Cours de DEA : Théorie des Modèles, les outils classiques
(Année 00 - 01)

1. Conventions et notation

Je précise la terminologie que j'utiliserai (je crois qu'elle est un peu différente de celle du cours fondamental).

(1.1) Soit $\mathcal{L}$ un langage, et T une théorie, c'est à dire un ensemble d'énoncés du langage $\mathcal{L}$.

Je dirai que T est consistante, si T ne prouve pas $(x \neq x)$. Je dirai que T est satisfaisable, si elle a un modèle M, et qu'elle est finiment satisfaisable si tout fragment fini de T a un modèle. Nous avons les équivalences suivantes:
T est consistante si et seulement si elle est satisfaisable, si et seulement si elle est finiment satisfaisable.

La notation $\varphi(v_1, \dots, v_n)$ indique que les variables libres de φ sont parmi $v_1, \dots, v_n$. Il arrive cependant parfois qu'on omette les variables complètement.

Si M et N sont des $\mathcal{L}$-structures, la notation $M \subseteq N$ indiquera (sauf mention explicite du contraire) que M est une sous-($\mathcal{L}$)-structure de N.

(1.2) **Diagrammes**. Soient $M \models T$, et $A \subseteq M$. Je dénote par $\mathcal{L}(A)$ le langage obtenu en ajoutant à $\mathcal{L}$ des symboles de constantes pour tous les éléments de A. On notera c_a la constante correspondant à l'élément a. Pour simplifier la notation, quand aucune confusion n'est possible, on utilisera a au lieu de c_a, pour $a \in A$. La $\mathcal{L}$-structure M a une expansion naturelle au langage $\mathcal{L}(A)$ (et c'est celle que nous utiliserons sauf mention du contraire): on interprète la constante c_a par a.

Le **diagramme simple de** A (dans M), ou bien le **diagramme sans quantificaeurs de** A, noté $\Delta(A)$, est l'ensemble des énoncés sans quantificateurs de $\mathcal{L}(A)$ satisfaits par la $\mathcal{L}(A)$-structure $(M, c_a)_{a\in A}$. Le **diagramme atomique de** A, noté $\Delta^+(A)$, est l'ensemble des énoncés atomiques de $\mathcal{L}(A)$ satisfaits par la $\mathcal{L}(A)$-structure $(M, c_a)_{a\in A}$. Le **diagramme complet de** A dans M, noté $Diag(A)$ (ou bien $Diag_M(A)$), est l'ensemble des énoncés de $\mathcal{L}(A)$ satisfaits par la $\mathcal{L}(A)$-structure $(M, c_a)_{a\in A}$.

(1.3) **Morphismes**. Soient M et N des $\mathcal{L}$-structures, $F : M \to N$ une application.

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

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

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

$$M \models R(\bar{a}) \iff N \models R(F(\bar{a})).$$

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

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

$$M \models \varphi(\bar{a}) \iff N \models \varphi(F(\bar{a})).$$

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

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

Ou tout simplement: si g induit un isomorphisme entre les $\mathcal{L}$-structures engendrées par A et B. On parle aussi d'**isomorphisme élémentaire partiel**, quand l'application g préserve toutes les formules, c'est à dire, pour toute formule $\varphi(\bar{x})$ et uplet $\bar{a}$ dans le domaine de g, on a

$$M \models \varphi(\bar{a}) \iff N \models \varphi(g(\bar{a})).$$

(1.4) **Remarques**. (1) Nous savons que si N est une $\mathcal{L}(A)$-structure satisfaisant $\Delta(A)$, alors il existe un isomorphisme partiel de M dans N, qui envoie les éléments de A sur l'interprétation dans N de la constante qui leur est associée. De même, si N est un modèle de $Diag(M)$, alors N contient une sous-structure élémentaire M' qui est isomorphe à M.

(2) Soient M et N des $\mathcal{L}$-structures, $F : M \to N$ une application, et A un sous-ensemble de M. Nous avons vu plus haut que M a une expansion naturelle au langage $\mathcal{L}(A)$. La fonction F nous permet de définir aussi une $\mathcal{L}(A)$-structure sur N, de la façon suivante: la constante c_a est interprétée par $F(a)$ dans N.

Les propriétés suivantes sont alors immédiates:

(1) F est un morphisme si et seulement si $N \models \Delta^+(M)$.
(2) F est un plongement si et seulement si $N \models \Delta(M)$.
(3) F est un plongement élémentaire si et seulement si $N \models Diag(M)$.
(4) Soit $F : A \to B$ une fonction. Alors F définit un isomorphisme partiel de M si et seulement si $N \models \Delta(A)$.
(5) Soit $F : A \to B$ une fonction. Alors F définit un isomorphisme élémentaire partiel de M si et seulement si $N \models Diag(A)$.

On peut se demander quelle est la signification de "isomorphisme partiel" de domaine vide. En effet, la fonction de domaine vide est certainement une fonction partielle. Si l'on regarde la définition, il reste cependant quelques formules à considérer: celles où aucune variable libre n'est présente, c'est à dire les énoncés sans quantificateurs. Quand il n'y a pas de symboles de constantes dans le langage, il n'y a pas d'énoncés sans quantificateurs. Cependant, dès qu'il y a des constantes, nous pouvons dire des choses du genre $c \neq d$. Pour que F soit un isomorphisme partiel, il faudra donc en particulier, que si les constantes c et d ont des interprétations distinctes dans la structure M, elles ont aussi des interprétations distinctes dans la structure N.

Donc, si F est de domaine vide, alors

- F est un isomorphisme partiel si et seulement si $\Delta_M(\emptyset) = \Delta_N(\emptyset)$,
- F est un isomorphisme partiel élémentaire si et seulement si $M \equiv N$.

2. Elimination des quantificateurs, théories modèles compètes

Dans cette section nous étudions certaines propriétés agréables de théories. Nous commencerons avec un théorème de compacité qui nous sera bien utile:

(2.1) **Théorème**. Soient T_1 et T_2 des théories du langage $\mathcal{L}$, et Δ un ensemble d'énoncés de $\mathcal{L}$ qui est clos par disjonction finie. Supposons que $T_1 \cup T_2$ est consistante. 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 M et N de T_1, si $M \models T_2$ et N satisfait tous les énoncés de Δ satisfaits par M, alors $N \models T_2$.

Démonstration. Il est clair que (1) implique (2). Supposons maintenant (2), et soit

$$\Gamma = \{\psi \in \Delta \mid T_1 \cup T_2 \models \psi\}.$$

Nous allons montrer que Γ est l'ensemble d'énoncés recherché. Certainement $T_1 \cup T_2 \vdash \Gamma$, et nous allons montrer que tout modèle de $T_1 \cup \Gamma$ est modèle de T_2. Soit $N \models T_1 \cup \Gamma$, et soit

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

Nous allons montrer que $T_1 \cup T_2 \cup \Sigma$ est consistante. Sinon, par compacité, il existe des énoncés $\psi_1, \dots, \psi_n \in \Delta$ telles que $\neg\psi_1, \dots, \neg\psi_n \in \Sigma$ et $T_1 \cup T_2 \vdash \neg(\neg\psi_1 \wedge \dots \wedge \neg\psi_n)$, c'est à dire, $T_1 \cup T_2 \vdash \psi_1 \vee \dots \vee \psi_n$. Mais $\psi_1 \vee \dots \vee \psi_n \in \Delta$, et donc $\psi_1 \vee \dots \vee \psi_n \in \Gamma$. Nous ne pouvons donc avoir $\neg\psi_1, \dots, \neg\psi_n \in \Sigma$, par définition de Σ et parce que $N \models \Gamma$.

Soit M un modèle de $T_1 \cup T_2 \cup \Sigma$. Alors tout énoncé de Δ satisfait par M est satisfait par N (à cause de Σ). Notre hypothèse entraine donc que $N \models T_2$, et donc, comme N était un modèle arbitraire de $T_1 \cup \Gamma$, que $T_1 \cup \Gamma \vdash T_2$.

Remarque. Si T_2 est finiment axiomatisée, alors on peut prendre Γ fini (par compacité).

(2.2) **Corollaire**. Soit T une théorie, $\varphi(\bar{v})$, $\bar{v} = (v_1, \dots, v_n)$, une formule telle que $T \cup \exists\bar{v}\ \varphi(\bar{v})$ est consistante. Soit Δ une ensemble de formules dans les variables $\bar{v}$, clos par disjonction. Les conditions suivantes sont équivalentes:
(1) Il existe des formules $\psi_1(\bar{v}), \dots, \psi_m(\bar{v}) \in \Delta$ telles que

$$T \vdash \forall\bar{v}\, [\varphi(\bar{v}) \leftrightarrow (\psi_1(\bar{v}) \wedge \dots \wedge \psi_m(\bar{v}))].$$

(2) Pour tous modèles M et N de T, pour tous n-uplets $\bar{a}$ et $\bar{b}$ de M et N respectivement, si $M \models \varphi(\bar{a})$, et toute formule $\psi(\bar{v}) \in \Delta$ qui est satisfaite par $\bar{a}$ dans M est satisfaite par $\bar{b}$ dans N, alors $N \models \varphi(\bar{b})$.
(3) Pour tout modèle M de T et uplet $\bar{a} \in M$ satisfaisant φ, il existe une formule $\psi(\bar{v})$ satisfaite par $\bar{a}$, qui est une conjonction finie de formules de Δ, et est telle que $T \vdash \forall\bar{v}\, (\psi(\bar{v}) \rightarrow \varphi(\bar{v}))$.

Démonstration. (1) implique (2), (2) implique (3) sont clairs. Pour (2) implique (1), on agrandit le langage en ajoutant des nouveaux symboles de constantes $c_1, \ldots, c_n$. Soit $\mathcal{L}'$ le langage $\mathcal{L} \cup \{c_1, \ldots, c_n\}$, et Δ' l'ensemble $\{\psi(\bar{c}) \mid \psi(\bar{v}) \in \Delta\}$. Alors l'énoncé de (2) est équivalent à :

(2') Pour toutes $\mathcal{L}'$-structures M et N qui sont modèles de T, si $M \models \varphi(\bar{c})$ et si N satisfait tous les énoncés de Δ' satisfaits par M, alors $N \models \varphi(\bar{c})$.

Par (2.1), on a donc qu'il existe $\psi_1(\bar{c}), \ldots, \psi_m(\bar{c}) \in \Delta'$ tels que

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

Comme les constantes $c_1, \ldots, c_n$ ne sont pas dans le langage $\mathcal{L}$, nous avons donc

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

Nous allons maintenant montrer que (3) implique (1) (ce qui aurait d'ailleurs suffi). Soit $\Delta_\wedge$ l'ensemble des conjonctions finies de formules de Δ, et soit Σ l'ensemble des formules des formules $\psi(\bar{v})$ de $\Delta_\wedge$ telles que $T \cup \exists \bar{v}\, \psi(\bar{v})$ est consistante, et $T \vdash \forall \bar{v}\, (\psi(\bar{v}) \to \varphi(\bar{v}))$.

Assertion. $T \models (\bigvee_{\psi \in \Sigma} \psi(\bar{v}) \leftrightarrow \varphi(\bar{v}))$.

Un petit mot d'explication : la disjonction $\bigvee_{\psi \in \Sigma} \psi(\bar{v})$ est une disjonction infinie. La notion de satisfaction s'étend sans problème aux disjonctions (ou conjonctions) infinies : si M est une $\mathcal{L}$-structure et $\bar{a}$ un n-uplet de M, alors $M \models \bigvee_{\psi \in \Sigma} \psi(\bar{a})$ si et seulement si il existe $\psi(\bar{v}) \in \Sigma$ telle que $M \models \psi(\bar{a})$. (Et pareillement pour les conjonctions infinies). Notre assertion dit donc :

Pour tout modèle M de T et uplet $\bar{a}$ de M, le uplet $\bar{a}$ satisfait $\varphi(\bar{v})$ si et seulement si il satisfait l'une des formules $\psi(\bar{v}) \in \Sigma$.

Donc, revenons à notre assertion. Par définition de Σ, il est clair que si M est un modèle de T et $\bar{a}$ est un n-uplet de M, alors $M \models \bigvee_{\psi \in \Sigma} \psi(\bar{a})$ implique que $M \models \varphi(\bar{a})$. Nous avons donc

$$T \models \forall \bar{v}\, (\bigvee_{\psi \in \Sigma} \psi(\bar{v}) \to \varphi(\bar{v})).$$

Soient maintenant M un modèle de T et $\bar{a}$ un uplet de M satisfaisant $\varphi(\bar{v})$. Par hypothèse, il existe $\theta(\bar{v}) \in \Sigma$ satisfaite par $\bar{a}$. Et donc, nous avons bien que $M \models \bigvee_{\psi \in \Sigma} \psi(\bar{a})$. Cela prouve l'assertion.

Notre assertion dit que la théorie suivante est inconsistante :

$$T \cup \{\varphi(\bar{v})\} \cup \{\neg\psi(\bar{v}) \mid \psi(\bar{v}) \in \Sigma\}.$$

(En effet, sinon nous aurions un uplet $\bar{a}$ dans un modèle M de T satisfaisant $\varphi(\bar{v})$ et ne satisfaisant aucune des formules $\psi(\bar{v})$, $\psi \in \Sigma$, ce qui contredirait notre assertion.) Donc, il existe $\psi_1(\bar{v}), \ldots, \psi_m(\bar{v}) \in \Sigma$ telles que $T \cup \{\varphi(\bar{v})\} \vdash \neg(\neg\psi_1(\bar{v}) \wedge \cdots \wedge \psi_m(\bar{v}))$, c'est à dire $T \vdash \varphi(\bar{v}) \to (\psi(\bar{v}) \vee \cdots \vee \psi_m(\bar{v}))$, et donc

$$T \vdash \forall \bar{v}\, [\varphi(\bar{v}) \to (\psi_1(\bar{v}) \vee \cdots \vee \psi_m(\bar{v}))].$$

Comme chaque formule de Σ implique $\varphi(\bar{v})$ modulo T, cela montre (1) (une disjonction finie de formules de $\Delta_\wedge$ est une conjonction finie de formules de Δ).

(2.3) Rappelons aussi le critère de Tarski-Vaught pour les sous-tructures élémentaires:

Théorème. Soient $M \subseteq N$ des $\mathcal{L}$-structures. Pour montrer que $M \prec N$ il suffit de montrer que pour toute formule $\varphi(x, \bar{y})$, et uplet $\bar{a}$ de M, il existe un élément $b \in M$ tel que

$$N \models \exists x\, \varphi(x, \bar{a}) \iff N \models \varphi(b, \bar{a}).$$

Remarquons que les deux notions de satisfaction sont dans la grande structure N, ce que nous imposons c'est de trouver l'élément b dans la petite structure M.

(2.4) **Corollaire**.

(1) Si $M_1 \prec M_2$ et $M_2 \prec M_3$ alors $M_1 \prec M_3$.

