Théorie des modèles des corps finis et pseudo-finis

Zoé Chatzidakis, CNRS/Paris 7, Mai 1996

Ces notes sont celles d'un cours de DEA, que j'ai donné à l'université de Paris 7 le printemps 1996. Le but du cours était d'étudier les propriétés modèle-théoriques des corps finis et pseudo-finis. Les connaissances requises sont minimales, aussi bien en théorie des modèles qu'en algèbre. Nous développons d'abord les résultats d'Ax, puis étudions de façon plus précise la structure des ensembles définissables. Nous concluons avec les applications données par Hrushovski et Pillay sur les groupes algébriques sur des corps finis.

Table des matières:

0. Théorie des modèles – Quelques résultats et notations

(0.1) Morphismes. Soient A et B des $\mathcal{L}$-structures, $F : A \to B$ une application.

(1) F est un (homo)morphisme (de $\mathcal{L}$-structures), si pour tout n-uplet $\bar{a}$ de A, fonction n-aire f et relation n-aire R,

$$A \models R(\bar{a}) \Rightarrow B \models R(F(\bar{a})), \text{ et } f(F(\bar{a})) = F(f(\bar{a})).$$

(2) F est un plongement si F est un homomorphisme injectif et pour tout n-uplet $\bar{a}$ de A et relation n-aire R,

$$A \models R(\bar{a}) \iff B \models R(F(\bar{a})).$$

(3) F est un isomorphisme si F est un plongement surjectif.

(4) F est un plongement élémentaire si $F(A)$, l'image de A par F, est une sous-structure élémentaire de B. De façon équivalente, si pour toute formule $\varphi(\bar{x})$ et n-uplet $\bar{a}$ de A,

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

(5) Un isomorphisme partiel entre A et B est une bijection g entre des sous-emsembles A_0 de A et B_0 de B satisfaisant: si $\varphi(\bar{x})$ est une formule sans quantificateurs de $\mathcal{L}$, et $\bar{a}$ un uplet de A_0, alors

$$A \models \varphi(\bar{a}) \text{ si et seulement si } B \models \varphi(g(\bar{a})).$$

Ou tout simplement: si g induit un isomorphisme entre les structures engendrées par A_0 et B_0. On parle aussi d'isomorphisme élémentaire partiel, quand l'application g préserve toutes les formules.

(0.2) Un test pour l'équivalence élémentaire. Soient $A \subseteq B$ des modèles. Alors $A \prec B$ si et seulement si pour toute formule $\varphi(\bar{x}, \bar{y})$ du langage, $\bar{x} = (x_1, \ldots, x_n)$, $\bar{y} = (y_1, \ldots, y_m)$, et pour tout n-uplet $\bar{a}$ de A,

$$B \models \exists \bar{y}\, \varphi(\bar{a}, \bar{y})$$

si et seulement s'il existe un m-uplet $\bar{b}$ de A tel que

$$B \models \varphi(\bar{a}, \bar{b}).$$

(0.3) Quelques résultats de préservation.

Nous commençons par un théorème de compacité qui nous sera très utile par la suite.

Théorème. Soient T_1 et T_2 des théories, avec $T_1 \cup T_2$ consistante, et soit Δ un ensemble d'énoncés clos par disjonction finie. Les conditions suivantes sont équivalentes:

(1) Il existe $\Gamma \subseteq \Delta$ tel que $T_1 \cup \Gamma$ axiomatise $T_1 \cup T_2$.

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

Démonstration. (1) implique (2) est clair. Supposons maintenant (2), et soit $\Gamma = \{\psi \in \Delta \mid T_1 \cup T_2 \vdash \psi\}$. Alors $T_1 \cup T_2 \models \Gamma$, et il suffit de montrer que $T_1 \cup \Gamma \models T_2$, c'est à dire que tout modèle de $T_1 \cup \Gamma$ est un modèle de T_2. Soit $B \models T_1 \cup \Gamma$, et soit

$$\Sigma = \{\neg\psi \mid \psi \in \Delta,\ B \models \neg\psi\}.$$

Nous allons montrer que $T_1 \cup T_2 \cup \Sigma$ est consistante. Sinon, (par compacité) il existerait $\neg\psi_1, \dots, \neg\psi_n \in \Sigma$, et $\varphi \in T_2$ tels que $T_1 \cup \{\neg\psi_1, \dots, \neg\psi_n, \varphi\}$ est inconsistante; nous obtenons alors:

$$T_1 \cup \{\varphi\} \vdash (\psi_1 \vee \cdots \vee \psi_n).$$

Comme Δ est clos par disjonction, l'énoncé $\psi_1 \vee \cdots \vee \psi_n$ est dans Γ, et donc ne peut appartenir à Σ, ce qui donne la contradiction souhaitée.

Soit A un modèle de $T_1 \cup T_2 \cup \Sigma$; si $\psi \in \Delta$ est satisfaite dans A, alors $\neg\psi \notin \Sigma$, ce qui montre que ψ est aussi satisfaite dans B. Donc B est un modèle de T_2, ce qui montre que Γ est une axiomatisation de T_2 modulo T_1.

Corollaire. Soit T une théorie, $\varphi(\bar{x})$, $\bar{x} = (x_1, \dots, x_n)$ une formule telle que $T \cup \exists\bar{x}\ \varphi(\bar{x})$ est consistante. Soit Δ une ensemble de formules dans les variables $\bar{x}$, clos par disjonction. Les conditions suivantes sont équivalentes:

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

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

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

Démonstration. On agrandit le langage en ajoutant des nouveaux symboles de constantes $c_1, \dots, c_n$. On applique alors le théorème, et on obtient des formules $\psi_1, \dots, \psi_m \in \Delta$ telles que

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

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

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

(0.4) Quelques propriétés En utilisant le critère (0.2), on montre facilement les résultats suivants:

(1) Si $A \prec B$ et $B \prec C$ alors $A \prec C$.
(2) Si $A \prec C$, $B \prec C$ et $A \subseteq B$ alors $A \prec B$.
(3) Soit $(A_i)_{i\in\mathbf{N}}$ une chaîne croissante de structures, telle que $A_i \prec A_{i+1}$ pour tout i, et soit $A = \bigcup_{i\in\mathbf{N}} A_i$. Alors $A_i \prec A$ pour tout i.

Les résultats suivants sont un peu plus difficiles à démontrer, et leur preuve utilise le théorème (0.3). Pour une démonstration, adapter par exemple celle de Chang et Keisler ([CK], Chapître 3.2). Soient $\varphi(\bar{x})$ une formule du langage et T une théorie.

(4) Les conditions suivantes sont équivalentes:
   (a) Pour tous modèles A et B de T, homomorphisme $F : A \to B$ et uplet $\bar{a}$ de A, si $A \models \varphi(\bar{a})$ alors $B \models \varphi(F(\bar{a}))$.
   (b) Il existe une formule positive $\psi(\bar{x})$ (c'est à dire construite à partir de formules atomiques en utilisant seulement les symboles logiques $\wedge$, $\vee$, $\exists$, $\forall$ mais pas le symbole logique $\neg$) telle que $T \models \forall \bar{x}\,(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$.

(5) Les conditions suivantes sont équivalentes:
   (a) Pour tous modèles A et B de T, avec $A \subseteq B$ et uplet $\bar{a}$ de A, si $A \models \varphi(\bar{a})$ alors $B \models \varphi(\bar{a})$.
   (b) Il existe une formule existentielle $\psi(\bar{x})$ telle que $T \models \forall \bar{x}\,(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$.

(6) Les conditions suivantes sont équivalentes:
   (a) Pour tous modèles A et B de T, avec $A \subseteq B$, et uplet $\bar{a}$ de A, si $B \models \varphi(\bar{a})$ alors $A \models \varphi(\bar{a})$.
   (b) Il existe une formule universelle $\psi(\bar{x})$ telle que $T \models \forall \bar{x}\,(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$.

(7) Les conditions suivantes sont équivalentes:
   (a) Pour toute suite croissante $(A_i)_{i \in \mathbf{N}}$ de modèles de T, et uplet $\bar{a}$ de A_0, si $A_i \models \varphi(\bar{a})$ pour tout $i \in \mathbf{N}$ alors $\bigcup_{i \in \mathbf{N}} A_i \models \varphi(\bar{a})$.
   (b) Il existe une formule $\forall\exists$ $\psi(\bar{x})$ telle que $T \models \forall \bar{x}\,(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$.

(0.5) Théories modèle complètes, élimination des quantificateurs

Définitions. Soit T une théorie du premier ordre.

(1) T est **modèle complète** si pour tous modèles A et B de T, si $A \subseteq B$ alors $A \prec B$.

(2) On dit que T **admet l'élimination des quantificateurs** (eq) si pour toute formule $\varphi(\bar{x})$ il existe une formule $\psi(\bar{x})$ sans quantificateurs, telle que

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

Remarques. Rappelons que le langage $\mathcal{L}(A)$ est obtenu en rajoutant à $\mathcal{L}$ des symboles de constantes pour tous les éléments de A. Nous notons $\Delta(A)$ le diagramme sans quantificateurs de A, c'est à dire l'ensemble des énoncés sans quantificateurs du langage $\mathcal{L}(A)$ qui sont vrais dans A. Une application facile du théorème de compacité donne:

(1) T est modèle complète si et seulement si, pour tout modèle A de T, la théorie $T \cup \Delta(A)$ est complète.

(2) T admet l'élimination des quantificateurs si et seulement si pour toute sous-structure A d'un modèle de T, $T \cup \Delta(A)$ est complète.

(3) Si T est modèle complète, alors elle admet une axiomatisation par des énoncés $\forall\exists$.

Démonstration. (1) B est un modèle de $T \cup \Delta(A)$ si et seulement si B contient une sous-structure isomorphe à A. Ce n'est vraiment qu'une retraduction de la propriété de modèle complétude.

(2) Compacité.

(3) La réunion d'une chaîne de modèles de T est un modèle de T; on applique le résultat de préservation pour conclure.

Proposition. Soit T une théorie.

(1) Pour montrer que T est modèle complète, il suffit de montrer que si $A \subseteq B$ sont deux modèles quelconques de T, $\varphi(\bar{x}, \bar{y})$ est une formule sans quantificateurs de $\mathcal{L}$, et $\bar{a}$ est un n-uplet de A, alors

$$B \models \exists \bar{y}\ \varphi(\bar{a}, \bar{y}) \quad \text{si et seulement si} \quad A \models \exists \bar{y}\ \varphi(\bar{a}, \bar{y}).$$

(On dit alors que A est **existentiellement clos** dans B, aussi noté par $A \prec_1 B$).

(2) T est modèle complète si et seulement si toute formule $\varphi(x)$ est équivalente modulo T à une formule existentielle $\psi(\bar{x})$ ($T \models \forall \bar{x}\, (\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$, si et seulement si toute formule $\varphi(\bar{x})$ est équivalente modulo T à une formule universelle $\psi(\bar{x})$.

(3) Pour montrer que T a l'élimination des quantificateurs, il suffit de montrer que, étant donnée une sous-structure C de deux modèles A et B de T, il existe un modèle D de T qui contient A et B comme sous-structures élémentaires.

(4) Pour montrer que T admet l'élimination des quantificateurs, il suffit de trouver un modèle M de T avec les deux propriétés suivantes:

(a) Tout modèle dénombrable de T se plonge élémentairement dans M.

(b) Si $F : A_0 \to B_0$ est un isomorphisme partiel entre deux sous-ensembles finis, et $c \in M$, alors il existe $d \in M$ tel que l'extension F' de F définie en posant $F'(c) = d$, est aussi un isomorphisme partiel.

La partie (4) est en fait conséquence d'un résultat plus géneral:

La méthode du va-et-vient. Soient A et B des $\mathcal{L}$-structures. Supposons qu'il existe une famille $\mathcal{I}$ d'isomorphismes (partiels) dont le domaine est contenu dans A et l'image dans B, et satisfaisant les deux conditions suivantes:

(i) Pour tout $a \in A$ et $F \in \mathcal{I}$, il existe $F' \in \mathcal{I}$ étendant F ayant a dans son domaine.

(ii) Pour tout $b \in B$ et $F \in \mathcal{I}$, il existe $F' \in \mathcal{I}$ étendant F ayant b dans son image.

Alors $A \equiv B$.

Démonstration. (1) Supposons que T satisfait à la condition indiquée, et soient $A \subseteq B$ deux modèles de T. Du fait que $A \prec_1 B$ on déduit que $Th(A, a)_{a \in A} \cup \Delta(B)$ est consistante. En effet notre hypothèse est équivalente à: toutes les formules universelles à paramètres dans A vraies dans A le sont aussi dans B. Soit $A_1 \models Th(A, a)_{a \in A} \cup \Delta(B)$, que l'on peut donc supposer être une extension élémentaire de A contenant B; en appliquant le même raisonnement à la paire $B \subseteq A_1$ de modèles de T, on obtient une extension élémentaire B_1 de B, contenant A_1.

On construit ainsi inductivement une chaîne

$$A_0 = A \subseteq B_0 = B \subseteq A_1 \subseteq B_1 \subseteq \cdots \subseteq A_n \subseteq B_n \subseteq A_{n+1} \subseteq \cdots$$

où $A_n \prec A_{n+1}$ et $B_n \prec B_{n+1}$. Alors $C = \bigcup_{n \in \mathbf{N}} A_n = \bigcup_{n \in \mathbf{N}} B_n$ est une extension élémentaire de A et de B, ce qui implique que $A \prec B$.

(2) Si toute formule est équivalente modulo T à une formule existentielle, alors elle est aussi équivalente modulo T à une formule universelle (puisque la négation d'une formule existentielle est une formule universelle). Cela montre l'équivalence des deux dernières conditions.

L'équivalence des deux premières conditions découle de la définition de modèle complète, et du résultat de préservation (0.4)(5).

(3) Si T n'admet pas l'élimination des quantificateurs, on peut trouver une sous-structure C de deux modèles A et B de T tels que $(A, c)_{c\in C} \not\equiv (B, c)_{c\in C}$; ces deux modèles ne peuvent évidemment pas se plonger de façon élémentaire dans un même modèle de T.

(4) Nous allons montrer le théorème du va-et-vient. On prouve par induction sur le nombre de quantificateurs d'une formule $\varphi(\bar{x})$ sous forme prénexe que: si $\bar{a}$ est un uplet dans le domaine d'un élément f de $\mathcal{I}$ alors

$$A \models \varphi(\bar{a}) \iff B \models \varphi(f(\bar{a})).$$

Pour les formules sans quantificateurs, c'est par définition d'isomorphisme partiel. Considérons la formule $\varphi(\bar{x}) = \exists y\, \psi(\bar{x}, y)$, et supposons le résultat vrai pour la formule $\psi(\bar{x}, y)$. Supposons que $\bar{a}$ est dans le domaine de la fonction $f \in \mathcal{I}$, et que $A \models \exists y\, \psi(\bar{a}, y)$; soit $b \in A$ tel que $A \models \psi(\bar{a}, b)$. Par hypothèse, il existe $f' \in \mathcal{I}$ étendant f et ayant b dans son domaine. Par hypothèse d'induction, on a $B \models \psi(f'(\bar{a}), f'(b))$, ce qui montre bien que $B \models \varphi(f(\bar{a}))$. On procède de la même façon pour montrer l'autre direction.

Exemples. Nous montrerons plus tard que la théorie du corps $\mathbf{C}$ admet l'élimination des quantificateurs dans le langage des anneaux $\{+, -, \cdot, 0, 1\}$.

Considérons maintenant le corps des réels; on peut montrer que sa théorie T est modèle complète. Cependant elle n'admet pas l'élimination des quantificateurs dans le langage des anneaux: soit C le corps $\mathbf{Q}(\alpha)$, où $\alpha^2 = 2$. On peut plonger C dans le corps des réels de deux façons différentes: en envoyant α sur $\sqrt{2}$ (la racine carrée positive de 2), ou bien sur $-\sqrt{2}$. Ces deux plongements sont incompatibles, car un modèle de T satisfait: $(\forall x \exists y\, (y^2 = x \vee y^2 = -x)) \wedge (\forall x, y\, (x^2 + y^2 = 0) \rightarrow x = y = 0)$. Donc en prenant $A = B = \mathbf{R}$, et en plongeant C dans A et B des deux manières décrites ci-dessus, on voit que T n'admet pas l'élimination des quantificateurs.

(0.6) Ultraproduits

Définitions. Soit I un ensemble, A_i une famille de $\mathcal{L}$-structures, indexée par l'ensemble I. Soit $\mathcal{F}$ un sous-ensemble de $\mathcal{P}(I)$ (l'ensemble des parties de I).

(1) $\mathcal{F}$ est un filtre (sur I) si: (i) $\emptyset \notin \mathcal{F}$, $I \in \mathcal{F}$; (ii) si $X, Y \in \mathcal{F}$ alors $X \cap Y \in \mathcal{F}$; (iii) si $X \subseteq Y$ et $X \in \mathcal{F}$ alors $Y \in \mathcal{F}$.

(2) $\mathcal{F}$ est un ultrafiltre si c'est un filtre maximal, c'est à dire s'il n'est contenu strictement dans aucun filtre. On peut montrer que $\mathcal{F}$ est un ultrafiltre si et seulement si c'est un filtre qui de plus satisfait:

$$\text{pour tout } X \subseteq I,\ X \in \mathcal{F} \iff (I \setminus X) \notin \mathcal{F}.$$

(3) Un filtre $\mathcal{F}$ est dit principal s'il existe un élément $i \in I$ tel que $\mathcal{F} = \{X \subseteq I \mid i \in X\}$. Autrement, $\mathcal{F}$ est appelé non-principal.

(4) Nous allons définir une $\mathcal{L}$-structure sur le produit cartésien des structures A_i de la façon suivante. $\prod_{i\in I} A_i$ est la structure dont l'univers est le produit cartésien des A_i, c'est à dire l'ensemble des fonctions a de I dans la réunion disjointe des A_i,

$i \in I$, satisfaisant $a(i) \in A_i$ pour tout i. Une telle fonction a est aussi notée $a = (a(i))_{i\in I}$. Les fonctions du langage sont définies coordonnée par coordonnée, c'est à dire, $f(a_1,\ldots,a_n)(i) = (f(a_1(i),\ldots,a_n(i)))_{i\in I}$; si c est un symbole de constante, et $c(i)$ est son interprétation dans A_i alors l'interprétation de c dans $\prod_{i\in I} A_i$ est tout simplement $(c(i))_{i\in I}$; enfin si R est un symbole de relation n-aire, alors $\prod_{i\in I} A_i \models R(a_1,\ldots,a_n)$ si et seulement si $A_i \models R(a_1(i),\ldots,a_n(i))$ pour tout $i \in I$.

(5) Soit $\mathcal{F}$ un filtre sur I. On définit une relation d'équivalence sur $\prod_{i\in I} A_i$ de la façon suivante:

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

On vérifie que cette relation d'équivalence est compatible avec les fonctions et relations de $\mathcal{L}$, ce qui nous permet de définir une $\mathcal{L}$-structure sur l'ensemble $\prod_{i\in I} A_i/\mathcal{F}$ des classes d'équivalence modulo $\equiv_{\mathcal{F}}$ des éléments de $\prod_{i\in I} A_i$: l'égalité est donnée par $\equiv_{\mathcal{F}}$; si $[a_1]_{\mathcal{F}},\ldots,[a_n]_{\mathcal{F}} \in \prod_{i\in I} A_i/\mathcal{F}$, alors $f([a_1]_{\mathcal{F}},\ldots,[a_n]_{\mathcal{F}}) = [f(a_1,\ldots,a_n)]_{\mathcal{F}}$, et $\prod_{i\in I} A_i/\mathcal{F} \models R([a_1]_{\mathcal{F}},\ldots,[a_n]_{\mathcal{F}})$ si et seulement si $\{i \in I \mid A_i \models R(a_1(i),\ldots,a_n(i))\} \in \mathcal{F}$; finalement l'interprétation de c est donnée par $[(c(i))_{i\in I}]_{\mathcal{F}}$. Cette structure est appellée le produit réduit des structures A_i relativement au filtre $\mathcal{F}$; si $\mathcal{F}$ est un ultrafiltre, on l'appelle **ultraproduit**, et si de plus toutes les structures A_i sont égales à une même structure A, on parle alors d'**ultrapuissance** de A.

(6) Notons que la $\mathcal{L}$-structure $\prod_{i\in I} A_i/\mathcal{F}$ est une structure quotient de la $\mathcal{L}$-structure $\prod_{i\in I} A_i$.

Le filtre le plus connu est le filtre de Fréchet sur I, qui est l'ensemble de toutes les parties cofinies de I. Si I est fini, tous les ultrafiltres sur I sont principaux. Si I est infini, les ultrafiltres non-principaux sont exactement ceux qui contiennent le filtre de Fréchet sur I. Nous avons implicitement supposé l'axiome du choix (sans lequel il serait impossible de parler de produit cartésien infini). Une application du Lemme de Zorn nous donne alors que tout filtre est contenu dans un ultrafiltre. La cardinalité d'un ultraproduit est soit finie, soit au moins égale à $2^{\aleph_0}$.

Théorème de Łos. Soit $\mathcal{F}$ un filtre sur I, (A_i), $i \in I$, une famille de $\mathcal{L}$-structures, et $A = \prod_{i\in I} A_i/\mathcal{F}$.

(1) Soit $\varphi(\bar{x})$, $\bar{x} = (x_1,\ldots,x_n)$, une formule positive, $\bar{a} = [\bar{a}(i)]_{\mathcal{F}}$ un n-uplet de A. Alors

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

(2) Supposons maintenant que $\mathcal{F}$ est un ultrafiltre, et soit $\varphi(\bar{x})$ une formule quelconque du langage, a un n-uplet de A. Alors,

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

Une conséquence immédiate du théorème de Łos est alors: soit A une structure, $\mathcal{F}$ un ultrafiltre sur l'ensemble I, et considérons l'ultrapuissance $A^{\mathcal{F}} = A^I/\mathcal{F}$. La structure A se plonge de façon naturelle dans $A^{\mathcal{F}}$ via: $a \mapsto [\hat{a}]_{\mathcal{F}}$, où $\hat{a}(i) = a$ pour tout $i \in I$. Ce plongement est élémentaire.

Théorème (Keisler, Shelah). Deux structures A et B sont élémentairement équivalentes si et seulement si elles ont des ultrapuissances isomorphes.

1. Les corps algébriquement clos

(1.1) Nous commençons par étudier la théorie des corps algébriquement clos. Dans ce chapître le langage sera celui des anneaux, $\mathcal{L} = \{+, -, \cdot, 0, 1\}$.

Considérons la théorie suivante, notée ACF, axiomatisée par:

— les énoncés universels dont les modèles sont les anneaux intègres commutatifs, avec unité 1 et zéro 0.

— $\forall x \exists y\,(x = 0 \vee xy = 1)$.

— pour tout entier $n > 1$ l'enoncé: $\forall x_1, \dots, x_n \exists y\ y^n + x_1 y^{n-1} + \cdots + x_{n-1} y + x_n = 0$.

Les modèles de ACF sont les corps algébriquement clos. Un exemple est le corps $\mathbf{C}$ des nombres complexes. Pour p un nombre premier, nous posons $ACF_p = ACF \cup \{p = 0\}$, et $ACF_0 = ACF \cup \{n \neq 0 \mid n \in \mathbf{N}, n > 0\}$.

(1.2) Lemme. Soient K et L des corps algébriquement clos, et supposons que $f : A \to B$ est un isomorphisme entre des sous-structures de K et L respectivement. Soit $a \in K$ un élément algébrique sur A. Alors il existe un isomorphisme f' étendant f et ayant a dans son domaine.

Démonstration. En passant au corps des quotients, on peut supposer que A et B sont des corps. Soit $P(X) \in A[X]$ le polynôme (unitaire) minimal de a au-dessus de A, et $f(P)(X) \in B[X]$ le polynôme obtenu en appliquant f aux coefficients de P. Puisque L est algébriquement clos, il existe $b \in B$, racine de $f(P)(X) = 0$. Nous avons donc

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

Donc f s'étend naturellement en un isomorphisme $f' : A(a) \to B(b)$ qui envoie a sur b.

(1.3) Théorème. La théorie ACF admet l'élimination des quantificateurs, et est donc aussi modèle complète. Les théories ACF_0 et ACF_p sont complètes.

Démonstration. Soient K et L des corps algébriquement clos, non dénombrables, de même caractéristique, et soit C une sous-structure dénombrable commune à K et L. Considérons la famille $\mathcal{I}$ d'isomorphismes f entre des sous-structures dénombrables de K et L contenant C. Nous allons montrer que cette famille satisfait la condition du va-et-vient:

Soit $a \in K$, et $f \in \mathcal{I}$, A le domaine de f, $B = f(A)$; si a est algébrique sur A, alors le lemme nous donne un isomorphisme partiel $f' \in \mathcal{I}$ ayant a dans son domaine. Supposons que a n'est pas algébrique sur A: puisque la cardinalité de L est plus grande que celle de B, il existe $b \in L$ qui n'est pas algébrique sur B. En posant $f'(a) = b$, on peut alors étendre 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 l'autre direction.

Le théorème du va-et-vient nous donne donc:

(1) 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 nouveaux symboles de constantes pour les éléments de C) est complète. Cela veut bien dire que ACF admet l'élimination des quantificateurs.

(2) Prenant $C = \emptyset$ ci-dessus, on obtient précisément que les théories ACF_p et ACF_0 sont complètes.

(1.4) Corollaire. Tout sous-ensemble définissable (avec paramètres) dans un corps algébriquement clos K est fini ou cofini.

Démonstration. Soit $S \subseteq K$ un ensemble définissable, par une formule $\varphi(x)$; grâce à l'élimination des quantificateurs, on peut supposer que $\varphi(x)$ s'écrit $\bigvee_i \varphi_i(x)$, où chaque $\varphi_i(x)$ est une conjonction d'équations et d'inéquations en **une** variable. Il suffit donc de montrer le résultat pour chacune des formules $\varphi_i(x)$. La formule $\varphi_i(x)$ est de la forme $\bigwedge_{j\in I}(p_j(x) = 0) \wedge \bigwedge_{k\in J}(q_k(x) \neq 0)$ pour des polynômes $p_j(x)$ et $q_k(x) \in K[x]$, que nous pouvons supposer non identiquement nuls. Si I est non vide, alors $\varphi(x)$ n'a qu'un nombre fini de solutions, puiqu'un polynôme non nul en une variable n'a qu'un nombre fini de solutions dans un corps. Si $I = \emptyset$, alors J est non-vide, $\varphi_i(x) = \bigwedge_{k\in J}(q_k(x) \neq 0)$, et $\neg\varphi_i(x)$ n'a qu'un nombre fini de solutions.

(1.5) Bases de transcendance. Soient $A \subseteq K$ des corps (ou même des anneaux intègres). Rappelons qu'un élément a de 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 $\bar{b}$ dans B, et polynôme non nul $f(\bar{X}) \in A[\bar{X}]$, $f(\bar{b}) \neq 0$.

Un sous-ensemble B de K algébriquement indépendant sur A et maximal avec cette propriété, est appelé une **base de transcendance de** K **sur** A. Par le lemme de Zorn, tout sous-ensemble de K qui est algébriquement indépendant sur A se complète en une base de transcendance de K sur A.

Remarquons aussi que si B est une base de transcendance de K sur A, alors K est algébrique sur $A(B)$. On montre aussi (de la même façon que pour les bases d'espaces vectoriels) que deux bases de transcendance de K sur A ont la même cardinalité. Cette cardinalité est appelée le **degré de transcendance de** K **sur** A.

(1.6) Automorphismes d'un corps algébriquement clos. Le lemme 1.2 et la preuve de (1.3) nous montrent qu'un corps algébriquement clos a beaucoup d'automorphismes. En effet, si A est 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 est l'identité sur A et envoie a sur b.

(2) Si c et d sont transcendants sur A, alors il existe un automorphisme de K qui est l'identité sur A et envoie c sur d.

Démonstration. (1) Le lemme 1.2 nous donne un isomorphisme partiel f, qui est l'identité sur A, et envoie a sur b. Soit maintenant B une base de transcendance de K sur A. Alors les corps $A(a)(B)$ et $A(b)(B)$ sont isomorphes, par un isomorphisme g qui prolonge f et est l'identité sur B. Des applications répétées du lemme 1.2 nous permettent de prolonger g à un isomorphisme entre la clôture algébrique de $A(a)(B)$ et celle de $A(b)(B)$, c'est à dire en un automorphisme de K.

(2) La démonstration est similaire: soient B_1 et B_2 des bases de transcendance de K sur A, avec B_1 contenant c et B_2 contenant d; puisqu'elles ont la même cardinalité, il existe une bijection $f : B_1 \to B_2$ qui envoie c sur d. On étend f à un isomorphisme $g : A(B_1) \to A(B_2)$ qui est l'identité sur A, et on conclut de la même façon que pour (1).

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

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

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

Remarques. Ces deux notions dépendent du modèle M (ou plutôt de son diagramme élémentaire) dans lequel on se place. En effet si $M \prec N$, les éléments de N algébriques sur $A \subseteq M$ seront dans M.

On montre très facilement les faits suivants:

$$A \subseteq acl(A), \quad A \subseteq B \text{ implique } acl(A) \subseteq acl(B), \quad acl(acl(A)) = acl(A),$$
$$A \subseteq dcl(A) \subseteq acl(A), \quad A \subseteq B \text{ implique } dcl(A) \subseteq dcl(B), \quad dcl(dcl(A)) = dcl(A).$$

(1.8) Nous allons maintenant considérer la relation entre les notions d'algébricité au sens de la théorie des modèles, et au sens algébrique (ie, de la théorie des corps). Soit K un corps algébriquement clos, $A \subseteq K$, $a \in K$, et $\varphi(x)$ une formule de $\mathcal{L}(A)$ satisfaite par a. On a vu que deux cas sont possibles pour l'ensemble défini par $\varphi(x)$: il est soit fini, soit cofini. Il est donc clair que les deux notions d'éléments algébriques sur A coïncident.

Nous allons maintenant étudier de plus près la clôture définissable de A dans K; sans perte de généralité, nous allons supposer que A est un sous-corps de K. Soit $a \in acl(A)$, et soit $p(X) \in A[X]$ son polynôme minimal sur A. Si p est de degré 1, alors $a \in A$. Supposons donc que le degré de p est plus grand que 1. Si b est une autre racine de $p(X) = 0$, par (1.6) il existe un automorphisme de K qui envoie a sur b et laisse A fixé. Cela implique que a et b satisfont les mêmes formules à paramètres dans A. Donc, $a \in dcl(A)$ si et seulement si le polynôme $p(X)$ a une seule racine; puisque p n'est pas linéaire, cela n'est possible que si la caractéristique est $p > 0$, et p est de la forme $X^{p^n} - c = 0$, pour un $c \in A$, $n \in \mathbf{N}$.

Rappelons qu'un corps est **parfait** si sa caractéristique est 0, ou bien si sa caractéristique est $p > 0$ et qu'il est clos par racines p-ièmes. La clôture parfaite d'un corps F de caractéristique $p > 0$ est l'ensemble des éléments de la clôture algébrique de F qui satisfont une équation de la forme $X^{p^n} - a = 0$, où $a \in F$ et $n \in \mathbf{N}$. Elle est notée F^{1/p^∞} et l'on vérifie que c'est un corps: rappelons que $(a+b)^p = a^p + b^p$, et donc $(a+b)^{1/p} = a^{1/p} + b^{1/p}$, ce qui implique que F^{1/p^∞} est clos par addition.

Nous résumons les résultats montrés dans la proposition suivante:

Proposition. Soit A un sous-ensemble du corps algébriquement clos K, et F le plus petit sous-corps de K contenant A. Soit $T = Th(K)$.

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

(2) Un élément de K est définissable sur A au sens de la théorie des modèles si et seulement si il est dans la clôture parfaite de F si et seulement si il est algébrique sur F et est fixé par tout automorphisme de K qui est l'identité sur A.

2. Ensembles algébriques, topologie de Zariski, variétés

Dans ce qui suit, nous avons un corps F, contenu dans un corps algébriquement clos K de cardinalité supérieure à celle de F. Nous notons $\tilde{F}$ la clôture algébrique de F dans K, et F_s la clôture séparable de F dans K.

(2.1) Soit $S \subseteq K^n$. On définit un idéal de $K[X]$, $\bar{X} = (X_1, \ldots, X_n)$:

$$I(S) = \{f(\bar{X}) \in K[\bar{X}] \mid f(\bar{a}) = 0 \text{ pour tout } \bar{a} \in S\}.$$

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

$$V(I) = \{\bar{a} \in K^n \mid f(\bar{a}) = 0 \text{ pour tout } f(\bar{X}) \in I\}.$$

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

$$\begin{gathered} V((0)) = K^n, \quad I(K^n) = (0), \quad V(K[\bar{X}]) = \emptyset, \quad I(\emptyset) = K[\bar{X}], \\ I \subseteq J \text{ implique } V(J) \subseteq V(I), \quad I \subseteq I(V(I)), \\ S \subseteq T \text{ implique } I(T) \subseteq I(S), \quad S \subseteq V(I(S)). \\ I(V(I(S))) = I(S), \quad V(I(V(I))) = V(I). \end{gathered}$$

(2.2) La topologie de Zariski. Les sous-ensembles de K^n de la forme $V(I)$ sont appelés des ensembles algébriques, ou aussi des fermés de Zariski. Si $S \subseteq K^n$, on définit la clôture de Zariski de S par $\tilde{S} = V(I(S))$; c'est bien sûr le plus petit fermé de Zariski contenant S.

Nous allons maintenant montrer que ces fermés définissent une topologie sur K^n, qui satisfait à la condition de chaîne descendante sur les fermés (cela s'appelle une topologie noethérienne). Soient S et T des fermés de K^n, et $I = I(S)$, $J = I(T)$. On vérifie facilement que $S \cap T = V(I, J)$, et donc l'intersection de deux fermés est un fermé. Considérons maintenant l'idéal $I \cap J$; il est clair que $V(I \cap J) \supseteq S \cup T$. Pour montrer l'autre inclusion, soit $\bar{a} \notin S \cup T$; par définition de I et J, il existe $f(\bar{X}) \in I$ et $g(\bar{X}) \in J$ tels que $f(\bar{a}) \neq 0$ et $g(\bar{a}) \neq 0$; cela implique que $f(\bar{a})g(\bar{a}) \neq 0$, et donc que $\bar{a} \notin V(I \cap J)$, puisque $f(\bar{X})g(\bar{X}) \in I \cap J$. Nous avons donc montré que la réunion de deux fermés est fermée.

Rappelons qu'un anneau (commutatif) R est noethérien si toute chaîne strictement croissante d'idéaux est finie, ou de façon équivalente si tout idéal est engendré par un nombre fini d'éléments. En effet, si $(I_n)_{n \in \mathbf{N}}$ est une chaîne croissante d'idéaux de R, alors $I = \bigcup_{n \in \mathbf{N}} I_n$ est engendré par un nombre fini d'éléments, qui se trouvent donc dans un des idéaux I_n, ce qui implique que $I = I_n$. Réciproquement, si $(I_n)_{n \in \mathbf{N}}$ est une suite strictement croissante d'idéaux de R, on prends un élément $a_n \in I_{n+1} \setminus I_n$ pour chaque entier n, et l'on vérifie que l'idéal engendré par les a_n, $n \in \mathbf{N}$, ne peut pas être engendré par un nombre fini d'éléments (puisque ce nombre fini d'éléments serait déjà dans un des idéaux I_n de la suite).

Les corps sont noethériens (puisqu'ils n'ont que l'idéal (0)). On montre que si R est noethérien, alors l'anneau de polynômes $R[X]$ sur R est aussi noethérien (voir par exemple [L2]). La classe des anneaux noethériens est close par quotient.

