'êtres triviaux sur des ouverts convenables de la base. Notons que la restriction du revêtement $Y \to X$ à un ouvert U de X n'est rien d'autre que le produit fibré $Y \times_X U \to U$ dans la catégorie des espaces topologiques. La proposition précédente justifie donc la terminologie. On a en fait plus qu'une analogie : la proposition dit exactement que les revêtements finis étales sont localement triviaux pour la topologie de Grothendieck dont les cribles couvrants sont donnés par les morphismes finis surjectifs localement libres.

2) Théorie de Galois pour les revêtements finis étales

Dans cette section, nous esquissons l'extension de la théorie de Galois des revêtements topologiques au cadre précédemment défini des revêtements finis étales.

Nous admettrons le lemme technique suivant :

Corollaire. *Soient $\varphi : X \to Y$ et $\psi : Y \to Z$ des morphismes de schémas. Si $\psi \circ \varphi$ est fini, et ψ séparé, φ est fini. Si de plus $\psi \circ \varphi$ et ψ sont finis étales, φ aussi.*

Proposition. *Soit $\varphi : X \to S$ un revêtement fini étale, $s : S \to X$ une section de φ. Alors s induit un isomorphisme de S sur un sous-schéma ouvert et fermée de X.*

Démonstration. Par le lemme, s est un morphisme fini étale, donc d'image ouverte et fermé dans X par une remarque ci-dessus. Comme s est injectif, on a le résultat. □

Corollaire. *Si $Z \to S$ est un S-schéma fermé, et $\varphi_1, \varphi_2 : Z \to X$ deux S-morphismes à valeurs dans un S-schéma fini étale X, avec $\varphi_1 \circ \bar{z} = \varphi_2 \circ \bar{z}$ pour un certain point géométrique $\bar{z} : \mathrm{Spec}(\Omega) \to Z$, alors $\varphi_1 = \varphi_2$.*

Démonstration. En utilisant les théorèmes de changement de base pour les morphismes étales, et quitte à considérer $Z \times_S X \to Z$, on peut supposer $S = Z$. On est donc ramené à prouver que si deux sections d'un revêtement fini étale $X \to S$ d'un schéma connexe S coïncident en un point géométrique, ils sont égaux. Cela résulte de la proposition précédente, car une telle section réalise un isomorphisme de S sur une composante connexe de X et est donc déterminée par l'image d'un point géométrique. □

Etant donné un morphisme de schémas $\varphi : X \to S$, on note $\mathrm{Aut}(X|S)$ le groupe des automorphismes de schémas de X préservant φ. Ces automorphismes agissent à gauche, par convention. Si $\bar{s} : \mathrm{Spec}(\Omega) \to S$ est un point géométrique, on a une action à gauche naturelle de $\mathrm{Aut}(X|S)$ sur la fibre géométrique $X_{\bar{s}}$ (par changement de base).

Corollaire. *Si $\varphi : X \to S$ est un revêtement fini étale connexe, les éléments non triviaux de $\mathrm{Aut}(X|S)$ agissent sans point fixe sur chaque fibre géométrique. Donc $\mathrm{Aut}(X|S)$ est fini.*

Démonstration. On appplique le corollaire précédent avec $\varphi_1 = \varphi$, $\varphi_2 = \varphi \circ \lambda$, pour $\lambda \in \mathrm{Aut}(X|S)$. Ceci montre la première assertion. Il s'ensuit que la représentation de permutation de $\mathrm{Aut}(X|S)$ dans les ensembles sous-jacents aux fibres géométriques est fidèle. D'où la seconde assertion. □

Soit $\varphi : X \to S$ un morphisme affine surjectif de schémas. Soit $G \subseteq \mathrm{Aut}(X|S)$ un sous-groupe fini. On définit l'espace annelé $G\backslash X$ et le morphisme d'espaces annelés $\pi : X \to G\backslash X$ comme suit. L'espace topologique sous-jacent à $G\backslash X$ est le quotient de X par l'action de G, et π vue comme application continue est la projection canonique. On défint enfin le faisceau structurel de $G\backslash X$ comme le sous-faisceau $(\pi_*\mathcal{O}_X)^G$ des éléments G-invariants dans $\pi_*\mathcal{O}_X$.

Proposition. *L'espace annelé $G\backslash X$ est un schéma, le morphisme π est affine surjectif, et φ se factorise : $\varphi = \psi \circ \pi$, avec $\psi : G\backslash X \to S$ morphisme affine.*

Démonstration. On peut supposer, comme φ est affine, que $X = \mathrm{Spec}(B)$ et $S = \mathrm{Spec}(A)$ sont affines, et que φ provient d'un morphisme d'anneaux $\lambda : A \to B$. Montrons que l'espace annelé $G\backslash X$ est isomorphe au spectre de B^G. Cela donnera le résultat, si l'on remarque en outre que B est entier sur B^G (si $b \in B$, b est racine du polynôme unitaire $\prod(X - \sigma(b)) \in B^G[X]$, σ décrivant G), donc que le morphisme de schémas associé est surjectif, par le théorème de Cohen-Seidenberg.