(2) Si $M_1 \prec M_3$, $M_2 \prec M_3$ et $M_1 \subseteq M_2$ alors $M_1 \prec M_2$.

(3) Soient α un ordinal limite, et $(M_i)_{i\in\alpha}$ une chaîne croissante de structures, telle que $M_i \prec M_j$ pour tout $i < j < \alpha$, et soit $M = \bigcup_{i\in\alpha} M_i$. Alors $M_i \prec M$ pour tout $i < \alpha$.

Démonstration. Les démonstrations sont faciles, en utilisant le critère de Tarski-Vaught (2.3). Nous allons donner celle de (3). La preuve est par induction sur la complexité des formules. L'hypothèse d'induction est la suivante, pour une formule $\varphi(\bar{x})$, $\bar{x}$ un uplet de variables:

$(*)$ Pour tous i et uplet $\bar{a}$ dans M_i,

$$M_i \models \varphi(\bar{a}) \iff M \models \varphi(\bar{a}).$$

Les formules sans quantificateurs satisfont $(*)$. Supposons que $\varphi(\bar{x}) = \exists y\, \psi(\bar{x}, y)$ et soient $i < \alpha$, $\bar{a}$ un uplet de M_i.

Supposons d'abord que $M_i \models \varphi(\bar{a})$, et soit $b \in M_i$ tel que $M_i \models \psi(\bar{a}, b)$. Par hypothèse d'induction, nous avons $M \models \psi(\bar{a}, b)$ et donc $M \models \varphi(\bar{a})$.

Supposons maintenant que $M \models \varphi(\bar{a})$, et soit $b \in M$ tel que $M \models \psi(\bar{a}, b)$. Alors il existe $j \geq i$ tel que $b \in M_j$. Par hypothèse d'induction (appliquée à ψ et M_j) nous avons que $M_j \models \psi(\bar{a}, b)$, et donc $M_j \models \varphi(\bar{a})$. Mais $M_i \prec M_j$, et cela entraîne que $M_i \models \varphi(\bar{a})$.

Nous avons donc prouvé que $\varphi(\bar{x})$ satisfait $(*)$, ce qui termine la démonstration. En effet, si maintenant $\varphi(\bar{x}) = \forall y\, \psi(\bar{x}, y)$, nous avons, par l'étape précédente que, pour tous i et $\bar{a}$ uplet de M_i:

$$M_i \models \neg\varphi(\bar{a}) \iff M \models \neg\varphi(\bar{a}),$$

ce qui nous donne $(*)$ pour φ en passant à la contraposée.

(2.5) **Définitions**. Soit T une théorie du premier ordre.

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

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

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

(2.6) **Lemme/Remarque**. Si T élimine les quantificateurs, alors T est modèle-complète.

Démonstration. Soient $M \subseteq N$ des modèles de T. Soient $\varphi(\bar{v})$ une formule, et $\bar{a}$ un uplet de M. Nous voulons montrer que

$$M \models \varphi(\bar{a}) \iff N \models \varphi(\bar{a}).$$

Mais c'est évident : par hypothèse, la fromule $\varphi(\bar{v})$ est équivalent modulo T à une formule $\psi(\bar{v})$ sans quantificateurs. Et nous avons certainement (puisque M est une sous-structure de N)

$$M \models \psi(\bar{a}) \iff N \models \psi(\bar{a}).$$

(2.7) **Proposition**. Soit T une théorie.

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

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

(3) Si T est modèle complète, alors la réunion d'une chaîne de modèles de T est un modèle de T. La théorie T a donc une axiomatisation par des formules $\forall\exists$.

(4) T est modèle complète si et seulement si toute formule $\varphi(\bar{v})$ est équivalente modulo T à une formule existentielle.

(4') (Duale) T est modèle complète si et seulement si toute formule $\varphi(\bar{v})$ est équivalente modulo T à une formule universelle.

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

(2) Soient M un modèle de T, A un sous-ensemble de M, et B la sous-structure de M engendrée par A. Alors tout élément de B est de la forme $t(\bar{a})$, où $t(\bar{x})$ est un terme du langage et $\bar{a}$ un uplet de A. Il s'ensuit que pour tous uplet $\bar{b}$ de B, et formule $\theta(\bar{y})$, si $\bar{t}(\bar{x})$ est un uplet de termes et $\bar{a}$ est uplet d'éléments de A tels que $\bar{b} - \bar{t}(\bar{a})$, alors nous avons, pour $\bar{c}$ et $\bar{d}$ les uplets de constantes correspondant à $\bar{a}$ et $\bar{b}$:

$$T \cup \Delta(B) \vdash \theta(\bar{d}) \iff T \cup \Delta(A) \vdash \theta(\bar{t}(\bar{c})),$$

puisque la formule $\bar{d} = \bar{t}(\bar{c})$ appartient à $\Delta(B)$. Cela entraîne équivalence des deux dernières conditions de (2).

Soit A une sous-ensemble d'un modèle M de T, et $\varphi(\bar{v})$ une formule de $\mathcal{L}$ et $\bar{c} = (c_1, \ldots, c_n)$ un uplet de constantes de $\mathcal{L}(A) \setminus A$. Supposons que T élimine les quantificateurs. Il existe donc une formule sans quantificateurs $\psi(\bar{v})$ qui est équivalente à $\varphi(\bar{v})$ modulo T. Cela entraîne que $T \vdash \varphi(\bar{c}) \leftrightarrow \psi(\bar{c})$. Comme l'une de $\psi(\bar{c})$, $\neg\psi(\bar{c})$ est dans $\Delta(A)$, cela montre que $T \cup \Delta(A)$ prouve l'une de $\varphi(\bar{v})$, $\neg\varphi(\bar{v})$.

Pour l'autre direction, soit $\varphi(\bar{v})$ une formule, et soit Δ l'ensemble des formules sans quantificateurs de $\mathcal{L}$, dont les variables libres sont parmi les éléments de $\bar{v}$. Par (2.2)(3), il suffit de montrer que si M est un modèle de T, et $\bar{a}$ un uplet de M satisfaisant φ, alors il existe une formule sans quantificateurs satisfaite par $\bar{a}$ et impliquant $\varphi(\bar{v})$ modulo T.

Soit $A = \{\bar{a}\}$, et soit $\bar{c}$ le uplet de constantes de $\mathcal{L}(A)$ correspondant à $\bar{a}$. Par hypothèse, $T \cup \Delta(A)$ est complète, et il existe donc une formule $\psi(\bar{v}) \in Delta$, telle que $T \cup \{\psi(\bar{c})\} \vdash \varphi(\bar{c})$. Puisque les éléments de $\bar{c}$ ne sont pas dans $\mathcal{L}$, nous avons donc

$$T \vdash \forall \bar{v}\, (\psi(\bar{v}) \to \varphi(\bar{v})).$$

(3) Soit $M_0 \subset M_1 \subset \cdots$ une chaîne (infinie) de modèles de T. Comme T est modèle-complète, nous avons $M_i \prec M_{i+1}$ pour tout i.

(4) Supposons d'abord que T est modèle-complète, soient Δ l'ensemble des formules existentielles et $\varphi(\bar{v})$ une formule. Nous voulons montrer qu'il existe un élément de Δ qui est équivalent à $\varphi(\bar{v})$ modulo T. Par (2.2)(3), il suffit de montrer que pour tous M modèle de T et uplet $\bar{a}$de M satisfaisant $\varphi(\bar{v})$ il existe une formule de Δ satisfaite par $\bar{a}$ et impliquant $\varphi(\bar{v})$ modulo T. On raisonne comme dans (2), et on obtient des uplets $\bar{c} \subseteq \bar{d}$ de constantes de $\mathcal{L}(M) \setminus \mathcal{L}$, avec $\bar{c}$ interprété par $\bar{a}$, et une formule sans quantificateurs $\theta(\bar{w})$ tels que

$$T \cup \theta(\bar{d}) \vdash \varphi(\bar{c}).$$

Nous avons alors :

$$T \vdash \forall \bar{w}\, [\theta(\bar{w}) \to \varphi(\bar{v})],$$

et si l'on écrit $\bar{w} = (\bar{v}, \bar{u})$, alors

$$T \vdash \forall \bar{v}\, [\exists \bar{u}\, \theta(\bar{v}, \bar{u}) \to \varphi(\bar{v})].$$

La formule $\psi(\bar{v}) = \exists \bar{u}\, \theta(\bar{v}, \bar{u})$ est dans Δ.

L'autre direction est plus facile : soient $M \subseteq N$ des modèles de T, et nous voulons montrer que N est un modèle de $Diag(M)$. Soit $\varphi(\bar{v}) \in \mathcal{L}$, telle que $\varphi(\bar{c}) \in Diag(M)$. Par hypothèse il existe une formule existentielle $\psi(\bar{v})$ qui est équivalent à $\varphi(\bar{v})$ modulo T, Nous avons donc $M \models \psi(\bar{c})$. Comme N contient M et $\psi(\bar{v})$ est existentielle, nous avons $N \models \psi(\bar{c})$, et comme N est un modèle de T, cela entraîne que $N \models \varphi(\bar{c})$.

(2.8) **Remarque**. Une théorie modèle-complète ou ayant l'élimination des quantificateurs n'est pas nécéssairement complète. Par exemple nous prouverons que la théorie des corps algébriquement clos élimine les quantificateurs dans la langage $\{+, -, cdot, 0, 1\}$; cependant, elle n'est pas complète : pour la compléter il faut spécifier la caractéristique du corps. Par exemple l'énoncé $1 + 1 = 0$ implique que la caractéristique est 2.

(2.9) **Remarque 2**. Rappelons que si $M \subseteq N$ sont des $\mathcal{L}$-structures, on dit que M est **existentiellement clos dans** N, noté $M \prec_1 N$, si les $\mathcal{L}(M)$-structures M et N satisfont les mêmes énoncés existentiels de $\mathcal{L}(M)$.

Soit T une théorie (consistante). Pour montrer que T est modèle-complète, il suffit alors de montrer la choses suivante :
Soient $M \subseteq N$ des modèles de$T$. Alors M est existentiellement clos dans N.

La nécéssité de cette condition est claire. Montrons maintenant qu'elle est suffisante. Nous avons besoin d'un sous-lemme :

Sous-lemme. Si $M \prec_1 N$ alors il existe une extension élémentaire M_1 de M qui contient N (comme sous-structure).

Démonstration. Il suffit de montrer que $Diag(M) \cup \Delta(N)$ est consistant. Sinon, il y aurait $\theta(\bar{d}) \in \Delta(N)$ telle que $Diag(M) \vdash \neg\theta(\bar{d})$. Ecrivons $\bar{d} = (\bar{c}_1, \bar{c}_2)$, où les éléments de $\bar{c}_1$ correspondent à des éléments de M, et ceux de $\bar{c}_2$ à des éléments de $N \setminus M$. Nous avons alors

$$Diag(M) \vdash \forall \bar{v}_2 \, \neg\theta(\bar{c}_1, \bar{v}_2)$$
$$N \models\vdash \exists \bar{v}_2 \, \theta(\bar{c}_1, \bar{v}_2).$$

Comme $M \prec_1 N$, nous obtenons une contradiction.

Soient $M \subseteq N$ des modèles de T. Par le sous-lemme, N est contenu dans une extension élémentaire M_1 de M. Par le sous-lemme appliqué maintenant aux modèles $N \subseteq M_1$ de T, il existe une extension élémentaire N_1 de N contenant M_1. Raisonnant ainsi, on construit une chaîne de modèles de T

$$M_0 = M \subseteq N_0 = N \subseteq M_1 \subseteq \cdots \subseteq M_i \subseteq N_i \subseteq N_{i+1} \subseteq \cdots$$

telle que $M_i \prec M_{i+1}$ et $N_i \prec N_{i+1}$ pour tout $i \in \mathbf{N}$. Soit $M_\omega = \bigcup_{i \in \mathbf{N}} M_i = \bigcup_{i \in \mathbf{N}} N_i$. Alors M_ω est une extension élémentaire de chacun des M_i et N_i, et en particulier est une extension élémentaire de M et de N. Comme $M \subseteq N$, on en déduit que $M \prec N$.

(2.10) **Remarque 3**. Rappelons que $T_\forall$ dénote l'ensemble des énoncés universels qui sont conséquence de T, et que tout modèle de $T_\forall$ se plonge dans un modèle de T. Si T est modèle complète, alors les modèles de T sont exactement les modèles de $T_\forall$ qui sont existentiellement clos dans tout modèle de $T_\forall$. En effet, tout modèle de $T_\forall$ se plonge dans un modèle de T.

Cette caractérisation des théories modèles complètes est utile quand on a une théorie universelle T_0, et on veut trouver une théorie modèle-complète la contenant.

(2.11) **Proposition**. Soit T une théorie consistante. Alors T élimine les quantificateurs si et seulement si, pour tous modèles M et N de T contenant A comme sous-structure, et pour toute formule sans quantificateurs $\psi(\bar{x}, y)$ et uplet $\bar{a}$ dans A, nous avons :

$$M \models \exists y \, \psi(\bar{a}, y) \iff N \models \exists y \, \psi(\bar{a}, y).$$

Démonstration. Notre hypothèse dit en fait que si $\psi(\bar{x}, y)$ est de la forme indiquée et $\bar{c}$ est un uplet de constantes de $\mathcal{L}(A) \setminus \mathcal{L}$, alors $T \cup \Delta(A) \vdash \exists y \, \psi(\bar{c}, y)$ ou bien $T \cup \Delta(A) \vdash \forall y \, \neg\psi(\bar{c}, y)$. Ce qui entraîne donc (puisque c'est vrai pour toute sous-structure d'un modèle de T, et par un raisonnement maintes fois utilisé) qu'il existe une formule sans quantificateurs $\theta(\bar{x})$ telle que

$$T \vdash \forall \bar{x}(\theta(\bar{x}) \leftrightarrow \exists y \, \psi(\bar{x}, y)).$$

En utilisant une induction sur le nombre de quantificateurs d'une formule écrite sous-forme prénexe, on montre que T élimine les quantificateurs.

3. Va-et-vient

(3.1) **Définition**. Soient M et N des $\mathcal{L}$-structures, et $\mathcal{I}$ une famille d'isomorphismes partiels entre M et N. Nous dirons que $\mathcal{I}$ a la **propriété du va-et-vient** si elle est non vide et satisfait aux conditions suivantes:

(a) (Le VA) Si $f \in \mathcal{I}$ et $a \in M$, alors il existe $g \in \mathcal{I}$ prolongeant f et ayant a dans son domaine.

(b) (Le VIENT) Si $f \in \mathcal{I}$ et $b \in N$ alors il existe $g \in \mathcal{I}$ prolongeant f et ayant b dans son image.