Une suite strictement décroissante de fermés donne, en passant aux idéaux associés, une suite strictement croissante d'idéaux de $K[\bar{X}]$, qui est donc finie. Cela montre: d'une part qu'il n'y a pas de suite infinie strictement décroissante de fermés dans K^n; et donc, que toute intersection de fermés est l'intersection d'un nombre fini d'entre eux. En particulier, si l'intersection d'une famille de fermés est vide, alors une sous-intersection finie est déjà vide. En passant au complémentaire: tout recouvrement par des ouverts de K^n est un recouvrement fini, c'est à dire que K^n est **compact** pour la topologie de Zariski. (Attention: nous n'éxigeons pas que la topologie soit séparée).

Nous avons donc montré:

La famille des fermés de Zariski est close par réunion finie et intersection arbitraire; toute suite strictement décroissante de fermés est finie. La topologie de Zariski sur K^n est compacte.

(2.3) Nous allons maintenant décrire les idéaux de la forme $I(S)$. Nous commençons par un lemme:

Lemme. Soit I un idéal (propre) de $K[\bar{X}]$. Alors $V(I)$ est non vide.

Démonstration. Soit M un idéal maximal contenant I. Le corps $K[X]/M$ contient naturellement K comme sous-corps, et sa clôture algébrique L est une extension élémentaire de K. Soient $f_1(\bar{X}), \dots, f_m(\bar{X})$ des générateurs de I. Puisque $I \subseteq M$, les éléments $\bar{x}$, les classes de $\bar{X}$ modulo M, satisfont alors: $f_1(\bar{x}) = f_2(\bar{x}) = \cdots = f_m(\bar{x}) = 0$. Comme K est une sous-structure élémentaire de L, $K \models \exists \bar{x}\, f_1(\bar{x}) = f_2(\bar{x}) = \cdots = f_m(\bar{x}) = 0$, ce qui montre $V(I) \neq \emptyset$.

Théorème (Nullstellensatz de Hilbert). Soit $I \subseteq K[\bar{X}]$ un idéal, et $f \in K[\bar{X}]$. Si $f \in I(V(I))$, alors il existe un entier k tel que $f^k \in I$.

Démonstration. Soit J l'idéal de l'anneau $K[\bar{X}, Y]$ engendré par I et par le polynôme $f(\bar{X})Y - 1$ (Y est une nouvelle variable). Nous savons que $V(J) = \emptyset$: par définition de $I(V(I))$, si $\bar{a} \in V(I)$ alors $f(\bar{a}) = 0$, et donc on ne peut trouver d'élément b tel que $f(\bar{a})b = 1$.

Donc $1 \in J$, et nous trouvons des éléments $g(\bar{X}, Y), g_1(\bar{X}, Y), \dots, g_m(\bar{X}, Y) \in K[\bar{X}, Y]$, et $f_1(\bar{X}), \dots, f_m(\bar{X}) \in I$ tels que

$$1 = g(\bar{X}, Y)(f(\bar{X})Y - 1) + f_1(\bar{X})g_1(\bar{X}, Y) + \cdots + f_m(\bar{X})g_m(\bar{X}, Y).$$

Si nous remplaçons chaque occurrence de la variable Y par $(1/f(\bar{X}))$, et multiplions l'équation par une puissance de $f(\bar{X})$ suffisamment grande pour chasser les dénominateurs, nous obtenons une égalité de la forme

$$f(\bar{X})^k = 0 + f_1(\bar{X})g_1(\bar{X}, 1/f(\bar{X}))f(\bar{X})^k + \cdots + f_m(\bar{X})g_m(\bar{X}, 1/f(\bar{X}))f(\bar{X})^k,$$

et la somme de droite est dans I, ce qui montre le théorème.

Il y a donc une bijection entre les idéaux radicaux (ie, satisfaisant: si $f^k \in I$ alors $f \in I$) et les fermés de Zariski de K^n.

(2.4) Corps de définition. Soit V un fermé de Zariski de K^n. On dit que V est défini sur F (un sous-corps de K) si l'idéal $I(V)$ est engendré par $I(V) \cap F[\bar{X}]$. On dit aussi que F est un corps de définition de V.

Théorème. 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 de tous les monômes de $K[\bar{X}]$, c'est à dire les éléments de la forme $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$. Alors M est une base du K-espace vectoriel $K[\bar{X}]$. Soit $B \subseteq M$, K-indépendant modulo I et maximal avec cette propriété; B forme donc une base du K-espace vectoriel R. A tout monôme m de $K[\bar{X}]$ on associe alors une combinaison linéaire A_m d'éléments de B telle que $m - A_m \in I$; cette combinaison linéaire est bien entendu unique. De plus I est engendré par les polynômes $m - A_m$ où m parcourt l'ensemble des monômes de $K[\bar{X}]$: soit $f(\bar{X}) \in I$, et écrivons $f(\bar{X}) = \sum_{m \in M} a_m m$. Alors

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

Donc $\sum_{m \in M} a_m A_m$ est une combinaison linéaire d'éléments de B, qui est dans I (parce que $f(\bar{X})$ et chacun des $(m - A_m)$ sont dans I). Par définition de B, cette somme est donc nulle, ce qui montre bien que $f(\bar{X})$ est dans l'idéal engendré par les $(m - A_m)$, $m \in M$.

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.

Nous donnons maintenant une preuve rapide du théorème quand la caractéristique est 0. L'unicité de la combinaison linéaire A_m implique que tout automorphisme σ de K satisfaisant $\sigma(I) = I$ est l'identité sur K_0. Soit K_1 un corps de définition de V. Alors tout automorphisme de K fixant K_1 satisfait $\sigma(I) = I$ (par définition d'un corps de définition) et donc σ fixe K_0. Cela implique que $K_0 \subseteq dcl(K_1)$, et donc $K_0 \subseteq K_1$ puisque nous sommes en caractéristique 0.

Pour le cas général, supposons V définie sur K_1, et soient $f_1(\bar{X}), \ldots, f_r(\bar{X}) \in K_1[\bar{X}]$ un système de générateurs de $I(V)$. Soit $m_0 \in M \setminus B$. Puisque $(m_0 - A_{m_0}) \in I(V)$, il existe $g_1(\bar{X}), \ldots, g_r(\bar{X}) \in K[\bar{X}]$ tels que

$$(m_0 - A_{m_0}) = f_1(\bar{X}) g_1(\bar{X}) + \cdots + f_r(\bar{X}) g_r(\bar{X}).$$

Ecrivons $f_i(\bar{X}) = \sum_{m \in M} a_{im} m$ et $g_i(\bar{X}) = \sum_{m \in M} b_{im} m$. Alors le coefficient du monôme m dans le polynôme $f_i(\bar{X}) g_i(\bar{X})$ est $\sum_{m_1 m_2 = m} a_{im_1} b_{im_2}$.

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

$$\begin{aligned} c_{m_0}(\bar{Y}) &= 1, \\ c_m(\bar{Y}) &= 0 \qquad \text{pour } m \in M \setminus B,\ m \neq m_0. \end{aligned}$$

Ce système a une solution dans K, (les b_{im}), et donc a une solution (d_{im}) dans K_1. Soit $h_i(\bar{X}) = \sum_{m \in S} d_{im} m$. Par notre choix des coefficients d_{im},

$$f_1(\bar{X}) h_1(\bar{X}) + \cdots + f_r(\bar{X}) h_r(\bar{X}) = m_0 + \sum_{m \in B} e_m m$$

pour des éléments $e_m \in K_1$. Le fait que B est une base modulo I implique que $A_{m_0} = -\sum_{m \in B} e_m m$ et donc que $(m_0 - A_{m_0}) \in K_1[\bar{X}]$.

Donc K_1 contient tous les coefficients des monômes apparaissant dans les polynômes $(m - A_m)$, $m \in M$. Il contient donc K_0.

Attention. Les notions de définition au sens de la théorie des modèles et de la géométrie algébrique diffèrent en caractéristique p positive: en effet l'ensemble des zéros de l'équation $f(x) = 0$ est aussi défini par la formule $f(x)^p = 0$. On a le résultat suivant: si le fermé V est défini par une formule à paramètres dans A, alors V est défini sur $dcl(A)$ au sens algébrique.

Remarques. (1) La démonstration du théorème montre que tout élément de $I(V) \subseteq K[\bar{X}]$ est une K-combinaison linéaire de polynômes $m - A_m$, $m \in M \setminus B$.

(2) Nous avons en fait montré: soit V une fermé de K^n, $I = I(V)$, K_0 le corps de définition de V, et σ un automorphisme de K. Alors,

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

En effet, si $f_1(\bar{X}), \dots, f_m(\bar{x}) \in K[\bar{X}]$ sont des générateurs de I, alors $\sigma(V) = V(\sigma(f_1)(\bar{X}), \dots, \sigma(f_m)(\bar{X}))$, ce qui montre la première équivalence. La deuxième équivalence est implicite dans la preuve du théorème.

(2.5) Supposons maintenant que L est un corps contenant K. On peut se demander si la topologie induite sur K^n par la topologie de Zariski sur L^n coïncide avec la topologie de Zariski sur K^n. Une direction est évidente: si $S \subseteq K^n$ est fermé au sens de K, alors il est la trace sur K^n d'un fermé de L^n.

Une démonstration très élégante de l'autre direction m'a été indiquée par W. Hodges. En fait l'hypothèse de clôture algébrique de K n'est pas nécéssaire. Soit $T \subseteq L^n$ un fermé; nous allons montrer que $T \cap K^n$ est défini par des équations à coefficients dans K. En effet, soient $f_1, \dots, f_m \in L[\bar{X}]$ des polynômes définissant T. Choisissons une base B du K-espace vectoriel L; alors $L[\bar{X}]$ est un $K[\bar{X}]$-module libre sur B. Ecrivons chaque $f_i(\bar{X})$ comme $\sum_{b \in B} g_{i,b}(\bar{X})b$, où les $g_{i,b}(\bar{X}) \in K[\bar{X}]$ sont presque tous nuls. Nous avons alors, pour $\bar{a} \in K^n$:

$$\begin{aligned} \bar{a} \in T &\iff f_1(\bar{a}) = \cdots = f_m(\bar{a}) = 0 \\ &\iff \sum_{b \in B} g_{i,b}(\bar{a})b = 0 \text{ pour tout } i = 1, \dots, m, \\ &\iff g_{i,b}(\bar{a}) = 0 \text{ pour tout } b \in B \text{ et } i = 1, \dots, m, \end{aligned}$$

ce qui montre le résultat.

(2.6) Composantes irréductibles. On dit qu'un fermé de K^n est une **variété**, ou bien 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.

Puisque la topologie est noethérienne, tout fermé se décompose en ses **composantes irréductibles**, c'est à dire s'écrit de façon unique (à permutation près) comme $V_1 \cup \cdots \cup V_m$, où chaque V_i est une variété, et aucun des V_i n'est contenu dans la réunion des autres.

En effet, soit V un fermé. Si V n'est pas irréductible, nous pouvons écrire $V = V_1 \cup V_2$ où V_1 et V_2 sont des fermés contenus strictement dans V. Si V_1 est irréductible, on ne fait rien, sinon on trouve des fermés V_{11} et V_{12} contenus strictement dans V_1 et tels que $V_1 = V_{11} \cup V_{12}$; on fait de même pour V_2, pour V_{11}, etc .... De cette façon on construit un arbre à branchement fini, qui n'a pas de branche infinie, car toute branche donne une suite strictement décroissante de fermés, et on sait qu'une telle suite est finie.

Donc V peut s'écrire comme $V_1 \cup \cdots \cup V_m$, où chaque V_i est un fermé irréductible. On peut maintenant supposer qu'aucun des V_i n'est contenu dans la réunion des autres: si $V_1 \subseteq V_2 \cup \cdots \cup V_m$ alors $V_1 = (V_1 \cap V_2) \cup \cdots \cup (V_1 \cap V_m)$; comme V_1 est irréductible, il existe i tel que $V_1 \cap V_i = V_1$, ce qui implique que $V_1 \subseteq V_i$.

Un résultat analogue est vrai pour les composantes F-irréductibles d'un fermé défini sur F.

On vérifie facilement que pour un fermé V défini sur F:

$$V \text{ est une variété si et seulement si } I(V) \text{ est premier,}$$
$$V \text{ est } F\text{-irréductible si et seulement si } I(V) \cap F[X] \text{ est premier.}$$

Vérifions par exemple la première équivalence. Supposons que $V = V_1 \cup V_2$, où V_1 et V_2 sont des fermés strictement contenus dans V. Alors les idéaux $I(V_1)$ et $I(V_2)$ contiennent strictement $I(V)$; soient $f(\bar{X}) \in I(V_1) \setminus I(V)$, $g(\bar{X}) \in I(V_2) \setminus I(V)$ et considérons le polynôme $f(\bar{X})g(\bar{X})$: il s'annule sur V_1 et sur V_2, donc sur V. Donc $f(\bar{X})g(\bar{X}) \in I(V)$, bien que $f(\bar{X})$ et $g(\bar{X})$ ne soient pas dans $I(V)$, ce qui montre que $I(V)$ n'est pas premier.

Réciproquement, supposons que $I(V)$ n'est pas premier, et soient $f(\bar{X})$ et $g(\bar{X})$ des polynômes qui ne sont pas dans $I(V)$ mais dont le produit est dans $I(V)$. Soient $V_1 = V(I(V), f(\bar{X}))$ et $V_2 = V(I(V), g(\bar{X}))$; ils sont strictement contenus dans V. D'autre part tout point $\bar{a}$ de V satisfait $f(\bar{a})g(\bar{a}) = 0$, et donc satisfait $f(\bar{a}) = 0$ ou $g(\bar{a}) = 0$, ce qui montre que $V = V_1 \cup V_2$ et que V n'est pas irréductible.

Les composantes irréductibles correspondent donc aux idéaux minimaux parmi les idéaux premiers contenant $I(V)$.

Il est clair que l'irréductibilité d'un fermé défini sur F implique son F-irréductibilité; la réciproque est cependant fausse: considérons le fermé défini par $x^2 + y^2 = 0$; il est $\mathbf{Q}$-irréductible, mais n'est pas $\mathbf{Q}(i)$-irréductible.

En fait on a le résultat suivant, qui sera montré dans (2.9): soit V un fermé défini sur F. Alors $V = V_1 \cup \ldots \cup V_m$, où les V_i sont des variétés définies sur une extension normale et finie E de F. Le groupe des automorphismes de E fixant F, $Aut(E/F)$, permute les composantes V_i; si V est F-irréductible, alors il les permute transitivement. La première assertion est plus ou moins évidente, puisque $Aut(E/F)$ induit un automorphisme de $E[\bar{X}]$ qui envoie $I(V)$ sur $I(V)$ et donc envoie un idéal premier minimal contenant $I(V)$ sur un autre idéal premier minimal contenant $I(V)$.

Donc en particulier, la notion de variété est indépendante du corps algébriquement clos dans lequel on travaille.

(2.7) Soit V un fermé de K^n. On définit l'anneau affine de V: $K[V] = K[X]/I(V)$; si V est défini sur F, on définira $F[V] = F[X]/(I(V) \cap F[X])$. Si V est irréductible, alors

$K[V]$ est un anneau intègre, et on notera $K(V)$ son corps de fractions (corps des fonctions rationnelles sur V). De même, si V est F-irréductible, on note $F(V)$ le corps des fractions de $F[V]$.

Si V est une variété, on définit la dimension de V, $dim(V)$, comme étant égale au degré de transcendance de $K[V]$ sur K; si V est un fermé quelconque, alors $dim(V)$ est égale au maximum des dimensions de ses composantes irréductibles.

Soit V un fermé F-irréductible défini sur F, et soit $\bar{a} \in K^n$. On dit que $\bar{a}$ est un point **générique** de V (sur F) si $\bar{a} \in V$ et le F-homomorphisme: $F[V] \to F[\bar{a}]$ qui envoie la classe de $\bar{X}$ modulo $I(V)$ sur le n-uplet $\bar{a}$, est un isomorphisme. Cela est équivalent à dire que $\bar{a} \in V$ et le degré de transcendance de $F(\bar{a})$ sur F est égal à $dim(V)$. Si $\bar{a}$ et $\bar{b}$ sont des génériques de V sur F, alors il existe un F-automorphisme de K qui envoie $\bar{a}$ sur $\bar{b}$, puisque les anneaux $F[\bar{a}]$ et $F[\bar{b}]$ sont F-isomorphes.

Soit $\bar{a} \in K^n$; on définit

$$I(\bar{a}/F) = \{f(\bar{X}) \in F[\bar{X}] \mid f(\bar{a}) = 0\}.$$

Les assertions suivantes sont des conséquences immédiates de la définition:

(1) $I(\bar{a}/F)$ est un idéal premier de $F[\bar{X}]$, et $F[\bar{a}] \simeq_F F[\bar{X}]/I(\bar{a}/F)$.

(2) Donc si V est le fermé de K^n défini par $I(\bar{a}/F)$, alors V est F-irréductible, et $\bar{a}$ est un générique de V sur F. On a, pour $\bar{b} \in K^n$:

$$\bar{b} \in V \iff I(\bar{b}/F) \supseteq I(\bar{a}/F) \iff I(\bar{b}/F) \supseteq I(V) \cap F[\bar{X}].$$

(3) Un élément $b \in V$ est générique de V sur F si et seulement si $I(\bar{b}/F) = I(V) \cap F[\bar{X}]$.

(4) Si $\bar{b} \in V$, alors il existe un homomorphisme: $F[\bar{a}] \to F[\bar{b}]$ qui est l'identité sur F et envoie $\bar{a}$ sur $\bar{b}$.

(5) Soit V un ensemble algébrique défini sur F, et supposons qu'il existe un point $\bar{a} \in V$ tel que pour tout $\bar{b} \in V$, il existe un F-homomorphisme $F[\bar{a}] \to F[\bar{b}]$ qui envoie $\bar{a}$ sur $\bar{b}$. Alors V est F-irréductible et $\bar{a}$ est un point générique de V sur F. En effet notre hypothèse entraîne que $I(\bar{b}/F)$ contient $I(\bar{a}/F)$ pour tout $\bar{b} \in V$; donc $I(V) \cap F[\bar{X}] = I(\bar{a}/F)$, et c'est un idéal premier.

(2.8) Soit A et B deux F-algèbres (contenues dans une F-algèbre C). On dit que A et B sont linéairement disjointes au-dessus de F, si tout ensemble d'éléments de A qui est linéairement indépendant au dessus de F, le reste au-dessus de B (par linéairement indépendant au-dessus de F nous voulons dire: linéairement indépendant au sens de l'espace vectoriel sur F). Nous allons montrer que cette définition est en fait symétrique.

Soient $a_1 \dots a_n \in A$ et supposons qu'ils sont linéairement indépendants sur F, mais ne le sont pas sur B. Soient $b_1, \dots, b_n \in B$ tels que $a_1 b_1 + \dots + a_n b_n = 0$; en renumérotant les éléments, on peut supposer que $b_1, \dots, b_m$ sont indépendants sur F, et que $b_{m+1}, \dots, b_n$ sont des F-combinaisons linéaires de $b_1, \dots, b_m$; écrivons les $b_j = \sum_{i=1}^{m} c_{ji} b_i$, pour $j =$

$m+1,\ldots,n$, et $c_{ji} \in F$. Alors

$$\begin{aligned}
0 &= a_1b_1 + \ldots + a_nb_n \\
&= a_1b_1 + \ldots + a_mb_m + a_{m+1}(\sum_{i=1}^{m} c_{m+1,i}b_i) + \cdots + a_n(\sum_{i=1}^{m} c_{ni}b_i) \\
&= (a_1 + \sum_{j=m+1}^{n} a_jc_{j1})b_1 + \cdots + (a_m + \sum_{j=m+1}^{n} a_jc_{jm})b_m.
\end{aligned}$$

La somme de droite est une combinaison linéaire de $b_1,\ldots,b_m$ à coefficients dans A, et ces coefficients sont non nuls parce qu'ils sont des F-combinaisons linéaires de $a_1,\ldots,a_n$.

Exemples. (1) Soit A une extension algébrique de F, et t un élément transcendant sur A. Alors A et $F(t)$ sont linéairement disjoints au-dessus de F.

(2) En géneral, si A et B sont linéairement disjoints au-dessus de F, et A' est une sous-algèbre de A, alors A' et B sont linéairement disjoints au-dessus de F.

(3) A et B sont linéairement disjoints au-dessus de F si et seulement si l'homomorphisme naturel $A\bigotimes_F B \to A[B]$ est un isomorphisme. ($A[B]$ désigne l'anneau engendré par A et B).

Rappelons que l'algèbre $A\bigotimes_F B$ est définie de la façon suivante: soient $A_0 \subseteq A$ et $B_0 \subseteq B$ des bases pour les F-espaces vectoriels A et B; nous supposerons que A_0 et B_0 contiennent 1. Alors $A\bigotimes_F B$ a comme F-espace vectoriel sous-jacent l'espace vectoriel avec base $\{a\otimes b \mid a\in A_0, b\in B_0\}$.

Pour $c \in A$ et $b \in B$, on définit de la façon suivante l'élément $a\otimes b \in A\bigotimes_F B$: écrivons $c = \sum_{a\in A_0} c_a a$, et $d = \sum_{b\in B_0} d_b b$, où les c_a et d_b sont des éléments de F presque tous nuls. Alors

$$c\otimes d = \sum_{a\in A_0, b\in B_0} c_a d_b a\otimes b.$$

Cette somme est bien définie car presque tout les $c_a d_b$ sont nuls.

On définit maintenant la multiplication sur les éléments de la base de la façon suivante: si $a,c\in A_0$ et $b,d\in B_0$ alors $(a\otimes b)(c\otimes d) = (ac)\otimes(bd)$.

La multiplication est ensuite étendue à $A\bigotimes_F B$ de la seule façon possible pour qu'elle satisfasse aux règles de distributivité. On vérifie que tout cela marche bien. Pour plus de détails, voir [L2].

Remarquons aussi que A et B se plongent de façon naturelle dans $A\bigotimes_F B$: les applications: $A\to A\bigotimes_F B$, $a\mapsto a\otimes 1$, et $B\to A\bigotimes_F B$, $b\mapsto 1\otimes b$, sont des isomorphismes de F-algèbres.

(4) Soient A et B des F-algèbres. Alors A et B sont linéairement disjoints 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 (c'est à dire pouvant être engendrées en tant que F-algèbres par un nombre fini d'éléments), A_0 et B_0 sont linéairement disjointes au-dessus de F.

(5) Soient a et b deux racines cubiques distinctes de 2. Alors $\mathbf{Q}(a)\cap\mathbf{Q}(b) = \mathbf{Q}$; cependant $\mathbf{Q}(a)$ et $\mathbf{Q}(b)$ ne sont pas linéairement disjoints au-dessus de $\mathbf{Q}$: en effet, le polynôme X^3-2 s'écrit $(X-a)(X-b)(X-2/(ab))$, et donc ne reste pas irréductible au-dessus de $\mathbf{Q}(a)$. Cependant, on a le résultat suivant:

(6) 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 $A \cap B = F$.

Il est clair que si $A \cap B \neq F$, alors A et B ne sont pas linéairement disjoints au-dessus de F. Pour la réciproque, par (4) 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 parce que A est une extension séparable finie de F), et soit $p(X)$ son polynôme minimal (unitaire) sur F, $q(X)$ son polynôme minimal (unitaire) sur B, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ les racines de $p(X)$. Alors $q(X)$ divise $p(X)$, et l'on a $p(X) = \prod_{i=1}^{m}(X - \alpha_i)$, et $q(X) = \prod_{i \in J}(X - \alpha_i)$ pour un sous-ensemble J de $\{1, \ldots, m\}$. Les coefficients de $q(X)$ sont donc dans le corps A, puisque A contient tous les α_i. Ils sont aussi dans B, et donc dans $A \cap B = F$. Comme $p(X)$ est irréductible sur F, cela implique que $q(X) = p(X)$ et donc que A et B sont linéairement disjoints au-dessus de F, puisque $[A : F] = [B(\alpha) : B]$.

(7) 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 (le corps engendré par E_1 et L) et E_2 sont linéairement disjoints au-dessus de E_1.

(2.9) Théorème. (Décomposition d'un fermé F-irréductible). Soient V un fermé défini sur F et F-irréductible, et $V_1, \ldots, V_m$ ses composantes irréductibles. Alors $V_1, \ldots, V_m$ sont définies sur une extension normale finie E de F; le groupe des automorphismes de E qui sont l'identité sur F, $G = Aut(E/F)$, agit transitivement sur les composantes V_i (c'est à dire, pour tout i et j il existe $\sigma \in G$ tels que $\sigma(V_i) = V_j$. On a $dim(V_i) = dim(V)$ pour tout i.

Démonstration. Nous allons d'abord montrer que les variétés V_i sont définies sur une extension algébrique de F. Soit $\sigma \in Aut(K/F)$. Alors $\sigma(V) = V$, et donc σ permute les composantes V_i. Comme le groupe des permutations de l'ensemble $\{1, \ldots, m\}$ a $m!$ éléments, cela implique que $\sigma^{m!}(V_i) = V_i$ pour tout i.

Donc, si $\sigma \in Aut(K/F)$, alors $\sigma^{m!}$ est l'identité sur le corps de définition de chaque V_i, et donc sur le plus petit corps E contenant les corps de définition des V_i. Notons que si E_i est le corps de définition de V_i, et $\sigma \in Aut(K/F)$, alors $\sigma(E_i)$ est le corps de définition de la variété $\sigma(V_i)$; cela montre que E est une extension normale de F.

Nous allons maintenant montrer que toutes les composantes de V ont la même dimension, qui est égale à $dim(V)$. Puisque chaque V_i est incluse dans V, il est clair que $dim(V_i) \leq dim(V)$.

Soit $\bar{a} \in K^n$ un générique de V sur F, et $\bar{b} \in K^n$ un générique de V_i sur $\tilde{F}$ ($\tilde{F}$ est la clôture algébrique de F dans K). Puisque $\bar{b} \in V$, il existe un F-homomorphisme $\varphi : F[\bar{a}] \to F[\bar{b}]$ qui envoie $\bar{a}$ sur $\bar{b}$. Cet homomorphisme s'étend à $\tilde{F}$ (par (1.2)), et nous avons donc un F-homomorphisme

$$\tilde{\varphi} : \tilde{F}[\bar{a}] \to \tilde{F}[\bar{b}].$$

La restriction de $\tilde{\varphi}$ à $\tilde{F}$ est un élément de $Aut(\tilde{F}/F)$, que nous noterons ψ. Puisque K est algébriquement clos, de degré de transcendance infini sur F, on peut trouver $\bar{c} \in K^n$, et un isomorphisme

$$\theta : \tilde{F}[\bar{a}] \to \tilde{F}[\bar{c}]$$

étendant ψ et envoyant $\bar{a}$ sur $\bar{c}$. Alors

$$\tilde{\varphi} \circ \theta^{-1} : \tilde{F}[\bar{c}] \to \tilde{F}[\bar{b}]$$

envoie $\bar{c}$ sur $\bar{b}$, est un $\tilde{F}$-homomorphisme (car $\psi \circ \psi^{-1} = id$). Soit j tel que $\bar{c} \in V_j$; puisque $\bar{c}$ est un générique de V sur F, il est un générique de V_j sur $\tilde{F}$ (car $dim(V_j) \leq dim(V)$), et nous avons donc:

$$I(V_j) \cap \tilde{F}[\bar{X}] = I(\bar{c}/\tilde{F}) \subseteq I(\bar{b}/\tilde{F}) = I(V_i) \cap \tilde{F}[\bar{X}].$$

Cela implique que $I(V_j) \subseteq I(V_i)$, et donc $V_i = V_j$ par définition de la décomposition en composantes irréductibles. Donc $\tilde{\varphi} \circ \theta^{-1}$ est un isomorphisme, ce qui entraîne que φ est aussi un isomorphisme.

Nous avons donc montré que toutes les composantes de V ont la même dimension que V. Cela implique qu'un générique de V_i sur $\tilde{F}$ est aussi un générique de V sur F. Si $\bar{a}$ et $\bar{b}$ sont deux génériques quelconques de V sur F, alors il existe un automorphisme $\sigma \in Aut(K/F)$ qui envoie $\bar{a}$ sur $\bar{b}$, ce qui montre bien que $Aut(K/F)$, et donc $Aut(E/F)$, permute transitivement les V_i.

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

Démonstration. Supposons que $F(\bar{a})$ et E sont linéairement disjoints au-dessus de F. Soit $f(\bar{X}) \in I(\bar{a}/E)$, soit C une base du F-espace vectoriel E, et écrivons $f(\bar{X}) = \sum_i c_i f_i(\bar{X})$, avec $c_i \in C$ et $f_i(\bar{X}) \in F[\bar{X}]$. Puisque $f(\bar{a}) = 0$, $\sum_i c_i f_i(\bar{a}) = 0$, ce qui entraîne que chaque $f_i(\bar{a}) = 0$ (par disjonction linéaire). Donc les polynômes $f_i(\bar{X})$ sont dans $I(\bar{a}/F)$, ce qui donne le résultat souhaité.

Réciproquement, supposons que $I(\bar{a}/E)$ est engendré par des polynômes de $F[\bar{X}]$. Pour montrer que $F(\bar{a})$ et E sont linéairement disjoints au-dessus de F, il suffit de montrer que $F[\bar{a}]$ et E sont linéairement disjoints au-dessus de F (pourquoi?). Soit M l'ensemble des monômes de $F[\bar{X}]$, et $B \subseteq M$ une base du F-espace vectoriel $F[\bar{X}]/I(\bar{a}/F)$. Alors $\{b(\bar{a}) \mid b \in B\}$ est une base du F-espace vectoriel $F[\bar{a}]$. Il suffit donc de montrer que cette base reste indépendante dans $E[\bar{a}]$. Soient $b_1, \ldots, b_r \in B$, $c_1, \ldots, c_r \in E$ et supposons que $b_1(\bar{a})c_1 + \cdots + b_r(\bar{a})c_r = 0$. Alors $b_1c_1 + \cdots b_rc_r \in I(\bar{a}/E)$. Puisque $I(\bar{a}/E)$ est engendré par $I(\bar{a}/F)$, par la remarque (2.4)(1) il existe des éléments $e_m \in E$, pour $m \in M \setminus B$, tels que

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

Cela donne

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

Puisque les monômes de M forment une base du E-espace vectoriel $E[\bar{X}]$, et que la somme de gauche est une combinaison linéaire d'éléments de B, nous en déduisons que $e_m = 0$ pour tout $m \in M \setminus B$, ce qui entraîne $b_1c_1 + \cdots + b_rc_r = 0$, et donc $c_1 = \cdots c_r = 0$.

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

Démonstration. Nous savons que V est définie sur une extension purement inséparable de F, mais pas nécessairement sur F. 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 $\sigma \in Aut(K/\tilde{F})$ tel que $\sigma(\bar{a}) = \bar{b}$ (autrement dit: 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 $I(\bar{a}/\tilde{F})$ (parce que $I(\bar{a}/F^{1/p^\infty}) = I(V) \cap F^{1/p^\infty}[\bar{X}]$);

(4) si $\bar{a}$ est un générique de V sur F, alors $F^{1/p^\infty}(\bar{a})$ et $\tilde{F}$ sont linéairement disjoints au-dessus de F^{1/p^∞} (par (2.10);

(5) $F^{1/p^\infty}(V)$ et $\tilde{F}$ sont linéairement disjoints au-dessus de F^{1/p^∞} (puisque $F(\bar{a}) \simeq_F F(V)$).

Il est donc clair, par (5), que si V est une variété, alors $F(V) \cap F_s = F$.

Pour la réciproque, nous savons par (2.8)(6) que $F(V) \cap F_s = F$ entraîne que $F(V)$ et F_s sont linéairement disjoints au-dessus de F. Par (2.10), 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; puisque $I(\bar{b}/F_s) = I(\bar{a}/F_s)$, il existe donc un automorphisme de K fixant F_s et envoyant $\bar{a}$ sur $\bar{b}$. Mais un tel automorphisme laisse $\tilde{F}$ fixé (puisque $\tilde{F}$ est une extension purement inséparable de F_s), ce qui montre que V n'a qu'une seule composante irréductible, et est donc une variété.

(2.12) Extensions régulières. Nous avons donc les critères suivants, pour $\bar{a}$ un n-uplet de K:

(1) Le fermé de K^n défini par $I(\bar{a}/F)$ est défini sur F si et seulement si $F(\bar{a})$ et F^{1/p^∞} sont linéairement disjoints au-dessus de F (voir exercice).

(2) Le fermé de K^n défini par $I(\bar{a}/F)$ est une variété si et seulement si $F(\bar{a}) \cap F_s = F$.

(3) Le fermé de K^n défini par $I(\bar{a}/F)$ est une variété définie sur F si et seulement si $F(\bar{a})$ et $\tilde{F}$ sont linéairement disjoints au-dessus de F.

Définition. Soit $L \subseteq K$ un corps contenant F; on dit que L est une extension régulière de F si L et $\tilde{F}$ sont linéairement disjoints au-dessus de F.

Remarques. Soit $\bar{a}$ un n-uplet de K. Si F est parfait, alors $F(\bar{a})$ satisfait aux conditions équivalentes de (1); pour que $F(\bar{a})$ soit régulière sur F, il suffit donc que $F(\bar{a}) \cap F_s = F$.

Si F est algébriquement clos, toutes ses extensions sont régulières.

(2.13) Théorème. Soient $\bar{a}, \bar{b} \in K^n$, et supposons que $I(\bar{a}/F) \subseteq I(\bar{b}/F)$. Alors

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

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

Démonstration. Puisque $I(\bar{a}/F) \subseteq I(\bar{b}/F)$ nous avons un F-homomorphisme $\varphi : F[\bar{a}] \to F[\bar{b}]$ qui envoie $\bar{a}$ sur $\bar{b}$. Supposons que $f(a_1, \ldots, a_r) = 0$, où $f(X_1, \ldots, X_r) \in F[X_1, \ldots, X_r]$; alors $\varphi(f(a_1, \ldots, a_r)) = 0 = f(b_1, \ldots, b_r)$, ce qui montre la première assertion.

Supposons que $deg.tr(\bar{a}/F) = deg.tr(\bar{b}/F)$. Nous voulons montrer que φ est un isomorphisme. En renumérotant les éléments du uplet, nous pouvons supposer que $b_1, \ldots, b_d$ forment une base de transcendance de $F(\bar{b})$ sur F. Alors $a_1, \ldots, a_d$ sont aussi algébriquement indépendants au-dessus de F, et donc forment une base de transcendance de $F(\bar{a})$ sur F (puisque $deg.tr(\bar{a}/F) = deg.tr(\bar{b}/F)$). En particulier, $Ker(\varphi) \cap F[a_1, \ldots, a_d] = (0)$.

Soit $c \in F[\bar{a}]$, $c \neq 0$, et $f(X) \in F(a_1, \ldots, a_d)[X]$ son polynôme minimal sur $F(a_1, \ldots, a_d)$; nous multiplions $f(X)$ par un élément de $F[a_1, \ldots, a_d]$ pour obtenir un polynôme $g(X)$ dont les coefficients sont des éléments non nuls de $F[a_1, \ldots, a_d]$. Alors les coefficients de $\varphi(g)(X)$ sont aussi non-nuls et $\varphi(c)$ en est une racine. Comme le coefficient constant de $\varphi(g)(X)$ est non-nul, 0 n'est pas une racine de $\varphi(g)(X)$, ce qui montre que $\varphi(c) \neq 0$.

Corollaire. Soient $V \subseteq W$ des fermés F-irréductibles. Alors $dim(V) \leq dim(W)$. Si $dim(V) = dim(W)$ alors $V = W$. Ou encore: si l'inclusion de V dans W est stricte, alors $dim(V) < dim(W)$.