Pour identifier les espaces topologiques sous-jacents à $G\backslash X$ et $X_G = \mathrm{Spec}(B^G)$, il suffit de les identifier commme ensembles, car un sous-ensemble fermé $V(I) \subseteq X$ donne un sous-ensemble fermé $V(I^G) \subseteq X_G$. On vient de voir que $\pi : X \to X_G$ est surjectif, et il nous faut donc montrer que les fibres de l'application $X \to X_G$ déduite de l'inclusion d'anneaux $B^G \to B$ sont les G-orbites de $\mathrm{Spec}(B)$. Supposons un instant que deux orbites $\{\sigma(P), \sigma \in G\}$ et $\{\sigma(Q), \sigma \in G\}$ de points de B vivent au-dessus du même point $P^G \in \mathrm{Spec}(B^G)$. Comme la fibre $X_{k(P^G)}$ est de dimension nulle, les $\sigma(P)$ et $\sigma(Q)$ induisent des idéaux maximaux $\bar{\sigma(P)}$ et $\bar{\sigma(Q)}$ de $\bar{B} = B \otimes_{B^G} k(P^G)$, avec $\bigcap \bar{\sigma(P)} = \bigcap \bar{\sigma(P)} = 0$. Cela contredit le théorème chinois, qui permet de choisir $\bar{b} \in \bar{B}$ dans tous les $\bigcap \bar{\sigma(P)}$ et dans aucun $\bigcap \bar{\sigma(Q)}$.

Il reste à voir que $(\pi_*\mathcal{O}_X)^G \simeq \mathcal{O}_{X_G}$. Le premier faisceau est quasi-cohérent, car c'est le noyau du morphisme de faisceaux quasi-cohérents

$$\pi_*\mathcal{O}_X \to \bigoplus_{\sigma \in G} \pi_*\mathcal{O}_X, \quad s \to (\dots, \sigma(s) - s, \dots).$$

Il suffit alors de vérifier qu'on a des isomorphismes sur les anneaux de sections sur X_G, qui sont égaux à B^G dans les deux cas. □

Nous dirons qu'un revêtement fini étale connexe $X \to S$ est galoisien si $\mathrm{Aut}(X|S)$ agit transitivement sur les fibres géométriques. On montre alors, comme en topologie, la proposition suivante.

Proposition. *Soit $\varphi : X \to S$ un revêtment fini étale galoisien. Si $\psi : Z \to S$ est un revêtemet fini étale connexe, tel que φ se factorise par ψ : $\varphi = \psi \circ \pi$, $\pi : X \to Z$, alors π est un revêtement fini étale galoisien, et $Z \simeq H\backslash X$, avec H sous-groupe de $G = \mathrm{Aut}(X|S)$. On obtient ainsi une bijection entre sous-groupes de G et revêtements intermédiaires Z comme précédemment. Le revêtement $\psi : Z \to S$ est galoisien si et seulement si H est un sous-groupe normal de G, et dans ce cas $\mathrm{Aut}(X|S) \simeq G/H$.*

Démonstration. Voir [23, Szamuely, proposition 5.3.8, p. 162]. □

Références

[1] J. Ax. The elementary theory of finite fields. *Annals of Math.*, 88 :239–271, 1968.

[2] N. Bourbaki. *Algèbre commutative*. Chapitres 1-4. Hermann, Paris, 1961.

[3] Z. Chatzidakis. *Théorie des modèles des corps finis et pseudo-finis*. notes de cours, 1996.

[4] Z. Chatzidakis, L. van den Dries, and A. Macintyre. Definable sets over finite fields. *J. reine u. ang. Math.*, 427 :107–135, 1992.

[5] J. Denef and F. Loeser. Definable sets, motives and p-adic integrals. *J. Amer. Math. Soc.*, 14 :429–469, 2001.

[6] J. Denef and F. Loeser. Motivic integration and the Grothendieck group of pseudo-finite fields. *Proceedings of the International Congress of Mathematicians*, Vol. II :13–23, Beijing, 2002. Higher Ed. Press.

[7] M. Fried and M. Jarden. *Field Arithmetic*. Springer-Ergebnisse, 1986.

[8] M. Fried and G. Sacerdote. Solving diophantine problems over all residue class fields of a number field and all finite fields. *Ann. Math.*, 100 :203–233, 1976.

[9] S. Ghorpade and Q. Lachaud. Number of solutions of equations over finite fields and a conjecture of Lang and Weil. *Number Theory and Discete Mathematics*, pages 269–291, 2000. Hindustan Book Agency, New Delhi.

[10] H. Gillet and C. Soulé. Descent, motives and K-theory. *J. Reine. Angew. Math.*, 478 :127–176, 1996.

[11] F. Guillen and V. Navarro Aznar. Un critère d'extension d'un foncteur défini sur les schéma lisses. 1995. Preprint.

[12] T. C. Hales. What is motivic measure ?

[13] T. C. Hales. Can p-adic integrals be computed ? *Contributions to automorphic forms, geometry, and number theory*, pages 313–329, 2004.

[14] R. Hartshorne. *Algebraic Geometry*. Springer, New-York, 1977.

[15] N. Katz. Lectures on Deligne's proof of the Riemann hypothesis for varieties over finite fields. notes by Spencer Bloch.

[16] D. Haran M. Fried and M. Jarden. Galois stratifications over Frobenius fields. *Adv. in Math.*, 51 :1–35, 1984.

[17] D Marker. *Model Theory : An Introduction*, volume 217 of *Grad. Texts Math.* Springer, New York, 2002.

[18] J. Nicaise. Relative motives and the theory of pseudo-finite fields. *Int. Math. Res. Pap.*, 1 :69, 2007.

[19] D. Perrin. *Géométrie algébrique : une introduction*. InterEditions, 1995.

[20] S. Raskin. The Weil conjectures for curves. 2007. Univ. of Chicago.

[21] T. Scanlon. Motivic integration : An outsider's tutorial. 2009. Durham, England, 21 and 22 July 2009.

[22] A. Seidenberg. Constructions in algebra. *Trans. A.M.S.*, 178 :273–313, 1974.

[23] T. Szamuely. *Galois Groups and Fundamental Groups*. Cambridge University Press, New-York, 2009.

[24] L. van den Dries and K. Schmidt. Bounds in the theory of polynomial rings over fields. *Invent. Mat.*, 76 :77–91, 1984.