(3.2) **Théorème**. Soient M et N des $\mathcal{L}$-structures. Supposons qu'il existe une famille $\mathcal{I}$ d'isomorphismes partiels entre M et N et ayant la propriété du va-et-vient. Alors $M \equiv N$. De plus, chaque $f \in \mathcal{I}$ est un isomorphisme élémentaire, et donc, si $\bar{a}$ est un uplet du domaine de f, alors $tp_M(\bar{a}) = tp_N(f(\bar{a}))$.

Démonstration. Nous allons montrer, par induction sur la complexité des formules (écrites sous forme prénexe), que les éléments de $\mathcal{I}$ sont des isomorphismes élémentaires, c'est à dire que pour toute formule $\varphi(x_1, \ldots, x_n) \in \mathcal{L}$

($*$) Si $f \in \mathcal{I}$ et $a_1, \ldots, a_n \in dom(f)$, alors pour toute formule $\varphi(x_1, \ldots, x_n) \in \mathcal{L}$

$$M \models \varphi(a_1, \ldots, a_n) \iff N \models \varphi(f(a_1), \ldots, f(a_n)).$$

Pour les formules sans quantificateurs, c'est par définition des isomorphismes partiels. Supposons que $\varphi(x_1, \ldots, x_n) = \exists y\, \psi(x_1, \ldots, x_n, y)$, et que la formule $\psi(x_1, \ldots, x_n, y)$ satisfasse ($*$). Soit $f \in \mathcal{I}$, et $a_1, \ldots, a_n \in dom(f)$. Il y a deux cas à considérer:

Cas 1. $M \models \varphi(a_1, \ldots, a_n)$.

Soit $a \in M$ tel que $M \models \psi(a_1, \ldots, a_n, a)$. Par la propriété du va, il existe g prolongeant f et ayant a dans son domaine. Par hypothèse d'induction, $N \models \psi(g(a_1), \ldots, g(a_n), g(a))$, et donc (comme $f(a_i) = g(a_i)$), $N \models \exists x\, \psi(f(a_1), \ldots, f(a_n), x)$. Cela prouve que $N \models \varphi(f(a_1), \ldots, f(a_n))$.

Cas 2. $M \models \neg\varphi(a_1, \ldots, a_n)$.

Dans ce cas, pour tout $a \in M$, nous avons $M \models \neg\psi(a_1, \ldots, a_n, a)$. Supposons que cependant $N \models \varphi(f(a_1), \ldots, f(a_n))$. Il existe donc $b \in N$ tel que $N \models \psi(f(a_1), \ldots, f(a_n), b)$. Appliquant maintenant la propriété du vient, et raisonnant comme dans le cas 1, nous obtenons une contradiction. Donc $N \models \neg\varphi(f(a_1), \ldots, f(a_n))$, ce qui termine la preuve que la formule $\varphi(x_1, \ldots, x_n)$ satisfait ($*$).

Nous avons donc prouvé que les éléments de $\mathcal{I}$ sont des isomorphismes élémentaires. Soit $f \in \mathcal{I}$, et φ un énoncé. Comme f est élémentaire, nous avons $M \models \varphi$ si et seulement si $N \models \varphi$, et donc $M \equiv N$.

(3.3) **Remarque/Théorème**. Supposons que M et N soient des structures dénombrables, et qu'il existe une famille $\mathcal{I}$ d'isomorphismes partiels entre M et N ayant la propriété du va-et-vient. Alors $M \simeq N$.

Démonstration. Exercice.

(3.4) L'existence d'une famille d'isomorphismes partiels entre deux $\mathcal{L}$-structures M et N ayant la propriété du va-et-vient est **plus forte que la simple équivalence élémentaire** de M et N. Par exemple si $M \prec N$ et $M \neq N$, alors les $\mathcal{L}(M)$-structures M et N sont élémentairement équivalentes. Cependant les seuls isomorphismes partiels entre M et N sont des restrictions de l'inclusion $M \subset N$. Il n'y a donc pas de famille d'isomorphismes partiels entre M et N ayant la propriété du va-et-vient.

Nous montrerons plus tard que si $M \equiv N$, alors il existe des extensions élémentaires M^* de M et N^* de N et une famille d'isomorphismes partiels entre M^* et N^* et ayant la propriété du va-et-vient. Nous verrons aussi que la technique des va-et-vient fournit des moyens de montrer la complétude d'une théorie, ou bien le fait qu'elle élimine les quantificateurs.

(3.5) **Remarque/Proposition**. Soit T une théorie, ayant la propriété suivante:

Si M et N sont des modèles de T, alors il existe des extensions élémentaires M^* et N^* de M et N respectivement, et une famille $\mathcal{I}(M^*, N^*)$ d'isomorphismes partiels entre M^* et N^* tels que:

(i) Si l'application vide est un isomorphisme partiel, alors $\mathcal{I}(M^*, N^*)$ est non vide et a la propriété du va-et-vient.

(ii) Si $\mathcal{I}(M^*, N^*)$ est non vide, tout isomorphisme partiel de domaine **fini** est la restriction d'une fonction de $\mathcal{I}(M^*, N^*)$.

Alors T élimine les quantificateurs.

Démonstration. Notons d'abord que M et N sont élémentairement équivalents si et seulement si l'isomorphisme vide est un isomorphisme partiel. D'où la nécéssité de la condition (i).

Supposons que T satisfait l'hypothèse de la proposition. Par le corollaire (2.2) appliqué à l'ensemble Δ des formules sans quantificateurs, il suffit de montrer que si M et N sont des modèles de T, et si $\bar{a}$ et $\bar{b}$ sont des uplets de M et N respectivement, tels que $\bar{b}$ satisfait (dans N) toutes les formules sans quantificateurs satisfaites par $\bar{a}$ dans M, alors l'application f qui envoie $\bar{a}$ sur $\bar{b}$ est un isomorphisme partiel élémentaire.

Notons d'abord que f est bien un isomorphisme partiel, car elle préserve les formules sans quantificateurs. Donc l'application vide est un isomorphisme partiel de M sur N, et aussi de donc de toutes extensions élémentaire M^* de M et N^* de N. Soient donc M^*, N^*, et $\mathcal{I}(M^*, N^*)$ satisfaisant aux conditions (i) et (ii). Alors f est la restriction d'une fonction g de $\mathcal{I}(M^*, N^*)$. Puisque $\mathcal{I}(M^*, N^*)$ a la propriété du va-et-vient, g est un isomorphisme partiel élémentaire entre M^* et N^*. Puisque $M \prec M^*$ et $N \prec N^*$, et par définition d'un isomorphisme partiel élémentaire, pour toute formule $\varphi(\bar{x})$ de $\mathcal{L}$ nous avons donc

$$M \models \varphi(\bar{a}) \iff N \models \varphi(\bar{b}).$$

Remarque. Nous montrerons plus tard que toute théorie T éliminant les quantificateurs satisfait l'hypothèse de cette proposition.

(3.6) **Exemple 1 - Les ordres denses sans extrémités**. Vous avez montré, en cours fondamental, que la théorie T_{od} des ordres denses sans extrémités est $\aleph_0$-catégorique, en construisant un isomorphisme entre deux modèles dénombrables quelconques de votre théorie. Votre preuve montre aussi la chose suivante:

Soient M et N des modèles de T_{od}, et soit $\mathcal{I}(M,N)$ la famille des isomorphismes partiels entre M et N ayant domaine fini. Alors $\mathcal{I}(M,N)$ a la propriété du va-et-vient.

En effet, soit $f \in \mathcal{I}(M,N)$, et écrivons $dom(f) = \{a_1, \ldots, a_n\}$, où $a_1 < a_2 < \cdots < a_n$, et $b_i = f(a_i)$ pour $i = 1, \ldots, n$. Soit $a \in M$. Si $a \in dom(f)$, il n'y a rien a prouver. Supposons donc que $a \notin dom(f)$. Alors soit $a \in (\infty, a_1[$, ou bien il existe un unique $i < n$ tel que $a \in]a_i, a_{i+1}[$, ou bien $a \in]a_n, +\infty)$. Raisonnant cas par cas, on montre que f s'étend à un isomorphisme partiel ayant a dans son domaine.

Corollaire. La théorie des ordres denses sans extrémités élimine les quantificateurs dans le langage $\{<\}$.

(3.7) **Exercice**. Soit maintenant T la théorie des ordres denses avec extrémités, dans le langage $\{<\}$. Montrez que cette théorie est complète (et en fait $\aleph_0$-catégorique). Que faut-il ajouter au langage, et quels axiomes faut-il ajouter à T, pour avoir l'élimination des quantificateurs?

(3.8) **Exemple 2 - Les groupes abéliens divisibles sans torsion**. Cette fois-ci nous considérons la théorie des groupes abéliens divisibles sans torsion, dans le langage $\{+, -, 0\}$. Vous avez montré que cette théorie est κ-catégorique pour tout cardinal non dénombrable κ. En fait votre preuve a montré que si M et N sont des groupes abéliens divisibles sans torsion non dénombrables, alors la famille $\mathcal{I}(M,N)$ des isomorphismes partiels de domaine **dénombrable** a la propriété du va-et-vient. Comme tout modèle a une extension élémentaire non-dénombrable, cela montre aussi que cette théorie admet l'élimination des quantificateurs.

(3.9) **Exemple 3 - La théorie des Z-groupes**. Maintenant, nous allons montrer qu'une certaine théorie T est complète. Nous exhiberons plus tard un langage dans lequel elle élimine les quantificateurs. Pour nous simplifier la vie, nous allons ajouter au langage une constante superflue, nous verrons plus tard comment on peut s'en dispenser.

Soit $\mathcal{L}$ the langage $\{+, -, 0.1\}$ des groupes abéliens augmenté par la constante 1. Considérons la théorie T axiomatisée par les axiomes suivants:

- groupe abélien sans torsion, avec 0 l'identité.
- pour tout $n > 1$ l'énoncé: $\forall x\, nx \neq 1$.
- pour tout $n > 1$ l'énoncé: $\forall x\, \exists y \bigvee_{i=0}^{n-1} ny = x - i$.

Un petit mot sur la notation. Ici, nx est une abréviation pour le terme $x + x + \cdots + x$ (n fois), et i est une abreviation pour le terme $1 + 1 + \cdots + 1$ (i fois). Certainement $(\mathbf{Z}, +, -, 0, 1)$ est un modèle de la théorie T, et nous l'appelerons le modèle standard de T. Il se plonge de manière unique dans tout modèle de T. Nous allons étudier les modèles non-standards de T. Nous aurons besoin de quelques résultats simples d'algèbre, qui sont rappelés en fin de chapître (voir (3.12)).

Fixons un modèle M non standard de T, nous noterons $\mathbf{Z}$ sa sous-structure engendrée par 1. Pour $m > 1$, on note

$$mM = \{ma \mid a \in M\}.$$

C'est un sous-groupe de M, et l'on considère

$$D = D(M) = \bigcap_{n>1} nM.$$

Assertion 1. D est divisible.

Soit $a \in D$, et $m > 1$ un entier. Nous voulons montrer qu'il existe $b \in D$ tel que $mb = a$. Par définition de D, nous savons qu'il existe $b \in M$ tel que $mb = a$, et nous voulons montrer que cet élément b est dans D. Notons que comme M est sans torsion, l'élément b est uniquement défini par $mb = a$ (si $mb = mc$ alors $m(b - c) = 0$, et $b = c$). Il faut montrer que $b \in \bigcap_n nM$. Soit donc $n > 1$, et soit $c \in M$ tel que $a = mnc$. Alors $m(nc) = a = mb$, et donc $b = nc$, ce qui montre que $b \in nM$. Puisque c'est vrai pour tout n, cela montre que $b \in D$.

Attention. L'hypothèse que M est sans torsion est essentielle.

Nous allons maintenant regarder le groupe abélien M/D. Notons que c'est aussi une $\mathcal{L}$-structure, et que c'est un modèle de T. Nous allons construire un plongement $M/D \to \hat{\mathbf{Z}}$ (voir (3.13) pour la définition de $\hat{\mathbf{Z}}$ et ses propriétés).

On note 1 l'élément de $\hat{\mathbf{Z}}$ défini par la suite infinie constante $(1)_{n\geq 2}$, et 0 l'élément défini par la suite infinie $(0)_{n\geq 2}$. Nous allons définir un homomorphisme $g : M \to \hat{\mathbf{Z}}$, avec $Ker(g) = D$. Soit $a \in M$. Pour chaque $n \geq 2$, il existe un unique élément $i \in \{0, 1, \ldots, n-1\}$ tel que $a - i$ est divisible par n, et nous notons a_n cet élément. Nous définissons alors

$$g(a) = (a_n)_{n\geq 2}.$$

On vérifie aisément que g est un homomorphisme de groupe, et que $g(1) = 1$, $Ker(g) = D$.

Soit $a = (a_n)_{n\geq 2} \in \hat{\mathbf{Z}}$. Alors "$g(x) = a$" est expressible par une collection de formules, plus précisément par la collection suivante:

$$p_a(x) = \{\exists y\, ny = (a - a_n) \mid n \geq 2\}.$$

Notons que chaque $p_a(x)$ est réalisable dans une extension élémentaire de M: en effet, $p_a(x)$ est finiment satisfaisable dans M, et donc il existe une extension élémentaire M^* de M, et un élément $b \in M^*$ qui satisfait toutes les formules de M^* (b est appelé une **réalisation du type partiel** $p_a(x)$, nous étudierons les types partiels plus en détail dans le chapître suivant). Notons que si $M \prec M^*$, alors l'homomorphisme g s'étend uniquement en un homomorphisme $g : M^* \to \hat{\mathbf{Z}}$, et que nous avons $g(b) = a$.

Soient M et N des modèles de T, et M^*, N^* des extensions élémentaires de M et de N, de cardinalité $\kappa > 2^{\aleph_0}$, et tels que pour tout $a \in \hat{\mathbf{Z}}$, M^* et N^* contiennent des réalisations de $p_a(x)$.

Assertion 2. $M^* \simeq N^*$.

Par (3.12), nous savons que $M^* = D(M^*) \oplus A$, avec $1 \in A$, et que $N^* = D(M^*) \oplus B$, avec $1 \in B$. Par hypothèse, tous les types $p_a(x)$ sont réalisés dans A et dans B, ce qui entraîne que $(A, 1) \simeq (\hat{\mathbf{Z}}, 1)$, et $(B, 1) \simeq (\hat{\mathbf{Z}}, 1)$. Il existe donc un isomorphisme h entre A et B, qui envoie 1 sur 1.

De plus, comme $|A| = |B| = 2^{\aleph_0} < \kappa$, nous avons $|D(M^*)| = |D(N^*)| = \kappa$, et les groupes abéliens divisibles sans torsion $D(M^*)$ et $D(N^*)$ sont donc isomorphes. Cela montre l'assertion.

Nous avons montré que deux modèles quelconques de T ont des extensions élémentaires isomorphes: la theórie T est donc complète.