(2.14) Proposition. 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, alors la réciproque de (1) est vraie: si L et M sont algébriquement indépendants au-dessus de F, alors ils sont linéairement disjoints au-dessus de F.

(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 $f(\bar{X}) \in M[\bar{X}]$, $\bar{X} = (X_1, \ldots, X_n)$, et $\bar{a} \in L^n$, et supposons que $f(\bar{a}) = 0$. Nous écrivons alors $f(\bar{a})$ comme une M-combinaison linéaire de monômes en $a_1, \ldots, a_n$, et la disjonction linéaire de L et M au-dessus de F entraîne alors l'existence d'un polynôme $g(\bar{X}) \in F[\bar{X}]$ tel que $g(\bar{a}) = 0$.

(2) Supposons que L et M sont algébriquement indépendants au-dessus de F, et soit $\bar{a} \in L^n$. Nous voulons montrer que $I(\bar{a}/F)$ engendre $I(\bar{a}/M)$. Puisque 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, $deg.tr(\bar{a}/F) = deg.tr(\bar{a}/M)$, ce qui montre que $\bar{a}$ est aussi un générique de V sur M par (2.13), et donc que $I(\bar{a}/F)$ engendre $I(\bar{a}/M)$. Par (2.10), nous en concluons que $F(\bar{a})$ et M sont linéairement disjoints au-dessus de F. Cela étant vrai pour tout uplet fini de L, nous en déduisons le résultat.

(3) Par hypothèse, L et $\tilde{F}$ sont linéairement disjoints au-dessus de F; le fait que M et L soient algébriquement indépendants au-dessus de F implique que $\tilde{F}M$ et $\tilde{F}L$ le sont aussi (passer de F à $\tilde{F}$ ne change rien au degré de transcendance). Donc, par (2) et (2.8)(7), L et $\tilde{F}M$ sont linéairement disjoints au-dessus de F, ce qui donne la conclusion.

3. Corps finis

Soit p un nombre premier. L'idéal $p\mathbf{Z}$ de $\mathbf{Z}$ est un idéal maximal, et $\mathbf{Z}/p\mathbf{Z}$ est un corps, avec p éléments. On le note $\mathbf{F}_p$ et on l'appelle le corps premier de caractéristique p. Il est contenu dans tout corps de caractéristique p, puisqu'il est engendré par 1.

Soit F un corps fini, avec n éléments. On regarde F comme un groupe additif, d'ordre n. Le sous-groupe de F engendré par 1, est donc un sous-groupe d'ordre m, pour un diviseur m de n, et ce sous-groupe est isomorphe à $\mathbf{Z}/m\mathbf{Z}$. En fait il est isomorphe à $\mathbf{Z}/m\mathbf{Z}$ en tant qu'anneau, ce qui implique que $\mathbf{Z}/m\mathbf{Z}$ est intègre, et donc que m est un nombre premier.

Nous avons donc montré que tout corps fini F contient un sous-corps isomorphe à $\mathbf{F}_p$ pour un nombre premier p. Le corps F a donc une structure naturelle d'espace vectoriel sur $\mathbf{F}_p$, ce qui implique en particulier que son ordre doit être un puissance de p.

Soit F un corps fini de caractéristique p, ayant $q = p^m$ éléments, et soit K un corps algébriquement clos le contenant. Considérons maintenant le groupe multiplicatif $F^\times = F \setminus \{0\}$. Il a exactement $q-1$ éléments, et donc tout élément a de $F^\times$ satisfait $a^{q-1} = 1$. Cela implique que tout élément de F est racine de l'équation

$$X^q - X = 0.$$

La dérivée du polynôme $X^q - X$ est égale à $qX^{q-1} - 1 = -1$ (puisque $q = 0$ dans F), et donc ne peut jamais être égale à 0. L'équation $X^q - X = 0$ a donc q racines distinctes, qui sont précisément les éléments de F. Nous avons alors

$$X^q - X = \prod_{a \in F} (X - a).$$

Remarquons que cela implique qu'il y a un seul corps de cardinalité q (dans K). Nous le noterons $\mathbf{F}_q$.

Réciproquement, soit $q = p^m$, et considérons l'ensemble S des solutions dans K de l'équation $X^q - X = 0$. Puisque la dérivée de ce polynôme égale -1, ses racines sont toutes distinctes et S a donc q éléments. Il est clair que S est clos par multiplication, et par inverse multiplicatif. Aussi, puisque nous sommes en caractéristique $p > 0$, et que q est une puissance de p, nous avons:

$$(a + b)^q = a^q + b^q$$

pour tout éléments a, b. Cela implique que S est clos par addition, et donc que S est un sous corps de K.

En résumé nous avons donc montré:

(3.1) Théorème. Soit F un corps fini. Alors il contient le corps $\mathbf{F}_p$ pour un p premier, et a $q = p^m$éléments, pour un entier m. Ses éléments sont exactement les racines de l'équation $X^q - X$.

Etant donnée une puissance q d'un nombre premier p, il existe un seul corps de cardinalité q, que nous noterons $\mathbf{F}_q$.

(3.2) Le groupe multiplicatif d'un corps fini est cyclique. Soit $F = \mathbf{F}_q$ un corps fini, $F^\times = F \setminus \{0\}$ son groupe multiplicatif, qui a donc $q-1$ éléments. Nous allons montrer que ce groupe est cyclique (c'est à dire engendré par un élément). $F^\times$ est un groupe abélien fini, et s'écrit donc comme la somme directe de ses composantes ℓ-aires $U(\ell)$, où ℓ parcourt l'ensemble des nombres premiers divisant $q-1$, et $U(\ell)$ est l'ensemble des éléments de $F^\times$ d'ordre une puissance de ℓ.

Rappelons que pour des entiers m, n,

$$\mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z} \text{ est cyclique} \iff \text{le pgcd } (m,n) = 1.$$

Il suffit donc de montrer que chaque $U(\ell)$ est cyclique. Nous savons que $U(\ell)$ s'écrit comme une somme directe de groupes cycliques. Supposons que $U(\ell)$ n'est pas cyclique, et soit ℓ^r son ordre. Alors $U(\ell) = A \oplus \mathbf{Z}/\ell^s\mathbf{Z}$, avec $1 \leq s < r$. Cela implique que tout élément de $U(\ell)$ satisfait l'équation $X^{\ell^{r-1}} = 1$. Mais une telle équation a au plus ℓ^{r-1} solutions!! C'est une contradiction et donc $F^\times$ est cyclique.

(3.3) Un corps fini est parfait. L'ordre de $F^\times$ est premier à p. Cela implique que l'endomorphisme multiplicatif $x \to x^p$ a un noyau trivial, et donc qu'il est surjectif, puisque $F^\times$ est fini.

(3.4) La clôture algébrique de $\mathbf{F}_p$. Fixons un nombre premier p. Soient m et n des entiers. Nous avons alors

$$\mathbf{F}_{p^m} \subseteq \mathbf{F}_{p^n} \iff m|n.$$

En effet, si $\mathbf{F}_{p^n}$ contient $\mathbf{F}_{p^m}$, il est alors un $\mathbf{F}_{p^m}$-espace vectoriel, et donc p^n est une puissance de p^m, ce qui implique que $m|n$. Réciproquement, si $m|n$, alors $(p^m-1)|(p^n-1)$, ce qui montre que $\mathbf{F}_{p^m} \subseteq \mathbf{F}_{p^n}$. Soient m et n des entiers, d leur plus grand diviseur commun, et $e = mn/d$:

$$\mathbf{F}_{p^m} \cap \mathbf{F}_{p^n} = \mathbf{F}_{p^d} \quad \text{et} \quad \mathbf{F}_{p^m}\mathbf{F}_{p^n} = \mathbf{F}_{p^e}.$$

On a aussi: si $n = mf$ alors $[\mathbf{F}_{p^n} : \mathbf{F}_{p^m}] = f$. Les extensions algébriques finies de $\mathbf{F}_p$ sont toutes des corps finis, et réciproquement tout corps fini de caractéristique p est une extension algébrique de $\mathbf{F}_p$. La clôture algébrique de $\mathbf{F}_p$ est donc obtenue en prenant la réunion de tous les corps finis:

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

avec les inclusions naturelles $\mathbf{F}_{p^m} \subseteq \mathbf{F}_{p^n}$ ssi m divise n.

(3.5) L'automorphisme de Frobénius. Groupes de Galois. Le corps $\mathbf{F}_q$ est l'ensemble des solutions de l'équation $X^q - X$, et c'est donc une extension normale de $\mathbf{F}_p$, séparable, donc une extension Galoisienne de $\mathbf{F}_p$. Considérons l'application $\varphi : \mathbf{F}_q \to \mathbf{F}_q$, $x \mapsto x^p$. C'est une bijection, et un automorphisme de $\mathbf{F}_q$. Si $a \in \mathbf{F}_p$ alors $a^p = a$, et donc φ est l'identité sur $\mathbf{F}_p$. Si $q = p^m$, nous avons alors: $\varphi^m = id$.

D'autre part l'ordre de φ est exactement m: le sous-corps de $\mathbf{F}_q$ fixé par φ^d pour un diviseur d de m, est l'ensemble des solutions de $X^{p^d} = X$, c'est à dire le sous-corps $\mathbf{F}_{p^d}$ de $\mathbf{F}_q = \mathbf{F}_{p^m}$, qui est un sous-corps propre de $\mathbf{F}_q$ si $d < m$.

Puisque le groupe de Galois $\mathcal{G}al(\mathbf{F}_q/\mathbf{F}_p)$ a exactement $[\mathbf{F}_q : \mathbf{F}_p] = m$ éléments, cela montre que φ engendre $\mathcal{G}al(\mathbf{F}_q/\mathbf{F}_p)$.

Remarquons aussi que le groupe de Galois $\mathcal{G}al(\mathbf{F}_q/\mathbf{F}_{p^d})$ est engendré par φ^d et a m/d éléments.

L'automorphisme $x \mapsto x^p$ de $\tilde{\mathbf{F}}_p$ est appelé l'automorphisme de Frobénius, noté $Frob$. Toutes les puissances entières de $Frob$ sont des automorphismes de $\tilde{\mathbf{F}}_p$, mais il y en a beaucoup d'autres, en fait $2^{\aleph_0}$. Nous allons montrer comment les construire.

Soit G le produit cartésien des groupes $\mathbf{Z}/n\mathbf{Z}$, où n parcourt l'ensemble des entiers positifs. On munit chaque $\mathbf{Z}/n\mathbf{Z}$ de la topologie discrète, et l'on considère la topologie produit sur G: une base d'ouverts est donnée par les ensembles de la forme $\prod_{n\in\mathbf{N}} U_n$, où $\{n \in \mathbf{N} \mid U_n \neq \mathbf{Z}/n\mathbf{Z}\}$ est fini. Alors G est un espace compact (théorème de Tychonoff), séparé (Hausdorff en anglais), et admet une base d'ouverts-fermés. C'est aussi un groupe topologique.

Pour m un diviseur de n, soit π_{mn} la projection naturelle $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$. Considérons le sous-groupe H de G défini de la façon suivante: H est l'ensemble des suites $(a_n)_{n\in\mathbf{N}}$ satisfaisant $\pi_{mn}(a_n) = a_m$ pour toute paire d'entiers (m,n) où $m|n$.

On vérifie sans peine que H est un sous-groupe fermé de G et donc compact: si $(b_i)_i \notin H$, il existe des entiers m et n tels que $m|n$ et $\pi_{mn}(b_n) \neq b_m$. L'ouvert de base $(\prod_{k\neq m,n} \mathbf{Z}/k\mathbf{Z}) \times \{b_m\} \times \{b_n\}$ contient $(b_i)_i$ et est disjoint de H.

Remarquons aussi que $\mathbf{Z}$ se plonge dans H, par l'application qui à un entier associe la suite de ses classes modulo n pour $n \in \mathbf{N}$. On vérifie que l'image de $\mathbf{Z}$ est dense dans H, c'est à dire coupe tout ouvert qui coupe H: cela provient du fait que tout système fini et consistant de congruences a une solution dans $\mathbf{Z}$.

Soit $\psi \in \mathcal{G}al(\tilde{\mathbf{F}}_p/\mathbf{F}_p) =_{\text{def}} \mathcal{G}(\mathbf{F}_p)$. A ψ nous associons l'élément $(a_n)_n$ de G de la façon suivante: pour $n \in \mathbf{N}$, a_n est l'unique élément de $\mathbf{Z}/n\mathbf{Z}$ tel que les restrictions de ψ et $Frob^{a_n}$ à $\mathbf{F}_{p^n}$ sont égales. On vérifie sans peine que cette association est un monomorphisme de groupe, et prend ses valeurs dans H.

Nous allons maintenant montrer que c'est un isomorphisme de $\mathcal{G}(\mathbf{F}_p)$ sur H. En effet, soit $(a_n)_n \in H$, et définissons

$$\psi(b) = b^{p^{a_m}} \qquad \text{si } b \in \mathbf{F}_{p^m}.$$

La définition de H garantit que la définition de $\psi(b)$ ne dépend pas de l'entier m choisi tel que $b \in \mathbf{F}_{p^m}$. En effet, soit n un entier divisible par m. Alors $a_n = a_m + km$ (identifiant ici a_m avec un élément de $\{0, 1, \cdots, m-1\}$ et a_n avec un élément de $\{0, 1, \cdots, n-1\}$). Nous avons donc

$$p^{a_n} = p^{km}p^{a_m}, \quad \text{ et donc } \ a^{p^{a_n}} = (a^{p^{km}})^{p^{a_m}} = a^{p^{a_m}}.$$

Il est clair que ψ définit un automorphisme de chaque corps $\mathbf{F}_{p^n}$, et donc un automorphisme de $\tilde{\mathbf{F}}_p$.

Notation. Le groupe H défini ci-dessus est noté $\hat{\mathbf{Z}}$, ou encore $\varprojlim_{n\in\mathbf{N}} \mathbf{Z}/n\mathbf{Z}$ (une limite inverse de groupes finis, indexée par les entiers, et avec pour morphismes les π_{mn} pour m

divisant n). Comme nous avons remarqué plus haut, il contient un sous-groupe isomorphe à $\mathbf{Z}$.

(3.6) Groupes profinis. Le but de la construction ci-dessus était de trouver un objet qui code toute l'information finie que nous avions. C'est à dire vraiment le système des groupes de Galois finis, avec les applications "restrictions" entre eux. Cette construction se généralise à des systèmes projectifs de groupes finis quelconques. Nous donnons rapidement les définitions, par souci de complétude — mais cette partie ne sera sans doute pas utilisée dans le cours.

Un groupe profini est un groupe topologique qui satisfait certaines propriétés (séparé, compact, ayant une base d'ouverts-fermés). Il y a plusieurs définitions équivalentes, et nous commencerons par la plus naturelle étymologiquement: la limite projective (aussi appelée limite inverse) de groupes finis. Cette limite est en fait définie par des propriétés universelles, mais qui donnent dans le cas des groupes un objet assez simple.

Nous avons un ensemble I partiellement ordonné, et pour chaque $i \in I$ un groupe fini G_i. Pour $i \leq j$ nous avons aussi un épimorphisme de groupe $\pi_{ij} : G_j \to G_i$, et ces épimorphismes satisfont:

$$\pi_{ii} = id; \qquad \text{si } i \leq j \leq k \text{ alors } \pi_{ik} = \pi_{ij} \circ \pi_{jk}.$$

Nous définissons la limite inverse du système $(G_i, \pi_{ij} \mid i, j \in I)$ comme étant le sous-groupe G du groupe $\prod_{i \in I} G_i$ défini par

$$(g_i)_i \in G \quad \iff \quad \pi_{ij}(g_j) = g_i \ \text{ pour tout } i \leq j.$$

On munit chaque groupe G_i de la topologie discrète, et on prend la topologie produit sur $\prod_{i \in I} G_i$. Le groupe G avec la topologie induite est alors un groupe topologique, et l'on vérifie qu'il est fermé. C'est donc un groupe compact, séparé, et dont une base de la topologie est donnée par des ouverts-fermés. Les projections de $\prod_{i \in I} G_i$ sur chacun des G_i induisent alors des homomorphismes continus $\pi_i : G \to G_i$, qui sont surjectifs. On écrit $G = \varprojlim_{i \in I} G_i$.

La propriété universelle satisfaite par G est la suivante: soit H un groupe, et supposons que nous avons des homomorphismes $h_i : H \to G_i$ pour chaque $i \in I$, et que ces homomorphismes satisfont $h_i = \pi_{ij} \circ h_j$ pour $i \leq j$. Il existe alors un unique homomorphisme $h : H \to G$ satisfaisant $\pi_i \circ h = h_i$ pour $i \in I$. En effet, si $a \in H$, alors l'élément $(\pi_i \circ h(a))_i$ est dans G.

De plus, si H est un groupe topologique et les morphismes h_i sont continus, alors h est aussi continu.

La seconde définition est tout simplement: un groupe profini est (isomorphe à) un sous-groupe fermé d'un produit de groupes finis, avec la topologie produit des topologies discrètes sur chacun des G_i.

(3.7) Groupes de Galois infinis. Nous allons montrer comment mettre ensemble l'information donnée par les groupes de Galois des extensions finies d'un corps au moyen des groupes profinis.

Soit F un corps, et soit $(L_i)_{i\in I}$ l'ensemble des extensions Galoisiennes finies de F. Remarquons que $card(I) \leq card(F) + \aleph_0$: en effet tout élément de la clôture séparable F_s de F est racine d'un polynôme à coefficients dans F, et $card(F[X]) = card(F) + \aleph_0$.

Pour chaque $i \in I$, posons $G_i = \mathcal{G}al(L_i/F)$; si $L_i \subseteq L_j$ la restriction définit un épimorphisme $res_{ij} : G_j \to G_i$. En effet, si $\sigma \in \mathcal{G}al(L_j/F)$, alors σ fixe F, et permute donc les racines du polynôme minimal $f(X)$ d'un élément $\alpha \in L_i$; comme L_i contient toutes les racines de $f(X)$ puisque L_i est normale, la restriction de σ à L_i est donc un élément de $\mathcal{G}al(L_i/F)$.

Nous définissons $\Phi : Aut(F_s/F) =_{\rm def} \mathcal{G}al(F_s/F) =_{\rm def} \mathcal{G}(F) \to \prod_{i\in I} G_i$ de la façon suivante: $\sigma \mapsto (\sigma_i)_{i\in I}$, où σ_i est la restriction de σ à L_i.

On vérifie que Φ est un morphisme de groupe, qui est injectif, et que

$$\Phi(\mathcal{G}(F)) = \{(g_i)_i \in \prod_{i\in I} G_i \mid \text{ si } L_i \subseteq L_j, \text{ alors } res_{ij}(g_j) = g_i\}.$$

On montre facilement que $\Phi(\mathcal{G}(F))$ est un sous-groupe fermé de $\prod_{i\in I} G_i$, et est donc un groupe profini. Nous identifions $\mathcal{G}(F)$ avec son image par Φ, et donc le considérons comme un groupe topologique.

La dualité de Galois finie s'étend sans peine aux groupes de Galois infinis. La seule différence est que les sous-groupes apparaissant dans la dualité seront fermés. A un sous-groupe fermé G de $\mathcal{G}(F)$ on associe le sous-corps de F_s fixé par tous les éléments de G. Réciproquement à un sous-corps E de F_s contenant F, on associe le sous-groupe de $\mathcal{G}(F)$ composé des éléments qui laissent E fixé.

Soit $F \subseteq E \subseteq F_s$, et montrons que le sous-groupe de $\mathcal{G}(F)$ qui laisse E fixé est un sous-groupe fermé; ce sous-groupe est en fait $\mathcal{G}al(F_s/E) = \mathcal{G}(E)$.

Soit $\sigma \in \mathcal{G}(F)$, et supposons que σ est l'identité sur E. Comme $E = \bigcup_{i\in I}(E \cap L_i)$, cela arrive si et seulement si la restriction de σ à L_i est l'identité sur $E \cap L_i$ pour tout $i \in I$. Pour chaque i, $\mathcal{G}al(L_i/E\cap L_i)$ est un sous-groupe de $G_i = \mathcal{G}al(L_i/E)$, et nous avons donc un plongement canonique $\prod_{i\in I} \mathcal{G}al(L_i/E \cap L_i) \subseteq \prod_{i\in I} G_i$. On a donc

$$\Phi(\mathcal{G}al(F_s/E)) = \Phi(\mathcal{G}al(F_s/F)) \cap \prod_{i\in I} \mathcal{G}al(L_i/E \cap L_i),$$

et l'intersection de deux groupes fermés est fermée.

Soit H un sous groupe (quelconque) de $\mathcal{G}(F)$, E le sous-corps de F_s fixé par H. Nous allons décrire la fermeture $\bar{H}$ de H et montrer que c'est le sous-groupe de $\mathcal{G}(F)$ qui fixe E. Pour $i \in I$, considérons l'homomorphisme de restriction $res_i : \mathcal{G}(F) \to G_i$, et soit $H_i = res_i(H)$; c'est donc un sous-groupe de G_i, et l'on vérifie que $\Phi(\mathcal{G}(F)) \cap \prod_{i\in I} H_i$ est le plus petit fermé de $\prod_{i\in I} G_i$ contenant $\Phi(H)$, et est donc l'image par Φ de $\bar{H}$. Puisque $res_i(\bar{H}) = H_i = \mathcal{G}al(L_i/E \cap L_i)$, le sous-corps de F_s fixé par $\bar{H}$ est E.

Les sous-groupes ouverts. Soit $i \in I$, et considérons le sous-groupe $U_i = \{(\sigma_j)_{j\in I} \mid \sigma_i = 1\} \cap \Phi(\mathcal{G}(F))$. C'est un sous-groupe ouvert de $\Phi(\mathcal{G}(F))$, dont le corps fixé est L_i, et que l'on identifie à $\mathcal{G}(L_i) = \mathcal{G}al(F_s/L_i)$. C'est un sous-groupe normal, et on a la suite exacte:

$$1 \to \mathcal{G}(L_i) \to \mathcal{G}(F) \to \mathcal{G}al(L_i/E) \to 1.$$

Soit U un sous-groupe ouvert de $\mathcal{G}(F)$. Par définition de la topologie produit, il existe un ensemble fini $J \subseteq I$ tel que $\Phi(U)$ contient l'intersection des sous- groupes U_i, $i \in J$ (cette intersection est ouverte); on voit alors que le sous-corps de F_s fixé par U est contenu dans le corps engendré par les L_i, $i \in J$, ce qui nous ramène à la théorie de Galois finie.

Quotients. De façon générale, si U est un sous-groupe fermé normal de $\mathcal{G}(F)$, et E est le sous-corps fixé par U, on a une suite exacte:

$$1 \to U \to \mathcal{G}(F) \to \mathcal{G}al(E/F) \to 1.$$

Ici, $\mathcal{G}al(E/F)$ est le groupe de Galois de E sur F, c'est à dire le groupe $Aut(E/F)$; on l'identifie à un sous-groupe fermé de $\prod_{i \in I, L_i \subseteq E} G_i$.

4. Bornes pour les idéaux de polynômes

Nous allons définir le degré d'un polynôme en plusieurs variables. Pour cela, nous définissons d'abord le degré du monôme $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ comme étant égal à $i_1+\ldots+i_n$; si $f(\bar X)$ est un polynôme en $\bar X=(X_1,\ldots,X_n)$, le degré de $f(\bar X)$ est le maximum des degrés des monômes apparaisant dans l'expression de $f(\bar X)$ avec un coefficient non nul. Si e est un entier positif, les polynômes de $K[\bar X]$ de degré $\leq e$ forment donc un espace vectoriel, qui est de dimension finie, puisqu'il n'y a qu'un nombre fini de monômes $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ avec $i_1+i_2+\cdots+i_n\leq e$.

(4.1) Théorème. Soient n,e des entiers positifs, $\bar X=(X_1,\ldots,X_n)$.

(1) Il existe une constante $A=A(n,e)$ telle que pour tout corps K, et polynômes $f_1(\bar X),\ldots,f_m(\bar X),g(\bar X)\in K[\bar X]$ de degré $\leq e$, si $g(\bar X)\in (f_1(\bar X),\ldots,f_m(\bar X))$ (l'idéal de $K[\bar X]$ engendré par $f_1(\bar X),\ldots,f_m(\bar X)$), alors
$$g(\bar X)=f_1(\bar X)h_1(\bar X)+\cdots f_m(\bar X)h_m(\bar X)$$
pour des polynômes $h_1(\bar X),\ldots,h_m(\bar X)\in K[\bar X]$ de degré $\leq A$.

(2) Il existe une constante $B=B(n,e)$ telle que pour tout corps K, et idéal I de $K[\bar X]$ engendré par des polynômes de degré $\leq e$, s'il existe k tel que $g(\bar X)^k\in I$, alors $g(\bar X)^B\in I$.

(3) Il existe une constante $C=C(n,e)$ telle que pour tout corps K, et idéaux I et J de $K[\bar X]$ engendrés par des polynômes de degré $\leq e$, les idéaux $I\cap J$ et $I:J$ $(=\{f\in K[\bar X]\mid fJ\subseteq I\})$ sont engendrés par des polynômes de degré $\leq C$.

(4) Il existe une constante $D=D(n,e)$ telle que pour tout corps K, et idéal I de $K[\bar X]$ engendré par des polynômes de degré $\leq e$, si I n'est pas premier, alors il existe des polynômes $g(\bar X),h(\bar X)$ de degré $\leq D$ tels que $g(\bar X),h(\bar X)\notin I$, et $g(\bar X)h(\bar X)\in I$.

(5) Il existe une constante $E=E(n,e)$ telle que pour tout corps K, et idéal I de $K[\bar X]$ engendré par des polynômes de degré $\leq e$, il y a au plus E idéaux premiers minimaux contenant I, et chacun est engendré par des polynômes de degré $\leq E$.

Les preuves de ces résultats se trouvent par exemple dans l'article de A. Seidenberg, Constructions in Algebra, Trans. A.M.S 197 (1974), 273 – 313. On peut aussi en trouver une démonstration qui utilise des ultraproduits dans: L. van den Dries et K. Schmidt, Bounds in the theory of polynomial rings over fields, Invent. Mat. 76 (1984), 77 – 91.

(4.2) Ces résultats nous permettent de trouver des formules dont les variables sont les coefficients des polynômes, qui expriment l'appartenance à un idéal, le fait que cet idéal est premier, radical, etc .... Soient r,n,e des entiers positifs, et $M(n,e)$ l'ensemble des monômes de degré $\leq e$ dans les variable $\bar X=(X_1,\ldots,X_n)$. Notons que si K est un corps, tout idéal de $K[\bar X]$ engendré par des polynômes de degré $\leq e$ est en fait engendré par au plus $card(M(n,e))$ d'entre eux. Ci-dessous, nous donnons deux applications.

(1) Il existe une formule $\alpha(\bar x_1,\ldots,\bar x_r,\bar x_{r+1})$, où $\bar x_i=(x_{im})_{m\in M(n,e)}$, telle que, pour tout corps K, si $f_i(\bar X)=\sum_{m\in M(n,e)}a_{i,m}m\in K[\bar X]$, alors
$$f_{r+1}(\bar X)\in (f_1(\bar X),\ldots,f_r(\bar X)) \iff K\models \alpha(\bar a_1,\bar a_2,\ldots,\bar a_r,\bar a_{r+1}).$$

(2) Il existe une formule $\beta(\bar x_1,\ldots,\bar x_r)$, où $\bar x_i=(x_{im})_{m\in M(n,e)}$, telle que, pour tout corps K, si $f_i(\bar X)=\sum_{m\in M(n,e)}a_{i,m}m\in K[\bar X]$, alors
$$(f_1(\bar X),\ldots,f_r(\bar X)) \text{ est premier } \iff K\models \beta(\bar a_1,\bar a_2,\ldots,\bar a_r).$$

Démonstration. (1) $f_{r+1}(\bar{X}) \in (f_1(\bar{X}), \ldots, f_r(\bar{X}))$ si et seulement s'il existe des polynômes $h_1(\bar{X}), \ldots, h_r(\bar{X})$ de degré $\leq A$ tel que $f_{r+1}(\bar{X}) = f_1(\bar{X})h_1(\bar{X}) + \cdots + f_r(\bar{X})h_r(\bar{X})$. Les monômes apparaissant dans les produits $f_i(\bar{X})h_i(\bar{X})$ ont degré $\leq e + A$, et leurs coefficients sont obtenus en évaluant certains termes du langage au uplet des coefficients des polynômes $f_i(\bar{X})$ et $h_i(\bar{X})$. Il existe donc une formule $\psi(\bar{x}_1, \ldots, \bar{x}_{r+1}, \bar{y}_1, \ldots, \bar{y}_r)$, qui est une conjonction d'équations, et telle que pour tout corps K, et uplets $\bar{a}_1, \ldots, \bar{a}_{r+1}$ et $\bar{b}_1, \ldots, \bar{b}_r$ de K, où $\bar{a}_i = (a_{im})_{m \in M(n,e)}$, $\bar{b}_i = (b_{im})_{m \in M(n,A)}$, on a, pour $f_i(\bar{X}) = \sum_{m \in M(n,e)} a_m m$ et $h_i(\bar{X}) = \sum_{m \in M(n,A)} b_{im} m$,

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

Nous prenons alors pour α la formule $\exists (\bar{y}_{im})_{1 \leq i \leq r, m \in M(n,A)}\ \psi(\bar{x}_1, \ldots, \bar{x}_{r+1}, \bar{y}_1, \ldots, \bar{y}_r)$.

(2) Les formules construites en (1) dépendent en fait des entiers n, e, r. La formule $\beta(\bar{x}_1, \ldots, \bar{x}_r)$ est alors obtenue en traduisant au premier ordre:
Pour tout $\bar{y} = (y_m)_{m \in M(n,D)}$, pour tout $\bar{z} = (z_m)_{m \in M(n,D)}$, si $\bar{t} = (t_m)_{m \in M(n,2D)}$ est la suite des coefficients du polynôme $(\sum_{m \in M(n,D)} y_m m)(\sum_{m \in M(n,D)} z_m m)$, alors
$\alpha_{n,2D,r}(\bar{x}_1, \ldots, \bar{x}_r, \bar{t}) \to \alpha_{n,D,r}(\bar{x}_1, \ldots, \bar{x}_r, \bar{y}) \vee \alpha_{n,D,r}(\bar{x}_1, \ldots, \bar{x}_r, \bar{z})$.

(4.3) Nous pouvons parler de façon élémentaire dans un corps K de fermés K-irréductibles définis sur K. Nous pouvons donc quantifier, avec une infinité de formules, sur l'ensemble des fermés K-irréductibles. Cependant, ce n'est pas tout à fait ce que nous voulons. En effet, la notion de K-irréductibilité n'est pas stable par extension de corps.

Puisque la théorie ACF des corps algébriquement clos admet l'élimination des quantificateurs, il existe une formule $\beta_0(\bar{x}_1, \ldots, \bar{x}_r)$ sans quantificateurs, qui est équivalente à $\beta(\bar{x}_1, \ldots, \bar{x}_r)$ modulo ACF.

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

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

en utilisant l'équivalence de β et β_0 modulo ACF, puis le fait que β_0 n'a pas de quantificateurs. Nous avons donc montré:

Théorème. (n, e, r fixés) Il existe un formule sans quantificateurs qui définit dans tout corps F les coefficients de polynômes $f_1(\bar{X}), \ldots, f_r(\bar{X})$ de degré $\leq e$ qui engendrent l'idéal d'une variété.

5. Les corps pseudo-finis

Nous allons maintenant décrire une théorie du premier ordre, Psf, dont les modèles seront appelés des corps pseudo-finis. Nous montrerons d'abord que les modèles infinis de la théorie T_f des corps finis sont des corps pseudo-finis. Ensuite nous étudierons les complétions de Psf, et donnerons des critères pour les extensions élémentaires. Finalement, nous conclurons en montrant que les corps pseudo-finis sont exactement les modèles infinis de la théorie T_f, et que les corps pseudo-finis de caractéristique 0 sont exactement les modèles infinis de la théorie de tous les corps premiers $\mathbf{F}_p$.

(5.1) Définition. Un corps F est pseudo-fini s'il possède les trois 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, c'est à dire un point dont toutes les coordonnées sont dans F.

Remarques. (1) Les corps ayant la propriété P3 sont appelés des corps pseudo-algébriquement clos (PAC). Ils ne sont pas necéssairement algébriquement clos, la raison étant que les seuls polynômes en une variable qui définisssent une variété sont les polynômes linéaires!!

C'est là en fait où intervient la différence entre variété et ensemble algébrique F-irréductible: si V est F-irréductible, mais n'est pas une variété, alors ses composantes irréductibles ne sont pas définies sur F.

(2) Bien entendu, les corps algébriquement clos sont PAC.

(3) On peut aussi prouver: tout corps F se plonge dans un corps E qui est PAC et tel que $\tilde{F} \cap E = F$ (F est relativement algébriquement clos dans E).

(4) Les corps finis satisfont les propriétés P1 et P2. Ils ne peuvent satisfaire à P3: soit $\mathbf{F}_q$ un corps fini, et considérons la variété $V \subseteq K^{q+2}$ définie par l'équation

$$y \prod_{0 \leq i < j \leq q} (x_i - x_j) = 1.$$

Cette équation ne peut être satisfaite dans $\mathbf{F}_q$ puisque tout $(q+1)$-uplet d'éléments de $\mathbf{F}_q$ a au moins deux coordonnées égales.

(5.2) La théorie Psf est obtenue en traduisant au premier ordre les propriétés P1, P2, P3 ci-dessus. Les axiomes pour P1 sont clairs: on donne les axiomes de la théorie des corps, et pour chaque nombre premier p on ajoute un axiome disant que si la caractéristique est p alors tout élément a une racine p-ième.

Les axiomes pour P3 sont aussi assez clairs, grâce aux résultats sur les idéaux de polynômes. En effet, pour chaque triplet (n, e, m) d'entiers, on peut exprimer au premier ordre:

Pour tout $f_1(\bar{X}), \dots, f_m(\bar{X}) \in F[\bar{X}]$ de degré $\leq e$, où $\bar{X} = (X_1, \dots, X_n)$, si "l'idéal engendré par $f_1(\bar{X}), \dots, f_m(\bar{X})$ dans $\tilde{F}[\bar{X}]$ est premier" (voir (4.3)), 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 alors une formule $Irr(\bar{x})$, $x = (x_1, \dots, x_n)$, qui dans tout corps F définit les n-uplets $\bar{a}$ tels que le polynôme $f(X) =$

$X^n + a_1X^{n-1} + \cdots + a_n$ soit irréductible sur F: on utilise tout simplement le fait que si $f(X) = g(X)h(X)$ alors les degrés de g et h sont $\leq n$.

Supposons montré le résultat suivant (il le sera dans (5.3)):

A 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, et tout n-uplet $\bar{a}$ de F, si le polynôme $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ est irréductible sur F et $\bar{b} \in F^m$ alors

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

Soit $\theta(\bar{y})$, $\bar{y} = (y_1, \ldots, y_n)$, la formule $\exists z\ z^n + y_1z^{n-1} + \cdots + y_n = 0$, et considérons l'énoncé suivant, où $\bar{x}$ et $\bar{y}$ sont comme ci-dessus:

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

Cet énoncé est alors une traduction au premier ordre de la propriété suivante: il existe une extension de F de degré n, et tout polynôme irréductible sur F de degré n y a une racine.

Un corps F ayant cette propriété a donc exactement **une** extension de degré n, puisque, s'il en avait deux distinctes, aucune des deux ne pourrait être contenue dans l'autre.

(5.3) Codage des extensions algébriques finies.

Soit F un corps, et $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ un polynôme irréductible à coefficients dans F, et soit α une racine de $f(X) = 0$. Nous allons montrer comment interpréter dans F un corps F-isomorphe à $F(\alpha)$.

Nous prenons comme base du F-espace vectoriel $F(\alpha)$ la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$; l'addition est donc définie coordonnée par coordonnée. Pour la multiplication, remarquons que la multiplication par α est une transformation linéaire de l'espace vectoriel $F(\alpha)$, et que sa matrice dans la base choisie est:

$$M_\alpha = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_n \\ 1 & 0 & \ldots & 0 & -a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_1 \end{pmatrix}.$$

La multiplication par α^i est aussi une transformation linéaire, et sa matrice est M_α^i. Nous définissons donc la multiplication de deux n-uplets de la façon suivante:

$$(x_1, \ldots, x_n)\tilde{\times}(y_1, \ldots, y_n) = (x_1I_n + x_2M_\alpha + \cdots + x_nM_\alpha^{n-1}) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Remarquons que la définition de $\tilde{\times}$ a besoin des paramètres $a_1, \ldots, a_n$, mais qu'elle est uniforme en ces paramètres. L'interprétation dans F d'une structure isomorphe à $F(\alpha)$, (en remarquant que le sous-corps F est l'ensemble des n-uplets $(a, 0, \ldots, 0)$), et l'uniformité de cette interprétation nous donne alors:

Proposition. Fixons un entier n. Soit $\mathcal{L}'$ le langage des anneaux auquel on a rajouté un prédicat unaire. A toute $\mathcal{L}'$-formule $\theta(\bar{y}, z)$, $\bar{y} = (y_1, \ldots, y_m)$, on peut associer une formule du langage des anneaux $\theta^*(\bar{x}, \bar{y})$, $\bar{x} = (x_1, \ldots, x_n)$, telle que, pour tout corps F et 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 α en est une racine, et si $\bar{b} \in F^m$ alors

$$F(\alpha) \models \theta(\bar{b}, \alpha) \iff F \models \theta^*(\bar{a}, \bar{b}).$$

(5.4) Le théorème de Lang-Weil. Soient m, n, e des entiers positifs. Il existe une constante positive $C = C(m, n, e)$ telle que, pour tout corps fini $F = \mathbf{F}_q$, et polynômes $f_1(\bar{Y}), \ldots, f_m(\bar{Y}) \in F[\bar{Y}]$ de degré plus petit ou égal à e, $\bar{Y} = (Y_1, \ldots, Y_n)$,

si les polynômes $f_1(\bar{Y}), \cdots, f_m(\bar{Y})$ engendrent l'idéal d'une variété V de dimension d, alors

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

Remarquons en particulier, que si $q > C^2$, alors $V \cap F^n$ doit être non-vide, puisque

$$0 < -Cq^{d-1/2} + q^d < card(V \cap F^n) < Cq^{d-1/2} + q^d.$$

Comme corollaire, nous obtenons immédiatement:

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

Démonstration. Nous avons déjà remarqué que les corps finis satisfont les propriétés P1 et P2. Pour P3, notons que le théorème de Lang-Weil implique (en gardant les mêmes notations):

si les polynômes $f_1(\bar{Y}), \cdots, f_m(\bar{Y})$ engendrent l'idéal d'une variété, et s'il existe au moins $C^2 + 1$ éléments distincts alors $\exists \bar{x}\ f_1(\bar{x}) = \ldots = f_m(\bar{x}) = 0$.

Cela entraîne qu'un modèle infini de T_f est bien un corps PAC.

(5.6) Exemples de corps pseudo-finis

(1) Le premier exemple est tout à fait naturel. Soit $\mathcal{U}$ un ultrafiltre non-principal sur l'ensemble des puissances de nombres premiers, et soit $F = \prod_q \mathbf{F}_q/\mathcal{U}$. Alors F est un modèle infini de la théorie des corps finis, et est donc pseudo-fini.

(2) Nous allons maintenant donner un exemple algébrique sur le corps premier $\mathbf{F}_p$. Un sous-corps F de $\tilde{\mathbf{F}}_p$ est pseudo-fini, si et seulement si il est infini, et a exactement une extension algébrique de degré n pour tout $n \in \mathbf{N}$. Remarquons que, comme tout corps fini est parfait, tout sous-corps de $\tilde{\mathbf{F}}_p$ est parfait, et donc la condition P1 est automatiquement vérifiée.

Pour P3, supposons que F est un sous-corps infini de $\tilde{\mathbf{F}}_p$ et soit V une variété définie sur F; le théorème de Lang-Weil montre alors que $V(F)$ $(= V \cap F^n)$ est non-vide.

Choisissons une fonction f définie sur l'ensemble des nombres premiers et prenant ses valeurs dans les entiers non-négatifs; supposons de plus qu'il existe une infinité de nombres premiers ℓ tels que $f(\ell) > 0$. Soit F le corps engendré par tous les corps $\mathbf{F}_{p^{\ell^{f(\ell)}}}$ pour ℓ parcourant l'ensemble des nombres premiers. Il est clair que F est infini, et donc satisfait

P3. Il nous reste donc à vérifier P2. Nous allons d'abord introduire quelques notations: soit $(\ell_i)_{i\in\mathbf{N}}$ une énumération croissante des nombres premiers; pour $m \in \mathbf{N}$ nous définissons F_m le corps engendré par les corps $\mathbf{F}_{p^{\ell^{f(\ell)}}}$ pour ℓ un premier $\leq l_m$. Les corps F_m, $m \in \mathbf{N}$, sont finis et forment une suite croissante, dont l'union est précisément F. Pour $m \in \mathbf{N}$, nous avons $[F_{m+1} : F_m] = \ell_{m+1}^{f(\ell_{m+1})}$.

Soit $n \in \mathbf{N}$ et choisissons m tel que tout nombre premier plus grand ou égal à ℓ_m est premier avec n. Soit E l'extension de F_m de degré n. Nous allons montrer que $[EF_{m'} : F_{m'}] = n$ pour tout $m' \geq m$: mais c'est clair, car pour tout $m' \geq m$, $[F_{m'} : F_m]$ n'est divisible que par des nombres premiers ne divisant pas n, et n divise $[EF_{m'} : F_m] = [EF_{m'} : F_{m'}][F_{m'} : F_m]$.

Nous avons donc montré que F a une extension de degré n, EF; s'il en avait deux distinctes, elles donneraient deux extensions distinctes de même degré d'un corps fini, ce qui est impossible.

(3) Fixons maintenant des nombres premiers p et ℓ et considérons l'extension infinie E de $\mathbf{F}_p$ définie par

$$E = \bigcup_{m\in\mathbf{N}} \mathbf{F}_{p^{\ell^m}}.$$

Ce corps est PAC, cependant, il n'a aucune extension de degré ℓ: en effet, supposons que α soit algébrique de degré ℓ sur E, et soit $m \in \mathbf{N}$ tel que le polynôme minimal de α ait ses coefficients dans $\mathbf{F}_{p^{\ell^m}}$; alors $\alpha \in \mathbf{F}_{p^{\ell^{m+1}}}$, et donc $\alpha \in E$.

(5.7) Lemme. Soient $K \subseteq L$ des corps parfaits.

(1) Supposons que K a au plus une extension de degré n pour tout $n \in \mathbf{N}$. Alors toutes ses extensions algébriques (finies) sont Galoisiennes, et leur groupe de Galois sur K est cyclique.

(2) Les conditions suivantes sont équivalentes:
 (a) Pour chaque entier positif n, K a exactement une extension de degré n.
 (b) $\mathcal{G}al(\tilde{K}/K) \simeq \hat{\mathbf{Z}}$.
 Ces conditions impliquent en particulier que toute extension Galoisienne finie de K a un groupe de Galois sur K qui est cyclique.

(3) Soit $\sigma \in \mathcal{G}al(\tilde{K}/K)$. Les conditions suivantes sont équivalentes:
 (a) Le sous-groupe de $\mathcal{G}al(\tilde{K}/K)$ engendré par σ est dense.
 (b) Pour toute extension finie E de K la restriction de σ à E engendre $\mathcal{G}al(E/K)$.
 (c) Le sous-corps de $\tilde{K}$ fixé par σ est K.
 Un tel élément σ est appelé un générateur topologique du groupe profini $\mathcal{G}al(\tilde{K}/K)$.

(4) Supposons que K satisfait l'une des conditions équivalentes de (2), et que σ est un générateur topologique de $\mathcal{G}al(\tilde{K}/K)$. Supposons de plus que K est relativement algébriquement clos dans L (c'est à dire, $\tilde{K} \cap L = K$ — on peut dire aussi que L est une extension régulière de K, parce que K est parfait), et soit $\tau \in \mathcal{G}al(\tilde{L}/L)$ un élément prolongeant σ, et M le sous-corps de $\tilde{L}$ fixé par τ.
 Alors τ est un générateur topologique de $\mathcal{G}al(\tilde{L}/M) \simeq \hat{\mathbf{Z}}$; K est relativement algébriquement clos dans M; si K_n est l'unique extension de K de degré n, alors K_nM est l'unique extension de M de degré n. L'application de restriction $\mathcal{G}al(\tilde{L}/M) \to \mathcal{G}al(\tilde{K}/K)$ est un isomorphisme continu.

Démonstration. (1) Soit E une extension Galoisienne finie de K. Nous allons montrer que $\mathcal{G}al(E/K)$ est cyclique. Comme tous les sous-groupes de $\mathcal{G}al(E/K)$ sont normaux, cela entraînera que toutes les extensions algébriques de K contenues dans E sont Galoisiennes, avec groupe de Galois sur K cyclique. Comme toute extension algébrique de K est contenue dans une extension Galoisienne, cela montrera le résultat souhaité.

Pour cela il suffit de montrer l'assertion suivante:

Sous-lemme. Soit G un groupe fini, et supposons que pour m divisant l'ordre de G, G a au plus un sous-groupe d'ordre m. Alors G est cyclique.

Par induction sur n, l'ordre de G; si n est premier, c'est clair. Remarquons que notre hypothèse implique que tous les sous-groupes de G sont normaux (distingués). Soit p un nombre premier divisant n, et $a \in G$ un élément d'ordre p. Par hypothèse d'induction, $G/\langle a\rangle$ est cyclique, engendré par un élément b, disons; puisque le sous-groupe $\langle a\rangle$ est d'ordre p, soit $\langle b\rangle$ contient $\langle a\rangle$, ce qui montre que G est cyclique; ou bien $\langle a\rangle \cap \langle b\rangle = (1)$, ce qui implique (puisque ces deux sous-groupes sont normaux) que $a^{-1}b^{-1}ab = 1$ et donc que $G = \langle a\rangle \times \langle b\rangle$. Puisque G n'a qu'un seul sous-groupe d'ordre p, p ne divise pas l'ordre de b, ce qui entraîne que G est cyclique.

(2) Supposons (a), et soit L une extension Galoisienne finie de degré n. Nous allons montrer que $\mathcal{G}al(L/K)$ est cyclique, ce qui revient à montrer que pour tout diviseur m de n, $\mathcal{G}al(L/K)$ a un seul sous-groupe d'ordre m (par le sous-lemme); mais les sous-groupes d'ordre m de $\mathcal{G}al(L/K)$ correspondent aux sous-corps de L de degré n/m sur K, et par hypothèse il y a un seul tel sous-corps pour chaque n. Nous avons donc montré que tous les groupes de Galois finis sont cycliques.

Par hypothèse, pour chaque n, K a une extension de degré n. On vérifie que cela entraîne que $\mathcal{G}al(\tilde{K}/K) \simeq \hat{\mathbf{Z}}$.

Supposons maintenant (b). Les extensions de K de degré m correspondent, par dualité de Galois, aux sous-groupes fermés de $\hat{\mathbf{Z}}$ d'indice m; mais un sous-groupe fermé d'indice fini est aussi ouvert, et le seul sous-groupe d'indice m dans $\hat{\mathbf{Z}}$ est la clôture du sous groupe $m\mathbf{Z}$ de $\mathbf{Z}$, c'est à dire les éléments $(a_n)_{n\in\mathbf{N}} \in \hat{\mathbf{Z}}$, où chaque a_n est divisible par m dans $\mathbf{Z}/n\mathbf{Z}$. On le voit facilement en écrivant $\hat{\mathbf{Z}} = \varprojlim_{n\in\mathbf{N}} \mathbf{Z}/n!\mathbf{Z}$

(3) Soit G_0 le sous-groupe de $\mathcal{G}al(\tilde{K}/K)$ engendré par σ. Vous allez montrer que c'est équivalent à ce que la projection canonique de G_0 sur chacun des groupes $\mathcal{G}al(E/K)$ (où E est une extension de Galois finie de K) est surjective. Or cette projection est engendrée par la restriction de σ à E, ce qui montre l'équivalence de (a) et (b).

L'équivalence de (b) et (c) est aussi immédiate.

Pour la dernière remarque, si E et F sont deux extensions de K de degré n, σ^n fixe E et F. Donc, la restriction de σ à EF est un élément d'ordre n qui engendre $\mathcal{G}al(EF/K)$, ce qui entraîne que $E = F$ et que $\mathcal{G}al(EF/K)$ est cyclique.

(4) $\tilde{K} \cap M = K$, puisque τ prolonge σ. Cela entraîne que $[K_nM : M] = [K_n : K] = n$. D'autre part, puisque M est le sous-corps de $\tilde{L}$ fixé par τ, nous savons que M a au plus une extension de chaque degré. Le fait que la restriction $\mathcal{G}al(\tilde{L}/M) \to \mathcal{G}al(\tilde{K}/K)$ soit un isomorphisme continu est immédiat.

(5.8) Lemme. Soit F un corps parfait PAC, contenu dans un corps K, et soient $\bar{a}$ un uplet de K, et A un sous-ensemble dénombrable de K.

(1) Si F est relativement algébriquement clos dans $F(\bar{a})$, alors il existe un F-homomorphisme: $F[\bar{a}] \to F$.
(2) Si F est $\aleph_1$-saturé et relativement algébriquement clos dans $F(A)$, alors il existe un F-homomorphisme : $F[A] \to F$.

Démonstration. (1) Considérons l'idéal $I(\bar{a}/F)$. Comme F est parfait et relativement algébriquement clos dans $F(\bar{a})$, cela entraîne que $F(\bar{a})$ et $\tilde{F}$ sont linéairement disjoints au-dessus de F. Par (2.10), l'idéal $I(\bar{a}/F)$ engendre donc l'idéal d'une variété V. Puisque F est PAC, $V(F)$ contient un point $\bar{b}$, et nous avons un F-homomorphisme: $F[\bar{a}] \to F$ qui envoie $\bar{a}$ sur $\bar{b}$ (puisque par définition, $\bar{a}$ est un point générique de V).

(2) Puisque A est dénombrable, il existe un sous-corps dénombrable F_0 de F tel que l'idéal $I(A/F)$ soit engendré par $I(A/F_0)$. On utilise maintenant la compacité, la partie (1), et le fait que F est $\aleph_1$-saturé.

(5.9) Lemme. Soient $K \subseteq E$ des corps parfaits, $\tilde{F}$ un corps algébriquement clos contenant K, et supposons que $\psi : \tilde{E} \to \tilde{F}$ est un $\tilde{K}$-isomorphisme. Soit $F = \psi(E)$. Alors l'application $\Psi : \mathcal{G}al(\tilde{E}/E) \to \mathcal{G}al(\tilde{F}/F)$ définie par

$$\Psi(\sigma) = \psi \circ \sigma \circ \psi^{-1}$$

est un isomorphisme. De plus, pour tout $a \in \tilde{K}$ et $\sigma \in \mathcal{G}al(\tilde{E}/E)$, $\Psi(\sigma)(a) = \sigma(a)$.

Démonstration. Il est clair que c'est un homomorphisme de groupe. Comme ψ est l'identité sur $\tilde{K}$, nous avons aussi la dernière assertion.

Soit $\Theta : \mathcal{G}al(\tilde{F}/F) \to \mathcal{G}al(\tilde{E}/E)$ définie par $\Theta(\tau) = \psi^{-1} \circ \tau \circ \psi$. Alors $\Theta \circ \Psi$ est l'identité sur $\mathcal{G}al(\tilde{E}/E)$, et de même, $\Psi \circ \Theta$ est l'identité sur $\mathcal{G}al(\tilde{F}/F)$, ce qui montre que Ψ est un isomorphisme.

(5.10) Lemme de plongement. Soit K un sous-corps des corps E et F. Supposons que K, E et F sont parfaits, K est relativement algébriquement clos dans E et F, E est dénombrable, et F est un corps pseudo-fini $\aleph_1$-saturé. Supposons de plus que nous avons un isomorphisme (continu) $\Phi : \mathcal{G}al(\tilde{F}/F) \to \mathcal{G}al(\tilde{E}/E)$ ($\simeq \hat{\mathbf{Z}}$) tel que pour tout $a \in \tilde{K}$, pour tout $\sigma \in \mathcal{G}al(\tilde{F}/F)$, $\Phi(\sigma)(a) = \sigma(a)$.

Alors il existe un plongement $\varphi : \tilde{E} \to \tilde{F}$, qui est l'identité sur $\tilde{K}$, envoie E dans F, et satisfait: pour tout $a \in \tilde{E}$, pour tout $\sigma \in \mathcal{G}al(\tilde{F}/F)$,

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

De plus, F est une extension régulière de $\varphi(E)$.

Démonstration. Nous montrons d'abord que nous pouvons 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 $(u_i)_{i\in I}$ (dans un grand corps algébriquement clos contenant tous les corps considérés) algébriquement indépendants au-dessus de F. Alors 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 $\tilde{K}(u_i)_{i\in I}$. Soit $E' = \psi(E)$. Puisque $\tilde{E}'$ et $\tilde{F}$ sont algébriquement indépendants au-dessus de $\tilde{K}$, ils sont linéairement disjoints au-dessus de $\tilde{K}$ par (2.14). Si l'on définit Ψ comme dans (5.9), on vérifie que $\Phi' = \Psi \circ \Phi$ satisfait la condition imposée à Φ. Nous pouvons donc remplacer E par E', Φ par Φ'; ensuite nous composerons le $\tilde{K}$-plongement φ' de $\tilde{E}'$ dans $\tilde{F}$ avec ψ pour obtenir le plongement $\varphi = \varphi' \circ \psi$ désiré. On vérifie aisément que pour tout $a \in \tilde{E}$, pour tout $\sigma \in \mathcal{G}al(\tilde{F}/F)$, $\varphi(\Phi(\sigma)(a)) = \sigma(\varphi(a))$.

Nous supposons donc que $\tilde{E}$ et $\tilde{F}$ sont linéairement disjoints au-dessus de $\tilde{K}$. Cela entraîne que le corps $\tilde{E}\tilde{F}$ est isomorphe au corps des fractions de $\tilde{E} \bigotimes_{\tilde{K}} \tilde{F}$. Soit σ_0 un générateur topologique de $\mathcal{G}al(\tilde{F}/F)$, et définissons $\tau_0 \in \mathcal{G}al(\tilde{E}\tilde{F}/EF)$ de la façon suivante:

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

pour $a \in E$ et $b \in F$, et prolongeons de la seule manière possible à $\tilde{E}\tilde{F}$.

Remarquons d'abord que τ_0 prolonge σ_0 et $\Phi(\sigma_0)$; d'autre part, la disjonction linéaire de $\tilde{E}$ et $\tilde{F}$ au-dessus de $\tilde{K}$, et le fait que σ_0 et $\Phi(\sigma_0)$ ont la même action sur $\tilde{K}$ entraînent que τ_0 est bien défini.

Soit maintenant $\tau \in \mathcal{G}al(\widetilde{EF}/EF)$ un prolongement de τ_0, et soit M le sous-corps de $\widetilde{EF}$ fixé par τ. Puisque σ_0 et $\Phi(\sigma_0)$ engendrent topologiquement les groupes $\mathcal{G}al(\tilde{F}/F)$ et $\mathcal{G}al(\tilde{E}/E)$, nous savons que E et F sont relativement algébriquement clos dans M. Nous avons aussi $\tilde{M} = \widetilde{EF} = \tilde{E}M = \tilde{F}M$.

Puisque $\tilde{M}$ est algébrique sur M, le corps $\tilde{F}M$ est en fait égal à l'anneau $M[\tilde{F}] = \tilde{F}[M]$. Chaque $a \in \tilde{E}$ s'écrit donc $\sum_{i \in I(a)} b_{a,i} y_{a,i}$, avec $b_{a,i} \in M$ et $y_{a,i} \in \tilde{F}$. Soit M_0 l'ensemble $E \cup \{b_{a,i} \mid a \in \tilde{E},\ i \in I(a)\}$, qui est donc dénombrable; nous avons $\tilde{E} \subseteq \tilde{F}[M_0]$.

L'extension $F[M_0]$ de F est régulière, puisque contenue dans M. Par (5.8), il existe donc un F-homomorphisme $\varphi_0 : F[M_0] \to F$, qui se prolonge en un $\tilde{F}$-homomorphisme $\varphi : \tilde{F}[M_0] \to \tilde{F}$ (car $I(M_0/\tilde{F})$ est engendré par $I(M_0/F)$). Notons que la restriction de φ à $\tilde{E}$ est un $\tilde{K}$-isomorphisme: puisque $\tilde{F}$ contient $\tilde{K}$, c'est un $\tilde{K}$-homomomorphisme; $\ker(\varphi) \cap \tilde{E}$ est alors un idéal propre de $\tilde{E}$, c'est à dire (0). Pour $a \in \tilde{E}$ nous avons

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

puisque τ est l'identité sur $\varphi(M_0) \subseteq F$. Nous avons aussi

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

puisque φ est un $\tilde{F}$-homomorphisme. Cela entraîne que

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

Comme σ_0 est un générateur de $\mathcal{G}al(\tilde{F}/F)$, cela montre que $\varphi(\Phi(\sigma)(a)) = \sigma(\varphi(a))$ pour tout $a \in \tilde{E}$ et $\sigma \in \mathcal{G}al(\tilde{F}/F)$. En effet, soit $a \in \tilde{E}$ et $\sigma \in \mathcal{G}al(\tilde{F}/F)$. Alors a est dans une extension finie L de E, et nous avons $\Phi(\sigma)|_L = \Phi(\sigma_0)^m|_L$ pour un entier m. Nous avons alors

$$\Phi(\sigma)(a) = \Phi(\sigma_0^m)(a) = \Phi(\sigma_0)^m(a) = \sigma_0^m(\varphi(a)) = \sigma(\varphi(a)).$$

Nous avons donc montré la première partie du théorème. Nous savons que $\varphi(E) \subseteq F$, et il nous faut montrer que $\varphi(E)$ est relativement algébriquement clos dans F, c'est à dire que $\varphi(\tilde{E}) \cap F = \varphi(E)$. Pour $a \in \tilde{E}$ nous avons

$$\begin{aligned} \varphi(a) \in F &\iff \sigma_0(\varphi(a)) = \varphi(a) \\ &\iff \varphi(\Phi(\sigma_0)(a)) = \varphi(a) \\ &\iff \Phi(\sigma_0)(a) = a \\ &\iff a \in E. \end{aligned}$$

La première et la dernière équivalence viennent du fait que σ_0 engendre $\mathcal{G}al(\tilde{F}/F)$, et donc $\Phi(\sigma_0)$ engendre $\mathcal{G}al(\tilde{E}/E)$; la deuxième équivalence provient de l'égalité $\varphi(\Phi(\sigma_0)(a)) = \sigma_0(\varphi(a))$, et la troisième de ce que φ est un isomorphisme.

Corollaire. Soient K_1 un sous-corps du corps E, et K_2 un sous-corps du corps F. Supposons que: K_1, K_2, E et F sont parfaits, K_1 est relativement algébriquement clos dans E, K_2 est relativement algébriquement clos dans F, E est dénombrable, et F est un corps pseudo-fini $\aleph_1$-saturé. Supposons de plus que nous avons un isomorphisme (continu) $\Phi : \mathcal{G}al(\tilde{F}/F) \to \mathcal{G}al(\tilde{E}/E)$ ($\simeq \hat{\mathbf{Z}}$) et un isomorphisme $\varphi_0 : \tilde{K}_1 \to \tilde{K}_2$ satisfaisant: pour tout $a \in \tilde{K}_1$, pour tout $\sigma \in \mathcal{G}al(\tilde{F}/F)$, $\varphi_0(\Phi(\sigma)(a)) = \sigma(\varphi_0(a))$.

Alors il existe un plongement $\varphi : \tilde{E} \to \tilde{F}$, qui prolonge φ_0, envoie E dans F, et satisfait: pour tout $a \in \tilde{E}$, pour tout $\sigma \in \mathcal{G}al(\tilde{F}/F)$,

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

De plus $\varphi(E)$ est relativement algébriquement clos dans F.

Démonstration. Nous pouvons étendre φ_0 en un isomorphisme ψ défini sur $\tilde{E}$: nous appliquons maintenant le résultat précédent au triplet K_2, $\psi(E)$ et F, et composons le plongement obtenu avec ψ pour obtenir un plongement de $\tilde{E}$ dans $\tilde{F}$.

(5.11) Théorème. 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. Nous allons commencer par la direction facile: supposons que $E \equiv_K F$. Nous savons que si $f(X) \in K[X]$, alors

$$E \models \exists x\ f(x) = 0 \iff F \models \exists x\ f(x) = 0,$$

et nous voulons en déduire que $E \cap \tilde{K} \simeq_K F \cap \tilde{K}$.

Soit L une extension normale finie de K, et soit $S_L = \{\sigma \in Aut(\tilde{K}/K) \mid \sigma(L \cap E) = L \cap F\}$. L'ensemble S_L est alors la réunion finie de cosets du sous-groupe $Aut(\tilde{K}/L)$ (la topologie sur $Aut(\tilde{K}/K)$ est celle induite par l'isomorphisme de $Aut(\tilde{K}/K)$ avec $\mathcal{G}al(K_s/K)$) et est donc fermé. Nous allons montrer que S_L est non-vide.

Supposons d'abord que L est séparable sur K, et soit α tel que $L \cap E = K(\alpha)$. Soit $f(X)$ le polynôme minimal de α sur K, et soit $\beta \in F$ une racine de $f(X) = 0$. Nous avons alors $[E \cap L : K] = [K(\beta) : K] \leq [F \cap L : K]$; par symétrie nous avons aussi $[F \cap L : K] \leq [E \cap L : K]$ donc ces degrés sont égaux. Soit $\sigma \in Gal(L/K)$ tel que $\sigma(\alpha) = \beta$; alors $\sigma(L \cap E) = L(\beta) = L \cap F$ et donc S_L est non-vide.

Supposons maintenant que L n'est pas séparable. Cela implique que K n'est pas parfait, et en particulier est infini. Soient $L_1, \ldots, L_n$ les images par les éléments de $Aut(L/K)$ du corps $L \cap F$. Soit $a \in L \cap E$; par hypothèse, il existe $b \in L \cap F$ ayant le même polynôme irréductible au-dessus de K. Donc $K(a) \simeq_K K(b)$, et il existe $\sigma \in Aut(L/K)$ tel que $\sigma(b) = a$. Nous avons donc $L \cap E \subseteq L_1 \cup \cdots \cup L_n$. Le sous-lemme démontré ci-dessous nous donne l'existence d'un i tel que $L \cap E \subseteq L_i$.

Sous-lemme. Soit K un corps infini, et V, $V_1, \ldots, V_n$ des espaces vectoriels sur K tels que $V \subseteq V_1 \cup \cdots \cup V_n$. Alors il existe i tel que $V \subseteq V_i$.

Démonstration. La preuve se fait par induction sur n. Si $n = 1$ il n'y a rien à montrer. Si $V_1 \cap V \subseteq V_2 \cup \cdots \cup V_n$, l'hypothèse d'induction nous donne le résultat. Supposons que $V_1 \cap V \not\subseteq V_2 \cup \cdots \cup V_n$. Soit $a \in V_1 \cap V$, $a \notin V_2 \cup \cdots \cup V_n$, et $b \in V$. Pour chaque $k \in K$, $ka + b \in V$, et il existe un indice i tel que $ka + b \in V_i$. Comme K est infini, il existe donc un indice i, et deux éléments $k \neq \ell$ de K tels que $ka + b$ et $\ell a + b$ sont dans V_i. Alors $0 \neq (ka + b) - (\ell a + b) = (k - \ell)a \in V_i$, ce qui montre que $i = 1$ et $b \in V_1$.

De $L \cap E \subseteq L_i$ nous déduisons que $[L \cap E : K] \leq [L_i : K] = [L \cap F : K]$. Comme dans le cas précédent, nous montrons ensuite que ces degrés sont égaux, ce qui montre que $L \cap E = L_i$, et donc que S_L est non-vide.

Pour toute extension Galoisienne finie L de K, nous avons montré que l'ensemble $S_L = \{\sigma \in \mathcal{G}al(\tilde{K}/K) \mid \sigma(L \cap E) = L \cap F\}$ est non vide; il est d'autre part fermé puisqu'il est une union finie de cosets de $\mathcal{G}al(\tilde{K}/L)$. Si $L_1, \ldots, L_m$ sont des extensions Galoisiennes finies de K, et $M = L_1 \cdots L_m$ alors $S_M \subseteq S_{L_1} \cap \cdots \cap S_{L_m}$. Par compacité de $\mathcal{G}al(\tilde{K}/K)$, l'intersection de tous les fermés S_L est donc non vide, ce qui montre que $E \cap \tilde{K} \simeq_K F \cap \tilde{K}$.

Pour l'autre direction, nous pouvons remplacer K par sa clôture algébrique relative dans E et F respectivement, et donc supposer que $\tilde{K} \cap E = \tilde{K} \cap F = K$. Par Löwenheim-Skolem appliqué au triplet (E, F, K), nous nous ramenons d'abord au cas où ils sont tous dénombrables; puis, passant à des extensions élémentaires de E et F, nous pouvons supposer que E et F sont $\aleph_1$-saturés. Pour pouvoir appliquer le lemme de plongement, il nous faut maintenant construire l'isomorphisme Φ entre les groupes de Galois.

Soit σ_1 un générateur topologique de $\mathcal{G}al(\tilde{E}/E)$ ($\simeq \hat{\mathbf{Z}}$), et σ_0 sa restriction à $\tilde{K}$. Par (5.7), σ_0 est un générateur topologique de $\mathcal{G}al(\tilde{K}/K)$. Nous voulons prolonger σ_0 à un générateur topologique σ_2 de $\mathcal{G}al(\tilde{F}/F)$. Pour chaque extension Galoisienne finie L de F, soit S_L l'ensemble des éléments $\sigma \in \mathcal{G}al(\tilde{F}/F)$ dont la restriction à L engendre $\mathcal{G}al(L/F)$ et prolonge σ_0 sur $(\tilde{K} \cap L)$. D'après sa définition, on voit que S_L est une réunion de cosets du groupe $\mathcal{G}al(\tilde{F}/L)$, et donc un fermé; nous allons montrer qu'il est non-vide. Les groupes $\mathcal{G}al(L/F)$ et $\mathcal{G}al(\tilde{K} \cap L/K)$ sont des groupes cycliques, et l'application restriction est un épimorphisme.

Il suffit donc de montrer que, étant donnés deux groupes cycliques **finis** A et B, et un épimorphisme $\theta : A \to B$, tout générateur de B se relève en un générateur de A. Comme les générateurs des groupes cycliques proviennent des générateurs des p-composantes, nous pouvons en fait supposer que A et B sont des p-groupes (c'est à dire que leur ordre est une puissance de p).

Soit a un générateur de A et b un générateur de B. Alors $\theta(a) = b^j$ pour un entier j nécessairement premier avec p (puisque $\theta(a)$ engendre B). Cela entraîne que a^j est aussi un générateur de A, et montre que tout générateur de B se relève en un générateur de A.

Chaque S_L est donc un fermé non vide de $\mathcal{G}al(\tilde{F}/F)$; si $L_1, \ldots, L_m$ sont des extensions Galoisiennes finies de F, et $M = L_1 \cdots L_m$, alors $S_M \subseteq S_{L_1} \cap \cdots \cap S_{L_m}$. Par compacité de $\mathcal{G}al(\tilde{F}/F)$, nous en déduisons qu'il existe un élément $\sigma_2 \in \bigcap_L S_L$, où L parcourt l'ensemble des extensions Galoisiennes finies de F. Par (5.7), σ_2 est un générateur topologique de $\mathcal{G}al(\tilde{F}/F)$, et par définition il prolonge σ_0.

Puisque $\mathcal{G}al(\tilde{E}/E)$ et $\mathcal{G}al(\tilde{F}/F)$ sont tous deux isomorphes à $\hat{\mathbf{Z}}$, l'application $\sigma_1 \to \sigma_2$ se prolonge de manière unique à un isomorphisme $\Phi : \mathcal{G}al(\tilde{E}/E) \to \mathcal{G}al(\tilde{F}/F)$, qui satisfait, pour tout $a \in \tilde{K}$ et $\sigma \in \mathcal{G}al(\tilde{E}/E)$, $\Phi(\sigma)(a) = \sigma(a)$.

Soit E_0 une sous-structure élémentaire dénombrable de E contenant K. Alors E_0 est relativement algébriquement clos dans E, et $\tilde{E}_0 E = \tilde{E}$ (puisque E_0 a exactement une extension de degré n pour tout n). Donc, l'homomorphisme restriction: $\mathcal{G}al(\tilde{E}/E) \to \mathcal{G}al(\tilde{E}_0/E_0)$ est un isomorphisme. L'isomorphisme Φ induit donc un isomorphisme $\Phi_0 : \mathcal{G}al(\tilde{E}_0/E_0) \to \mathcal{G}al(\tilde{F}/F)$.

Par (5.10), il existe donc un $\tilde{K}$-isomorphisme $\varphi_0 : \tilde{E}_0 \to \tilde{F}$ tel que $\varphi_0(E_0) \subseteq F$, F est une extension régulière de $\varphi_0(E_0)$, et pour tout $a \in E_0$, et $\sigma \in \mathcal{G}al(\tilde{F}/F)$, $\varphi_0(\Phi_0^{-1}(\sigma)(a)) = \sigma(\varphi_0(a))$.

Soit F_0 une sous-structure élémentaire dénombrable de F contenant $\varphi_0(E_0)$. Nous avons un isomorphisme $\Psi_0 : \mathcal{G}al(\tilde{E}/E) \to \mathcal{G}al(\tilde{F}_0/F_0)$, et par (5.10), nous pouvons trouver un isomorphisme $\psi_0 : \tilde{F}_0 \to \tilde{E}$ qui prolonge φ_0^{-1}, tel que $\psi_0(F_0) \subseteq E$ et E est une extension régulière de $\psi_0(F_0)$, et pour tout $\sigma \in \mathcal{G}al(\tilde{E}/E)$ et $a \in F_0$,

$$\psi_0(\Psi_0(\sigma)(a)) = \sigma(\psi_0(a)).$$

Nous construisons de cette manière deux familles d'isomorphismes partiels φ_i et ψ_i, $i \in \mathbf{N}$, satisfaisant:

(i) Le domaine de φ_i est la clôture algébrique d'une sous-structure élémentaire dénombrable E_i de E contenant $\psi_{i-1}(F_{i-1})$.

(ii) Le domaine de ψ_i est la clôture algébrique d'une sous-structure élémentaire dénombrable F_i de F contenant $\varphi_i(E_i)$.

(iii) φ_i prolonge ψ_{i-1}^{-1} et ψ_i prolonge φ_i^{-1}.

(iv) Pour tout $\sigma \in \mathcal{G}al(\tilde{E}/E)$, pour tout $a \in E_i$ et $b \in F_i$,

$$\varphi_i(\sigma(a)) = \Phi(\sigma)(\varphi_i(a)) \quad \text{et} \quad \psi_i(\Phi(\sigma)(b)) = \sigma(\psi_i(b)).$$

Soient $E_\omega = \bigcup_{i \in \mathbf{N}} E_i$, $F_\omega = \bigcup_{i \in \mathbf{N}} F_i$. Alors $E_\omega \prec E$ et $F_\omega \prec F$. De plus l'application $\cup_{i \in \mathbf{N}} \varphi_i$ définit un isomorphisme $\varphi_\omega : \tilde{E}_\omega \to \tilde{F}_\omega$, dont l'inverse est $\psi_\omega = \cup_{i \in \mathbf{N}} \psi_i$. Donc $\varphi_\omega(E_\omega) = F_\omega$, et $E_\omega \equiv_K F_\omega$, ce qui entraîne que $E \equiv_K F$.