(3.10) **Remarques et commentaires**. Nous arrêtons pour le moment l'étude de cet exemple. Nous verrons plus tard que:

(1) Les 1-types complets (c'est à dire les ensembles de formules à 1-variable libre, consistants avec T, et maximaux pour ces deux propriétés) sont (presque) décrits par les ensembles $p_a(x)$. Plus précisément:
   - Si $a \in \hat{\mathbf{Z}}$, $a \notin \mathbf{Z}$, alors le type $p_a(x)$ est complet.
   - Si $a \in \mathbf{Z}$, alors le type $p_a(x)$ a deux complétions, qui sont obtenues en rajoutant à $p_a(x)$ la formule $x = a$ ou bien sa négation.

(2) Si l'on rajoute à $\mathcal{L}$ des prédicats binaires $\equiv_n$, $n \geq 2$, et à T les énoncés

$$x \equiv_n y \iff \exists z\, nz = (x - y),$$

pour obtenir une nouvelle théorie T', alors T' élimine les quantificateurs dans ce nouveau langage.

(3) La constante 1 peut en fait être supprimée. Pour chaque $n \geq 2$, on remplace les deux énoncés de T dépendant de n par un seul énoncé qui exprime que M/nM a exactement n éléments, et en fait est cyclique d'ordre n:

$$\exists x\, \forall y\, (\bigwedge_{i=1}^{n-1} ny \neq ix) \wedge \exists z \bigvee_{i=0}^{n-1} (y - ix) = nz. \tag{n}$$

On aura un théorème d'élimination des quantificateurs similaire.

(4) Notons que $\mathbf{Q}^{(\kappa)} \oplus \mathbf{Z}$ est aussi un modèle de T, de cardinalité κ, mais il ne réalise pas tous les types $p_a(x)$, $a \in \mathbf{Z}$.

(3.11) **Exemple 4 - Corps algébriquement clos**. Soit $\mathcal{L} = \{+, -, \cdot, 0, 1\}$, et T la théorie suivante:

– T contient les axiomes de corps, avec 0 l'élement neutre de l'addition, et 1 celui de la multiplication. $0 \neq 1$.

– Pour chaque $n > 1$, T contient l'énoncé:
$\forall x_1, \ldots, x_n\, \exists y\, y^n + x_1 y^{n-1} + \cdots + x_{n-1} y + x_n = 0$.

Nous allons montrer que cette théorie élimine les quantificateurs. Elle n'est cependant pas complète, puisqu'elle ne dit rien sur la caractéristique. Notons que le fait que 1 soit dans le langage est essentiel: c'est grâce à lui que nous pouvons spécifier la caractéristique sans utiliser de quantificateurs.

Soient K_1 et K_2 des corps algébriquement clos. Nous voulons appliquer le critère donné par (3.5). Passant à des extensions élémentaires nous pouvons donc supposer que K_1 et K_2 ne sont pas dénombrables.

Soit $\mathcal{I}(K_1, K_2)$ la famille d'isomorphismes partiels de domaine dénombrable. Nous allons montrer que si elle n'est pas vide, alors elle a la propriété du va-et-vient.

Premièrement, notons qu'elle n'est pas vide si et seulement si les sous-corps premiers de K_1 et K_2 sont isomorphes (le sous-corps premier d'un corps est le plus petit sous-corps de ce corps : c'est $\mathbf{F}_p$ si la caractéristique est $p > 0$, ou $\mathbf{Q}$ si la caractéristique est nulle).

Soient $f \in \mathcal{I}(K_1, K_2)$, et $a \in K_1$. Observons que si A_1 dénote le sous-corps de K_1 engendré par $dom(f)$, alors f s'étend uniquement en un isomorphisme défini sur A_1, et avec image le sous-corps A_2 de K_2 engendré par $Im(f)$. De plus, A_1 et A_2 sont aussi dénombrables. Nous pouvons donc supposer que $dom(f) = A_1$, $Im(f) = A_2$. Définissons

$$I(a/A_1) = \{g(X) \in A_1[X] \mid g(a) = 0\}.$$

C'est un idéal premier de $A_1[X]$ (si un produit de deux polynomes s'annule en a, alors l'un des deux s'annule). Comme A_1 est un corps, l'anneau $A_1[X]$ est un anneau euclidien, ce qui entraîne que $I(a/A_1)$ est un idéal principal de $A_1[X]$ (c'est à dire qu'il existe $g(X) \in I(a/A_1)$ qui divise tous les éléments de $I(a/A_1)$), et que $I(a/A_1)$ est maximal (car premier).

Notons aussi que f s'étend en un isomorphisme $A_1[X] \to A_2[X]$, obtenu en posant $f(X) = X$. Nous avons maintenant deux cas à considérer.

Cas 1. $I(a/A_1) = (0)$.

Cela veut dire que a est transcendental sur A_1. Soit A_2' l'ensemble des éléments de K_1 qui sont algébriques sur A_2. Nous savons que chaque élément de A_2' satisfait une équation (non triviale) à coefficient dans A_2; d'autre part, un polynôme en une variable de degré n a au plus n racines. Cela entraîne que A_2' est dénombrable (car $A_2[X]$ est dénombrable). Nos hypothèses de cardinalité entraînent qu'il existe $b \in K_2$, $b \notin A_2'$. Comme $b \notin A_2'$, nous avons $I(b/A_2') = (0)$ et nous prolongeons f en envoyant a sur b.

Cas 2. $I(a/A_1) \neq (0)$, c'est à dire $g(X) \neq 0$.

Soit $b \in K_2$ tel que $f(g)(b) = 0$. L'homomorphisme $h : A_1[X] \to A_2[b]$ défini par $h(s(X)) = f(s)(b)$, s'annule sur $I(a/A_1)$. Mais $I(a/A_1)$ est maximal, et donc $Ker(h) = I(a/A_1)$. D'autre part, par définition, $I(a/A_1)$ est le noyau de l'homomorphisme $A_1[X] \to A_1[a]$ qui est l'identité sur A_1 et envoie X sur a. Cela montre que nous pouvons prolonger f à $A_1[a] = A_1(a)$ en posant $f(a) = b$.

Nous avons prouvé que notre famille a la propriété du va. Par symétrie elle a aussi celle du vient.

Résultats d'algèbre

(3.12) **Lemme**. Soient $D \subseteq M$ des groupes abéliens, et supposons que D est divisible. Alors il existe un sous-groupe A de M tel que $M = D \oplus A$, ce qui veut dire:

$$D \cap A = (0) \qquad \text{et} \qquad D + A = M.$$

(Rappel: $D + A = \{d + a \mid d \in D, a \in A\}$. La condition $A \cap D = (0)$ implique que tout élément de M s'écrit de façon unique comme la somme d'un élément de D et d'un élément de A.)

De plus, si B est un sous-groupe de M tel que $B \cap D = (0)$, alors on peut trouver A contenant B.

Démonstration. Il est équivalent de montrer qu'il existe un homomorphisme de groupe $f : M \to D$, qui est l'identité sur D, et dont le noyau contient B. En effet, si un tel A existe, alors la projection sur D satisfait bien cette condition.

Si un tel f existe, on pose $A = Ker(f)$. Certainement, $D \cap A = (0)$ puisque f est l'identité sur D. Si $a \in M$, alors $a = f(a) + (a - f(a))$, et $f(a) \in D$; on a $f(a - f(a)) = f(a) - f(f(a)) = f(a) - f(a) = 0$ (nous avons utilisé d'abord que f est un homomorphisme de groupe, puis que f est l'identité sur D et que $f(a) \in D$). Cela montre que $M = D \oplus Ker(f)$.

Soit $\mathcal{F}$ la famille de tous les homomorphismes $f : C \to D$ tels que le domaine C de f est un sous-groupe de M contenant D et B, f est l'identité sur D, et est 0 sur B. Cette famille est non-vide : par hypothèse $D + B = D \oplus B$ puisque $D \cap B = (0)$, et l'homomorphisme $f_0 : D \oplus B \to D$ qui est l'identité sur D et envoie B sur 0 est dans $\mathcal{F}$. D'autre part, si nous ordonnons $\mathcal{F}$ de la façon naturelle: $f \leq g$ si et seulement si g étend f, alors la famille $\mathcal{F}$ est inductive: toute chaîne croissante d'éléments de $\mathcal{F}$ a un sup.

Soit $f \in \mathcal{F}$ un élément maximal (qui existe par le Lemme de Zorn), de domaine C. Nous allons montrer que si $a \in M$, alors f s'étend à une fonction de $\mathcal{F}$ avec a dans son domaine, ce qui montrera que $C = M$ (par maximalité de f). Soit donc $a \in M$.

Cas 1. Pour tout $n > 0$, $na \notin C$. Alors le sous-groupe $\langle a \rangle$ de M engendré par a est isomorphe à $\mathbf{Z}$, et $\langle a \rangle \cap C = (0)$. Nous pouvons donc définir $f(a) = 0$, et étendre f à $C + \langle a \rangle$, en posant $f'(c + na) = f(c)$, pour $c \in C, n \in \mathbf{Z}$.

Cas 2. Il existe $n \in \mathbf{Z}$, $n \neq 0$, tel que $na \in C$.

Si $a \in C$, nous n'avons rien à faire. Sinon, soit $I = \{n \in \mathbf{Z} \mid na \in C\}$. C'est un idéal de $\mathbf{Z}$, et donc est de la forme $m\mathbf{Z}$, pour un $m \in \mathbf{N}$, et $m > 1$ (parce que $a \notin C$). Soit $b \in C$ tel que $ma = b$. Puisque D est divisible, il existe $c \in D$ tel que $mc = f(b)$. On pose alors $f'(d + na) = f(d) + nc$, pour $d \in C$ et $n \in \mathbf{Z}$.

Il faut vérifier que f' est bien définie. Supposons que l'élément $d + na$ s'écrive aussi $d' + n'a$, avec $d' \in C$ et $n' \in \mathbf{Z}$. On a alors

$$(d - d') = (n - n')a,$$

ce qui entraîne que $n - n' \in I$ (puisque $d - d' \in C$), c'est à dire que $n - n' = mj$ pour un $j \in \mathbf{Z}$. Donc $d - d' = mja = jb$, ce qui implique $f(d) = f(d') + jf(b)$. Par définition $f'(na) = nc = (n' + mj)c = n' + jf(b)$, ce qui montre que f' est bien définie. Il est clair que f' prolonge f.

(3.13) **Le groupe $\hat{\mathbf{Z}}$.** On définit $\hat{\mathbf{Z}}$ comme l'ensemble des suites $(a_n)_{n \geq 2}$ satisfaisant les deux conditions suivantes:

(i) Pour tout $n \geq 2$, $a_n \in \{0, 1, \ldots, n-1\}$.

(ii) Si m divise n alors $a_n \equiv a_m$ (m).

On peut donc identifier $\hat{\mathbf{Z}}$ à un sous-ensemble de $\prod_{n \geq 2} \mathbf{Z}/n\mathbf{Z}$, en identifiant $\mathbf{Z}/n\mathbf{Z}$ avec l'ensemble $\{0, 1, \ldots, n-1\}$. Ce produit est un groupe, si on définit

$$(a_n)_n + (b_n)_n = (c_n)_n \iff a_n + b_n \equiv c_n \ (n) \text{ pour tout } n \geq 2.$$

On définit la loi de groupe sur $\hat{\mathbf{Z}}$ comme étant la restriction de la loi de groupe du produit à $\hat{\mathbf{Z}}$. On vérifie aisément que c'est bien un sous-groupe.

On peut aussi définir $\hat{\mathbf{Z}}$ comme étant la limite inverse des groupes $\mathbf{Z}/n\mathbf{Z}$, voir ci-dessous (3.17).

(3.14) **Produits de $\mathcal{L}$-structures**. Soit $\mathcal{L}$ un langage, I un ensemble, et (A_i), $i \in I$, une famille de $\mathcal{L}$-structures indexée par I. La $\mathcal{L}$-structure $\prod_{i \in I} A_i$ est définie de la façon suivante. Son univers est le produit cartésien des A_i, $i \in I$. Si $c \in \mathcal{L}$ est un symbole de constante, l'interprétation de c dans le produit est l'élément $(c_i)_i$, où chaque c_i est l'interprétation de c dans A_i.

Si R est une relation n-aire du langage, et $a^1 = (a_i^1)_i, \ldots, a^n = (a_i^n)_i$ sont des éléments du produit, alors

$$R(a^1, \ldots, a^n) \iff A_i \models R(a_i^1, \ldots, a_i^n) \text{ pour tout } i \in I.$$

Si f est une fonction n-aire du langage, et $a^1, \ldots, a^n$ sont comme ci-dessus, on définit

$$f(a^1, \ldots, a^n) = (f(a_i^1, \ldots, a_i^n))_i.$$

On peut vérifier que si $\varphi(\bar{x})$ est une formule atomique, et $\bar{a} \in \prod_i A_i$, alors $\prod_i A_i \models \varphi(\bar{a}) \iff A_i \models \varphi(\bar{a}_i)$ pour tout $i \in I$. Cependant, cela devient faux si l'on a des négations: la formule $x \neq c$ fournit un contre-exemple immédiat. Même les disjonctions posent problème, par exemple la formule $R(x) \vee S(x)$.

Notons aussi que chacune des projections $\pi_j : \prod_{i \in I} A_i \to A_j$ est un homomorphisme.

(3.15) **Somme directe de groupes**. Nous avons vu plus haut quand deux sous-groupes d'un groupe sont en somme directe. En fait on peut définir la somme directe de groupes directement.

Soient A_i, $i \in I$, une famille de groupes. Ici, nous écrirons la loi de groupe multiplicativement, c'est à dire que le langage est $\{\cdot, {}^{-1}, 1\}$. La notation additive est réservée aux groupes abéliens (et le langage est alors $\{+, -, 0\}$). On définit $\bigoplus_{i \in I} A_i$ comme étant le sous-groupe de $\prod_{i \in I} A_i$ consistant des éléments $(a_i)_i$ tels que $\{i \in I \mid a_i \neq 1\}$ est **fini**. Notons que c'est bien un sous-groupe: il contient 1, et est clos par inverse et par produit.

En notation additive, cela devient:

$$\bigoplus_{i \in I} A_i = \{(a_i)_i \in \prod_{i \in I} A_i \mid \{i \mid a_i = 0\} \text{ est fini}\}.$$

Par exemple, notre groupe $\mathbf{Q}^{(\kappa)} \oplus \mathbf{Z}$ est tout simplement le sous groupe de $\mathbf{Q}^\kappa \times \mathbf{Z}$ avec univers

$$\{((a_i)_{i<\kappa}, b) \in \mathbf{Q}^\kappa \times \mathbf{Z} \mid \{i \mid a_i \neq 0\} \text{ est fini }\}.$$

Il faut aussi remarquer que quand I est fini, alors le produit et la somme directe coïncident. Cela est faux bien sûr quand I est infini. Si κ est infini, notons aussi que la cardinalité de $\mathbf{Q}^\kappa$ égale 2^κ, alors que celle de $\mathbf{Q}^{(\kappa)}$ est seulement κ.