(5.12) Théorème. Soient E et F des corps pseudo-finis de même caractéristique, et k leur sous-corps premier ($\mathbf{Q}$ ou $\mathbf{F}_p$).

(1)
$$E \equiv F \iff E \cap \tilde{k} \simeq F \cap \tilde{k}.$$

(2) La théorie $\text{Psf} \cup \{\exists x\, f(x) = 0 \mid f(x) \in \mathbf{Z}[X],\ E \models \exists x\, f(x) = 0\} \cup \{\forall x\, f(x) \neq 0 \mid f(x) \in \mathbf{Z}[X],\ E \models \forall x\, f(x) \neq 0\}$ est complète.

(3) Soit φ un énoncé du langage $\mathcal{L}$ des anneaux. Alors il existe un énoncé ψ, qui est une combinaison booléenne d'enoncés de la forme $\exists x\, f(x) = 0$, où $f(X) \in \mathbf{Z}[X]$, telle que
$$\text{Psf} \vdash (\varphi \leftrightarrow \psi).$$

Démonstration. (1) et (2) sont immédiats par (5.11). Pour (3) nous appliquons le résultat (0.3) à l'ensemble Δ des combinaisons booléennes d'énoncés de la forme $\exists x\, f(x) = 0$, où $f(X) \in \mathbf{Z}[X]$.

(5.13) Théorème. Soient E et F des corps pseudo-finis contenant un sous-corps K.

(1) La théorie $\text{Psf} \cup \{\exists x\, f(x) = 0 \mid f(x) \in K[X],\ E \models \exists x\, f(x) = 0\} \cup \{\forall x\, f(x) \neq 0 \mid f(x) \in K[X],\ E \models \forall x\, f(x) \neq 0\}$ est complète.

(2) Soit $\varphi(\bar{x})$, $\bar{x} = (x_1, \ldots, x_n)$, une formule du langage $\mathcal{L}(K)$ ($\mathcal{L}$ auquel nous avons ajouté des symboles de constantes pour les éléments de K). Alors il existe une formule $\psi(\bar{x})$, qui est une combinaison booléenne d'énoncés de la forme $\exists t\, f(\bar{x}, t) = 0$, où $f(\bar{X}, T) \in K[\bar{X}, T]$, telle que
$$\text{Psf} \cup \Delta(K) \vdash \forall \bar{x} (\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})).$$
($\Delta(K)$ est l'ensemble des énoncés sans quantificateurs du langange $\mathcal{L}(K)$ vrais dans K).

Démonstration. (1) est immédiat par (5.11). Pour (2), nous utiliserons de nouveau (0.3). Soient F_1 et F_2 des corps pseudo-finis, $\bar{a} \in F_1^n$ et $\bar{b} \in F_2^n$. Soit Δ l'ensemble des combinaisons booléennes d'énoncés de la forme $\exists t\, f(\bar{x}, t) = 0$, où $f(\bar{X}, T) \in K[\bar{X}, T]$. Alors Δ est clos par disjonction, et contient toutes les formules sans quantificateurs avec variables libres $\bar{x}$. Par (0.3), il nous faut montrer que si $\bar{b}$ satisfait dans F_2 toutes les formules de Δ satisfaites par $\bar{a}$ dans F_1, alors $F_2 \models \varphi(\bar{b})$.

Supposons donc que $\bar{b}$ satisfait dans F_2 toutes les formules de Δ satisfaites par $\bar{a}$ dans F_1. Nous avons alors $K(\bar{a}) \simeq_K K(\bar{b})$.

Nous avons montré dans la démonstration de (5.11), que si deux corps E et F contenant K satisfont les mêmes énoncés de la forme $\exists t\ f(t) = 0$, où $f(X) \in K[X]$, alors $E \cap \tilde{K} \simeq_K F \cap \tilde{K}$. Appliquant ce résultat aux corps isomorphes $K(\bar{a})$ et $K(\bar{b})$ nous obtenons un isomorphisme θ entre la clôture algébrique relative de $K(\bar{a})$ dans F_1 et la clôture algébrique relative de $K(\bar{b})$ dans F_2 qui envoie $\bar{a}$ sur $\bar{b}$. Le théorème (5.11) nous dit alors que l'isomorphisme partiel θ est élémentaire, ce qui montre que $F_2 \models \varphi(\bar{b})$.

(5.14) Théorème. Soient $E \subseteq F$ des corps pseudo-finis. Alors

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

Démonstration. Appliquer le théorème précédent à $K = E$.

(5.15) Pour chaque $n \in \mathbf{N}$, $n > 1$, nous prenons des nouveaux symboles de constantes $c_{i,n}$, $1 \leq i \leq n$. Soit $\mathcal{L}_c$ le langage $\mathcal{L} \cup \{c_{i,n} \mid n \in \mathbf{N},\ n > 1,\ 1 \leq i \leq n\}$, et soit Psf_c la théorie obtenue en rajoutant à Psf, pour chaque entier $n > 1$, l'énoncé exprimant que le polynôme $x^n + c_{1,n}x^{n-1} + \cdots + c_{n,n}$ est irréductible.

Théorème. La théorie Psf_c est modèle complète.

Démonstration. Soient $(E, \bar{c}) \subseteq (F, \bar{c})$ des modèles de Psf_c. Alors 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. Donc $E \prec F$.

Remarque. En fait on peut affaiblir l'axiomatisation: il suffit de rajouter à Psf_c, pour chaque $n > 1$, l'axiome $\forall x\ x^n + c_{1,n}x^{n-1} + \cdots + c_{n,n} \neq 0$: en effet, soient $(E, \bar{c}) \subseteq (F, \bar{c})$ des corps pseudo-finis modèles de ces axiomes. Si E n'est pas relativement algébriquement clos dans F, alors il existe $n > 1$ tel que F contienne l'extension E_n de E de degré n. Cependant, E_n contient une racine de l'équation $x^n + c_{1,n}x^{n-1} + \cdots + c_{n,n} = 0$, et par hypothèse, $F \models \forall x\ x^n + c_{1,n}x^{n-1} + \cdots + c_{n,n} \neq 0$. Nous obtenons donc une contradiction, ce qui montre que $\tilde{E} \cap F = E$.

(5.16) Théorème. 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 $f(\bar{X}, T) \in \mathbf{Z}[\bar{X}, T]$, qui est équivalente à $\varphi(\bar{x})$ modulo la théorie des corps parfaits PAC.

Démonstration. Remarquons d'abord que nous pouvons supposer que la formule $\varphi(\bar{x})$ est positive. En effet, toute formule $g(\bar{x}) \neq 0$ est équivalente, modulo la théorie des corps, à la formule $\exists t\ g(\bar{x})t - 1 = 0$. Nous remplaçons donc toute sous-formule négation d'atomique par une formule existentielle, et nous réduisons donc à une formule $\varphi(\bar{x})$ de la forme

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

où $\bar{y} = (y_1, \ldots, y_m)$, et la formule $\theta(\bar{x}, \bar{y})$ est une conjonction d'équations.

Soit Δ l'ensemble des disjonctions finies de formules de la forme $\exists t\ f(\bar{x}, t) = 0$, où $f(\bar{X}, T) \in \mathbf{Z}[\bar{X}, T]$. Soient F_1 et F_2 deux corps PAC parfaits, soient $\bar{a} \in F_1^n$ et $\bar{b} \in F_2^n$. Supposons que $F_1 \models \exists \bar{y}\ \theta(\bar{a}, \bar{y})$, et que $\bar{b}$ satisfait dans F_2 toutes les formules de Δ satisfaites par $\bar{a}$ dans F_1. Comme dans (5.13), nous en déduisons que les corps F_1 et F_2 ont la même caractéristique, et que, si k est leur sous-corps premier, alors $k(\bar{a})$ 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 $k(\bar{a})$, et est de la forme $k(\bar{a}, \alpha)$ pour un élément α séparable sur $k(\bar{a})$. De plus, l'ensemble algébrique V des zéros dans K^m de $I(\bar{c}/k(\bar{a}, \alpha))$ est une variété (par (2.11)), définie (au sens de la géométrie algébrique) sur la clôture parfaite de $k(\bar{a}, \alpha)$.

Soit $p(\bar{X}, T) \in \mathbf{Z}[\bar{X}, T]$ 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 $p(\bar{b}, \beta) = 0$, et nous avons donc un isomorphisme $\psi : k(\bar{a}, \alpha) \to k(\bar{b}, \beta)$, qui envoie $(\bar{a}, \alpha)$ sur $(\bar{b}, \beta)$. Prolongeant ψ^{-1} en un automorphisme de K, nous pouvons donc remplacer F_2 par une copie isomorphe, qui contient $\bar{a}$ et α, et supposer que $(\bar{b}, \beta) = (\bar{a}, \alpha)$. Comme F_2 est parfait, la variété V est définie sur F_2; comme F_2 est PAC, nous pouvons donc trouver un point $\bar{d} \in V(F_2) = V \cap F_2^m$. Puisque $\bar{c}$ est un point générique de V, nous avons donc un $k(\bar{a}, \alpha)$-homomorphisme: $k(\bar{a}, \alpha)[\bar{c}] \to k(\bar{a}, \alpha)[\bar{d}]$. Comme la formule $\theta(\bar{x}, \bar{y})$ est positive, sans quantificateurs, et satisfaite par $(\bar{a}, \bar{c})$, elle est aussi satisfaite par $(\bar{a}, \bar{d}) = (\bar{b}, \bar{d})$, ce qui montre que $F_2 \models \exists \bar{y}\ \theta(\bar{b}, \bar{y})$.

En appliquant (0.3), nous concluons que modulo la théorie des corps PAC parfaits, la formule $\varphi(\bar{x})$ est équivalente à une conjonction de formules de Δ. Le résultat s'ensuit, si l'on remarque que, modulo la théorie des corps, toute formule de Δ est équivalente à une formule de la forme $\exists t\ f(\bar{x}, t) = 0$

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

(1) $\mathrm{Psf}_c \vdash \varphi(\bar{x}) \leftrightarrow \bigvee_I \psi_I(\bar{x}))$.

(2) 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 $\{\bar{t} \in F^m \mid F \models \theta_I(\bar{a}, \bar{t})\}$ a au plus N_I éléments.

Démonstration. Nous savons, par (5.15) et (5.16), que $\varphi(\bar{x})$ est équivalente modulo Psf_c à une formule que nous écrirons sous la forme $\exists t_1, \ldots, t_s\ \bigwedge_{i=1}^{s} f_i(\bar{x}, \bar{c}, t_i) = 0$, où $f_i(\bar{X}, \bar{C}, T_i) \in \mathbf{Z}[\bar{X}, \bar{C}, T_i]$.

Soit $(F, \bar{c}) \models \mathrm{Psf}_c$ et $\bar{a} \in F^n$ satisfaisant $\varphi(\bar{x})$. Il est clair que si les polynômes $f_i(\bar{a}, \bar{c}, T_i)$ ne sont pas identiquement nuls, alors ils n'ont qu'un nombre fini de racines. Il se peut cependant que pour certaines valeurs de $\bar{a}$ et $\bar{c}$, ils deviennent identiquement nuls, et dans ce cas l'ensemble des solutions de $f_i(\bar{a}, \bar{c}, T_i) = 0$ est infini, et en fait la condition est vide.

Pour chaque sous-ensemble I de $\{1, \ldots, s\}$, considérons la formule $\psi_I(\bar{x})$ qui exprime les propriétés suivantes:

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

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

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

Il est clair que $\varphi(\bar{x})$ est équivalente modulo Psf_c à la disjonction des formules $\psi_I(\bar{x})$, où I parcourt l'ensemble des sous-ensembles de $\{1, \ldots, s\}$. Il nous faut maintenant montrer que les formules $\psi_I(\bar{x})$ satisfont la condition désirée. La condition (i) est positive sans quantificateurs, et si (ii) est vérifiée et $i \in I$, alors l'ensemble des t_i satisfaisant $f_i(\bar{x}, \bar{c}, t_i) = 0$ est fini.

Il nous reste donc à montrer que nous pouvons exprimer la condition (ii) de façon positive. Observons que la disjonction $\bigvee(y_j \neq 0)$ est équivalente modulo la théorie des corps, à la formule $\exists u\ \prod_j (y_j u - 1) = 0$. Pour chaque $i \in I$, nous avons donc une formule $\exists u_i\ p_i(\bar{x}, \bar{c}, u_i) = 0$, où $p_i(\bar{x}, \bar{c}, U_i)$ est un polynôme avec un coefficient égal à 1, qui exprime que le polynôme $f_i(\bar{x}, \bar{c}, T_i)$ n'est pas identiquement nul.

La formule $\psi_I(\bar{x})$ est donc équivalente modulo Psf_c à une formule de la forme souhaitée. La borne N_I est alors égale au 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. Soit F un corps pseudo-fini, et $S \subseteq F^m$ un sous-ensemble définissable. Alors il existe un ensemble algébrique $V \subseteq F^{m+n}$ 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. Nous nous plaçons dans le langage $\mathcal{L}_c$, et trouvons des interprétations pour les constantes $c_{i,n}$ de $\mathcal{L}_c$ telles que $(F, \bar{c}) \models \mathrm{Psf}_c$. Soit $\varphi(\bar{x}, \bar{y})$ et $\bar{a}$ un uplet de F tels que S est défini par la formule $\varphi(\bar{a}, \bar{y})$.

Soient $\psi_I(\bar{x}, \bar{y})$ les formules obtenues en appliquant la proposition à la formule $\varphi(\bar{x}, \bar{y})$. Pour chaque I, l'ensemble défini par la formule $\psi_I(\bar{a}, \bar{y})$ est alors la projection de l'ensemble algébrique défini par la formule $\theta_I(\bar{a}, \bar{y}, \bar{t})$, et au dessus-d'un point $(\bar{a}, \bar{b})$ satisfaisant $\psi_I(\bar{a}, \bar{y})$ il y a au plus N_I uplets $\bar{t}$.

Nous mettons tous ces ensembles algébriques ensemble, et obtenons la conclusion.

6. Théorie des corps finis et décidabilité

Nous avons donc obtenu une description des complétions de la théorie Psf, et montré que les modèles infinis de la théorie des corps finis sont des corps pseudo-finis. Il nous reste à montrer que tout corps pseudo-fini est un modèle de la théorie des corps finis.

(6.1) Proposition. Soit E un corps parfait, et supposons que E a au plus une extension de degré n pour chaque n. Alors il existe un corps pseudo-fini F contenant E et tel que E est relativement algébriquement clos dans F.

Démonstration. Nous commençons par construire une extension parfaite E_0 de E telle que $\tilde{E} \cap E_0 = E$ et $\mathcal{G}al(\tilde{E}_0/E_0) \simeq \hat{\mathbf{Z}}$. Pour cela, nous avons besoin du résultat suivant, qu'on peut trouver par exemple dans le livre de S. Lang, Fundamentals of Diophantine geometry.

Fait: Soit E un corps. Il existe une famille d'extensions Galoisiennes L_n de $E(t)$, où n parcourt l'ensemble des entiers plus grands que 1, qui est linéairement disjointe au-dessus de $E(t)$, et tel que pour $n > 1$, L_n est une extension régulière de E et $\mathcal{G}al(L_n/E(t)) \simeq S_n$ (le groupe de permutations de l'ensemble à n éléments).

L'hypothèse de régularité et de disjonction linéaire des extensions L_n nous dit que, si nous prenons pour L le corps engendré par les L_n pour $n > 1$:

$$\mathcal{G}al(\tilde{E}L/E(t)) \simeq \prod_n S_n \times \mathcal{G}al(\tilde{E}/E).$$

En utilisant le fait que chaque S_n contient un élément τ_n d'ordre n, nous prolongeons d'abord σ en un élément $\tau \in Aut(\tilde{E}L/E(t))$ tel que le sous-corps de $\tilde{E}L$ fixé par τ ait une extension de degré n pour chaque $n \in \mathbf{N}^{>1}$ (nous prenons τ égal à τ_n sur L_n, égal à σ sur $\tilde{E}$)), puis prolongeons τ en un élément σ_0 de $Aut(\widetilde{E(t)}/E(t))$; soit E_0 le sous-corps de $\widetilde{E(t)}$ fixé par σ_0. Puisque σ_0 prolonge σ, $\tilde{E} \cap E_0 = E$; alors E_0 a une extension de degré n pour chaque $n > 1$ puisque σ_0 prolonge τ, et donc $\mathcal{G}al(\tilde{E}_0/E_0) \simeq \hat{\mathbf{Z}}$.

Nous allons maintenant construire une chaîne croissante $(E_n)_{n\in\mathbf{N}}$ de corps satisfaisant pour chaque n:

(i) $\tilde{E}_n \cap E_{n+1} = E_n$,

(ii) $\mathcal{G}al(\tilde{E}_n/E_n) \simeq \hat{\mathbf{Z}}$, est engendré topologiquement par σ_n qui prolonge σ_0,

(iii) Si V est une variété définie sur E_n, alors $V(E_{n+1}) \neq \emptyset$.

Supposons E_n construit, et soit V_i, $i < \kappa$ une énumération de toutes les variétés V_i définies sur E_n. Nous construisons alors une suite croissante F_i, $i < \kappa$, d'extensions régulières de E_n, en adjoignant des points génériques des variétés V_i. Plus précisément, supposons F_α construite, telle que $V_i(F_\alpha) \neq \emptyset$ pour tout $i < \alpha$. Choisissons $\bar{c} \in V_\alpha$, générique sur F_α, et posons $F_{\alpha+1} = F_\alpha(\bar{c})$; alors $F_{\alpha+1}$ est une extension régulière de F_α et donc de E_n. Pour α limite on pose $F_\alpha = \bigcup_{i<\alpha} F_i$.

L'extension F_κ est donc une extension régulière de E_n qui satisfait la condition (iii). Si σ_{n+1} est une extension de σ_n à $\tilde{F}_\kappa$, et E_{n+1} est le sous-corps de $\tilde{F}_\kappa$ fixé par σ_{n+1}, alors E_{n+1} satisfait toutes les conditions.

Soit $F = \bigcup_{n\in\mathbf{N}} E_n$. C'est alors un corps PAC, parfait, qui a exactement une extension de degré n pour chaque entier positif n. De plus, $\tilde{E} \cap F = E$. C'est le corps cherché.

(6.2) Théorème. Tout corps pseudo-fini est un modèle de la théorie T_f des corps finis. De plus tout corps pseudo-fini de caractéristique 0 est élémentairement équivalent à un ultraproduit de corps premiers finis.

Démonstration. Montrons d'abord le cas facile, en caractéristique p. Etant donné un corps pseudo-fini F de caractéristique p, il nous faut trouver un ultraproduit F^* de corps finis tel que $\tilde{\mathbf{F}}_p \cap F \simeq \tilde{\mathbf{F}}_p \cap F^*$. Il y a deux cas à considérer:

Cas 1: le corps $\tilde{\mathbf{F}}_p \cap F$ est infini.

Soit $(F_n)_{n\in\mathbf{N}}$ une suite croissante de sous-corps finis de F tels que $F \cap \tilde{\mathbf{F}}_p = \bigcup_{n\in\mathbf{N}} F_n$, et soit $\mathcal{U}$ un ultrafiltre non-principal sur $\mathbf{N}$ et $F^* = \prod_n F_n/\mathcal{U}$. Alors $\tilde{\mathbf{F}}_p \cap F^* \simeq \bigcup_n F_n$.

Cas 2: le corps $\tilde{\mathbf{F}}_p \cap F = F_0$ est fini.

Soit Q l'ensemble des nombres premiers ne divisant pas $[F_0 : \mathbf{F}_p]$; c'est un ensemble infini. Pour $q \in Q$, soit F_q l'extension de F_0 de degré q. Soit $\mathcal{U}$ un ultrafiltre non-principal sur Q, et $F^* = \prod_q F_q/\mathcal{U}$. Alors $F^* \cap \tilde{\mathbf{F}}_p = F_0$.

Pour la caractéristique 0, la démonstration est plus difficile et utilise un théorème puissant: le théorème de Tchebotarev. Nous ne donnons pas de détails. Disons quand même que cela utilise la théorie des corps valués. Une des conséquences de ce théorème est la suivante:

Pour un entier n, et des polynômes $f_1(T), \dots, f_n(T), g(T) \in \mathbf{Z}[T]$, soit L l'extension obtenue en adjoignant à $\mathbf{Q}$ toutes les racines des polynômes $f_i(T)$ et $g(T)$. S'il existe un sous-corps E de L tel que $\mathcal{G}al(L/E)$ est cyclique et $E \models \bigwedge_{i=1}^n (\exists t\ f_i(t) = 0) \wedge (\forall t\ g(t) \neq 0)$, alors il y a une infinité de nombres premiers p tels que $\mathbf{F}_p \models \bigwedge_{i=1}^n (\exists t\ f_i(t) = 0) \wedge (\forall t\ g(t) \neq 0)$.

Cela nous permet de prouver la dernière assertion, et donc aussi la première en caractéristique 0: en effet, soit E un sous-corps de $\tilde{\mathbf{Q}}$, ayant au plus une extension de chaque degré, et considérons l'ensemble d'énoncés $\Sigma = \{\exists x\, f(x) = 0 \mid f(x) \in \mathbf{Z}[X],\ E \models \exists x\, f(x) = 0\} \cup \{\forall x\, f(x) \neq 0 \mid f(x) \in \mathbf{Z}[X],\ E \models \forall x\, f(x) \neq 0\}$.

Chaque fragment fini de Σ est satisfait par une infinité de corps finis premiers. Une application standard de la compacité nous donne alors un ultraproduit F^* de corps finis premiers qui satisfait Σ et est infini. Nous avons alors $\tilde{\mathbf{Q}} \cap F^* \simeq E$.

Remarque. Notons deux conséquences immédiates du résultat précédent. Soit φ un énoncé.

Tous les corps pseudo-finis satisfont φ si et seulement si il existe une constante C telle que tous les corps finis de taille supérieure à C satisfont φ.

Ou encore, prenant la contraposée:

Il existe une infinité de corps finis satisfaisant φ si et seulement si il existe un corps pseudo-fini satisfaisant φ.

Donc l'étude des corps pseudo-finis nous donne des propriétés asymptotiques des corps finis: pour tout corps fini suffisamment grand ...

(6.3) Résultats de décidabilité.

Nous avons un énoncé φ, et voulons décider si $T_f \vdash \varphi$. Remarquons que nous avons prouvé les résultats suivants:

$$\mathrm{Psf} = T_f \cup \{\text{ il existe une infinité d'éléments}\},$$
$$\mathrm{Psf}_0 = Th(\mathbf{F}_p)_{p \text{ premier}} \cup \{\text{ il existe une infinité d'éléments}\},$$

où Psf_0 dénote la théorie des corps pseudo-finis de caractéristique 0. Nous avons aussi

$$T_f \subseteq \mathrm{Psf} \subseteq \mathrm{Psf}_0.$$

Enumérons les énoncés ψ qui sont des combinaisons booléennes d'énoncés de la forme $\exists t\ f(t) = 0$, où $f(T) \in \mathbf{Z}[T]$. Nous savons que l'un de ces énoncés est équivalent à φ modulo Psf. Nous prenons aussi une énumération des preuves à partir de Psf. A l'étape n, nous regardons si la n-ième preuve prouve que l'un des n premiers énoncés ψ est équivalent à φ. Il y a forcément un tel n.

La preuve que $\mathrm{Psf} \vdash (\varphi \leftrightarrow \psi)$ n'utilise qu'un nombre fini d'énoncés exprimant que le corps est PAC. Avec le théorème de Lang-Weil, nous produisons donc une constante C_1 telle que si $q > C_1$, alors $\mathbf{F}_q \models \varphi \leftrightarrow \psi$.

Il nous suffit donc de savoir décider la validité de l'énoncé ψ dans tous les corps pseudo-finis, et la validité de l'énoncé φ dans chacun des corps finis de taille plus petite ou égale à C_1. La deuxième partie est évidemment récursive, il nous reste à traiter la première.

Nous avons donc un énoncé ψ, combinaison booléenne d'énoncés de la forme $\exists t\ f(t) = 0$. D'après les résultats précédents, il nous faut montrer que tout sous-corps E de la clôture algébrique du corps premier k, tel que $\mathcal{G}al(\tilde{k}/E)$ est cyclique, satisfait l'énoncé ψ. Ecrivons d'abord ψ comme une disjonction d'énoncés de la forme $\bigwedge_i \exists t_i\ f_i(t) = 0 \wedge \forall t\ g(t) \neq 0$, et remarquons que les énoncés de cette forme où $g(T)$ n'est pas identiquement constant non-nul, ne peuvent être satisfaits dans $\tilde{k}$ ($\mathcal{G}al(\tilde{k}/\tilde{k})$ est cyclique). Nous nous ramenons donc au cas où l'énoncé ψ est positif.

Nous traitons d'abord le cas de caractéristique 0; soit L le corps de décomposition des polynômes apparaissant dans l'énoncé ψ. On peut calculer de façon effective son groupe de Galois sur $\mathbf{Q}$, ainsi que les sous-corps de L fixés par des éléments de ce groupe de Galois. On peut donc décider si tous ces sous-corps satisfont l'énoncé ψ. Si non, alors Psf_0 n'entraîne pas φ, et donc il en est de même des théories Psf et T_f. Si oui, alors $\mathrm{Psf}_0 \vdash \psi$, et donc $\mathrm{Psf}_0 \vdash \varphi$. Nous avons donc montré que la théorie Psf_0 est décidable.

Supposons donc que $\mathrm{Psf}_0 \vdash \psi$; il existe alors une preuve à partir de Psf_0 de l'énoncé φ; cette preuve n'utilise qu'un nombre fini d'énoncés exprimant que la caractérique est $\neq p$, et donc nous trouvons une constante C_2 telle que tous les corps pseudo-finis de caractéristique $> C_2$ satisfont ψ. Nous regardons alors ce qui se passe pour ceux de caractéristique $\leq C_2$: puisque ψ est existentielle, il suffit de regarder si $\mathbf{F}_p \models \psi$ pour $p \leq C_2$. Cela est évidemment effectif.

Nous avons donc montré que les théories suivantes sont décidables: Psf_0, Psf, T_f. En fait on peut montrer qu'elles sont primitives récursives, mais nous ne le ferons pas.

(6.4) Théorème. Soit $\varphi(\bar{x},\bar{y})$ une formule $\bar{x}=(x_1,\dots,x_n)$, $\bar{y}=(y_1,\dots,y_m)$. Il existe un ensemble fini D de paires $(d,\mu)\in\{0,1,\dots,n\}\times\mathbf{Q}^{>0}$ et une constante $C>0$ tels que, pour tout corps fini $\mathbf{F}_q$, et m-uplet $\bar{a}$ de $\mathbf{F}_q$, si l'ensemble $\varphi(\mathbf{F}_q^n,\bar{a})=_{\text{def}}\{\bar{b}\in\mathbf{F}_q^n \mid \mathbf{F}_q\models\varphi(\bar{b},\bar{a})\}$ est non vide, alors

$$(*)\qquad |card(\varphi(\mathbf{F}_q^n,\bar{a}))-\mu q^d|<Cq^{d-1/2},$$

pour une paire $(d,\mu)\in D$.

Pour chaque paire $(d,\mu)\in D$ il existe une formule $\varphi_{d,\mu}(\bar{y})$ qui définit, dans tout corps $\mathbf{F}_q$, l'ensemble des m-uplets $\bar{a}$ satisfaisant $(*)$.

Remarques. (1) Dans le cas où $\varphi(\bar{x},\bar{a})$ définit une variété V, c'est tout simplement le théorème de Lang-Weil; on a alors $d=dim(V)$ et $\mu=1$.

(2) Supposons que $n=1$. Nous avons alors seulement deux possibilités pour d: $d=0$ ou $d=1$. De cela, nous produisons des constantes $A>0$ et $r>0$ telles que, pour tout corps fini $\mathbf{F}_q$ et m-uplet $\bar{a}$ de $\mathbf{F}_q$,

$$card(\varphi(\mathbf{F}_q^n,\bar{a}))>A \quad\rightarrow\quad card(\varphi(\mathbf{F}_q^n,\bar{a}))>rq.$$

En effet, soit $A_0=\sup\{\mu \mid (0,\mu)\in D\}$, et soit $r_0=\inf\{\mu \mid (1,\mu)\in D\}$. Nous avons alors, par $(*)$: $card(\varphi(\mathbf{F}_q^n,\bar{a}))<A_0+Cq^{-1/2}$ ou $card(\varphi(\mathbf{F}_q^n,\bar{a}))>-Cq^{1/2}+r_0q$. Prenant par exemple $r=r_0/2$ et $A=\sup\{A_0+C,4C^2/r_0^2\}$, on vérifie que $card(\varphi(\mathbf{F}_q^n,\bar{a}))>A$ entraîne $card(\varphi(\mathbf{F}_q^n,\bar{a}))>rq$ pour tout q.

Esquisse de démonstration du théorème.

Etape 1: nous allons commencer par le cas où la formule φ est sans quantificateurs. En remarquant que l'ensemble des x non nuls est en bijection avec l'ensemble des paires (x,y) satisfaisant $xy=1$, nous pouvons supposer que φ est positive, et donc définit un ensemble algébrique W.

Soit F un corps pseudo-fini, et $\bar{a}\in F^m$. Nous regardons l'ensemble $W(\bar{a})(F)=\{\bar{b}\in F^n \mid (\bar{b},\bar{a})\in W\}$. C'est la trace sur F^n d'un fermé de $\tilde{F}^n$. Soit V la clôture de Zariski de $W(\bar{a})(F)$, et soient $V_1,\dots,V_s$ les composantes irréductibles de V. On vérifie qu'elles sont définies sur la clôture algébrique relative de $\bar{a}$ dans F (voir commentaires ci-après). On peut aussi prouver que, étant donnée une formule sans quantificateurs $\psi(\bar{x},\bar{y})$, l'ensemble des $\bar{y}$ tels que $\psi(\bar{x},\bar{y})$ définit une variété de dimension d, est définissable (le seul problème est de définir la dimension).

Il existe donc une formule du premier ordre $\theta_a(\bar{y})$, qui est satisfaite par $\bar{a}$, et qui exprime: il existe des variétés $V_1,\dots,V_s$, définies sur une extension algébrique de $k(\bar{a})$ (k est le corps premier) telles que $W(\bar{a})(F)=V_1\cup\dots\cup V_s$; m de ces variétés sont de dimension maximale, égale à d.

En effet, nous remarquons que les polynômes définissant les variétés V_i sont donnés: nous avons donc une borne sur leur degré, et connaissons aussi les polynômes minimaux sur $k(\bar{a})$ des coefficients qui apparaissent dans ces polynômes.

Prenant toutes les formules $\theta_a(\bar{y})$ possibles (c'est à dire F parcourant l'ensemble des corps pseudo-finis, et $\bar{a}$ l'ensemble des m-uplets de F), nous avons donc

$$\mathrm{Psf}\models\bigvee_a \forall\bar{y}\ \theta_a(\bar{y}).$$

Par compacité, Psf prouve une disjonction finie, disons $\theta_1 \vee \cdots \vee \theta_r$. Alors D est l'ensemble des paires (d_i, m_i) correspondantes.

Donc tout corps fini suffisamment grand satisfait la même disjonction. Soit $\bar{a} \in \mathbf{F}_q^m$ et supposons que $\mathbf{F}_q \models \theta_i(\bar{a})$; alors $W(\bar{a})(\mathbf{F}_q) = V_{i,1}(\mathbf{F}_q) \cup \cdots \cup V_{i,s}(\mathbf{F}_q)$, et les variétés $V_{i,j}$ sont définies sur $\mathbf{F}_q$; d'après le théorème de Lang-Weil, l'ensemble $V_{i,j}(\mathbf{F}_q)$ a à peu près $q^{dim(V_{i,j})}$ points, et donc $W(\bar{a})(\mathbf{F}_q)$ a à peu près $m_i q^{d_i}$ points. On peut calculer alors précisément la constante C. Observons que les formules θ_i nous donnent les formules $\varphi_{d,\mu}$.

Etape 2: nous passons maintenant au deuxième cas, celui d'une formule existentielle, de la forme $\exists \bar{t}\ (\bar{x}, \bar{y}, \bar{t}) \in W$, avec la propriété suivante:

si $(\bar{b}, \bar{a}, \bar{d}) \in W$ alors l'ensemble $\{\bar{t} \mid (\bar{b}, \bar{a}, \bar{t}) \in W\}$ est fini (de taille bornée).

Etant donnés un corps $\mathbf{F}_q$ et un m-uplet $\bar{a}$ de $\mathbf{F}_q$, nous savons estimer la taille de l'ensemble $W(\bar{a})(\mathbf{F}_q) = \{(\bar{b}, \bar{d}) \mid (\bar{b}, \bar{a}, \bar{d}) \in W(\mathbf{F}_q)\}$ (par l'étape 1). Cependant, nous comptons certains des points $\bar{b}$ plusieurs fois, puisqu'il y a en général plusieurs uplets $\bar{d}$ tels que $(\bar{b}, \bar{a}, \bar{d}) \in W(\mathbf{F}_q)$. Il nous faut donc tenir compte des différentes possibilités. En rajoutant des variables existentielles, on montre que l'ensemble W_e des points $(\bar{b}, \bar{a})$ tels qu'il existe au moins e uplets $\bar{d}$ avec $(\bar{b}, \bar{a}, \bar{d}) \in W(\mathbf{F}_q)$, est la projection d'un ensemble algébrique, où l'on peut estimer la taille des fibres. On utilise un peu de combinatoire, et on trouve les possibilités pour les paires (d, μ), ainsi que les formules $\varphi_{d,\mu}$.

Etape 3: par (5.17), la formule $\varphi(\bar{x}, \bar{y})$ est équivalente modulo la théorie Psf_c à une formule existentielle $\psi(\bar{x}, \bar{y}, \bar{c})$ satisfaisant les hypothèse de l'étape 2. Par compacité, il existe une formule $\theta(\bar{c})$ telle que Psf $\vdash \forall \bar{z}\ \theta(\bar{z}) \to (\varphi(\bar{x}, \bar{y}) \leftrightarrow \psi(\bar{x}, \bar{y}, \bar{z}))$. La même chose est vraie dans tous les corps finis de taille suffisamment grande, et nous concluons en appliquant l'étape 2 à la formule $\psi(\bar{x}, \bar{y}, \bar{z})$, où $(\bar{y}, \bar{z})$ sont les variables correspondant aux paramètres. Les formules $\varphi_{d,\mu}$ sont alors construites en quantifiant sur $\bar{z}$.

Remarques. (1) L'étape 1 est un peu moins innocente qu'elle ne paraît. Prenons par exemple le cas où $m = 0$, c'est à dire qu'il n'y a pas de paramètres, et que l'ensemble W est défini sur $\mathbf{Z}$. Soit F un corps pseudo-fini de caractéristique 0, et supposons pour fixer les idées que W est $\mathbf{Q}$-irréductible, mais n'est pas une variété. Si aucune composante irréductible de W n'est définie sur F, alors tous les points de $W(F)$ seront en fait dans un ensemble algébrique beaucoup plus petit: l'intersection W_0 de toutes les composantes irréductibles de W. La dimension de cet ensemble est plus petite que celle de W. On regarde maintenant les composantes F-irréductibles de W_0: certaines sont des variétés, aux autres nous devons encore appliquer la procédure d'intersection. Après un nombre fini d'étapes, on arrive finalement à un ensemble algébrique V, dont toutes les composantes irréductibles sont définies sur F, et tel que $W(F) = V(F)$.