(3.16) **Limites projectives de $\mathcal{L}$-structures**. Aussi appelées limites inverses. A partir d'un certain data, nous allons construire une $\mathcal{L}$-structure.

Le data (appelé **système inverse ou projectif de $\mathcal{L}$-structures**) Nous avons un ensemble I avec un ordre partiel $<$ (c'est à dire une relation binaire, antisymétrique et transitive; pas nécéssairement un ordre total). Pour chaque $i \in I$, nous avons une $\mathcal{L}$-structure A_i, et si $i < j$, nous avons un $\mathcal{L}$-homomorphisme $f_{i,j} : A_i \to A_j$. Les homomorphismes $f_{i,j}$ satisfont aux conditions de compatibilité suivantes:

$$\text{Si } i < j < k, \text{ alors } f_{i,k} = f_{j,k} f_{i,j}.$$

A partir de ce data, nous définissons une $\mathcal{L}$-structure $A = lim_{\leftarrow} A_i$, appelée la limite inverse ou projective du système $(A_i, f_{i,j} \mid i < j \in I)$, de la façon suivante:

L'univers de A est l'ensemble des éléments $(a_i)_i \in \prod_{i \in I} A_i$ satisfaisant

$$\text{Pour tout } i < j \in I,\ f_{i,j}(a_i) = a_j.$$

La $\mathcal{L}$-structure sur A est celle induite par la $\mathcal{L}$-structure de $\prod_{i \in I} A_i$. On vérifie que A est bien une sous-structure du produit (c'est à dire contient les interprétations des constantes et est close pour les fonctions du langage).

Attention. Si les applications $f_{i,j}$ ne sont pas surjectives, et si le langage ne contient aucun symboles de constante, il se peut très bien que A soit **vide**!!

(3.17) **Retour sur $\hat{\mathbf{Z}}$.** Soit I l'ensemble des entiers ≥ 2, et $\leq$ la relation "être divisible par". Pour $n \in I$, soit $A_n = \mathbf{Z}/n\mathbf{Z}$. Donc si m divise n, alors nous avons une application $f_{n,m} : \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$. Le système $(\mathbf{Z}/n\mathbf{Z}, f_{n,m} \mid n \leq m)$ satisfait aux conditions de compatibilités. On vérifie que $\hat{\mathbf{Z}} = lim_{\leftarrow} \mathbf{Z}/n\mathbf{Z}$.

(3.18) **Propriétés universelles des limites projectives**. Soient $(A_i, f_{i,j} \mid i \leq k\}$ un système projectif de $\mathcal{L}$-structures, et A la $\mathcal{L}$-structure $\lim_{\leftarrow} A_i$ définie ci-dessus. Notons par $\pi_j : A \to A_j$ la restriction à A de la projection $\prod_{i \in I} A_i \to A_j$. Supposons que nous ayons une $\mathcal{L}$-structure B, et pour chaque $i \in I$ un $\mathcal{L}$-homomorphisme $g_i : B \to A_i$, satisfaisant

$$\text{si } i < j, \text{ alors } f_{i,j} g_i = g_j.$$

Alors il existe un unique homomorphisme $g : B \to A$, qui satisfait $\pi_i g = g_i$ pour tout $i \in I$. En effet on pose tout simplement $g(b) = (g_i(b))_i$.

(3.19) **Groupes profinis**. Comme leur nom l'indique ce sont des limites inverses de groupes finis. Mais ils ont un peu plus de structure: ce sont aussi des groupes topologiques, c'est à dire qu'ils ont une topologie, pour laquelle les opérations de groupe (multiplication et inverse) sont continues.

Nous avons donc un groupe G, qui est une limite inverse de groupes finis $(G_i, f_{i,j} \mid i < j)$, et est en particulier un sous-groupe de $\prod_{i \in I} G_i$. On donne à chacun des groupes finis G_i la topologie discrète, au produit des G_i 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 $\{i \in I \mid U_i \neq G_i\}$ est fini). Alors G est en fait un sous-groupe fermé de $\prod_{i \in I} G_i$. Comme un produit d'espaces compacts est compact, et qu'un fermé d'un compact est compact (Théorème de Tychonoff), cela entraîne que G est compact.

Les groupes profinis ont été introduits pour étudier la structure des extensions de Galois **infinies** d'un corps K. Soient K un corps, et K^s sa clôture séparable (c'est à dire le sous corps de la clôture algébrique $\tilde{K}$ de K consistant des éléments qui sont racine simple d'un polynome à coefficients dans K). On peut alors écrire $K^s = \bigcup\{L \mid L \text{ extension de Galois finie de } K\}$. Si $L \subset M$ sont des extensions de Galois finies de K, on définit $\pi_{M,L} : \mathcal{G}al(M/K) \to \mathcal{G}al(L/K)$ comme étant l'application restriction.

On définit alors $\mathcal{G}al(K^s/K) = \lim_{\leftarrow}(\mathcal{G}al(L/K), \pi_{N,M})$. Notons que ce groupe coïncide avec $Aut(K^s/K)$, mais que nous avons l'information topologique en plus. Les ouverts de base de cette topologie sont de la forme

$$U_{\sigma,L} = \{\tau \in Aut(K^s/K) \mid \tau|_L = \sigma|_L\},$$

pour L une extension de Galois finie de K et $\sigma \in Aut(K^s/K)$.

4. Types, espaces de types.

(4.1) **Définitions**. Fixons une théorie T (consistante) dans un langage $\mathcal{L}$, et soit $\bar{v}$ un uplet de variables, que nous supposons fini en général.

(1) Soit $\Sigma(\bar{v})$ un ensemble de formules du langage, avec variables libres parmi les éléments de $\bar{v}$, qui contient T et est clos par déductions logiques (si $\Sigma(\bar{v}) \vdash \varphi(\bar{v})$ alors $\varphi(\bar{v}) \in \Sigma(\bar{v})$). Nous appelons alors $\Sigma(\bar{v})$ un **type partiel**. Les types partiels considérés sont en général des ensembles infinis de formules.

(2) Nous dirons que le type partiel $\Sigma(\bar{v})$ est **consistant**, ou **satisfaisable**, s'il existe un modèle M de T, et un uplet $\bar{a} \in M$ de la même longueur que $\bar{v}$, et qui satisfait toutes les formules de $\Sigma(\bar{v})$.

(3) $\Sigma(\bar{v})$ est un type complet s'il est consistant, et pour toute formule $\varphi(\bar{v})$, nous avons $\Sigma(\bar{v}) \vdash \varphi(\bar{v})$ ou bien $\Sigma(\bar{v}) \vdash \neg\varphi(\bar{v})$. Autrement dit, $\Sigma(\bar{v})$ est maximal consistant.

(4.2) **Remarques**. (1) Tout type complet spécifie en particulier une complétion de T.

(2) Nous avons un critère facile de satisfaisabilité d'un type: le type $\Sigma(\bar{v})$ est consistant si et seulement si pour tout $\varphi(\bar{v}) \in \Sigma(\bar{v})$, $T \cup \{\exists \bar{v}\, \varphi(\bar{v})\}$ est consistant.

(3) Si l'on considère maintenant les types du langage $\mathcal{L}(A)$, où $A \subset M \models T$, nous parlerons de types au-dessus de A. Nous appellerons aussi les types définis dans la section précédente des types sur $\emptyset$.

(4) Les types complets sont en général dénotés par $p(\bar{v})$, ou $q(\bar{v})$. Souvent on omet les variables (p, q, etc.).

(4.3) **Exemple et définition**. Soient $M \models T$, et $\bar{a}$ un n-uplet de M, $\bar{v}$ un n-uplet de variables. Alors

$$tp(\bar{a}) = tp(\bar{a}/\emptyset) = \{\varphi(\bar{v}) \in \mathcal{L} \mid M \models \varphi(\bar{a})\}$$

est un type complet. Nous dirons que $\bar{a}$ **realise le type complet** $tp(\bar{a})$. Remarquons que $tp(\bar{a})$ contient $Th(M)$.

Soit maintenant $A \subset M$. Alors le type de $\bar{a}$ sur A (dans M),

$$tp(\bar{a}/A) = \{\varphi(\bar{v}) \in \mathcal{L}(A) \mid M \models \varphi(\bar{v})\},$$

est un type complet du langage $\mathcal{L}(A)$. Nous voyons aussi que $tp(\bar{a}/A)$ contient $Diag(A)$.

(4.4) **Rappels sur les espaces topologiques**. Un espace topologique est un ensemble X donné avec une famille $\mathcal{T}$ d'ouverts satisfaisant aux conditions suivantes:

(i) $\emptyset, X \in \mathcal{T}$.

(ii) $\mathcal{T}$ est close par intersections **finies** et unions **quelconques**.

Les **fermés** de X sont les complémentaires des ouverts. La famille des fermés de X contient donc $\emptyset$ et X, et est close par unions **finies** et intersections **quelconques**. Un **voisinage** d'un point $x \in X$ est un sous-ensemble Y de X contenant un ouvert auquel x appartient. Un **ouvert-fermé** est un ouvert qui est aussi fermé (et son complémentaire sera aussi ouvert-fermé).

Une **base d'ouverts** pour la topologie de X est un sous-ensemble $\mathcal{U}$ de $\mathcal{T}$ tel que pour tout $U \in \mathcal{T}$, pour tout $x \in U$, il existe $U_0 \in \mathcal{U}$ tel que $x \in U_0$ et $U_0 \subset U$.

Si $\mathcal{U}$ est une base d'ouverts de $\mathcal{T}$, tout élément de $\mathcal{T}$ s'écrira comme une union d'éléments de $\mathcal{U}$.

Soient X et Y des espaces topologiques. Une fonction $f : X \to Y$ est **continue** si pour tout ouvert U de Y, l'ensemble $f^{-1}(U)$ est un ouvert de X. La fonction f est **ouverte** si pour tout ouvert U de X, l'ensemble $f(U)$ est un ouvert de Y. Finalement, nous dirons que f est un homéomorphisme si f est bijective, continue et ouverte. Notons que si f est un homéomorphisme alors $f^{-1} : Y \to X$ est aussi un homéomorphisme.

On notera $C(X, Y)$ l'ensemble des fonctions continues de X dans Y. On considère souvent la droite réelle $\mathbf{R}$ munie de la topologie euclidienne (les ouverts de base sont les intervalles ouverts), et on considère alors $C(X, \mathbf{R})$. C'est un anneau (addition et multiplication sont définies point par point: $(f + g)(x) = f(x) + g(x)$).

Si Y est un sous-ensemble de X, la **topologie induite sur** Y est la topologie dont les ouverts sont de la forme $U \cap Y$, pour U un ouvert de X. En général, les ensembles $U \cap Y$ ne sont pas des ouverts de X; cependant, si Y est ouvert, alors ils le sont. De même les fermés de Y ne seront en général pas des fermés de X, sauf si Y est un fermé.

$x \in X$ est un **point isolé** de X si $\{x\}$ est un ouvert de X. Soit $A \subset X$. On dit que $x \in X$ est un **point d'accumulation** de A si tout ouvert U de X contenant x coupe $A \setminus \{x\}$. (Remarques: x peut être un point d'accumulation de A sans y appartenir; un point isolé n'est jamais point d'accumulation).

(4.5) Un espace topologique X est **séparé** (aussi appelé Hausdorff ou bien T_2) si et seulement si

Si $x \neq y \in X$, il existe des ouverts disjoints U et V, tels que $x \in U$ et $y \in V$.

Il existe toute une série d'axiomes de séparation: par exemple, l'axiome T_1 dit que tout singleton est fermé, c'est à dire: si $x \neq y$, alors il existe $U \in \mathcal{T}$ tel que $y \in U$ et $x \notin U$. Cette propriété est plus faible que T_2. Mentionnons aussi les deux propriétés suivantes:

– si F est un fermé ne contenant pas le point x, il existe des ouverts disjoints U et V, avec $x \in U$ et $F \subset V$.

– Deux fermés disjoints sont contenus dans des ouverts disjoints.

– Si F est un fermé ne contenant pas le point x, alors il existe une fonction continue $f : X \to \mathbf{R}$ telle que f s'annule sur F et $f(x) = 1$.

On dira que l'espace topologique X est **compact**, s'il est séparé et a la propriété du recouvrement fini, c'est à dire:

Si $U_i, i \in I$ est une famille d'ouverts de X telle que $X = \bigcup_{i \in I} U_i$, alors il existe un **sous-ensemble fini** J de I tel que $X = \bigcup_{i \in J} U_i$.

Attention. En anglais, compact est seulement "avoir la propriété du recouvrement fini". Par exemple, pour eux l'espace topologique X avec la topologie triviale (les seuls ouverts sont $\emptyset$ et X) est compact.

Il arrive souvent qu'on parle de propriétés **locales** d'un espace topologique (localement compact, par exemple). On dit qu'un espave topologique est **localement P** (où P est une certain propriété) si tout point a un voisinage ayant la propriété P. Par exemple, $\mathbf{R}$ n'est pas compact, mais il est localement compact (car tout intervalle fermé borné de $\mathbf{R}$ est compact). De même les espaces euclidiens $\mathbf{R}^n$ sont localement compacts.

(4.6) **Exemples de topologies**.

Nous avons déjà vu la topologie triviale, et la topologie euclidienne sur $\mathbf{R}$. L'espace $\{1,2\}$ dont les ouverts sont $\emptyset, \{1,2\}$ et $\{1\}$ n'est pas séparé. Le point 1 est isolé, cependant $\{1\}$ n'est pas fermé.

Si X est un ensemble, on peut aussi lui donner la **topologie discrète**: tout sous-ensemble de X est ouvert (et donc fermé). Tous les points de X seront donc des points isolés. Par exemple en général $\mathbf{N}$ est muni de la topologie discrète. Il n'est pas compact, mais il est localement compact.

Soit X un espace localement compact. Le compactifié d'Alexandroff de X est l'espace topologique $X^* = X \cup \{\infty\}$, dont les ouverts de base sont les ensembles U tels que U est un ouvert de X, ou bien, si $\infty \in U$, alors $X \setminus U$ est compact. Notons que X est ouvert dans X^*. Il existe plusieurs façons de plonger un espace X dans un compact, mentionnons aussi la compactification de Stone-Cech de X, notée βX, dont les points correspondent aux idéaux maximaux de $C(X, \mathbf{R})$.

(4.7) **Quelques propriétés**. Les espaces topologiques compacts satisfont toutes les propriétés de séparation énoncées plus haut. Soit X un espace topologique, et Y un sous-ensemble de X muni de la topologie induite. Si Y est compact, alors Y est nécéssairement un fermé de X. La réciproque est vrai quand X est compact: un sous-ensemble fermé d'un compact est compact (pour la topologie induite).