(2) L'hypothèse de non-vacuité de l'ensemble définissable est nécessaire. Si l'on veut s'en dispenser, on est obligé de rajouter à D la paire $(0, 0)$.

En fait, nous le ferons en général, pour ne pas avoir à distinguer de cas particulier. Les valeurs de μ seront donc positives, excepté dans la paire correspondant à l'ensemble vide. La formule $\varphi_{0,0}(\bar{y})$ sera tout simplement la formule $\forall \bar{x}\ \neg\varphi(\bar{x}, \bar{y})$.

(6.5) Interprétation dans les corps pseudo-finis.

Soit $\varphi(\bar{x}, \bar{y})$ une formule, $\bar{x} = (x_1, \ldots, x_n)$, $\bar{y} = (y_1, \ldots, y_m)$, et soit D l'ensemble de paires associé, auquel on a rajouté $(0, 0)$, et C la constante. Alors, pour tout corps $\mathbf{F}_q$

fini de taille suffisamment grande, et pour tout m-uplet $\bar{a}$ de $\mathbf{F}_q$, il existe une seule paire $(d, \mu) \in D$ telle que $|card(\varphi(\mathbf{F}_q^n, \bar{a})) - \mu q^d| < C q^{d-1/2}$. Donc, il existe une seule paire $(d, \mu) \in D$ telle que $\mathbf{F}_q \models \varphi_{d,\mu}(\bar{a})$. La même chose est alors vraie dans tous les corps pseudo-finis.

Etant donnés un corps pseudo-fini F, et un ensemble $S \subseteq F^n$ défini par la formule $\varphi(\bar{x}, \bar{a})$, où $\bar{a} \in F^m$, nous définissons la paire $(\dim(S), \mu(S))$ comme étant l'unique paire $(d, \mu) \in D$ telle que $F \models \varphi_{d,\mu}(\bar{a})$.

Pour avoir une première idée de la signification de ces nombres, nous allons supposer que F est un ultraproduit de corps finis, $F = \prod_q \mathbf{F}_q / \mathcal{U}$. Nous savons que tout corps pseudo-fini se plonge de façon élémentaire dans un tel ultraproduit (voir (6.2)), donc cette hypothèse peut être faite sans perte trop importante de généralité. Nous gardons les notations du paragraphe ci-dessus. Alors le m-uplet $\bar{a}$ provient d'un m-uplet $(\bar{a}_q)_q \in \prod_q \mathbf{F}_q$, et donc $S = \prod_q S_q / \mathcal{U}$, où $S_q = \varphi(\mathbf{F}_q^n, \bar{a}_q)$. Nous savons que pour un ensemble d'indices $Q \in \mathcal{U}$, nous avons $\mathbf{F}_q \models \varphi_{d,\mu}(\bar{a}_q)$, et donc $card(S_q) \sim \mu q^d$ pour tout $q \in Q$ (suffisamment grand).

(6.6) Proposition. Soit F un corps pseudo-fini, $S \subseteq F^n$ un ensemble définissable, et $\varphi(\bar{x}, \bar{y})$ une formule, $\bar{x} = (x_1, \ldots, x_n)$, $\bar{y} = (y_1, \ldots, y_m)$.

(1) Soit V une variété définie sur F. Alors $dim(V(F)) = dim(V)$ et $\mu(V(F)) = 1$.

(2) Soit $\tilde{S}$ la clôture de Zariski de S (dans $\tilde{F}^n$). Alors la dimension de l'ensemble algébrique $\tilde{S}$ est égal à la dimension de S définie ci-dessus.

(3) Si $T \subseteq F^n$ est définissable et S et T sont disjoints, alors

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

(4) Soit $f : S \to T$ une fonction définissable. Si pour tout $\bar{a} \in T$, $dim(f^{-1}(\bar{a})) = d$ alors $dim(S) = dim(T) + d$. Si de plus nous avons pour tout $\bar{a} \in T$, $\mu(f^{-1}(\bar{a})) = m$, alors $\mu(S) = m\mu(T)$.

(5) Le nombre μ peut être utilisé pour définir une mesure sur les sous-ensembles définissables de S, de la façon suivante:

$$m_S(T) = \begin{cases} 0 & \text{si } dim(T) < dim(S), \\ \mu(T)/\mu(S) & \text{si } dim(T) = dim(S). \end{cases}$$

Cette mesure est (finiment) additive, et $m_S(S) = 1$.

(6) Il existe un nombre M, indépendant du corps pseudo-fini F, tel que toute suite $(\bar{a}_i)_i$ telle que les ensembles $\varphi(F^n, \bar{a}_i)$ forment une suite strictement croissante de sous-ensembles de F^n, est de longueur $\leq M$.

(7) (La propriété S_1) Il existe un nombre M, indépendant du corps pseudo-fini F, tel que toute suite $(\bar{a}_i)_i$ satisfaisant pour tous $i \neq j$:

$$dim(S \cap \varphi(F^n, \bar{a}_i)) = dim(S) = d,$$
$$dim(S \cap \varphi(F^n, \bar{a}_i) \cap \varphi(F^n, \bar{a}_j)) < d,$$

est de longueur $\leq M$.

Démonstration. (1) est clair, par la définition des nombres d et μ. Remarquons que cela donne immédiatement que les deux notions de dimension coïncident pour un ensemble algébrique, à condition qu'il ait une composante de dimension maximale définie sur F.

(3), (4) et (5) sont immédiats si l'on pense à la définition de μ dans les corps finis. La propriété (4) est l'une des plus importantes de la dimension.

(2) Par (5.17), S est l'image par une projection π à fibres finies des points F-rationnels d'un ensemble algébrique V, et $dim(V(F)) = dim(S)$ (on vérifie cette égalité soit en regardant l'étape 2 de l'esquisse de preuve de (6.4), soit en utilisant (4)). Nous pouvons supposer que $V(F)$ est dense dans V (sinon, on remplace V par la clôture de Zariski de $V(F)$), et l'on a alors $dim(S) = dim(V)$. Comme les fibres de π sont finies, la dimension de V est égale à la dimension de la clôture de Zariski de $\pi(V)$, qui contient $\tilde{S}$. Mettant tout ensemble, nous obtenons le résultat.

(6) Supposons qu'il n'existe pas de tel M; par compacité, il existe un corps pseudo-fini F et une suite $\bar{a}_i$, $i \in \mathbf{N}$, de m-uplets, telle que $\varphi(F^n, \bar{a}_i)$ est strictement contenu dans $\varphi(F^n, \bar{a}_{i+1})$ pour tout $i \in \mathbf{N}$. Comme l'ensemble D des paires associées à $\varphi(\bar{x}, \bar{y})$ est fini, en passant à une sous-suite de la suite $(\bar{a}_i)_{i\in\mathbf{N}}$ nous pouvons supposer que pour tout $i \in \mathbf{N}$, $F \models \varphi_{d,\mu}(\bar{a}_i)$ pour une paire (d, μ) fixée. Posons $S_i = \varphi(F^n, \bar{a}_i)$.

Nous allons montrer que c'est impossible, par induction sur d. Si $d = 0$, nous savons que la taille des ensembles finis S_i est exactement μ; toute suite strictement croissante ne peut donc avoir qu'**un** élément. Supposons donc le résultat montré pour toutes les suites uniformément définissables d'ensembles de dimension $\leq (d-1)$, et considérons les ensembles $S_i \setminus S_1$, pour $i \in I$. Ils forment une suite strictement croissante d'ensembles, définis par la formule $\neg\varphi(\bar{x}, \bar{a}_1) \wedge \varphi(\bar{x}, \bar{a}_i)$ et nous pouvons appliquer l'hypothèse d'induction à la suite $S_i \setminus S_1$: comme $S_1 \subseteq S_i$, $dim(S_1) = dim(S_i)$ et $\mu(S_1) = \mu(S_i)$, et $S_i \setminus S_1 \neq \emptyset$, (3) implique que $dim(S_i \setminus S_1) < d$ pour tout i. La suite $S_i \setminus S_1$ est donc finie, ce qui entraîne que la suite de départ était elle aussi finie, et nous donne la contradiction souhaitée.

(7) Supposons que S est défini par la formule $\psi(\bar{x}, \bar{b})$, et soit D' l'ensemble de paires associé à la formule $\psi(\bar{x}, \bar{z}) \wedge \varphi(\bar{x}, \bar{y})$. Soit $r = \inf\{\mu \mid (d, \mu) \in D'\}$. Considérons la mesure m_S, et posons $S_i = S \cap \varphi(F^n, \bar{a}_i)$. Alors notre hypothèse sur la suite $(\bar{a}_i)$ se traduit de la façon suivante:

$$m_S(S_i) \geq r/\mu(S), \qquad \text{et} \qquad m_S(S_i \cap S_j) = 0.$$

D'après les propriétés de base des mesures, cela entraîne que la suite $(\bar{a}_i)$ a au plus $\mu(S)/r$ éléments, et nous donne la constante M.

7. Groupes algébriques

(7.1) Morphismes. Nous nous plaçons dans un grand corps algébriquement clos K. Soit $V \subseteq K^n$ un ensemble algébrique, et U un ouvert de V.

Définition. Une application $f : U \to K$ est régulière si pour tout $\bar{a} \in U$ il existe $p(\bar{X}), q(\bar{X}) \in K[\bar{X}]$, et un ouvert $U' \subseteq U$ contenant $\bar{a}$ tels que pour tout $\bar{b} \in U'$, $q(\bar{b}) \neq 0$ et $f(\bar{b}) = p(\bar{b})/q(\bar{b})$.

Les éléments de $K[V]$ définissent des fonctions régulières sur U; si U est défini par $g(\bar{x}) \neq 0$, les éléments de $K[V, 1/g(\bar{x})]$ sont des fonctions régulières sur U.

Définition. Soit $W \subseteq K^m$ un autre ensemble algébrique. Une fonction $f = (f_1, \dots, f_m) : U \to W$ est un morphisme si chacune des fonctions f_i est régulière sur U.

Si f est bijective, et f^{-1} est un morphisme, alors on dit que f est un isomorphisme. Attention, un morphisme bijectif n'est pas nécessairement un isomorphisme, par exemple, en caractéristique $p > 0$, la fonction $x \mapsto x^p$ est un morphisme bijectif, mais n'est pas un isomorphisme algébrique, puisque l'application inverse est $x \mapsto x^{1/p}$, qui n'est pas une fonction polynômiale.

Voici quelques propriétés simples des morphismes:

(1) Une composition de morphismes est un morphisme.

(2) Un morphisme est continu pour la topologie de Zariski induite sur U.

(3) Supposons que V est F-irréductible. Alors la clôture de Zariski $f(U)\check{}$ de $f(U)$ dans W est aussi F-irréductible: supposons que W_1 et W_2 sont des ensembles algébriques définis sur F et tels que $f(U)\check{} = W_1 \cup W_2$; alors $U = f^{-1}(W_1) \cup f^{-1}(W_2)$, et comme les ensemble $f^{-1}(W_i)$ sont fermés pour la topologie induite et que V est irréductible, V est contenu dans la clôture de Zariski de $f^{-1}(W_i)$ pour un i, ce qui entraîne que $f(U) \subseteq W_i$.

(4) Supposons que f est un isomorphisme entre U et un sous-ensemble ouvert U' de W. Alors f induit une bijection entre les composantes irréductibles de V et celles de W.

(7.2) Groupes algébriques. Un groupe algébrique est un groupe G, dont l'univers sous-jacent est un ouvert de Zariski d'un ensemble algébrique, tel que les deux applications $m : G \times G \to G$ et $\imath : G \to G$ définies par $m(g, h) = gh$ et $\imath(g) = g^{-1}$ pour tous éléments $g, h \in G$, sont des morphismes (d'ensembles algébriques).

Remarque. De même que toutes nos variétés étaient affines, nous nous restreignons aux groupes algébriques qui sont "affines", c'est à dire des sous-ensembles de l'espace **affine** K^n pour un n.

Exemples (1) Le groupe additif $\mathbf{G}_a$: l'ensemble algébrique est K, la loi de groupe est l'addition.

(2) Le groupe multiplicatif $\mathbf{G}_m$: l'ensemble est l'ouvert $K \setminus \{0\}$, la loi de groupe est la multiplication.

(3) Le groupe $GL_n(K)$ des matrices $n \times n$ qui sont inversibles. Nous considérons l'ensemble des n^2-uplets $(\bar{x})$ de K, où $\bar{x} = (x_{ij} \mid 1 \leq i \leq n,\ 1 \leq j \leq n)$, satisfaisant $det(x_{ij}) \neq 0$. La loi de groupe est donnée par la multiplication des matrices $n \times n$.

Définition. Soit G un groupe algébrique; un sous-groupe algébrique de G est un sous-groupe qui est fermé pour la topologie de Zariski induite sur G.

Exemple. Le sous-groupe $SL_n(K)$ de $GL_n(K)$ est défini par l'équation $\det(x_{ij}) - 1 = 0$; c'est donc un sous-groupe algébrique de $GL_n(K)$.

Le groupe GL_n est particulièrement important, à cause du résultat suivant:

Théorème. Tout groupe algébrique affine est isomorphe à un sous-groupe algébrique d'un groupe GL_n pour un certain n.

(7.3) Lemme. (1) Soit $S \subseteq K^n$ un ensemble constructible (c'est à dire défini par une combinaison booléenne d'équations), et $\tilde{S}$ sa clôture de Zariski. Il existe un ouvert U tel que $\tilde{S} \cap U \subseteq S$ et $\tilde{S} \cap U$ est dense dans $\tilde{S}$.

(2) Soit V une variété. Si U est un ouvert de K^n qui coupe V, alors $U \cap V$ est dense dans V.

(3) Soit V une variété définie sur un corps PAC F. Alors $V(F)$ est dense dans V.

(4) Soit F un corps pseudo-fini, $S \subseteq F^n$ un ensemble définissable sur un sous-corps A de F, et soit $d = dim(S)$; si F est $(|A| + \aleph_0)^+$ saturé, alors il existe $\bar{a} \in S$ tel que $deg.tr(\bar{a}/A) = d$. Nous appellerons un tel élément un **générique** de S sur A.

Démonstration. (1) Soient $\tilde{S}_i$, $i = 1 \ldots, m$, les composantes irréductibles de $\tilde{S}$ et $S_i = \tilde{S}_i \cap S$. Il suffit de montrer le résultat pour chacun des S_i, et nous pouvons donc supposer que $\tilde{S}$ est irréductible. Comme S est définissable, S est la réunion d'ensembles non-vides V_i définis par des conjonctions d'équations et d'inéquations. Supposons que V_i est défini par: $\bigwedge_j f_{ij}(\bar{x}) = 0 \wedge g_i(\bar{x}) \neq 0$, et soit T l'ensemble algébrique défini par $\prod_i g_i(\bar{x}) = 0$. Alors $\tilde{S} \setminus T \subseteq S$. De plus, comme V_i est non-vide et contenu dans $\tilde{S}$, les polynômes $g_i(\bar{x})$ ne sont pas dans $I(\tilde{S})$. Comme $I(\tilde{S})$ est premier, cela montre que $\tilde{S} \cap T$ est un fermé strictement contenu dans $\tilde{S}$. Posons $U = \tilde{S} \setminus T$.

(2) Tout ouvert de K^n est une réunion d'ouverts de la forme $U_g = \{\bar{x} \mid g(\bar{x}) \neq 0\}$ pour des polynômes $g[\bar{X}]$ à coefficients dans K. Si $U \cap V \neq \emptyset$, alors $U_g \cap V \neq \emptyset$ pour un g tel que $U_g \subseteq U$, et nous pouvons donc supposer que U est de la forme U_g. Soit donc un autre ouvert U' coupant V, que l'on peut supposer de la forme U_h. Puisque $U_g \cap V \neq \emptyset$, $U_h \cap V \neq \emptyset$, les polynômes $g(\bar{X})$ et $h(\bar{X})$ ne sont pas dans l'idéal premier $I(V) \subseteq K[\bar{X}]$, et donc leur produit non plus. Par le Nullstellensatz, l'ensemble $U_{gh} \cap V$ est non-vide.

(3) Soit $U \subseteq K^n$ un ouvert, avec $U \cap V \neq \emptyset$. Comme la topologie de Zariski sur $\tilde{F}^n$ coïncide avec la topologie induite par celle de K^n, nous pouvons supposer que U est défini sur $\tilde{F}$. Donc $U \cap V$ est dense dans V, puisque V est irréductible. De plus, nous pouvons supposer que U est de la forme U_g pour un polynôme $g(\bar{X})$ à coefficients dans $\tilde{F}$, $g \notin I(V)$. Cela entraîne que chacun des conjugués de U_g au-dessus de F coupe V, et donc leur intersection U' coupe aussi V (par (2)). Si $h(\bar{X})$ est le produit des conjugués de $g(\bar{X})$ au-dessus de F, alors $U' = U_h$ et $h(\bar{X}) \in F[\bar{X}]$.

Considérons maintenant l'ensemble algébrique $W \subseteq K^{n+1}$ défini par $\{(\bar{x}, y) \mid \bar{x} \in V,\ yh(\bar{x}) = 1\}$. Alors W est défini sur F, et $K[W] = K[V, 1/h(\bar{x})]$ est un anneau intègre (puisque V est une variété). Donc W est une variété définie sur F, et a un point $(\bar{a}, b) \in F^{n+1}$; le point $\bar{a}$ est alors dans $V(F) \cap U_h$.

(4) Par (6.6)(2), nous savons que $dim(S) = dim(\tilde{S}) = d$. De plus les composantes irréductibles de $\tilde{S}$ sont définies sur F: si V est une composante irréductible de $\tilde{S}$ alors $V \cap S$ est dense dans V par définition de la clôture. Soit donc V une composante de $\tilde{S}$ de dimension d; elle est définie sur un corps B contenant A, de taille $|A| + \aleph_0$; d'autre part

l'ensemble des inéquations exprimant que $\bar{x}$ est un élément de $V \cap S$ générique sur B, est finiment satisfaisable dans $V \cap S$ (par densité); par saturation, il est donc satisfait dans $V \cap S$.

(7.4) Définitions. Un groupe algébrique est connexe si sa clôture de Zariski est irréductible.

Si G est un groupe algébrique, nous noterons G^0 la trace sur G de la composante irréductible de $\tilde{G}$ qui contient l'élément identité e (ou parfois 1) du groupe. Nous allons commencer avec quelques propriétés simples des groupes algébriques.

Proposition. Soit G un groupe algébrique défini sur un corps (parfait) F.

(1) Soit $g \in G$; les application $h \mapsto gh$, $h \mapsto hg$ et $h \mapsto h^{-1}$ sont des homéomorphismes de G.

(2) Les composantes irréductibles de G (ou, plus exactement, les traces sur G des composantes irréductibles de $\tilde{G}$) sont disjointes. La composante G^0 est définie sur F; c'est un sous-groupe normal de G, et les autres composantes sont des cosets de G^0 dans G.

(3) Soit H un sous-groupe (quelconque) de G, et $\tilde{H}$ sa clôture de Zariski (dans G). Alors $\tilde{H}$ est un sous-groupe algébrique de G. Si H est abélien, $\tilde{H}$ l'est aussi.

(4) Soient U et V des ouverts denses de G. Alors $U \cdot V = G$.

(5) Soit H un sous-groupe de G qui est constructible (i.e., définissable sans quantificateurs); alors H est un sous-groupe algébrique de G.

(6) Soient H un groupe algébrique, et $f : H \to G$ un morphisme de groupes algébriques (un homomorphisme de groupe qui est aussi un morphisme d'ensembles algébriques). Alors $f(H)$ est un sous-groupe fermé de G. Le noyau de f, $\ker f$, est un fermé. Nous avons $dim(H) = dim(f(H)) + dim(\ker(f))$.

(7) Le centre de G, $Z(G)$, est un fermé (Rappelons qu'un élément est central dans un groupe s'il commute avec tous les éléments de ce groupe; l'ensemble des éléments centraux est appelé le centre).

(8) Un sous-groupe fini normal d'un groupe algébrique connexe est central.

(9) Soit g un générique de G (sur F), et $h \in G$ algébriquement indépendant de g au-dessus de F. Alors gh et hg sont des génériques de G sur F, indépendants de h au-dessus de F. Si de plus h est générique, alors gh et hg sont aussi indépendants avec g au-dessus de F. Tout élément de G est le produit de deux génériques.

Démonstration. (1) On observe que ces trois applications sont des isomorphismes d'ensembles algébriques; ce sont donc des homéomorphismes par (7.1)(2).

(2) Ecrivons $G = G_1 \cup \cdots \cup G_m$, où $\tilde{G}_1, \ldots, \tilde{G}_m$ sont les composantes irréductibles de $\tilde{G}$. Pour chaque $g \in G$, la multiplication par g étant un homéomorphisme, elle permute les composantes irréductibles de G. Soit $g \in G_1$, $g \notin G_2 \cup \cdots \cup G_m$, et soit $h \in G$. Alors $(hg^{-1})g = h$; comme g appartient à une unique composante irréductible de G, il en est de même de h. Comme h était arbitraire, cela montre que les composantes irréductibles de G sont disjointes.

Il nous faut maintenant montrer que celle qui contient e, G^0, est un sous-groupe normal de G. Comme ${}^{-1}$ est un homéomorphisme, $(G^0)^{-1}$ est une composante irréductible de G, et elle contient $e^{-1} = e$. Donc $(G^0)^{-1} = G^0$. De même, si $g \in G^0$, gG^0 est une composante irréductible de G qui contient $ge = g$, et donc égale à G^0. Finalement, soit $g \in G$: $g^{-1}G^0g$ est une composante irréductible de G qui contient $g^{-1}eg = e$, et donc égale à G^0.

Il est aussi clair que chacun des cosets de G^0 dans G est une des composantes irréductibles de G. Nous allons maintenant montrer que $e \in G(F)$: en effet, e est l'image par le morphisme $g \mapsto (g, g) \mapsto gg^{-1}$ de l'ensemble G; c'est donc un ensemble algébrique défini sur F, autrement dit: $e \in F$. Tout élément de $\mathcal{G}al(\tilde{F}/F)$ envoie la composante G^0 sur elle-même, ce qui montre qu'elle est définie sur F.

(3) Comme $g \mapsto g^{-1}$ est un homéomorphisme de G, si W est un fermé de G contenant H, alors W^{-1} $(= \{g^{-1} \mid g \in W\})$ contient aussi H. Cela montre que $\tilde{H}$ est clos par $^{-1}$. Soit $g \in H$; en raisonnant de la même façon, $g\tilde{H} = \tilde{H}$, et donc $H\tilde{H} = \tilde{H}$. Si $g \in \tilde{H}$, alors $Hg \subseteq \tilde{H}$, et donc la clôture de Zariski de Hg, $\tilde{H}g$, est contenue dans $\tilde{H}$, ce qui montre que $\tilde{H}\tilde{H} = \tilde{H}$.

Soit $g \in H$; alors $\{h \in G \mid [g, h] \neq e\}$ est un ouvert, qui ne coupe pas H, et donc ne coupe pas $\tilde{H}$. Donc, tout élément de H commute avec tout élément de $\tilde{H}$; si $h \in \tilde{H}$, l'ensemble $\{g \in G \mid [g, h] = e\}$ est alors un fermé qui contient H, ce qui montre que $\tilde{H}$ est abélien.

On peut montrer des résultats analogues pour les groupes résolubles, nilpotents, en fait pour toutes les propriétés exprimables au moyen de formules universelles positives.

(4) Soit $g \in G$. Alors gV^{-1} est dense dans G, et $U \cap gV^{-1} \neq \emptyset$; soit $v \in V$ tel que $h = gv^{-1} \in U$: alors $g = hv$.

(5) Par (7.3)(1), il existe un ouvert U tel que $\tilde{H} \cap U \subseteq H$ et $\tilde{H} \cap U$ est un ouvert dense de $\tilde{H}$; par (3), $\tilde{H}$ est un sous-groupe de G, et par (4), $H \supseteq (\tilde{H} \cap U) \cdot (\tilde{H} \cap U) = \tilde{H}$, ce qui montre que H est fermé dans G.

(6) $f(H)$ est un sous-groupe constructible de G et est donc fermé par (5). Soit $\bar{a} \in H$ et $\bar{b} = f(\bar{a})$; alors le fermé $f^{-1}(\bar{b})$ est isomorphe (comme ensemble algébrique) à $\ker f$, par l'application: $\bar{c} \mapsto \bar{c}\bar{a}^{-1}$. Donc $dim(f^{-1}(\bar{b})) = dim(\ker f)$. Pour tout $\bar{a} \in H$ nous avons $deg.tr(\bar{a}/F) \leq deg.tr(f(\bar{a})/F) + dim(\ker f)$, et il existe des éléments pour lesquels ces deux nombres sont égaux. Cela montre que $dim(H) = dim(f(H)) + dim(\ker f)$.

(7) Soit $Z = Z(G)$, et $g \in G$; l'ensemble des éléments qui commutent avec g est un fermé contenant Z et donc $\tilde{Z}$. Cela montre que $\tilde{Z} = Z(G)$.

(8) Soit N un sous-groupe normal fini de G, et $g \in N$; comme N est normal et fini, g n'a qu'un nombre fini de conjugués, et donc le centralisateur $C_G(g)$ de g dans G est un sous-groupe d'indice fini dans G. Comme $C_G(g)$ est défini par des équations, c'est un sous-groupe fermé de G, d'indice fini, qui doit donc être égal à G. Cela montre que $N \subseteq Z(G)$.

(9) Soit $d = dim(G)$. Nous savons que $gh, hg \in F(g, h)$ et $g \in F(h, gh)$, $g \in F(h, hg)$. Nous avons donc:

$$\begin{aligned} deg.tr(g, h/F) &= deg.tr(g/F) + deg.tr(h/F) = d + deg.tr(h/F) \\ &\leq deg.tr(h, gh/F) = deg.tr(h/F) + deg.tr(gh/F(h)) \\ &\leq deg.tr(h/F) + d, \end{aligned}$$

ce qui montre que $deg.tr(gh/F(h)) = d$, et donc que gh est un générique de G, indépendant de h. On raisonne de la même façon pour montrer l'assertion pour hg.

Si de plus h est générique, alors (par la première partie) gh et hg sont des génériques qui sont indépendants de g.

Soit $g \in G$, et h un générique de G indépendant de g; alors g^{-1} est aussi un générique, ainsi que gh, et nous avons $h = g^{-1}(gh)$.

(7.5) Proposition. Soit G un groupe algébrique, défini sur un corps pseudo-fini F.

(1) Si G est connexe, alors $G(F)$ est dense dans G.

(2) Si G est connexe alors tout élément central dans $G(F)$ est central dans G.

(3) Soit H un sous-groupe de $G(F)$, définissable dans F. Nous avons $dim(G(F)) = dim(G)$, et

$$dim(H) = dim(G(F)) \iff [G(F) : H] < \infty.$$

En particulier, H est d'indice fini dans $\tilde{H}(F)$.

(4) Si $f : H \to G$ est un morphisme de groupe algébriques connexes, qui est surjectif et a un noyau fini, alors

$$card(\ker f \cap H(F)) = [G(F) : f(H(F))].$$

(1) C'est (7.3)(3).

(2) Soit $g \in G(F)$ et supposons qu'il existe $h \in G$ tel que $[g, h] \neq 1$. La condition $\bar{x} \in G \wedge [g, \bar{x}] \neq 1$ définit alors un ouvert non vide U de G. Par (7.3)(3), cet ouvert contient donc un point de $G(F)$, ce qui montre que g n'est pas central dans $G(F)$.

Attention, ce résultat est faux si l'on ne suppose pas que G est connexe: il se peut en effet dans ce cas que $G(F)$ ne soit pas dense dans G.

(3) Nous savons que $dim(G^0) = dim(G)$, et G^0 est connexe et défini sur F. Par (6.4), nous avons donc $dim(G(F)) \geq dim(G^0(F)) = dim(G)$.

Supposons que H est définissable d'indice fini dans $G(F)$: chaque coset de H a la même dimension que H (par (6.6)(4)), et $G(F)$ est la réunion d'un nombre fini de ces cosets, donc $dim(G(F)) = dim(H)$.

Supposons maintenant que H est définissable mais d'indice infini dans $G(F)$. Soient g_i, $i \in \mathbf{N}$, des éléments de G tels que $g_i^{-1}g_j \notin H$ pour $i \neq j$; les cosets g_iH sont alors disjoints, uniformément définissables, et de la même dimension que H. Par (6.6)(5), nous avons donc $dim(H) < dim(G)$.

Nous savons que $dim(H) = dim(\tilde{H}) = dim(\tilde{H}(F))$; par le résultat ci-dessus, il faut donc que H soit d'indice fini dans $\tilde{H}(F)$.

(4) Comme G et H sont connexes, nous avons $\mu(G(F)) = \mu(H(F)) = 1$. D'autre part, les hypothèses sur f entraînent $dim(G) = dim(H) = dim(f(H))$; par (6.4) nous avons $dim(f(H(F)) = dim(G(F))$, et donc

$$\mu(kerf \cap H(F))\mu(f(H(F))) = \mu(H(F)) \quad \text{et} \quad \mu(f(H(F)))[G(F) : f(H(F))] = \mu(G(F)),$$

ce qui donne l'égalité désirée.

(7.6) Théorème. Soit G un groupe algébrique de dimension n (> 0) défini sur le corps pseudo-fini F. Soit U un sous-ensemble définissable de $G(F)$, de dimension n, et H le sous-groupe de $G(F)$ engendré par U. Alors H est définissable, d'indice fini dans $G(F)$, et il existe un entier m tel que tout élément de H est le produit d'au plus m éléments de $U \cup U^{-1}$.

Démonstration. Nous supposons que tout est défini avec paramètres sur un sous-corps A de F, relativement algébriquement clos dans F, et que F est suffisamment saturé.

Soit $W = \{g \in G(F) \mid dim(U \cap gU) = n\}$. L'ensemble $U \cap gU$ est définissable, uniformément en g, et par (6.4), l'ensemble W est aussi définissable.

Etape 1: $W \subseteq U \cdot U^{-1}$.

Soit $g \in W$, et $h \in U \cap gU$; si $u \in U$ est tel que $h = gu$, alors $g = hu^{-1}$.

Etape 2: $dim(W) = n$.

Pour cela, prenons des éléments $h_1, h_2 \in U$, algébriquement indépendants au dessus de A, et de degré de transcendance sur A égal à n (c'est à dire, des génériques de G). Par (7.4)(9), l'élément $g = h_1 h_2^{-1}$ est un générique de G sur A, et il est indépendant de h_1 au-dessus de A. Comme h_1 est générique, cela entraîne que h_1 est générique sur $A(g)$; d'autre part $h_1 = gh_2 \in U \cap gU$, ce qui montre que $g \in W$ et donc que $dim(W) = n$.

Etape 3: Un nombre fini de translatés de W recouvre H.

Supposons que non, et soit g_i, $i \in \mathbf{N}$, une suite d'éléments de H tels que $g_i \notin \bigcup_{j<i} g_j W$ pour tout i; pour $j < i$ nous avons alors $g_j^{-1} g_i \notin W$, et par la définition de W, cela veut dire que $dim(U \cap g_j^{-1} g_i U) < n$, ou bien encore, que $dim(g_j U \cap g_i U) < n$; nous remarquons que $dim(g_i U) = dim(U) = n$, que tous ces ensembles sont définissables, contenus dans $G(F)$ qui est aussi de dimension n, et ont une petite intersection. Cela contredit la propriété S_1 (6.6)(7), et montre donc qu'il suffit d'un nombre fini de translatés de W pour recouvrir H.

Soient donc $g_1, \dots, g_r \in H$ tels que $H = \bigcup_{i=1}^r g_i W$. Nous en déduisons l'existence de m (puisque chaque g_i est un produit fini d'éléments de $U \cup U^{-1}$), et donc la définissabilité de H; nous avons $n = dim(U) \leq dim(H) \leq dim(G(F)) = n$, et donc H est un sous-groupe d'indice fini dans $G(F)$.

(7.7) Théorème. Soit G un groupe algébrique défini sur le corps pseudo-fini F, et soit S_i, $i \in I$, une famille de sous-ensembles de $G(F)$ définissables dans F, et tels que, pour tout $i \in I$, $e \in S_i$ et $\tilde{S}_i$ est une variété.

Soit H le sous-groupe de $G(F)$ engendré par les ensembles S_i, $i \in I$. Alors $\tilde{H}$ est le sous-groupe de G engendré par les ensembles $\tilde{S}_i$, $i \in I$; c'est un groupe connexe, et H est d'indice fini dans $\tilde{H}(F)$. De plus il existe des indices $i_1, \dots, i_m$ (peut-être avec répétitions) tels que

$$H = S_{i_1}^{\pm 1} \cdot \ldots \cdot S_{i_m}^{\pm 1} \quad \text{et} \quad \tilde{H} = \tilde{S}_{i_1}^{\pm 1} \cdot \ldots \cdot \tilde{S}_{i_m}^{\pm 1}.$$

Démonstration. Nous allons d'abord montrer le résultat pour le sous-groupe H_0 de G engendré par les $\tilde{S}_i$, $i \in I$. Sans perte de généralité, nous supposerons que pour tout $i \in I$ il existe $j \in I$ tel que $S_i = S_j^{-1}$. Nous nous plaçons dans un grand corps algébriquement clos K. Nous avons un sous-corps A au-dessus duquel tout est défini.

Pour chaque suite finie α d'éléments de I, disons, $\alpha = (\alpha(1), \dots, \alpha(m))$, nous définissons $W_\alpha \subseteq G$ comme étant l'image de $S_\alpha = \tilde{S}_{\alpha(1)} \times \cdots \times \tilde{S}_{\alpha(m)}$ par le morphisme multiplication: $(g_1, \dots, g_m) \mapsto g_1 \cdots g_m$. Comme chaque $\tilde{S}_i$ est irréductible, S_α est aussi irréductible (exercice), et donc $\tilde{W}_\alpha$ est irréductible par (7.1)(3). C'est donc une variété.

Comme chaque S_i contient e, si $\alpha \subseteq \beta$, alors $W_\alpha \subseteq W_\beta$, et donc $dim(\tilde{W}_\alpha) \leq dim(\tilde{W}_\beta)$. Comme cette dimension est bornée par $dim(G)$, il existe donc une suite finie α telle que la variété $\tilde{W}_\alpha$ contient toutes les autres. Comme la famille S_i est close par inverses, il existe β tel que $W_\alpha^{-1} = W_\beta$, ce qui montre que $\tilde{W}_\alpha = \tilde{W}_\alpha^{-1}$. Nous avons aussi $W_\alpha W_\alpha \subseteq \tilde{W}_\alpha$. Nous avons maintenant besoin d'un résultat auxiliaire:

Assertion. Si X et Y sont des sous-ensembles de G, alors $\tilde{X} \cdot \tilde{Y} \subseteq \widetilde{X \cdot Y}$.

En effet, si $g \in X$, alors $gY \subseteq X \cdot Y$ et donc $\widetilde{gY} \subseteq \widetilde{X \cdot Y}$. Par conséquent, pour tout $h \in \tilde{Y}$, $Xh \subseteq \widetilde{X \cdot Y}$, ce qui implique que $\tilde{X}h \subseteq \widetilde{X \cdot Y}$, et donc que $\tilde{X} \cdot \tilde{Y} \subseteq \widetilde{X \cdot Y}$.

Ce résultat entraîne, en prenant $X = Y = W_\alpha$, que $\tilde{W}_\alpha \cdot \tilde{W}_\alpha \subseteq \tilde{W}_\alpha$, c'est à dire que $\tilde{W}_\alpha$ est un sous-groupe de G (nous savons déjà que $\tilde{W}_\alpha = \tilde{W}_\alpha^{-1}$). Comme W_α est dense dans $\tilde{W}_\alpha$, nous en déduisons par (7.4)(4) que $W_\alpha \cdot W_\alpha = \tilde{W}_\alpha$.

Nous avons montré que $W_\alpha \cdot W_\alpha$ est un sous-groupe algébrique de G, qui contient chacun des $\tilde{S}_i$: c'est donc le sous-groupe H_0 de G engendré par les $\tilde{S}_i$, $i \in I$.

Supposons que α est de longueur m, et considérons l'ensemble $U \subseteq G(F)$ défini par $S_{\alpha(1)} \cdot \ldots \cdot S_{\alpha(m)} \cdot S_{\alpha(1)} \cdot \ldots \cdot S_{\alpha(m)}$. D'après l'assertion, $\tilde{U} = H_0$ et donc $dim(U) = dim(H_0)$. De plus, nous avons $U \subseteq H_0(F) \subseteq H_0$; par (7.6), le sous-groupe H_1 engendré par U est définissable, d'indice fini dans $H_0(F)$. Il n'y a qu'un nombre fini de groupes entre H_1 et $H_0(F)$, donc l'un d'entre eux doit être égal à H, et il est définissable, puisqu'il est engendré au-dessus de H_1 par un nombre fini d'éléments, qui se trouvent dans un produit fini d'ensembles S_i. Puisque $U \subseteq H$, nous avons $dim(H) = dim(H_0)$, ce qui montre que $\tilde{H} = H_0$.

(7.8) Corollaire. Soit G un groupe algébrique défini sur un corps pseudo-fini F, et soit S_i, $i \in I$ une famille de sous-ensembles de $G(F)$ définissables dans F. Alors il existe un sous-groupe définissable H de $G(F)$, contenu dans le sous-groupe de $G(F)$ engendré par les S_i, $i \in I$, et tel que, pour tout $i \in I$, S_iH/H est fini.

Démonstration. Les composantes irréductibles de chaque $\tilde{S}_i$ sont définies sur F, et nous pouvons supposer, quitte à agrandir la collection d'ensembles considérés, que chaque $\tilde{S}_i$ est irréductible. Pour $i \in I$, soit $g_i \in S_i$, et soit $T_i = g_i^{-1}S_i$. Alors $\tilde{T}_i$ est irréductible; par (7.7), le sous-groupe H de $G(F)$ engendré par les T_i, $i \in I$, est définissable. D'autre part, $g_i^{-1}S_i \subseteq H$, ce qui montre le résultat.

(7.9) Corollaire. Soit G un groupe algébrique défini sur un corps pseudo-fini F. Si $G(F)$ est définissablement simple, et non-abélien, alors il est simple.

Démonstration. Supposons que $G(F)$ est définissablement simple. On peut supposer que G est connexe: sinon, G^0 est un sous-groupe algébrique de G définissable sur F, et nous avons $G^0(F) = G(F)$. Nous pouvons donc remplacer G par G^0. De plus, puisque G n'est pas abélien, $G(F)$ n'est pas abélien par (7.5)(2), et donc $Z(G(F))$ est un sous-groupe définissable propre de $G(F)$, qui doit donc être trivial.

Supposons que H est un sous-groupe normal de $G(F)$. S'il est fini, soit $g \in H$; alors le centralisateur de g dans $G(F)$ est un sous-groupe définissable de $G(F)$ d'indice fini plus grand que 1 puisque $Z(G(F)) = (1)$; en prenant l'intersection de ses conjugués, nous obtenons un sous-groupe normal définissable propre de $G(F)$, ce qui contredit notre hypothèse.

Nous pouvons donc supposer que H est infini, et que tous ses éléments ont une classe de conjugaison infinie. Soit $g \in H$, et considérons $X = \{h^{-1}gh \mid h \in G(F)\}$; c'est un ensemble définissable de $G(F)$, et sa clôture de Zariski est irréductible parce que G est connexe. D'après (7.7), le sous-groupe H_0 engendré par $g^{-1}X$ est définissable; il est infini, normal et contenu dans H. Cela entraîne: $G(F) = H_0 = H$.

(7.10) Théorème. Soit G un groupe algébrique défini sur un corps pseudo-fini F, et supposons qu'il est presque simple (almost simple en anglais; cela veut dire qu'il n'a pas de sous-groupe algébrique normal infini, et qu'il n'est pas abélien).

Alors $G(F)$ a un plus petit sous-groupe normal d'indice fini H, et H est définissable dans F. Le centre $Z(H)$ de H est fini, $Z(H) = Z(G) \cap H$, et $H/Z(H)$ est simple. L'indice $[G(F) : H]$ est borné indépendamment de F.

Démonstration. Notre hypothèse sur G entraîne que G est connexe, et que ses seuls sous-groupes algébriques normaux sont finis et donc contenus dans $Z(G)$, qui est fini.

Etape 1. Tout sous-groupe normal infini de $G(F)$ est d'indice fini et définissable.

Soit N un sous-groupe normal infini de $G(F)$, et soit $g \in N$, $g \notin Z(G)$. Soit $X = \{[h,g] \mid h \in G(F)\}$; par (7.7) (en raisonnant comme dans (7.9)), le sous-groupe H_0 de $G(F)$ engendré par X dans $G(F)$ est définissable, normal, et d'indice fini dans le sous-groupe $\tilde{H}(F)$, où $\tilde{H}$ est le sous-groupe de G engendré par $\tilde{X}$; comme $\tilde{H}$ est algébrique par (7.4), $\tilde{H} = G$ et donc H_0 est d'indice fini dans $G(F)$.

Donc, $[N : H_0]$ est fini, ce qui montre que N est définissable.

Etape 2. $G(F)$ a un plus petit sous-groupe normal infini. Il est définissable et d'indice fini.

Nous avons montré dans l'étape 1 que tout sous-groupe normal infini de $G(F)$ est définissable, et est d'indice fini. La conclusion est une simple application du théorème de compacité: supposons qu'il n'y en ait pas de plus petit, et soit H_i, $i \in \mathbf{N}$, une suite strictement décroissante de sous-groupes normaux infinis de $G(F)$. En passant à une extension élémentaire de F, nous pouvons supposer que F est ω_1-saturé. Alors $\bigcap_i H_i$ est un sous-groupe normal infini de $G(F)$, et d'indice infini dans $G(F)$, ce qui contredit l'étape 1.

Soit H le plus petit sous-groupe normal infini de $G(F)$. Notons d'abord que $\tilde{H} = G$: en effet, H est d'indice fini dans $G(F)$ qui est dense dans G, et G est connexe.

Cela entraîne que $Z(H) \subseteq Z(G)$: en effet, le centralisateur de $Z(H)$ dans G est fermé pour la topologie de Zariski et contient H, ce qui montre que $Z(H)$ est centralisé par G tout entier.

Il nous faut maintenant montrer que $H/Z(H)$ est simple. Il est clair que H n'a aucun sous-groupe propre d'indice fini. Soit N un sous-groupe normal de H; si N est fini, alors $C_H(N)$ est d'indice fini dans H, et donc $N \subseteq Z(H)$.

Nous pouvons donc supposer que N est infini. Soit $g \in N$, $g \notin Z(G)$, et considérons les ensembles $X = \{[h,g] \mid h \in G(F)\}$ et $Y = \{[h,g] \mid h \in H\}$. Comme H est dense dans G, nous avons $\tilde{X} = \tilde{Y} = \{[h,g] \mid h \in G\}$, et $\tilde{X}$ est une variété. Cela montre aussi que $dim(X) = dim(Y)$; par (7.7), nous en concluons que le sous-groupe H_0 de H engendré par Y et le sous-groupe H_1 de $G(F)$ engendré par X sont définissables, et que $[H_1 : H_0]$ est fini; comme H_1 est un sous-groupe normal infini de $G(F)$, il contient H, ce qui montre que $H_0 \cap H$ est d'indice fini dans H, et donc que $H_0 = H$.

Nous avons montré que tout sous-groupe normal propre de H est contenu dans $Z(H)$, ce qui implique que $H/Z(H)$ est simple.

La borne sur $[G(F) : H]$ résulte elle aussi de la compacité (en utilisant des ultraproduits).

(7.11) Groupes simplement connexes. Soit G un groupe algébrique connexe, et H un groupe algébrique. On dit que $f : H \to G$ est une **isogénie** si c'est un morphisme surjectif de groupes algébriques dont le noyau est fini. On dit que G est **simplement connexe** si toutes les isogénies $f : H \to G$ sont injectives. Nous allons montrer que si G est presque simple, alors il a une enveloppe simplement connexe. Pour cela nous avons besoin d'un résultat auxiliaire que nous ne montrerons pas. Si on le compare avec (5.17), il n'est pas très surprenant.

Théorème. Soit G un groupe algébrique connexe défini sur un corps pseudo-fini F, et soit H_0 un sous-groupe de $G(F)$ d'indice fini et définissable dans F. Alors il existe un groupe algébrique connexe H et une isogénie $f : H \to G$, définis sur F, et tels que $f(H(F))$ est un sous-groupe de H_0 d'indice fini.

Nous avons donc une correspondance entre les sous-groupes définissables d'indice fini de $G(F)$ et les isogénies $f : H \to G$; remarquons que, par (7.5)(4), f ne peut être un isomorphisme si H_0 est un sous-groupe propre de $G(F)$. Nous allons maintenant utiliser (7.10) pour déduire l'existence d'une enveloppe simplement connexe dans le cas où G est presque simple.

Théorème. Soit G un groupe algébrique presque simple. Soit $\mathcal{H}$ la famille des paires (H, f) où $f : H \to G$ est une isogénie, et H est un groupe algébrique connexe. Alors $\mathcal{H}$ a un élément universel (H, f), c'est à dire que si $(H', f') \in \mathcal{H}$, alors il existe un épimorphisme (définissable, pas nécessairement de groupes algébriques) $h : H \to H'$ satisfaisant $f = f' \circ h$.

Démonstration. Soit K_0 un corps algébriquement clos suffisamment saturé sur lequel G est défini, et soit F un corps pseudo-fini contenant K_0. Soit H_0 le sous-groupe normal infini minimal de $G(F)$; il est donc définissable par (7.10). Soit $(H, f) \in \mathcal{H}$ tel que $f(H(F))$ est un sous-groupe de H_0 d'indice fini; nous avons alors $f(H(F)) = H_0$ par minimalité de H_0. Nous voulons montrer que (H, f) est universel.

Etape 1. Si $(H', f') \in \mathcal{H}$, alors $|\ker f'| \leq |\ker f|$.

En effet, par saturation de K_0 il existe $(H_1, f_1) \in \mathcal{H}$ défini sur K_0, et un isomorphisme $h : H' \to H_1$ tel que $f' = f_1 \circ h$. Nous avons donc $\ker f' \simeq \ker f_1$ et il nous suffit de montrer que $|\ker f_1| \leq |\ker f|$. Comme f_1 et H_1 sont définis sur le corps algébriquement clos K_0, $\ker f_1 \subseteq H_1(K_0) \subseteq H_1(F)$. D'autre part, par (7.5)(4), $|\ker f_1| = [G(F) : f_1(H_1(F))] \leq [G(F) : H_0] = |\ker f|$. Cela montre notre assertion.

Soit $(H', f') \in \mathcal{H}$. Considérons le produit fibré $H \times_G H'$ défini par: $\{(h, h') \in H \times H' \mid f(h) = f'(h')\}$. C'est un sous-groupe algébrique du groupe algébrique $H \times H'$. Soit J la composante connexe de $H \times_G H'$, et $p : J \to H$, $p' : J \to H'$ les morphismes induits par les projections $H \times H' \to H$ et $H \times H' \to H'$. Alors p et p' sont surjectifs (par connexité de H et H'), et $\ker p \subseteq \{e\} \times \ker f'$ et $\ker p' \subseteq \ker f \times \{e\}$.

Par définition de $H \times_G H'$, les applications $f \circ p$ et $f' \circ p'$ sont égales, ont leur noyau contenu dans $(\ker f \times \ker f') \cap J$, et définissent donc une isogénie $\varphi : J \to G$. Par l'étape 1, nous avons $|\ker \varphi| \leq |\ker f|$; comme $\varphi = f \circ p$, $\ker \varphi$ est fini et f est surjective, nous en déduisons que $|\ker p| = 1$, c'est à dire que p est un isomorphisme. Définissons maintenant $h : H \to H'$ par $H = p' \circ p^{-1}$; nous avons alors $f' \circ h = f' \circ p' \circ p^{-1} = f$, ce qui montre que (H, f) est universel.

(7.12) Eléments unipotents et nilpotents dans $M_n(K)$. Soit n un entier et p un nombre premier. Supposons que la caractéristique du corps F est p ou 0. Nous travaillons dans le groupe $GL_n(F)$.

Rappelons qu'une matrice $v \in M_n(F)$ est nilpotente si une puissance de v est égale à 0_n. Un élément $u \in GL_n(F)$ est unipotent si $(u - I_n)$ est nilpotent. Des applications log et exp sont aussi définies pour certaines matrices, voir (2) ci-dessous.

(1) Soit u une matrice unipotente de $GL_n(F)$. Alors $(u - I_n)^n = 0_n$. Si F est de caractéristique $p \geq n$, alors $u^p = I_n$.

(2) Pour u un unipotent de $GL_n(F)$, nous définissons

$$\log(u) = (u - I_n) - (u - I_n)^2/2 + \cdots + (-1)^{n-1}(u - I_n)^{n-1}/(n-1),$$

et pour v un nilpotent de $M_n(F)$, nous définissons

$$\exp(v) = v + v^2/2! + \cdots + v^{n-1}/(n-1)!.$$

L'application log définit une bijection entre l'ensemble des matrices unipotentes de $GL_n(F)$ et celui des matrices nilpotentes de $M_n(F)$. L'inverse de log est donné par exp.

(3) Si u et v sont des matrices unipotentes qui commutent entre elles, alors $\log(uv) = \log(u) + \log(v)$.

(4) Soit $u \in GL_n(F)$ unipotente. Alors l'ensemble $X(u, F) = \{\exp(t \log(u)) \mid t \in F\}$ est un sous-groupe de $GL_n(F)$, qui est isomorphe au groupe additif de F. Si $F = \tilde{F}$, c'est un sous-groupe algébrique connexe de $GL_n(F)$. Si $F = \mathbf{F}_p$, où $p \geq n$, alors c'est le sous-groupe de $GL_n(\mathbf{F}_p)$ engendré par u. De plus, $\{\exp(t \log(u)) \mid t \in \tilde{\mathbf{F}}_p\} \cap GL_n(\mathbf{F}_p) = \langle u \rangle$.

Démonstration. (1) Il suffit de montrer que si $v \in M_n(F)$ est nilpotent, alors $v^n = 0_n$. Supposons que $v^m = 0_n$, et pour $i \leq m$, considérons le sous-espace vectoriel $\ker(v^i)$ de F^n. Nous avons alors $\ker(v^i) \subseteq \ker(v^{i+1})$, et $\ker(v^m) = F^n$. Nous allons montrer que si $\ker(v^i) = \ker(v^{i+1})$, alors $\ker(v^i) = F^n$, ce qui montrera que $v^i = 0_n$. Remarquons que pour $i \geq 1$,

$$\ker(v^i) = \ker(v^{i+1}) \iff \ker(v^i) \cap Im(v) = (0).$$

En effet, si $a \in \ker(v^{i+1}) \setminus \ker(v^i)$, alors $v(a)$ est un élément non nul de $Im(v) \cap \ker(v^i)$; réciproquement, si $b = v(a)$ est un élément non nul de $\ker(v^i)$, alors $a \in \ker(v^{i+1}) \setminus \ker(v^i)$.

Supposons que $\ker(v^i) = \ker(v^{i+1})$; alors $\ker(v^{i+1}) \cap Im(v) = (0)$, ce qui entraîne que $\ker(v^{i+1}) = \ker(v^{i+2})$. Nous en déduisons que $\ker(v^i) = \ker(v^{i+1}) = \ker(v^{i+2}) = \cdots = F^n$. Comme F^n est de dimension n, toute suite strictement croissante de sous-espaces de $F6n$ est de longueur au plus n, et donc $v^n = 0_n$.

En caractéristique $p \geq n$ nous avons $u^p = (u - I_n + I_n)^p = (u - I_n)^p + I_n^p = I_n$.

(2) et (3) sont prouvés à partir de simples calculs.

(4) Il est immédiat que $X(u, F)$ est un sous-groupe: $\exp(t_1 \log(u)) \exp(t_2 \log(u)) = \exp((t_1 + t_2) \log(u))$; $exp(t \log(u))^{-1} = \exp(-t \log(u))$. Il est aussi clair qu'il est isomorphe au groupe additif de F, et ce, de façon définissable.

Nous avons donc un isomorphisme algébrique entre $X(u, \tilde{F})$ et $\tilde{F}$; comme le groupe algébrique $\tilde{F}$ est connexe, $X(u, \tilde{F})$ l'est aussi.

Regardons maintenant ce qui se passe pour $F = \mathbf{F}_p$, où $p \geq n$. Les valeurs de $t \in \mathbf{F}_p$ nous donnent alors les éléments de $\langle u \rangle$. Réciproquement, soit $t \in \tilde{\mathbf{F}}_p$ et supposons que $\exp(t \log(u)) \in GL_n(\mathbf{F}_p)$; cela entraîne que $t \log(u) \in M_n(\mathbf{F}_p)$, et comme d'autre part $\log(u) \in M_n(\mathbf{F}_p)$, nous en déduisons que $t \in \mathbf{F}_p$, ce qui prouve la dernière assertion.

(7.13) Théorème. Soit $n > 1$ un entier. Il existe un entier k tel que tout sous-groupe G de $GL_n(\mathbf{F}_p)$ qui est engendré par des éléments d'ordre p est de la forme $\langle g_1 \rangle \cdots \langle g_k \rangle$ pour des éléments $g_1, \ldots, g_k \in G$ d'ordre p.

Il existe un entier d (qui dépend seulement de n), tel que si G^* est le sous-groupe algébrique de $GL_n(\tilde{\mathbf{F}}_p)$ engendré par les ensembles $\tilde{X}(u) = \{\exp(t \log(u)) \mid t \in \tilde{\mathbf{F}}_p\}$, où u parcourt l'ensemble des éléments de G d'ordre p, alors $[G^*(\mathbf{F}_p) : G] \leq d$. Si $p > d$, alors tous les éléments de $G^*(\mathbf{F}_p)$ d'ordre p sont dans G.

Démonstration. Considérons la formule $\varphi(x, y)$ (x et y sont des éléments du groupe, c'est à dire des uplets du corps) qui exprime: y est un unipotent de $GL_n(F)$ et il existe $t \in F$ tel que $x = \exp(t \log(y))$. C'est une formule dans le langage des corps, sans paramètres. Si b est un unipotent de $GL_n(F)$, alors $\varphi(x, b)$ définit un sous-groupe de $GL_n(F)$ dont la clôture de Zariski est irréductible.

Supposons qu'il n'existe pas de tel k. Nous pouvons donc trouver une suite croissante $p(i)$, $i \in \mathbf{N}$, de nombres premiers, et pour chaque i, un ensemble A_i d'éléments de $GL_n(\mathbf{F}_{p(i)})$ d'ordre $p(i)$, tel que le sous-groupe G_i de $GL_n(\mathbf{F}_{p(i)})$ engendré par A_i, ne peut être écrit comme produit $\langle a_1 \rangle \cdots \langle a_i \rangle$ pour des éléments $a_1, \ldots, a_i \in G_i$ qui sont d'ordre $p(i)$.

Soit M_i la structure $(\mathbf{F}_{p(i)}, +, \cdot, A_i)$, et soit $M = (F, +, \cdot, A)$ un ultraproduit non-principal des M_i. Alors F est un corps pseudo-fini de caractéristique 0, et A est un ensemble d'éléments unipotents de $GL_n(F)$.

Pour $a \in A$, soit $X(a)$ le sous-groupe de $GL_n(F)$ défini par la formule $\varphi(x, a)$; c'est donc un sous-groupe, dont la clôture de Zariski est le groupe algébrique connexe $\{\exp(t \log(a)) \mid t \in \tilde{F}\}$. Par (7.7), le sous-groupe engendré par les $X(a)$, $a \in A$, est définissable, et contenu dans un produit de la forme $X(a_1) \cdots X(a_r)$ pour certains $a_1, \ldots, a_r \in A$.

Il existe une formule $\psi(x_1, \ldots, x_r)$ satisfaite par $a_1, \ldots, a_r$ dans M et exprimant que $X(a_1) \cdots X(a_r)$ est un sous-groupe de $GL_n(F)$ contenant A; donc, il existe un ensemble infini J d'entiers i tels que les uplets $(a_1(i), \ldots, a_r(i))$ satisfont ψ. Ce qui veut dire: $X(a_1(i)) \cdots X(a_r(i))$ est un sous-groupe de $GL_n(\mathbf{F}_{p(i)})$ contenant A_i. Cela contredit notre hypothèse, et montre l'existence d'une borne k.

Par (7.7), $[G^*(\mathbf{F}_p) : G]$ est fini; par compacité, il est donc borné. Appelons d cette borne.

Supposons $p > d$, et soit $a \in G^*(\mathbf{F}_p)$ un élément d'ordre p. Si B est le groupe engendré par a, il est d'ordre p, et son intersection avec G est d'ordre p ou 1. Si $B \cap G = (1)$, alors les cosets bG pour $b \in B$ sont tous distincts, ce qui contredit $[G^*(\mathbf{F}_p) : G] \leq d < p$. Nous en concluons que $B \subseteq G$, ce qui finit la démonstration du théorème.

8. Réduction mod p; sous-groupes Zariski denses

Soit G un groupe algébrique défini sur $\mathbf{Q}$; il peut donc être défini par des équations dont les coefficients sont dans $\mathbf{Z}$; en passant à $\mathbf{Z}/p\mathbf{Z}$, nous obtenons alors un objet G_p défini sur $\mathbf{Z}/p\mathbf{Z}$, dont une interprétation est: $G \ mod \ p$. Nous allons ci-dessous généraliser tout cela et montrer formellement quelques résultats.

(8.1) Théorème. Soit R un anneau intègre, finiment engendré en tant qu'anneau. Si R est un corps, alors R est fini. Si R est infini et a est un élément non nul de R, alors il existe une infinité d'idéaux maximaux de R qui ne contiennent pas a.

Démonstration. La preuve est par induction sur le nombre de générateurs de R. Il suffit de prouver la deuxième assertion, car elle entraîne la première. Pour $R = \mathbf{Z}$ ou $R = \mathbf{F}_p$, le résultat est immédiat. Supposons le résultat vrai pour le sous-anneau S de R, et supposons que $R = S[t]$. Il y a deux cas à considérer:

Cas 1: t ne satisfait aucune équation à coefficients dans S.

Alors $S[t]$ est un anneau de polynômes sur S. Supposons d'abord que S est fini. Comme il est intègre, c'est donc un corps. Si $a(t)$ est un élément non-nul de R, il existe une infinité de polynômes irréductibles dans R qui sont relativement premiers avec $a(t)$; de tels polynômes engendrent des idéaux maximaux ne contenant pas $a(t)$.

Supposons maintenant que S est infini, et soit $a(t) \neq 0$ un élément de R. Comme S est infini, il contient une infinité d'éléments c tels que $a(c) \neq 0$. Pour chaque $c \in S$ tel que $a(c) \neq 0$, si P est un idéal maximal de S ne contenant pas $a(c)$ (il en existe par hypothèse d'induction), alors $(P, t - c)$ est un idéal maximal de R ne contenant pas a.

Cas 2: t est algébrique sur S.

Si S est fini, alors $S[t]$ est un corps fini. Nous pouvons donc supposer que S est infini. Soit a un élément non nul de R, et $f(X) \in S[X]$ un polynôme ayant a comme racine et de degré minimal. Alors le coefficient constant b de $f(X)$ est non nul puisque $a \neq 0$. Soit P un idéal maximal de S ne contenant pas b, et P' un idéal maximal de R contenant P. Comme S/P est un corps, $P' \cap S = P$. Comme $b \notin P'$, $f(a) - b = -b \notin P'$, ce qui entraîne que $a \notin P'$ (puisque X divise $f(X) - b$, et donc a divise $-b$). Par hypothèse d'induction, il existe une infinité d'idéaux maximaux de S ne contenant pas b, et donc une infinité d'idéaux maximaux de R ne contenant pas a.

(8.2) Soit R un anneau intègre, engendré par $a_1, \ldots, a_n$. Soit $X = \mathcal{M}ax(R)$ l'ensemble des idéaux maximaux de R. Nous définissons une topologie sur X de la façon suivante: les ouverts de bases sont les ouverts $\mathcal{O}_a = \{P \in X \mid a \notin P\}$ pour $a \in R$.

Proposition. Soit R un anneau intègre infini, engendré par $a_1, \ldots, a_n$.

(1) Si P est un idéal maximal, alors R/P est un corps fini.
(2) Soit $m \in \mathbf{N}$. L'ensemble $\{P \in X \mid |R/P| \leq m\}$ est fini.
(3) Si $a, b \in R$ alors $\mathcal{O}_a \cap \mathcal{O}_b = \mathcal{O}_{ab}$. Donc une intersection finie d'ouverts de base est un ouvert de base. L'espace X est compact, et tout singleton est fermé.
(4) Soit $a \in R$, $a \neq 0$. Alors $\mathcal{O}_a$ est infini.

Démonstration. (1) Le quotient R/P est un corps, et il est engendré par $a_1/P, \ldots, a_n/P$; par (8.1) il doit être fini.

(2) Pour $P, P' \in X$, nous avons: $P = P'$ si et seulement si les n-uplets $(a_1/P, \dots, a_n/P)$ et $(a_1/P', \dots, a_n/P')$ satisfont les mêmes équations à coefficients dans $\mathbf{Z}$. Donc, $P = P'$ si et seulement si les structures $(R/P, +, \cdot, a_1/P, \dots, a_n/P)$ et $(R/P', +, \cdot, a_1/P', \dots, a_n/P')$ sont isomorphes. Mais il n'y a qu'un nombre fini de classes d'isomorphisme de corps $(\mathbf{F}_q, +, \cdot, c_1, \dots, c_n)$ avec $q \leq m$, et nous en déduisons le résultat.

(3) Un idéal maximal est en particulier premier, et nous avons donc: $ab \notin P \iff a \notin P$ et $b \notin P$.

Soit $P \in X$; pour chaque $P \neq Q \in X$, nous pouvons trouver $b_Q \in Q \setminus P$ (comme Q est maximal, $Q \not\subseteq P$). Nous avons alors $\{P\} = \bigcap_{Q \in X,\, Q \neq P} \mathcal{O}_{b_Q}$.

Soit maintenant $U_i, i \in I$, une famille d'ouverts de X telle que $\bigcup_i U_i = X$. Par la première partie, tout ouvert est une réunion d'ouverts de base, et donc nous pouvons supposer que chaque U_i est de la forme $\mathcal{O}_{a_i}$ pour un élément $a_i \in R$. En passant au complémentaire, le fait que $X = \bigcup_i U_i$ est alors équivalent à: aucun élément de X ne contient tous les éléments $a_i, i \in I$, c'est à dire: l'idéal engendré par $\{a_i \mid i \in I\}$ est R tout entier.

Il existe donc $b_1, \dots, b_m \in R$, et $i(1), \dots, i(m) \in I$ tels que $1 = a_{i(1)}b_1 + \cdots + a_{i(m)}b_m$. Nous avons alors: $X = \mathcal{O}_{a_{i(1)}} \cup \cdots \cup \mathcal{O}_{a_{i(m)}}$.

(4) Soit $a \neq 0$. Nous allons d'abord montrer que $\mathcal{O}_a$ est non vide. Soit $R' = R[1/a]$; c'est un anneau intègre, finiment engendré. Prenons P' un idéal maximal de R' et posons $P = P' \cap R$. Comme R' est finiment engendré, R'/P' est un corps fini. D'autre part, $P \cap R$ est un idéal premier, et le morphisme $R \to R' \to R'/P'$ induit une inclusion $(R/P) \subseteq (R'/P')$; (R/P) est un sous-anneau d'un corps fini, c'est donc un corps, ce qui montre que $P \in X$. Comme $a \notin P'$, nous avons $P \in \mathcal{O}_a$.

Nous savons que R est infini, et que si $b \neq 0$, alors $\emptyset \neq \mathcal{O}_{ab} \subseteq \mathcal{O}_a$. De cela on déduit facilement que $\mathcal{O}_a$ est infini.

(8.3) Soit maintenant W un ensemble algébrique défini sur le corps des fractions de R. Il peut donc être défini par des équations à coefficients dans R. Pour P un idéal de R, nous considérons alors l'ensemble algébrique W_P défini sur (R/P) par $I(W) \cap R[\bar{X}] + P$.

Soit G un groupe algébrique défini sur le corps des quotients de R; on peut considérer le graphe de la multiplication, M, comme un sous-ensemble algébrique de G^3. Pour P un idéal de R, nous regardons alors la structure (G_P, M_P), où M_P est le graphe d'une relation ternaire. Nous désignerons aussi cette structure par G_P.

Proposition. Soit R un anneau intègre infini, engendré par $a_1, \dots, a_n$, et soit G un groupe algébrique connexe défini sur le corps des quotients de R. Il existe $a \in R$, $a \neq 0$, tel que pour tout $P \in \mathcal{O}_a$:
(1) G_P est un groupe algébrique connexe.
(2) Si de plus G est presque simple, alors G_P est presque simple.
(3) Supposons G presque simple. Il existe d (qui dépend seulement de G) tel que tous les sous-groupes normaux de $G_P(R/P)$ sont soit finis de taille plus petite que d et centraux, ou bien d'indice $\leq d$.

Démonstration. Soit (b_n), $n \in \mathbf{N}$, une énumération des éléments non nuls de R. Les trois résultats sont prouvés par contradiction, en utilisant des ultraproduits. Le résultat central à toutes les démonstrations est le suivant:

Assertion. Soit $P(m)$, $m \in \mathbf{N}$, une suite d'idéaux maximaux de R satisfaisant $b_1 \cdots b_m \notin P(m)$ pour tout $m \in \mathbf{N}$, et soit $\mathcal{U}$ un ultrafiltre non principal sur $\mathbf{N}$. Alors l'homomorphisme $R \to \prod_{m \in \mathbf{N}}(R/P(m)) \to \prod_{m \in \mathbf{N}}(R/P(m))/\mathcal{U}$ (induit par les applications naturelles $R \to R/P(m)$), est un plongement.

En effet, pour chaque élément non nul b de R, l'ensemble $\{m \in \mathbf{N} \mid b \notin P(m)\}$ est cofini, et donc appartient à $\mathcal{U}$.

Fixons un ultrafiltre non-principal $\mathcal{U}$ sur $\mathbf{N}$.

(1) Supposons que la conclusion est fausse. Soient $f_1(\bar{X}, \bar{T}), \ldots, f_m(\bar{X}, \bar{T})$, $g_1(\bar{X}, \bar{Y}, \bar{T}), \ldots, g_r(\bar{X}, \bar{Y}, \bar{T})$ des polynômes à coefficients dans $\mathbf{Z}$ tels que les équations $f_1(\bar{x}, \bar{a}) = \cdots = f_m(\bar{x}, \bar{a}) = 0$ définissent G, les équations $g_1(\bar{x}, \bar{y}, \bar{a}) = \cdots = g_r(\bar{x}, \bar{y}, \bar{a}) = 0$ définissent M ($\bar{a} = (a_1, \ldots, a_n)$). Il existe alors une formule sans quantificateurs $\varphi(\bar{z})$ qui définit dans tout corps K les n-uplets $\bar{c}$ satisfaisant:

(a) L'ensemble algébrique W défini par les équations $f_1(\bar{x}, \bar{c}) = \cdots = f_m(\bar{x}, \bar{c}) = 0$ est une variété.

(b) L'ensemble algébrique défini par les équations $g_1(\bar{x}, \bar{y}, \bar{c}) = \cdots = g_r(\bar{x}, \bar{y}, \bar{c}) = 0$ définit une loi de groupe sur W.

Puisqu'il n'existe pas de a satisfaisant la conclusion de (1), pour tout $m \in \mathbf{N}$, nous pouvons trouver $P(m) \in \mathcal{O}_{b_1 \cdots b_m}$ tel que $G_{P(m)}$ n'est pas un groupe algébrique connexe. Nous avons donc $R/P(m) \models \neg\varphi(a_1/P(m), \ldots, a_n/P(m))$.

Soit $F = \prod_{m \in \mathbf{N}}(R/P(m))/\mathcal{U}$. D'après l'assertion, nous pouvons identifier R avec un sous-anneau de F, et donc $F \models \varphi(a_1, \ldots, a_n)$ (φ est sans quantificateurs). Par notre choix des $P(m)$ nous avons $(R/P(m)) \models \neg\varphi(a_1/P(m), \ldots, a_n/P(m))$, ce qui contredit le théorème de Łos.

(2) Soit $b \in R$ satisfaisant la conclusion de (1). Supposons qu'il n'existe pas de a satisfaisant la conclusion de (2). Alors, pour tout $m \in \mathbf{N}$ nous pouvons trouver $P(m) \in \mathcal{O}_{bb_1 \cdots b_m}$ tel que $G_{P(m)}$ n'est pas simple; c'est à dire qu'il existe un corps algébriquement clos K_m contenant $R/P(m)$ et un sous-groupe normal propre infini H_m de $G_{P(m)}(K_m)$.

Considérons les structures $B_m = (R/P(m), K_m, H_m)$, et soit $B = \prod_{m \in \mathbf{N}} B_m/\mathcal{U}$. Alors $B = (F, K, H)$ où F est un corps pseudo-fini contenant R, K est un corps algébriquement clos contenant F, et H est un sous-groupe normal propre infini de $G(K)$. Mais par (7.5), si $g \in H \setminus Z(G)$, H contient le sous-groupe algébrique engendré par la variété $\{[h, g] \mid h \in G(K)\}$, ce qui contredit la presque simplicité de G.

(3) Soit maintenant b satisfaisant la conclusion de (1) et (2). En appliquant le théorème (7.10), soit $d \in \mathbf{N}$ tel que si F est un corps pseudo-fini contenant R, alors tout sous-groupe normal de $G(F)$ d'indice supérieur à d est central dans G, et de taille inférieure à d (on prend $d \geq |Z(G)|$).

Supposons qu'il n'existe pas d'élément a satisfaisant la conclusion de (3). Pour tout $m \in \mathbf{N}$ nous pouvons donc trouver $P(m) \in \mathcal{O}_{bb_1 \cdots b_m}$, et un sous-groupe normal H_m de $G_{P(m)}(R/P(m))$ d'indice plus grand que d, et qui est soit de taille plus grande que d, soit non-central.

Considérons les structures $C_m = (R/P(m), H_m)$ et soit $C = \prod_{m \in \mathbf{N}} C_m/\mathcal{U}$. Alors $C = (F, H)$, où F est un corps pseudo-fini contenant R, et H est un sous-groupe normal de $G(F)$ d'indice plus grand que d. Par notre choix de d, H est central de taille inférieure à d. Cela contredit le choix des H_m et le théorème de Łos.

Remarque. Quand l'anneau R est $\mathbf{Z}$ ou bien une extension algébrique finie de $\mathbf{Z}$, les ouverts $\mathcal{O}_a$ sont en fait cofinis pour $a \neq 0$. Donc "pour tout $P \in \mathcal{O}_a$" devient: "en dehors d'un ensemble fini S d'idéaux maximaux", ou de façon équivalente, "pour presque tout P".

(8.4) Théorème. Soit G un sous-groupe algébrique de GL_n défini sur $\mathbf{Q}$, presque simple et simplement connexe. Soit Γ un sous-groupe de $G(\mathbf{Q})$ qui est finiment engendré, et dense (au sens de la topologie de Zariski) dans G.