Si X est compact, et $f : X \to Y$ est une application continue, alors $f(X)$ est compact, et en particulier est fermé. Donc une application continue surjective d'un espace compact dans un espace quelconque est nécéssairement ouverte.

Un espace topologique séparé fini est nécéssairement discret. Un espace topologique compact infini a nécéssairement des points d'accumulation, et donc ne peut être discret.

Les espace Booléens (aussi appelés parfois espaces de Stone) sont des espaces topologiques compacts ayant une base d'ouverts consistant d'ouverts-fermés. On peut montrer que si Y est un fermé de l'espace Booléen X, alors Y est aussi Booléen. De plus, tout ouvert-fermé de Y est de la forme $Y \cap U$ où U est un ouvert-fermé de X (ceci utilise la compacité de Y).

(4.8) **Algèbres de Boole**. Les algèbres de Boole sont des structures du langage $\mathcal{L} = \{\cap, \cup, 0, 1\}$, où $\cap$ et $\cup$ sont des opérations binaires, et auquel on ajoute parfois une autre opération binaire notée $\setminus$.

L'exemple typique est l'ensemble $\mathcal{P}(I)$ des parties d'un ensemble I, où $\cap$ et $\cup$ sont les opérations usuelles d'intersection et de réunion, $0 = \emptyset$ et $1 = I$. L'opération $\setminus$ correspond alors à la différence ensembliste: $A \setminus B = \{i \in A \mid i \notin B\}$.

Les algèbres de Boole sont alors des $\mathcal{L}$-structures satisfaisant les axiomes suivants:

– Les opérations $\cup$ et $\cap$ sont commutatives, transitives, et distributives (Pour tous a, b, c: $(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$, $(a \cup b) \cap c = (a \cap c) \cup (b \cap c)$).

– Pour tout a: $0 \cap a = 0$, $1 \cap a = a$, $0 \cup a = a$, $1 \cup a = 1$.

– $\forall a \, \exists b \, (a \cap b = 0) \wedge (a \cup b = 1)$.

– $\forall a$, $a \cap a = a \cup a = a$.

– $\forall a, b$, $a \cup (a \cap b) = a = a \cap (a \cup b)$.

Si l'on ajoute $\setminus$ au langage, on a de plus les axiomes:

– Pour tous a, b: $a \setminus b = a \cap (1 \setminus b)$, $(1 \setminus a) \cap (1 \setminus b) = 1 \setminus (a \cup b)$ et $(1 \setminus a) \cup (1 \setminus b) = 1 \setminus (a \cap b)$.

– Pour tout a: $a \cap (1 \setminus a) = 0$, $a \cup (1 \setminus a) = 1$.
– $\forall a$, $1 \setminus (1 \setminus a) = a$.

On peut définir une relation d'ordre sur une algèbre de Boole $\mathcal{B}$ en posant $a \subseteq b \iff a \cap b = a$. Notons que réciproquement (si $\mathcal{B}$ est une algèbre de Boole, bien sûr) les opérations $\cup$, $\cap$, $\setminus$ sont définissables dans la structure $(\mathcal{B}, \subseteq)$: on dit que $a \cup b$ est le "sup" de a et b pour $\subseteq$: $a \cup b = c$ si et seulement si $a \subseteq c$, $b \subseteq c$ et pour tout d, $(a \subseteq d \wedge b \subseteq d) \rightarrow c \subseteq d$. De même, $a \cap b$ est l'"inf" de a et de b, 0 est le plus petit élément, 1 est le plus grand.

(4.9) **Autre exemple typique**. Soit T une théorie dans un langage $\mathcal{L}'$. On définit $\mathcal{B}(T)$ comme étant l'ensemble des énoncés de $\mathcal{L}'$ quotientés par la relation d'équivalence "être équivalents modulo T". Si je note la classe de φ par $[\varphi]$, nous posons alors $[\varphi] \cap [\psi] = [\varphi \wedge \psi]$, etc. Notons aussi que $[\varphi] \subseteq [\psi]$ is et seulement si $T \vdash \varphi \rightarrow \psi$.

De même, si on a un uplet de variable $\bar{v}$, on peut considérer l'algèbre de Boole des formules avec variables libres $\bar{v}$ à équivalence modulo T près.

(4.10) **Idéaux dans les algèbres de Boole**. Un idéal d'une algèbre de Boole $\mathcal{B}$ est un sous-ensemble I tel que
– si $a, b \in I$ alors $a \cup b \in I$.
– si $a \in I$, $b \in \mathcal{B}$ alors $a \cap b \in I$.

On voit donc en particulier que tout idéal non-vide contient $\emptyset$, et qu'un idéal propre ne peut contenir 1. Si I est tel que tout idéal le contenant proprement contient 1, on dira que I est un idéal **maximal**. On a la propriété suivante (exercice): un idéal I est maximal si et seulement si pour tout $a \in \mathcal{B}$, $a \in I \iff (1 \setminus a) \notin I$. (Ce qui est important n'est pas qu'il ne puisse contenir a et $1 \setminus a$, c'est qu'il soit obligé de contenir l'un des deux).

(4.11) **Anneaux de Boole**. Certains d'entre vous ont déja entendu parler des anneaux de Boole: il s'agit d'anneaux unitaires de caractéristique 2, dans lequel tous les éléments sont **idempotents**, c'est à dire satisfont $x^2 = x$. Un tel anneau est forcément commutatif ($(x+y)^2 = x + y = x^2 + y^2 + xy + yx$, d'où $xy + yx = 0$, $xy = yx$).

Si $\mathcal{B}$ est une algèbre de Boole, elle devient un anneau de Boole si l'on pose $ab = a \cap b$ et $a+b = (a \cup b) \setminus (a \cap b)$. Réciproquement, tout anneau de Boole peut être muni d'une structure d'algèbre de Boole en posant $a \cap b = ab$ et $a \cup b = a + b + ab$. Dans l'algèbre de Boole $\mathcal{P}(I)$, l'addition correspond alors à la différence symétrique $A \Delta B = \{i \in A \cup B \mid i \notin A \cap B\}$.

Les notions d'idéaux de $\mathcal{B}$ au sens de l'algèbre de Boole $\mathcal{B}$ et au sens de l'anneau de Boole $\mathcal{B}$ coïncident.

(4.12) Un premier résultat important dit que toute algèbre de Boole est isomorphe à une sous-algèbre de Boole d'un $\mathcal{P}(I)$. La **dualité de Stone** établit une correspondance entre les algèbres de Boole et les espaces Booléens, de la façon suivante.

A un espace topologique X, on associe l'algèbre de Boole $\mathcal{B}(X)$ des ouverts-fermés de X (avec les opérations $\cup$, $\cap$, $\setminus$ évidentes, et $0 = \emptyset$, $1 = X$. Notons que pour cette définition nous n'avons pas besoin que X soit Booléen.)

Réciproquement, si $\mathcal{B}$ est une algèbre de Boole, on définit $X(\mathcal{B})$, l'espace de Stone de $\mathcal{B}$, comme étant l'espace topologique défini de la façon suivante :

Les points de $X(\mathcal{B})$ sont les idéaux maximaux de $\mathcal{B}$ (voir (4.10)). Une base d'ouverts de $X(\mathcal{B})$ est donnée par les ensembles $O_a = \{I \in X(\mathcal{B}) \mid a \notin I\}$ pour $a \in \mathcal{B}$. Notons que chaque O_a est un ouvert-fermé, avec complémentaire O_{1-a}, et que $O_0 = \emptyset$, $O_1 = X$.

Le théorème de Stone dit que le foncteur $\mathcal{B}$ de la catégorie des algèbres de Boole dans celle des espace topologiques Booléens est une dualité, avec foncteur dual le foncteur X. En particulier, si $\mathcal{B}$ est une algèbre de Boole, alors il existe un isomorphisme canonique entre $\mathcal{B}$ et $\mathcal{B}(X(\mathcal{B}))$ $(a \mapsto O_a)$, et si X est un espace Booléen, il existe un homéomorphisme canonique entre X et $X(\mathcal{B}(X))$ $(x \mapsto I_x = \{a \in \mathcal{B}(X) \mid x \notin a\})$.

(4.13) **Remarque**. Soit $\mathcal{B}(T)$ l'algèbre de Boole définie en (4.9). Les points de $X(\mathcal{B}(T))$ correspondent alors aux complétions de T: si T' est une complétion de T, alors $\{[\psi] \mid T' \vdash \neg\psi\}$ est un idéal maximal de $\mathcal{B}(T)$. Et réciproquement.

(4.14) **Exercice**. Soient X un espace Booléen, et $\mathcal{B}$ une algèbre de Boole.

(1) Montrer que l'application $a \mapsto O_a$ définit un isomorphisme entre les algèbres de Boole $\mathcal{B}$ et $\mathcal{B}(X(\mathcal{B}))$.

(2) Montrer que l'application $x \mapsto I_x$ définie ci-dessus définit un homéomorphisme entre X et $X(\mathcal{B}(X))$.

(3) Soient Y un espace Booléen et $f : X \to Y$ une application continue. Montrer que l'application $f^* : \mathcal{B}(Y) \to \mathcal{B}(X)$, $U \mapsto f^{-1}(U)$, définit un homomorphisme d'algèbres de Boole.

(4) Montrer que si f est surjective, alors f^* est un plongement.

(5) Soit $F = f(X)$, et $I(F) = \{a \in \mathcal{B}(Y) \mid a \cap F = \emptyset\}$. Montrer que c'est un idéal de $\mathcal{B}(Y)$, qui égale le noyau de f^*.

(4.15) **Espaces de types**. Soit n un entier, et $A \subset M \models T$.

Soit $S_n(T)$ l'ensemble de tous les types complets étendant la théorie T, et avec variables le n-uplet $\bar{v} = (v_1, \dots, v_n)$. (Le nom des variables n'est pas important, ce qui est important est leur nombre: n). On utilise aussi la notation $S_n(\emptyset)$ au lieu de $S_n(T)$.

Nous définissons une topologie sur $S_n(T)$ de la façon suivante: les ouverts de bases sont $\langle\varphi(\bar{v})\rangle$, où $\varphi(\bar{v}) \in \mathcal{L}$, et

$$\langle\varphi(\bar{v})\rangle = \{p(\bar{v}) \mid S_n(T) \mid p(\bar{v}) \vdash \varphi(\bar{v})\}.$$

On vérifie (grâce au théorème de compacité) que $S_n(T)$ muni de cette topologie est compact séparé.

De même, si $A \subset M \models T$, on dénote par $S_n(A)$ l'ensemble des types complets du langage $\mathcal{L}(A)$ ayant n variables libres et étendant la théorie $Th(M, a)_{a \in A}$. On met aussi la topologie dont les ouverts de bases sont les ouverts $\langle\varphi(\bar{v})\rangle$, où $\varphi(\bar{v})$ est cette fois une formule de $\mathcal{L}(A)$.

Remarque. On pourrait aussi définir cet espace de type comme étant les types maximaux de $\mathcal{L}(A)$ réalisés dans un modèle de T. Le fait que nous n'aurions pas une théorie complète de $\mathcal{L}(A)$ complique beaucoup les choses. Dans la pratique de toute façon, quand on s'intéresse à $S_n(A)$, c'est parce qu'on travaille dans un modèle de T fixé contenant A, et dans les extensions élémentaires de M.

(4.16) Il est clair que si un type partiel $\Sigma(\bar{v})$ est finiment satisfaisable, alors il a une réalisation dans un modèle M de T, c'est à dire un n-uplet $\bar{a}$ d'éléments de M qui satisfait toutes les formules de $\Sigma(\bar{v})$.

Notons aussi que si $\Sigma(\bar{v})$ est un type partiel consistant, alors les types complets étendant $\Sigma(\bar{v})$ sont précisément les éléments du fermé

$$F_\Sigma = \bigcap\{\langle\varphi(\bar{v})\rangle \mid \varphi(\bar{v}) \in \Sigma(\bar{v})\}.$$

(4.17) **Quelques fonctions entre les espaces de types**.

(1) Soient $n \leq m$, et $i(1), \ldots, i(n)$ n éléments distincts de $\{1, \ldots, m\}$. Alors l'application $\pi_i : S_m(T) \to S_n(T)$ définie par

$$p(v_1, \ldots, v_m) \mapsto \{\varphi(v_1, \ldots, v_n) \mid \varphi(v_{i(1)}, \ldots, v_{i(n)} \in p(v_1, \ldots, v_m))\}$$

est continue et surjective.

(2) Une permutation σ de $\{v_1, \ldots, v_n\}$ induit un homéomorphisme de $S_n(T)$, qui au type $p(\bar{v})$ associe le type

$$p^\sigma(\bar{v}) = \{\varphi(v_1, \ldots, v_n) \mid \varphi(v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(n)}) \in p(\bar{v})\}.$$

(3) Soient maintenant $A \subset B \subset M \models T$. Nous avons aussi une application $S_n(B) \to S_n(A)$, appelée la **restriction de** B **à** A, $p(\bar{v}) \mapsto p(\bar{v})|_A$, et définie par $p(\bar{v})|_A = p(\bar{v}) \cap \mathcal{L}(A)$. Cette application est continue et surjective.

(4) Enfin, supposons que $F : A \to B$ soit un isomorphisme partiel élémentaire entre M et N, où M et N sont des modèles de T (donc élémentairement équivalents). Nous obtenons alors un homéomorphisme

$$F^* : S_n(A) \to S_n(B),$$

défini par:

$$p^F = F^*(p(\bar{v})) = \{\varphi(F(a_1), \ldots, F(a_m), \bar{v}) \mid m \in \mathbf{N},\ a_1, \ldots, a_m \in A,\ \text{et } \varphi(a_1, \ldots, a_m, \bar{v}) \in p(\bar{v})\},$$

pour $p = p(\bar{v}) \in S_n(A)$.

(4.18) **Exercice**. Vérifiez que les applications définies en (1) et (3) ci-dessus sont continues, et que celles définies en (2) et (4) sont des homéomorphismes.

(4.19) **Omission de types**. Soit $\Sigma(\bar{v})$ un type (partiel ou complet), et M un modèle de T. On dit que M réalise $\Sigma(\bar{v})$ si M contient une réalisation de $\Sigma(\bar{v})$, i.e., un n-uplet $\bar{a}$ qui satisfait toutes les formules de $\Sigma(\bar{v})$. Sinon, on dit que M **omet** le type $\Sigma(\bar{v})$.