Pour p un nombre premier, soit $\mathbf{Z}_{(p)}$ le sous-anneau de $\mathbf{Q}$ des fractions dont le dénominateur n'est pas divisible par p. L'homomorphisme de réduction modulo p: $\mathbf{Z} \to \mathbf{F}_p$ se prolonge naturellement en un homomorphisme $\pi_p : \mathbf{Z}_{(p)} \to \mathbf{F}_p$.

Alors, pour presque tout nombre premier p, $\pi_p(\Gamma) = G_p(\mathbf{F}_p)$.

Démonstration. Soient $a_1, \ldots, a_r$ des générateurs de Γ. Soit m un entier tel que G et sa loi de groupe sont définis sur $\mathbf{Z}[1/m]$, et $a_1, \ldots, a_r, a_1^{-1}, \ldots, a_r^{-1} \in G(\mathbf{Z}[1/m])$. Alors $\Gamma \subseteq G(\mathbf{Z}[1/m])$. Donc si p ne divise pas m, alors $\pi_p(\Gamma)$ est bien défini.

Soit S un ensemble fini de nombres premiers contenant les diviseurs de m, et tel que pour $p \notin S$, G_p est un groupe algébrique presque simple (voir (8.3)).

Supposons que le résultat est faux. Nous pouvons donc trouver une suite infinie (croissante) de nombres premiers $p(i) \notin S$, $i \in \mathbf{N}$, telle que pour $i \in \mathbf{N}$, $\Gamma_i = \pi_{p(i)}(\Gamma)$ est un sous-groupe propre de $G_i = G_{p(i)}(\mathbf{F}_{p(i)})$.

Considérons les structures $M_i = (\mathbf{F}_{p(i)}, +, \cdot, \Gamma_i, \pi_{p(i)}(a_1), \ldots, \pi_{p(i)}(a_r))$; alors, les éléments $\pi_{p(i)}(a_1), \ldots, \pi_{p(i)}(a_r)$ engendrent Γ_i.

Soit $M = (F, +, \cdot, \Gamma', a'_1, \ldots, a'_r)$ un ultraproduit non principal des structures M_i. Alors F est un corps pseudo-fini de caractéristique 0, et l'inclusion $\mathbf{Z}[1/m] \subseteq F$ ainsi que la définition des éléments $\pi_{p(i)}(a_j)$ montrent que $(a'_1, \ldots, a'_r) = (a_1, \ldots, a_r)$. Le groupe Γ' est donc un sous-groupe propre de $G(F)$ qui contient Γ; c'est donc un sous-groupe dense de G.

Etape 1. Γ' contient un élément unipotent.

Ici, nous avons besoin d'un résultat d'algèbre:

Résultat. Soit n un entier fixé. Il existe un entier d tel que si G est un sous-groupe de $GL_n(\mathbf{F}_q)$ pour une puissance première q et G ne contient pas d'élément unipotent, alors G a un sous-groupe abélien d'indice au plus d.

Si Γ' ne contient pas d'élément unipotent, alors la plupart des Γ_i non plus; ils ont donc un sous-groupe abélien H_i d'indice au plus d; l'ultraproduit des H_i est alors un sous-groupe abélien H de Γ' d'indice fini, et comme G est connexe et Γ' est dense dans G, cela montre que $\tilde{H} = G$ est abélien, ce qui est absurde.

Etape 2. Soit $u \in \Gamma'$ un unipotent, et $U = \{\exp(t \log u) \mid t \in F\}$. Alors U est un sous-groupe de Γ'.

En effet, écrivons $u = (u_i)_{i \in \mathbf{N}}$ où $u_i \in \Gamma_i$; alors pour presque tout i (au sens de l'ultrafiltre), u_i est unipotent, et donc le sous-groupe engendré par u_i est précisément le groupe $\{\exp(t \log u_i) \mid t \in \mathbf{F}_{p(i)}\}$. Cela prouve l'assertion.

Donc U est un sous-groupe définissable de Γ', et $\tilde{U}$ est une variété. Par (7.7), le sous-groupe H de Γ' engendré par $\{U^g \mid g \in \Gamma'\}$ est définissable ($U^g = g^{-1}Ug$). Soit N son normalisateur dans $G(F)$: $N = \{g \in G(F) \mid H^g = H\}$; c'est un sous-groupe définissable de $G(F)$ qui contient Γ', puisque H est normal dans Γ'. De cela on déduit que N est Zariski dense dans G, et donc que $dim(N) = dim(G) = dim(G(F))$; par (7.5)(3), N est un sous-groupe d'indice fini de $G(F)$. Mais comme G est simplement connexe, nous savons que $G(F)$ n'a pas de sous-groupe définissable d'indice fini. Donc $N = G(F)$, et H est un sous-groupe normal infini de $G(F)$ contenu dans Γ'. Cela contredit (7.10).

(8.5) Réduction mod p d'anneaux intègres finiment engendrés.

Soit R un anneau intègre finiment engendré de caractéristique 0, L son corps des fractions, et $K_0 = \tilde{\mathbf{Q}} \cap L$. Alors le corps des fractions de $R_0 = K_0 \cap R$ est K_0. Ecrivons R comme $R_0[\bar{c}]$, et soit V la variété définie sur K_0 dont $\bar{c}$ est un point générique.

En raisonnant de la même façon que dans (8.3) (voir aussi la démonstration du (2) de la proposition ci-dessous), on montre que pour presque tout idéal maximal P de R_0, l'ensemble algébrique défini en réduisant les équations définissant V modulo P, est une variété V_P définie sur le corps fini $K_P = R_0/P$. L'homomorphisme $R_0 \to K_P$ s'étend alors en un homomorphisme $\pi_P : R \to K_P[\bar{c}_P] = R_P$, où $\bar{c}_P$ est un point générique de V_P. Soit $L_P = K_P(V_P)$.

Lemme 1. Soit R_1 un sous-anneau finiment engendré de $\tilde{\mathbf{Q}}$ contenant R_0. Alors presque tout idéal maximal de R_0 s'étend en un idéal maximal de R_1.

Démonstration. Soit R_2 l'anneau engendré par les images de R_1 par les automorphismes de $\tilde{\mathbf{Q}}$. Alors R_2 est finiment engendré car R_1 n'a qu'un nombre fini de conjugués. Il suffit de montrer l'assertion pour R_2: si l'idéal engendré par P dans R_1 contient 1, il en est de même dans R_2.

Soit P un idéal maximal de R_0, et supposons que l'idéal qu'il engendre dans R_2 contient 1. Alors la même chose est vraie de tous les conjugués de P au-dessus de $\mathbf{Q}$, c'est à dire de tous les idéaux premiers de R_0 contenant $P \cap \mathbf{Z}$ (car ils sont tous maximaux et tous conjugués). Donc, si p est le nombre premier engendrant $P \cap \mathbf{Z}$, alors p n'est contenu dans aucun idéal de R_2, ce qui implique que p est inversible dans R_2. Comme R_2 est finiment engendré, il n'y a qu'un nombre fini de nombres premiers inversibles dans R_2, et donc un nombre fini d'idéaux premiers de R_0 qui deviennent impropres dans R_1.

Lemme 2. Soit $\varphi(\bar{x}, \bar{y})$ une formule sans quantificateurs, et soit $\bar{a}$ un uplet de R_0, et supposons que $R \models \varphi(\bar{a}, \bar{c})$. Alors pour presque tout P, $L_P \models \varphi(\pi_P(\bar{a}), \pi_P(\bar{c}))$.

Démonstration. Il suffit de le montrer quand φ est atomique ou une négation d'atomique. Si φ est atomique, c'est clair puisque π_P est un homomorphisme d'anneau. Supposons donc que $\varphi(\bar{x}, \bar{y})$ est de la forme $g(\bar{x}, \bar{y}) \neq 0$, où g est un polynôme à coefficients entiers. En agrandissant $\bar{a}$, nous pouvons supposer que $\mathbf{Z}[\bar{a}] = R_0$.

Puisque $g(\bar{a}, \bar{c}) \neq 0$, $g(\bar{a}, \bar{X}) \notin I(V)$. Soient $f_1(\bar{Y}, \bar{X}), \ldots, f_r(\bar{Y}, \bar{X})$ des polynômes à coefficients entiers tels que $f_1(\bar{a}, \bar{X}), \ldots, f_r(\bar{a}, \bar{X})$ engendrent $I(V) \cap R_0[\bar{X}]$. Par les résultats du chapître 4, il existe une formule sans quantificateurs $\psi(\bar{y})$ satisfaite par $\bar{a}$ dans R_0, et telle que si F est un corps algébriquement clos et $\bar{b}$ est un uplet de F, alors $F \models \psi(\bar{b})$ si et seulement si l'idéal de $F[\bar{X}]$ engendré par $f_1(\bar{b}, \bar{X}), \ldots, f_r(\bar{b}, \bar{X})$ est un idéal premier, qui ne contient pas $g(\bar{b}, \bar{X})$.

Nous avons donc réduit le problème à l'assertion suivante:

Si $\psi(\bar{y})$ est une formule sans quantificateurs satisfaite par $\bar{a}$ dans R_0, alors pour presque tout P, $K_P \models \psi(\pi_P(\bar{a}))$.

Il suffit de le montrer pour ψ atomique ou négation d'atomique; le cas atomique est clair puisque π_P est un homomorphisme; le cas où ψ est une négation d'atomique découle de la remarque à la fin de (8.3).

Proposition. Soit $f(T) \in R[T]$ un polynôme n'ayant pas de racine dans $\tilde{\mathbf{Q}}L$. Soit $g(T) \in R[T]$ tel que, si α est une racine de $f(T)$, alors $g(\alpha) \notin \tilde{\mathbf{Q}}L$.

(1) Pour presque tout P, le polynôme $\pi_P(f)(T)$ n'a pas de racine dans L_P, et si α_P est une racine de $\pi_P(f)(T)$, alors $\pi_P(g)(\alpha_P) \notin L_P$.

(2) Supposons que $f(T)$ est irréductible et $L(\alpha)$ est une extension régulière de $\mathbf{Q}$ pour α une racine de $f(T)$. Pour P un idéal maximal de R_0, soit α_P une racine de $\pi_P(f)(T)$. Alors, pour presque tout P, $\pi_P(f)(T)$ est irréductible au-dessus de L_P, $[L_P(\alpha_P) : L_P] = [L(\alpha) : L]$, et $[L_P(g(\alpha_P)) : L_P] = [L(g(\alpha)) : L]$.

Démonstration. (2) Ecrivons $f(T) = F(\bar{c}, T)$ (F à coefficients entiers) et soit $h(\bar{c})$ le coefficient du terme de plus haut degré en T de $f(T)$. L'idéal de $\tilde{\mathbf{Q}}[\bar{X}, T]$ engendré par $I(V)$ et $F(\bar{X}, T)$ est l'idéal d'une variété W. Donc, pour presque tout idéal maximal P de R_0, l'ensemble algébrique défini par $I(V_P)$ et $\pi_P(F)(\bar{X}, T)$ est une variété W_P, et $\pi_P(h)(\bar{X}) \notin I(W_P)$. Soit α_P tel que $(\bar{c}_P, \alpha_P)$ est un point générique de W_P. Alors $\pi_P(f)(\alpha_P) = 0$, et le polynôme $\pi_P(f)(T)$ est irréductible, de même degré en T que $f(T)$. On obtient donc $[L_P(\alpha_P) : L_P] = [L(\alpha) : L]$.

Pour la deuxième assertion, on applique la première partie à un polynôme irréductible $h(T) \in R[T]$ dont $g(\alpha)$ est une racine.

(1) Soit M le corps de décomposition de $f(T)$, et $K_1 = M \cap \tilde{\mathbf{Q}}$; soit R_1 un anneau finiment engendré contenant R_0 et dont le corps des fractions est K_1. Alors le corps des fractions de $R_1R = R_1[\bar{c}]$ est $L_1 = K_1(\bar{c})$. Soient $g_1(T), \ldots, g_s(T) \in R_1[\bar{c}, T]$ des polynômes irréductibles et $r \in R_1[\bar{c}]$ tels que $g_1(T) \cdots g_s(T) = rf(T)$. Par hypothèse, le degré des $g_i(T)$ est plus grand que 1.

Par (2) et le lemme 2, pour presque tout idéal maximal P' de R_1, $\pi_{P'}(r) \neq 0$, et pour $i = 1, \ldots, s$, le polynôme $\pi_{P'}(g_i)(T)$ est irréductible au-dessus de $(R_1/P')(\bar{c}_P)$, de degré égal à celui de $g_i(T)$ (et donc supérieur à 1). Comme $\pi_{P'}(g_1)(T) \cdots \pi_{P'}(g_s)(T) = \pi_{P'}(r)\pi_{P'}(f)(T)$, les racines de $\pi_{P'}(f)(T)$ ne sont pas dans $(R_1/P')(\bar{c}_P)$, et si $\alpha_{P'}$ est une racine de $\pi_{P'}(f)(T)$, alors $\pi_{P'}(g)(\alpha_{P'}) \notin (R_1/P')(\bar{c}_P)$.

En utilisant le lemme 1, on en déduit le résultat souhaité.

(8.6) Réduction mod p de variétés abéliennes.

Rappelons d'abord la définition de l'espace projectif de dimension n. Soit K un grand corps algébriquement clos, et considérons l'ensemble S des $(n+1)$-uplets $(x_0, \ldots, x_n)$, avec $(x_0, \ldots, x_n) \neq (0, \ldots, 0)$. Nous définissons une relation d'équivalence $\sim$ sur S en posant $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ s'il existe $a \neq 0$ tel que $(x_0, \ldots, x_n) = (ay_0, \ldots, ay_n)$. Nous définissons alors $\mathbf{P}^n(K)$ comme étant l'ensemble $S/\sim$ des classes d'équivalence de $\sim$ dans S. Il est clair d'après sa définition que $\mathbf{P}^n(K)$ est interprétable dans K. Les éléments de $\mathbf{P}^n(K)$ sont notés $(x_0 : \cdots : x_n)$.

Un sous-ensemble algébrique de $\mathbf{P}^n(K)$ est défini comme étant l'ensemble des zéros de polynômes homogènes de $K[X_0, \ldots, X_n]$ (ou plutôt son image dans $S/\sim$). Comme dans le cas affine, une variété projective est un ensemble algébrique irréductible (au sens de la topologie de Zariski induite sur $\mathbf{P}^n(K)$). Une variété abélienne est une variété projective munie d'une loi binaire définie par des fonctions rationnelles en $(X_0, \dots, X_n)$ qui en font un groupe. On peut montrer que la loi de groupe d'une variété abélienne est commutative. On note sa loi de groupe additivement.

Nous gardons les notations introduites dans (8.5): R est un anneau intègre finiment engendré, $R_0 = \tilde{\mathbf{Q}} \cap R$, L est le corps des fractions de R et K_0 celui de R_0; $R = R_0[\bar{c}]$, et V est la variété dont $\bar{c}$ est un point générique. Pour P un idéal maximal de R_0, nous avons l'application $\pi_P : R \to K_P(\bar{c}_P)$, où $\bar{c}_P$ est un point générique de l'ensemble algébrique V_P.

Soit A une variété abélienne définie sur L. Les équations la définissant peuvent donc être prises dans R, et en appliquant π_P, nous obtenons un sous-ensemble algébrique projectif A_P défini sur R_P, avec un sous-ensemble algébrique $M_P \subseteq A_P^3$, image par π_P du graphe M de l'addition de A. En raisonnant de la même façon que dans (8.3), on montre que pour presque tout idéal maximal P de R_0, (A_P, M_P) est une variété abélienne, définie sur L_P.

Remarquons maintenant que tout point de $A(L)$ peut s'écrire $(x_0 : \cdots : x_n)$ avec $x_0, \dots, x_n \in R$. L'application π_P induit donc une application $A(L) \to A_P(L_P)$, qui est un morphisme de groupe pour presque tout P.

Théorème. Avec les notations ci-dessus, supposons que $A(\tilde{\mathbf{Q}}L)$ est finiment engendré. Alors pour presque tout idéal maximal P de R_0, π_P est injective sur $A(L)$.

Démonstration. La preuve se décompose en plusieurs étapes.

Etape 1. Nous pouvons supposer que $A(L) = A(\tilde{\mathbf{Q}}L)$.

Comme $A(\tilde{\mathbf{Q}}L)$ est finiment engendré, il est contenu dans $A(K_1L)$ pour une extension finie K_1 de K_0. Par le lemme 1, nous pouvons remplacer K_0 par K_1, R_0 par un anneau finiment engendré dont le corps des fractions est K_1, L par LK_1, etc ....

Ecrivons $A(L) = A_{tor}(L) \oplus \Gamma$, où $A_{tor}(L)$ est un groupe fini, et Γ est un groupe sans torsion (et donc isomorphe à une somme de copies de $\mathbf{Z}$).

Etape 2. Pour presque tout P, π_P est injective sur le sous-groupe de torsion de $A(L)$.

Le sous-groupe de torsion de $A(L)$ est fini. On applique le lemme 2 à la formule sans quantificateurs exprimant que les points de ce sous-groupe sont distincts.

Fixons un nombre premier ℓ tel que $A(\tilde{\mathbf{Q}}L)$ n'ait pas de point d'ordre ℓ.

Etape 3. Pour presque tout P, $A_P(L_P)$ n'a pas de point d'ordre ℓ.

Soit D l'ensemble des points de A d'ordre exactement ℓ; pour chaque point d de D, nous fixons un $(n+1)$-uplet le représentant et ayant une coordonnée égale à 1. Soit M l'extension Galoisienne de L obtenue en rajoutant ces représentants. Alors toute extension de L contenant tous les points d'ordre ℓ de A contient M. Soit α tel que $M = L(\alpha)$, et choisissons le de telle façon que tous les uplets représentant les éléments de D soient dans $R[\alpha]$. Pour tout $\bar{a} = (a_0 : \cdots : a_n) \in D$, il existe des polynômes $g_{\bar{a},i}(T) \in R[T]$, $i = 0, \dots, n$, tels que $a_i = g_{\bar{a},i}(\alpha)$, et un indice $i(a)$ tel que $a_{i(a)} \notin \tilde{\mathbf{Q}}L$. Nous pouvons alors appliquer la Proposition (8.5)(1) à un polynôme irréductible $f(T) \in R[T]$ dont α est une racine, et aux polynômes $g_{\bar{a},i(\bar{a})}(T)$, $\bar{a} \in D$, $i = 0, \dots, n$.

Donc pour presque tout P: si α_P est une racine de $\pi_P(f)(T)$, et $\bar{a} \in D$ alors le point $\bar{a}_P = \big(\pi_P(g_{\bar{a},0})(\alpha_P) : \cdots : \pi_P(g_{\bar{a},n})(\alpha_P)\big)$ est un point de A_P d'ordre ℓ, l'une de ses coordonnées est égale à 1, et une autre n'est pas dans L_P.

D'autre part, en utilisant l'étape 2 pour une extension finiment engendrée de R_0 dont le corps des quotients est $M \cap \tilde{\mathbf{Q}}$, on déduit que (gardant les notations introduites ci-dessus): pour presque tout P, l'application $\bar{a} \mapsto \bar{a}_P$ est injective sur D.

Comme A et A_P ont $\ell^{2dim(A)}$ points d'ordre ℓ si $\ell \notin P$, tous les points d'ordre ℓ de A_P sont de la forme $\bar{a}_P$, et donc ne sont pas dans $A_P(L_P)$.

Etape 3. Pour presque tout P, $\pi_P(\ell\Gamma) = \pi_P(\Gamma) \cap \ell A_P(L_P)$, et π_P induit une injection $\Gamma/\ell\Gamma \to A_P(L_P)/\ell A_P(L_P)$.

Soit $\Gamma' = \{\bar{a} \in A(\tilde{L}) \mid \ell\bar{a} \in \Gamma\}$. Comme Γ est finiment engendré, et A n'a qu'un nombre fini d'éléments d'ordre ℓ, $[\Gamma' : \Gamma]$ est fini. Soit T un sous-ensemble de Γ' représentant les cosets de Γ dans Γ' et contenant 0_A (l'élément identité de A). Pour chaque $\bar{b} \in T$ choisissons un $(n+1)$-uplet $(b_0, \cdots, b_n)$ avec l'une des coordonnées égale à 1, et tel que $\bar{b} = (b_0 : \cdots : b_n)$. Alors l'extension M obtenue en adjoignant à L les uplets $(b_0, \cdots, b_n)$ pour $\bar{b} \in T$, est une extension Galoisienne finie de L. De plus pour $\bar{b} \neq \bar{d} \in T$, nous avons $\bar{b} - \bar{d} \notin A(L)$.

Soit $\alpha \in M$ tel que $M = L(\alpha)$ et les uplets représentant les éléments de T sont dans $L[\alpha]$; soit $f(T) \in R[T]$ un polynôme irréductible dont α est une racine. On raisonne comme dans l'étape 2, et on obtient:

Pour presque tout P, si α_P est une racine de $\pi_P(f)(T)$, et π'_P est l'extension de π_P qui envoie α sur α_P, et $\bar{b} \neq \bar{d} \in T$ alors $\pi'_P(\bar{b} - \bar{d}) \notin A_P(L_P)$.

Nous avons donc montré que pour presque tout P: $[\Gamma' : \Gamma] = [\pi'_P(\Gamma')A_P(L_P) : A_P(L_P)]$. Comme Γ' contient tous les éléments d'ordre ℓ de $A(L)$, pour presque tout P $\pi'_P(\Gamma')$ contient tous les éléments d'ordre ℓ de $A_P(L_P)$, et donc π'_P induit un isomorphisme entre le sous-groupe des éléments d'ordre ℓ de $A(\tilde{L})$ et celui de $A_P(\tilde{L}_P)$.

Soit $\bar{a} \in \Gamma$ et supposons qu'il n'est pas divisible par ℓ dans Γ; soit $\bar{b} \in \Gamma'$ tel que $\ell\bar{b} = \bar{a}$. Alors les solutions de l'équation $\ell\bar{x} = \bar{a}$ sont obtenues en ajoutant à $\bar{b}$ les éléments d'ordre ℓ de $A(M)$. De même, les solutions de l'équation $\ell\bar{x} = \pi_P(\bar{a})$ sont obtenues en rajoutant à $\pi'_P(\bar{b})$ les éléments d'ordre ℓ de $A_P(L(\alpha_P))$. Les solutions de $\ell\bar{x} = \bar{a}$ sont donc congrues modulo Γ à des éléments non nuls de T, ce qui entraîne que leurs images par π'_P sont congrues modulo $A_P(L_P)$ à des éléments non nuls de $\pi'_P(T)$, ce qui montre que l'équation $\ell\bar{x} = \pi_P(\bar{a})$ n'a pas de solution dans $A_P(L_P)$.

La dernière assertion est évidente.

Etape 4. Pour presque tout P, π_P est injective sur $A(L)$.

Par l'étape 2, il suffit de le montrer pour le groupe libre Γ. L'application $\pi_P : \Gamma \to A_P(L_P)$ induit donc une injection $\Gamma/\ell\Gamma \to A_P(L_P)/\ell A_P(L_P)$. Nous avons maintenant besoin d'un lemme:

Lemme. Soient B et C des groupes abéliens, tels que B est libre et C n'a pas de ℓ-torsion. Soit $f : B \to C$ un morphisme de groupe, et supposons que l'application induite par f: $B/\ell B \to C/\ell C$ est injective. Alors f est injective.

En effet, soit $a \in B$, $a \neq 0$. Comme B est libre, il existe un entier k tel que $a \in \ell^k B$, $a \notin \ell^{k+1}B$. Soit $b \in B$ tel que $\ell^k b = a$; alors $b \notin \ell B$, et donc $f(b) \neq 0$. Comme C n'a pas de ℓ-torsion, $f(a) = \ell^k f(b) \neq 0$.

Cela termine la preuve du théorème, en utilisant les étapes 2 et 3.

Remarques. (1) Par un résultat de Mordell-Weil-Néron, l'hypothèse que $A(\tilde{\mathbf{Q}}L)$ est finiment engendrée est vérifiée si A n'a pas de sous-groupe algébrique isogène à une variété définie sur $\tilde{\mathbf{Q}}$.

(2) Ce résultat est utilisé par Hrushovski, pour montrer comment obtenir la validité de la conjecture de Lang pour les corps de fonctions en caractéristique 0, à partir de de la validité de celle en caractéristique $p > 0$.

La conjecture de Lang pour les corps de fonctions a été prouvée par Manin en caractéristique 0, et par Hrushovski en caractéristique $p > 0$ (en 1993-94). Voici un énoncé du résultat:

Soit K un corps finiment engendré (comme corps) au dessus de la clôture algébrique k du corps premier. Soit A une variété abélienne définie sur K, V une sous-variété de A et Γ un sous-groupe finiment engendré de A. Supposons que $V \cap \Gamma$ est dense dans V.

Alors il existe une variété abélienne A_0 définie sur k, une sous-variété V_0 de A_0 aussi définie sur k, et un homomorphisme rationnel surjectif h d'un sous-groupe (algébrique) de A sur A_0, et $a \in A$ satisfaisant $V = a + h^{-1}(V_0)$.

Bibliographie.

[A] J. Ax, The elementary theory of finite fields, Annals of Math. 88 (1968), 239 – 271.

[CK] C.C. Chang, H.J. Keisler, Model theory, North-Holland, Amsterdam 1977.

[CDM] Z. Chatzidakis, L. van den Dries, A. Macintyre, Definable sets over finite fields, J. reine u. ang. Math. 427 (1992), 107 – 135.

[vdD] L. van den Dries, A remark on Ax's theorem on solvability modulo primes, Math. Z. 208, 65-70 (1991).

[vdDS] L. van den Dries, K. Schmidt, Bounds in the theory of polynomials rings over fields. A non-standard approach. Invent. Math. 76 (1984), 77 – 91.

[H] E. Hrushovski, Proof of Manin's theorem by reduction to positive characteristic, manuscrit 1996 (à paraître dans les proceedings de la conférence de Manchester 1994).

[HP1] E. Hrushovski, A. Pillay, Groups definable in local fields and pseudo-finite fields, Israel J. of Math. 85 (1994), 203 –262.

[HP2] E. Hrushovski, A. Pillay, Definable subgroups of algebraic groups over finite fields, J. reine angew. Math. 462 (1995), 69 –91.

[L1] S. Lang, Introduction to algebraic geometry, Addison-Wesley Pub. Co., Menlo Park 1973.

[L2] S. Lang, Algebra, Addison-Wesley Pub. Co., Menlo Park 1984.

[LW] S. Lang, A. Weil, Number of points of varieties in finite fields, Am. J. of Math. 76 (1954), 819 –827.

Cours de théorie des modèles des corps finis et pseudo-finis — Exercices (à rendre le 12/03/96)

Exercice 1. Soit V un fermé de Zariski défini sur F et F-irréductible. Nous allons montrer que $F(V)$ et F^{1/p^∞} sont linéairement disjoints au-dessus de F.

(a) Soit $a \in F$ tel que $a^{1/p} \notin F$. Montrer que si $F(a^{1/p})$ et $F(V)$ ne sont pas linéairement disjoints au-dessus de F, alors $a^{1/p} \in F(V)$.

(b) Il existe donc des polynômes $g(\bar{X}), h(\bar{X}) \in F[\bar{X}]$ tels que $(*)$ $g(\bar{X}) - a^{1/p}h(\bar{X}) \in I(V)$. Nous utilisons les notations de (2.4). En se servant du fait que B est une base pour le F-espace vectoriel $F[V]$ et pour le K-espace vectoriel $K[V]$, dériver de $(*)$ la nullité d'une certaine combinaison linéaire d'éléments de B. En déduire une contradiction.

(c) Nous avons donc montré: si $a \in F \setminus F^p$, alors $F(V)$ et $F(a^{1/p})$ sont linéairement disjoints au-dessus de F. Nous remplaçons F par $F_1 = F(a^{1/p})$, sur lequel V et aussi définie, et obtenons: si $b \in F_1 \setminus F_1^p$ alors $F_1(b^{1/p})$ et $F_1(V)$ sont linéairement disjoints au-dessus de F_1.

Cela entraîne que $F(a^{1/p}, b^{1/p})$ et $F(V)$ sont linéairement disjoints au-dessus de F: on utilise (2.8)(3), et le fait que $F(V) \bigotimes_F F(a^{1/p}, b^{1/p})$ est canoniquement isomorphe à $(F(V) \bigotimes_F F_1) \bigotimes_{F_1} F_1(b^{1/p})$. Procédant de proche en proche, on montre donc que $F(V)$ et F^{1/p^∞} sont linéairement disjoints au-dessus de F.

Exercice 2. Soit V une variété, définie sur F^{1/p^∞}.

(a) Montrer que l'idéal $I(V) \cap F[\bar{X}]$ est premier.

(b) Soit $F[V] = F[\bar{X}]/(I(V) \cap F[\bar{X}])$, et $F(V)$ son corps de fractions. En se servant du résultat de l'exercice 1, montrer que V est définie sur F si et seulement si $F(V)$ et F^{1/p^∞} sont linéairement disjoints au-dessus de F.

Exercice 3. Soit $(G_i)_{i\in I}$ une famille de groupes finis, et soit G un sous-groupe fermé de $\prod_{i\in I} G_i$, où chaque G_i est muni de la topologie discrète, et $\prod_{i\in I} G_i$ de la topologie produit. Rappelons que les ouverts de base de $\prod_{i\in I} G_i$ sont de la forme $\prod_{i\in I} U_i$, où chaque U_i est un ouvert de G_i, et l'ensemble des i tels que $U_i \neq G_i$ est fini. Les ouverts sont alors des réunions (arbitraires) d'intersections finies d'ouverts de base.

Le groupe G avec la topologie induite est donc un groupe profini. Supposons que pour tout $j \in I$ la projection naturelle $\pi_j : G \to G_j$ (induite par la projection $\prod_{i\in I} G_i \to G_j$) est surjective.

(1) Soit H un sous-groupe ouvert de G. Montrer qu'il existe un sous-ensemble fini I_0 de I tel que H contient

$$U(I_0) = \{g \in G \mid \pi_i(g) = 1 \text{ pour tout } i \in I_0\}.$$

(2) Montrer que tout ouvert est une réunion de cosets de sous-groupes ouverts de la forme $U(I_0)$.

(3) Montrer qu'un sous-ensemble X de G est dense dans G si et seulement si pour tout sous-ensemble fini I_0 de I, on a $XU(I_0) = G$.

(4) Soit K un corps, et $G = \mathcal{G}al(K_s/K)$ son groupe de Galois, et considérons le comme un sous-groupe de $\prod \mathcal{G}al(L/K)$, où L parcourt l'ensemble des extensions de Galois finies de K.

Soit H un sous-groupe de G, M le sous-corps de $\tilde{K}$ fixé par H, et $H_1 = \{g \in G \mid \forall a \in M\ g(a) = a\}$. Montrer que H_1 est la clôture topologique de H dans G (on sait qu'il est fermé; il faut donc montrer que H est dense dans H).

Examen du cours: Théorie des modèles des corps finis et pseudo-finis, DEA de Logique et Fondements de l'informatique, 09 Mai 1996.

Tous les problèmes sont indépendants. A l'intérieur d'un même problème, vous pouvez supposer les résultats antérieurs, ie se servir de la conclusion de (a) pour montrer (b). Une grande importance sera attachée à la rédaction: il faudra se réfèrer de façon précise aux résultats utilisés.

Problème 1. (a) Soient X et Y des espaces topologiques, et supposons que nous avons sur $X \times Y$ une topologie satisfaisant aux deux conditions suivantes:

(i) Si U et V sont des fermés de X et Y alors $U \times V$ est un fermé de $X \times Y$.

(ii) Si W est un fermé de $X \times Y$ et $(a, b) \in X \times Y$ alors $\{c \in Y \mid (a, c) \in W\}$ est fermé dans Y, et $\{c \in X \mid (c, b) \in W\}$ est fermé dans X.

Montrer que si U et V sont des fermés irréductibles de X et Y respectivement, alors le fermé $U \times V$ est irréductible dans $X \times Y$. (Procéder de la manière suivante: soient F_1 et F_2 deux fermés de $X \times Y$ dont la réunion est $U \times V$; on considère les ensembles $A_i = \{x \in U \mid \{x\} \times V \subseteq F_i\}$, et l'on montre que A_1 et A_2 sont des fermés, dont la réunion est U.)

On peut montrer que la topologie de Zariski dont les fermés sont les ensembles algébriques définis sur un corps algébriquement clos fixé K vérifie ces deux propriétés. Cependant cela est faux si l'on ne considère que les fermés définis sur un corps non algébriquement clos.

(b)(ne pas y passer trop de temps) Soit F un corps parfait non algébriquement clos. Donner un exemple de deux ensembles algébriques F-irréductibles définis sur F, dont le produit n'est pas F-irréductible (on peut imposer à ces ensembles d'être finis).

Problème 2. (a) Rappelons qu'un sous-ensemble X du groupe profini G est dense si pour tout sous-groupe ouvert N de G, $XN = G$. Montrer que si G est un groupe profini dont toutes les images continues finies peuvent être engendrées par e éléments, alors il existe un sous-groupe G_0 de G, engendré par e éléments, et dense dans G.

(b) Soit G le groupe profini $(\mathbf{Z}/2\mathbf{Z})^I$. Trouver une condition sur I pour que G soit finiment engendré en tant que groupe topologique (c'est à dire, ait un sous-groupe G_0 finiment engendré et dense).

(c) Même question pour $G = \hat{\mathbf{Z}}^I$.

Problème 3. Soit F un corps parfait, $S \subseteq F^n$ un ensemble définissable dans F. On considère la clôture de Zariski $\tilde{S}$ de S dans $\tilde{F}^n$.

(a) Montrer que si V est une composante irréductible de $\tilde{S}$, alors $V \cap S$ est dense dans V.

(b)(ne pas y passer trop de temps) Montrer que les composantes irréductibles de $\tilde{S}$ sont définies sur F.

(c)(Facile) Soit V une composante irréductible de $\tilde{S}$. Montrer que si F est ω-saturé, alors S contient un point générique de V (par générique, je veux dire générique sur le corps de définition F_0 de V).

Problème 4. (a) Soit $f(T)$ un polynôme à coefficients entiers. Montrer que les conditions suivantes sont équivalentes:

(i) Il existe une infinité de nombres premiers p tels que $\mathbf{F}_p \models \forall x \; f(x) \neq 0$.

(ii) Soit $M \subseteq \tilde{\mathbf{Q}}$ le corps de décomposition de $f(T)$. Il existe un sous-corps E de M ne contenant aucune racine de $f(T)$, et tel que $\mathcal{G}al(M/E)$ est cyclique.

(b) Ces deux conditions sont-elles équivalentes à: il existe une infinité de corps finis $\mathbf{F}_q$ satisfaisant $\forall x \; f(x) \neq 0$.

(c) Trouver une condition sur $f(T)$ qui implique: pour presque tout nombre premier p, $\mathbf{F}_p \models \forall x \; f(x) \neq 0$. Est-ce une condition intéréssante?

Problème 5. Montrer le résultat suivant: soit n un entier. Alors n est un carré si et seulement si son image dans chacun des corps $\mathbf{F}_p$ est un carré.

Ce résultat se généralise-t-il aux puissances ℓ-ièmes, ℓ un nombre premier: un entier n est une puissance ℓ-ième si et seulement si son image dans chacun des corps $\mathbf{F}_p$ est une puissance ℓ-ième.

Problème 6. Montrer que si G est un groupe presque connexe et simplement connexe, et si F est un corps pseudo-fini sur lequel G est défini, alors $G(F)$ est simple.

Problème 7. Soit K un corps algébriquement clos, et S un sous-ensemble de $GL_n(K)$. Supposons que S contient tous les génériques de $\tilde{S}$, que $S = S^{-1}$, et que si a, b sont deux génériques indépendants de S alors $ab \in S$. Montrer que $\tilde{S}$ est un sous-groupe de $GL_n(K)$.