Les points isolés de $S_n(T)$ sont appelés des **types isolés**. Si $p(\bar{v})$ est isolé, il existe donc une formule $\varphi(\bar{v})$ (consistante avec T) telle que $T \cup \varphi(\bar{v}) \vdash p(\bar{v})$. Cette formule $\varphi(\bar{v})$ est appellée la formule **isolant** $p(\bar{v})$. Elle est **complète**, c'est à dire que si $\psi(\bar{v})$ est une formule de $\mathcal{L}$, alors $T \cup \varphi(\bar{v}) \vdash \psi(\bar{v})$, ou bien $T \cup \varphi(\bar{v}) \vdash \neg\psi(\bar{v})$. On remarque que si T est complète un type isolé de $S_n(T)$ ne peut être omis: en effet, si $\varphi(\bar{v})$ est une formule complète isolant ce type, alors $T \vdash \exists\bar{v}\,\varphi(\bar{v})$.

(4.20) **Théorème d'omission des types**. Soit $\mathcal{L}$ un langage **dénombrable**, T une théorie consistante, et $\Sigma(\bar{v})$ un type partiel consistant. Si le fermé $\bigcap\{\langle\varphi(\bar{v})\rangle \mid \varphi(\bar{v}) \in \Sigma(\bar{v})\}$

est d'intérieur vide (c'est à dire, ne contient aucun ouvert non-vide), alors il existe un modèle de T qui omet le type $\Sigma(\bar{v})$.

Démonstration. Nous ferons une construction à la Henkin. Soient $C = \{c_0, c_1, \ldots\}$ un ensemble dénombrable de nouveaux symboles de constantes, et $\mathcal{L}' = \mathcal{L} \cup C$. Soit maintenant $\varphi_0, \varphi_1, \ldots$ une énumération des énoncés de $\mathcal{L}'$ telle que $\varphi_m \in \mathcal{L} \cup \{c_0, \ldots, c_m\}$. Nous allons construire une suite de théories consistantes

$$T_0 \subset T_1 \subset T_2 \cdots$$

telles que:
(1) Chaque T_m est une extension finie de T, $T_m \subset \mathcal{L} \cup \{c_0, \ldots, c_m\}$.
(2) L'une de φ_m, $\neg\varphi_m$ est dans T_{m+1}.
(3) Si $\varphi_m = \exists x\, \psi(x)$ et $\varphi_m \in T_{m+1}$, alors $\psi(c_{m+1}) \in T_{m+1}$.
(4) Si $\bar{c}$ est un n-uplet d'éléments de $\{c_0, \ldots, c_m\}$, il existe une formule $\sigma(\bar{v}) \in \Sigma(\bar{v})$ telle que $\neg\sigma(\bar{c}) \in T_{m+1}$.

Nous posons $T_0 = T$. Supposons que nous ayons défini T_m satisfaisant aux conditions ci-dessus, et écrivons la $T_m = T \cup \{\theta_1, \ldots, \theta_r\}$. Soit W l'ensemble des n-uplets de $\{c_0, \ldots, c_m\}$. Nous voulons trouver des formules $\psi_{\bar{c}}(\bar{v}) \in \Sigma(\bar{v})$ pour chaque $\bar{c} \in W$, telles que $T_m \cup \{\neg\psi_{\bar{c}}(\bar{c}) \mid \bar{c} \in W\}$ est consistante. Supposons que ce ne soit pas le cas. Alors nous avons

$$T \cup \{\theta_1, \ldots, \theta_r\} \vdash \bigvee_{\bar{c} \in W} \Sigma(\bar{c}).$$

Considérons pour un instant les constantes $c_0, \ldots, c_m$ comme des variables. La conjonction infinie $\Sigma(\bar{c})$ définit donc un fermé $F_{\bar{c}}$ de $S_{m+1}(T)$. Ceci nous dit alors que dans $S_{m+1}(T)$, la réunion des fermés $F_{\bar{c}}$, $\bar{c} \in W$, contient un ouvert non-vide (celui défini par la formule $\theta_1 \wedge \cdots \wedge \theta_r$). Cela entraîne qu'il existe $\bar{c} \in W$ tel que $F_{\bar{c}}$, contienne un ouvert non vide. [En effet, la réunion de deux fermés d'intérieur vide est d'intérieur vide: soit U un ouvert contenu dans $F_1 \cup F_2$, et supposons que les intérieurs de F_1 et de F_2 soient vides. Alors $U \cap (X \setminus F_1)$ est un ouvert contenu dans F_2, donc vide. Cela entraîne que $U \subseteq F_1$, et donc que U est vide.] Mais cela contredit notre hypothèse: en effet, l'application $\pi : S_{m+1}(T) \to S_n(T)$ définie en (4.17)(1) est continue et envoie $F_{\bar{c}}$ sur un fermé contenu dans F_Σ, et cela entrainerait que l'image de $F_{\bar{c}}$ dans $S_n(T)$, et donc aussi F_Σ, contiendrait aussi un ouvert, contradiction.

Nous avons donc montré que $T_m \nvdash \bigvee_{\bar{c} \in W} \Sigma(\bar{c})$. Toujours avec notre identification des constantes c_i avec des variables, nous avons alors que l'ouvert-fermé $F = \langle \theta_1 \wedge \cdots \wedge \theta_r \rangle$ de $S_{m+1}(T)$ n'est pas contenu dans la réunion des $F_{\bar{c}}$. Soit $p(c_0, \ldots, c_m) \in F \setminus \bigcup_{\bar{c} \in W} F_{\bar{c}}$, et pour chaque $\bar{c} \in W$, choisissons une formule $\psi_{\bar{c}}(\bar{v})$ telle que $\neg\psi_{\bar{c}}(\bar{c})$ appartienne à $p(c_0, \ldots, c_m)$. Alors $T^1 =_{\text{df}} T_m \cup \{\neg\psi_{\bar{c}}(\bar{c}) \mid \bar{c} \in W\}$ est consistante.

Si $T^1 \cup \{\varphi_m\}$ est consistante, nous définissons $T^2 = T^1 \cup \{\varphi_m\}$, et sinon nous définissons $T^2 = T^1 \cup \{\neg\varphi_m\}$. Enfin, si $\varphi_m = \exists x\ \psi(x) \in T^2$, nous définissons $T_{m+1} = T^2 \cup \{\psi(c_{m+1})\}$, et si φ_m n'est pas de cette forme ou bien si $\neg\varphi_m \in T^2$, alors nous prenons $T_{m+1} = T^2$. Comme la constante c_{m+1} n'apparait pas dans les formules de T^2, la théorie T_{m+1} est consistante. Nous avons défini T_{m+1} de façon à ce qu'elle satisfasse (4), (2) et (3). Elle satisfait évidemment à (1).

Soit $T_\omega = \bigcup_m T_m$. C'est une théorie consistante du langage $\mathcal{L}'$, qui est complète à cause de (2). Soit M un modèle de T_ω, et M_0 le sous-ensemble de M constitué des interprétations des constantes c_i, $i \in \mathbf{N}$.

Assertion. $M_0 \prec M$.

Il est clair que M_0 contient toutes les constantes c_i. Il faut d'abord montrer que c'est une sous-$\mathcal{L}$-structure de M, c'est-à-dire contient toutes les interprétations de constantes de $\mathcal{L}$ et est close par les fonctions de $\mathcal{L}$: notons que si c est un symbole de constante de $\mathcal{L}$, alors l'énoncé $\exists x\, x = c$ est l'un des φ_m, et est impliqué par T, donc appartient à T_{m+1}. Par la condition (3), T_{m+1} contient $c_{m+1} = c$. De même si f est un symbole de fonction n-aire, et $\bar{d}$ est un n-uplet de constantes du langage $\mathcal{L}'$, il existera un entier k tel que $c_k = f(\bar{d}) \in T_k$.

Il reste à montrer que l'inclusion est élémentaire. Soient $\bar{c}$ un uplet d'éléments de M_0, $\varphi(\bar{x}, y)$ une formule de $\mathcal{L}$, et supposons que $M \models \exists y\, \varphi(\bar{c}, y)$. La formule $\exists y\, \varphi(\bar{c}, y)$ est aussi un énoncé de $\mathcal{L}'$, donc égale φ_m pour un certain m. Comme $M \models T_\omega$ et T_ω est complète, $\varphi_m \in T_{m+1}$ (condition (2)), et $\varphi(\bar{c}, c_{m+1}) \in T_{m+1}$ (condition (3)). Nous avons donc montré que si $\bar{c}$ est un uplet d'éléments de M_0, $\varphi(\bar{x}, y)$ une formule de $\mathcal{L}$, et $M \models \exists y\, \varphi(\bar{c}, y)$, alors il existe $b \in M_0$ tel que $M \models \varphi(\bar{c}, b)$. Par le test de Tarski-Vaught, cela montre que $M_0 \prec M$.

Par la condition (4), aucun n-uplet de M_0 ne réalise le type $\Sigma(\bar{v})$.

Remarque. Nous avons utilisé un raccourci. L'autre démonstration, sans raccourci, est la suivante. On quotiente C par la relation d'équivalence E définie par

$$E(c_i, c_j) \iff T_\omega \vdash c_i = c_j$$

et on met une $\mathcal{L}'$-structure sur $M_0 = C/E$ de la façon imposée par T_ω: les symboles de constantes c_i sont interprétés par c_i/E (la classe d'équivalence de c_i pour E). Si $f(x_1, \ldots, x_m)$ est une fonction de $\mathcal{L}$, et $i(1), \ldots, i(m) \in \mathbf{N}$, alors il existe k tel que $T_\omega \vdash f(c_{i(1)}, \ldots, c_{i(m)}) = c_k$, et on définit $f : M_0^m \to M_0$ de façon consistante avec T_ω. De même si R est un symbole de relation ou de constante de $\mathcal{L}$. Grâce à (3), nous avons que $M_0 \models T_\omega$, et (4) entraine que M_0 ne réalise pas le type $\Sigma(\bar{v})$.

Citons maintenant un théorème très important, qui est en fait un corollaire des résultats prouvés ci-dessus.

(4.21) **Théorème**. (Ryll-Nardzewski) Soit T une théorie complète dans un langage $\mathcal{L}$-dénombrable. Alors T est $\aleph_0$-catégorique si et seulement si pour tout entier $n \in \mathbf{N}$, l'espace $S_n(T)$ est fini.

Démonstration. Supposons que T soit $\aleph_0$-catégorique. Alors tous les types de $S_n(T)$ sont réalisés dans tout modèle dénombrable de T. D'après le théorème d'omission des types (4.20), cela entraîne que tous les types de $S_n(T)$ sont isolés (car d'intérieur non vide). Cependant, un espace infini et compact contient nécéssairement des points non-isolés. Chaque $S_n(T)$ doit donc être fini. Cela prouve une direction.

Pour l'autre, soient M et N des modèles dénombrables de T. Nous savons qu'ils sont élémentairement équivalents (car T est complète). Soit $\mathcal{I}$ la famille de tous les isomorphismes partiels élémentaires entre M et N ayant domaine **fini**. Il nous faut montrer que cette famille est non-vide, et a la propriété du va-et-vient.

Tout d'abord $\mathcal{I}$ est non-vide: soit f la fonction avec domaine vide. Comme $M \equiv N$, $f \in \mathcal{I}$. Soit $f \in \mathcal{I}$, et $a \in M$, $a \notin dom(f)$, et écrivons $dom(f) = \{a_1, \ldots, a_n\}$. Comme $S_{n+1}(T)$ est fini, $tp(a_1, \ldots, a_n, a)$ est isolé, et soit $\varphi(x_1, \ldots, x_n, x)$ une formule qui l'isole. Alors $N \models \exists x\, \psi(f(a_1), \ldots, f(a_n), x)$, car f est élémentaire. Soit $b \in N$ tel que $N \models \psi(f(a_1), \ldots, f(a_n), b)$. Alors, puisque $\varphi(x_1, \ldots, x_n, x)$ isole $tp(a_1, \ldots, a_n, a)$, nous avons que $tp_M(a_1, \ldots, a_n, a) = tp_N(f(a_1), \ldots, f(a_n), b)$. Nous étendons f à une fonction g avec domaine $dom(f) \cup \{a\}$ en définissant $g(a) = b$. Alors g est élémentaire.

Cela prouve que notre famille a la propriété du va. La propriété du vient est prouvée de la même façon. Par (3.3), nous avons $M \simeq N$, et donc T est $\aleph_0$-catégorique.

(4.22) **Exercice**. Que peut-on dire sur la théorie T si nous savons que $S_n(T)$ est fini pour tout $n \in \mathbf{N}$? (Nous ne supposons plus que T est complète).

(4.23) **Exercice**. (1) Soit T_1 la théorie des ordres denses sans extrémités. Quelle est la cardinalité de $S_n(T_1)$ pour $n \geq 1$. Quelle est celle de $S_1(\mathbf{Q})$? (Plongez $\mathbf{Q}$ dans $\mathbf{R}$). Exhibez au moins deux types de $S_1(\mathbf{Q})$ qui ne sont pas réalisés dans $\mathbf{R}$. Soit $r \in \mathbf{R} \setminus \mathbf{Q}$. Peut-on trouver $s \neq r$, $s \in \mathbf{R}$, tel que $tp(s/\mathbf{Q}) = tp(r/\mathbf{Q})$?

(2) Soit T_2 la théorie des ordres denses avec extrémités. Quelle est la cardinalité de $S_n(T_2)$ pour $n \geq 1$?

(4.24) **Cardinalité des espaces de types**. Soit $\mathcal{L}$ un langage, T une $\mathcal{L}$-théorie consistante, et $S_n(T)$ les espaces de types associés à T. Soit $\kappa = |\mathcal{L}| + \aleph_0$. Alors, il y κ formules de $\mathcal{L}$, et donc 2^κ sous-ensembles de formules. Cela entraîne que

$$|S_n(T)| \leq 2^\kappa.$$

En particulier, soient M un modèle de T, et $A \subseteq M$. Alors $|S_n(A)| \leq 2^\kappa$, où $\kappa = |\mathcal{L}| + |A| + \aleph_0$. La cardinalité des espaces $S_n(T)$ apporte des information sur la théorie T. Nous avons vu que si T est complète et tous les $S_n(T)$ sont finis alors T est $\aleph_0$-catégorique.

(4.25) **Proposition**. Si $S_n(T)$ est dénombrable, alors les points isolés de $S_n(T)$ sont denses, c'est à dire que tout ouvert non vide de $S_n(T)$ contient un point isolé.

Démonstration. Sinon, nous aurions un ouvert non vide U de $S_n(T)$ ne contenant aucun point isolé. Passant à un sous-ouvert de base de U, nous pouvons supposer que U est un ouvert-fermé. Puisque U ne contient pas de points isolés, il a au moins deux points. Il existe donc des ouverts fermés U_0 et U_1 qui forment une partition de U. Raisonnant de la même façon avec U_0 et U_1, on construit par induction une famille (U_σ) indexée par $2^{<\omega}$ (les suites finies de 0 et de 1), et telle que, pour tout $\sigma \in 2^{<\omega}$, $U_{\sigma^\frown 0}$ et $U_{\sigma^\frown 1}$ partitionnent U_σ. Soit maintenant $\tau \in 2^\omega$. Alors, par compacité, chaque fermé $U_\tau =_{\mathrm{df}} \bigcap\{U_{\tau|_n} \mid n \in \mathbf{N}\}$ est non vide, et donc contient au moins un élément de $S_n(T)$. Cela contredit notre hypothèse que $S_n(T)$ est dénombrable.

(4.26) **Théorème d'omission des types généralisé**. Soient $\mathcal{L}$ un langage **dénombrable**, T une théorie consistante, et pour chaque $r \in \mathbf{N}$ un type partiel Σ_r en les variables $(v_0, \ldots, v_{n(r)})$, où $n(r) \in \mathbf{N}$.

Supposons que pour tout $r \in \mathbf{N}$, le fermé F_{Σ_r} de $S_{n(r)}(T)$ soit d'intérieur non vide. Alors il existe un modèle M de T qui omet tous les types Σ_r.

Démonstration. La démonstration est pratiquement identique à celle de (4.20) : on remplace tout simplement la condition (4) par la condition suivante

(4') Pour tout $r \leq m$, si $\bar{c}$ est un $n(r)$-uplet d'éléments de $\{c_0, \dots, c_m\}$, alors il existe une formule $\sigma(\bar{v}) \in \Sigma_r(\bar{v})$ telle que $\neg\sigma(\bar{c}) \in T_{m+1}$.

La construction de T_{m+1} à partir de T_m est pratiquement identique : posons $N = \sup\{n(r) \mid r = 0, \dots, m\}$. Chaque Σ_r peut être considéré comme un N-type partiel (et son fermé associé sera d'intérieur vide dans $S_N(T)$). On considère alors le type partiel $\Sigma = \bigvee_{r=0}^{m} \Sigma_r$, et on définit T_{m+1} comme dans la démonstration de (4.20). (Notons que Σ est bien (équivalent à) un type, car une disjonction finie de conjonctions infinies est une conjonction infinie de disjonctions finies).

(4.27) Supposons que le langage $\mathcal{L}$ soit dénombrable, et soit T une théorie, que nous supposerons complète.

On peut montrer que si $|S_n(T)| > \aleph_0$, alors $|S_n(T)| = 2^{\aleph_0}$. C'est évident si dans un des $S_n(T)$ les point isolés ne sont pas denses.

Définition. Soit λ un cardinal infini. La théorie T est λ-stable si pour tout modèle M de T, et sous-ensemble A de M de cardinalité $\leq \lambda$, $|S_1(A)| \leq \lambda$.

Notons tout d'abord que l'on peut remplacer $S_1(A)$ par $S_n(A)$ ($n \geq 1$) dans la définition ci-dessus (pourquoi?). Un résultat absolument remarquable a été montré par Shelah:

(4.28) **Théorème**. Soit T une théorie complète dans un langage dénombrable. Alors T satisfait l'une des conditions suivantes:

(1) T est ω-stable, et dans ce cas elle est λ-stable pour tout λ.
(2) T est λ-stable pour tout $\lambda \geq 2^{\aleph_0}$. Dans ce cas on dira que T est **superstable**.
(3) T est λ-stable pour tout cardinal $\lambda = \lambda^{\aleph_0}$. Dans ce cas on dira que T est **stable**.
(4) T n'est λ-stable pour aucun cardinal λ. Nous dirons alors que T est **instable**. Dans ce cas, il existe un modèle M de T, un sous-ensemble infini I de M, et une formule $\varphi(x, y)$ tels que $\{(x, y) \in I^2 \mid M \models \varphi(x, y)\}$ définit une relation d'ordre (linéaire) sur I.

5. Modèles premiers, modèles saturés

(5.1) **Définitions**. Soit M un modèle de T.
(1) M est **atomique** si tout uple fini d'éléments de M réalise un type isolé.
(2) M est **premier** s'il se plonge élémentairement dans tout modèle de T.

Quelques remarques immédiates : par Löwenheim Skolem, un modèle premier est nécéssairement de cardinalité $\leq |\mathcal{L}| + \aleph_0$. De plus, une théorie ayant un modèle premier est complète, puisque deux modèles quelconques ont des sous-structures élémentaires isomorphes.

(5.2) **Conventions**. A partir de maintenant, nous fixons une théorie T **complète**. Attention, nous supposerons souvent que $\mathcal{L}$ est dénombrable.

(5.3) **Proposition**. ($\mathcal{L}$ dénombrable)
(1) Un modèle premier est atomique.
(2) Un modèle atomique dénombrable est premier.
(3) Deux modèles premiers sont isomorphes.

Démonstration. (1) Supposons que le modèle M de T réalise un n-type $p(\bar{v})$ qui ne soit pas isolé. Par le théorème d'omission des types (4.20), il existe un modèle N de T qui ne réalise pas $p(\bar{v})$, et il est certainement impossible que M se plonge élémentairement dans N.

(2) Soient M un modèle atomique dénombrable de T et N un modèle de T. Fixons une énumération $\{a_i \mid i \in \mathbf{N}\}$ de M. Nous voulons trouver $b_i \in N$, $i \in \mathbf{N}$, tels que pour tout $i \in \mathbf{N}$, nous ayons $tp_M(a_0, \ldots, a_i) = tp_N(b_0, \ldots, b_i)$. Supposons que nous ayons déjà trouvé $b_0, \ldots, b_i$, et soit $\varphi(x_0, \ldots, x_{n+1})$ la formule isolant $tp(a_0, \ldots, a_{i+1})$. Alors $M \models \exists y\, \varphi(a_0, \ldots, a_i, y)$; par hypothèse d'induction, $tp_M(a_0, \ldots, a_i) = tp_N(b_0, \ldots, b_i)$, et cela entraîne qu'il existe $b_{i+1} \in N$ tel que $N \models \varphi(b_0, \ldots, b_{i+1})$. Puisque $\varphi(x_0, \ldots, x_{i+1})$ est complète, nous avons bien $tp_M(a_0, \ldots, a_{i+1}) = tp_N(b_0, \ldots, b_{i+1})$.

(3) Soient M et N des modèles premiers de T. Nous savons que M et N sont dénombrables et atomiques (par (1)). La même preuve que celle du théorème de Ryll-Nardzewski (4.21) montre que la famille $\mathcal{I}(M, N)$ des isomorphismes partiels de domaine fini a la propriété du va-et-vient.

(5.4) **Proposition**. ($\mathcal{L}$ dénombrable) La thórie T a un modèle premier si et seulement si pour chaque $n \in \mathbf{N}$, les points isolés sont denses dans $S_n(T)$.

Démonstration. Soit $n \in \mathbf{N}$, et supposons que les points isolés ne soient pas denses dans $S_n(T)$. Il existe donc un ouvert non vide qui ne contient aucun point isolé, et passant à un sous-ouvert, nous pouvons supposer qu'il est de la forme $\langle \varphi(\bar{v}) \rangle$. Mais tout modèle de T contient des n-uplets satisfaisant $\varphi(\bar{v})$ (car T est complète), et aucun de ceux-ci ne satisfait de type isolé. Donc aucun modèle de T n'est atomique, et T ne peut avoir de modèle premier.

(5.5) **Exercice**. Soit T une théorie complète dans un langage dénombrable, et supposez que T est ω-stable (la définition est donnée dans (4.27)). Montrer que si A est un sous-ensemble dénombrable d'un modèle M de T alors il existe $M_0 \prec M$ contenant A, et possédant la propriété suivante: si N est un modèle de $Diag(A)$, alors il existe un $\mathcal{L}(A)$-plongement élémentaire de M_0 dans N. (Un tel modèle est appelé **premier au-dessus de** A). Montrer que cette propriété caractérise M_0 à $\mathcal{L}(A)$-isomorphisme près.

(5.6) **Les indiscernables**. Soit M un modèle de T, A un sous-ensemble de M, et $\bar{a}_i$, $i \in I$, une suite de n-uplets d'éléments de M. Nous supposerons que l'ensemble I est muni d'un ordre total $<$.

On dit que la suite $(\bar{a}_i)_{i\in I}$ est **indiscernable au-dessus de** A si pour tout $m \in \omega$, pour toute formule $\varphi(\bar{v}_1, \ldots, \bar{v}_m)$, et pour toutes suites $i(1) < \cdots < i(m)$ et $j(1) < \cdots < j(m)$ d'éléments de I, nous avons

$$M \models \varphi(\bar{a}_{i(1)}, \ldots, \bar{a}_{i(m)}) \iff M \models \varphi(\bar{a}_{j(1)}, \ldots, \bar{a}_{j(m)}).$$

Nous dirons que la suite $(\bar{a}_i)_{i\in I}$ est **totalement indiscernable au-dessus de** A si pour tout $m \in \omega$, pour toute formule $\varphi(\bar{v}_1, \ldots, \bar{v}_m)$, si $\{i(1), \ldots, i(m)\}$ et $\{j(1), \ldots, j(m)\}$ sont deux sous-ensembles de I de cardinalité m, alors

$$M \models \varphi(\bar{a}_{i(1)}, \ldots, \bar{a}_{i(m)}) \iff M \models \varphi(\bar{a}_{j(1)}, \ldots, \bar{a}_{j(m)}).$$

Attention. Certains auteurs utilisent une autre terminologie : ce qu'ils appellent *indiscernable* est ce que nous appelons *totalement indiscernable*, et ils appellent *ordre-indiscernable*, ou bien *indiscernable dans l'ordre* ce que nous avons appelé indiscernable.

(5.7) En fait, la propriété démontrée dans (5.5) est vraie pour les théories ω-stables sans restriction de cardinalité sur A: il existe un modèle premier sur A, et il est unique à A-isomorphisme près. La preuve est bien plus compliquée dans le cas général, et utilise la notion de **rang de Morley**. On peut en trouver une démonstration dans le livre de G. Sacks, *Saturated model Theory.* Ce modèle premier M_0 est caractérisé par les deux propriétés suivantes: M_0 est atomique au-dessus de A, et toute suite de uplets (finis) de M_0 qui est indiscernable au-dessus de A est au plus dénombrable.

(5.8) **Définitions**. Soient κ un cardinal (infini), et M un modèle de T.
(1) On dit que M est **κ-saturé** si pour tout sous-ensemble A de M de taille $< \kappa$, tout 1-type sur M est réalisé dans M.
(2) On dit que M est **saturé** s'il est $|M|$-saturé.
(3) On dit que M est **κ-universel** si tout modèle de T de taille $< \kappa$ se plonge élémentairement dans M.
(4) On dit que M est **κ-homogène** si la famille $\mathcal{I}_\kappa(M.M)$ des isomorphismes partiels élémentaires (entre M et M) de domaine de taille $< \kappa$ a la propriété du va-et-vient.
(5) On dit que M est saturé (resp. homogène, universel) s'il est $|M|$-saturé (resp. $|M|$-homogène, $|M|$-universel).

Remarque. Soient $\lambda < \kappa$ des cardinaux infinis. Alors la κ-saturation entraîne la λ-saturation, la κ-homogénéité la λ-homogénéité, et la κ-universalité la λ-universalité.

(5.9) **Exercice**. (1) Pourquoi M ne peut-il être $|M|^+$-saturé?

(2) Montrez que si M est κ-saturé, et $n \in \mathbf{N}$, $A \subset M$ est un sous-ensemble de taille $< \kappa$, alors tout n-type sur A est réalisé dans M.

(3) Montrez que si M est κ-saturé, alors M est κ^+-universel.

(5.10) **Théorème**. Les conditions suivantes sont équivalentes pour un modèle (infini) M de T, et un cardinal infini κ :
(1) M est κ-saturé.
(2) M est κ^+-universel et κ-homogène.
(3) M est κ-universel et κ-homogène.

Démonstration. (1) $\to$ (2) La démonstration que la κ-saturation entraîne la κ^+-universalité est laissée en exercice. Soient $\mathcal{I}_\kappa(M,M)$ l'ensemble des isomorphismes partiels élémentaires de domaine de taille $< \kappa$, $f \in \mathcal{I}_\kappa(M,M)$, et $a \in M$. Soient $p(v) = tp(a/dom(f))$, et $p^f(v)$ son image par f (voir (4.17)). Comme f est élémentaire, nous savons que $p^f(v)$ est un type consistant sur $Im(f)$. Par κ-saturation, $p^f(v)$ esr réalisé dans M par un élément b. Alors, l'application g qui étend f et envoie a sur b est un isomorphisme partiel élémentaire, donc dans $I_\kappa(M,M)$.

(2) $\to$ (3) est évident. (3) $\to$ (1). Soit M un modèle de T qui est κ-saturé et κ^+-universel, et soit $A \subset M$, $|A| < \kappa$, et $p(v) \in S_1(A)$. Nous savons qu'il existe un modèle N de T de taille $< \kappa$, contenant A et contenant une réalisation b de p. Par κ-universalité de M, il existe un plongement élémentaire $f : N \to M$. La restriction de f à A est un élément de $\mathcal{I}_\kappa(M,M)$, et par κ-homogénéité, il existe $g \in \mathcal{I}(M,M)$ prolongeant $f|_A$ et ayant b dans son image. Alors $g^{-1}(b)$ realise $p(v)$.

(5.11) Remarquons d'abord que la condition de κ-homogénéité pour un modèle M de T, peut être réécrite de la façon suivante:

Si $\lambda < \kappa$ et $(a_\alpha)_{\alpha<\lambda}$ et $(b_\alpha)_{\alpha<\lambda}$ sont deux suites telles que

$$(M, a_\alpha)_{\alpha<\lambda} \equiv (M, b_\alpha)_{\alpha<\lambda}$$

et si $a \in M$ alors il existe $b \in M$ tel que

$$(M, a_\alpha, a)_{\alpha<\lambda} \equiv (M, b_\alpha, b)_{\alpha<\lambda}.$$

En effet, dire que $(M, a_\alpha)_{\alpha<\lambda} \equiv (M, b_\alpha)_{\alpha<\lambda}$ est tout simplement dire que l'application f qui envoie a_α sur b_α pour tout $\alpha < \lambda$, est un isomorphisme partiel élémentaire.

Lemme. Soit M un modèle κ-homogène. Supposons que pour chaque ordinal $\alpha < \kappa$ nous ayons une suite $a^\alpha = (a^\alpha_\xi)_{\xi<\alpha}$ d'éléments de M satisfaisant, pour tout $\alpha < \beta < \kappa$:

$$(M, a^\alpha_\xi)_{\xi<\alpha} \equiv (M, a^\beta_\xi)_{\xi<\alpha}.$$

Alors il existe une suite $(a_\xi)_{\xi<\kappa}$ telle que pour tout $\alpha < \kappa$ nous ayons

$$(M, a^\alpha_\xi)_{\xi<\alpha} \equiv (M, a_\xi)_{\xi<\alpha}.$$

Autrement dit, nous pouvons "recoller" les suites a^α en une suite de longueur κ.

Démonstration. Nous construisons la suite a_ξ par induction. Supposons que nous ayons construit a_ξ pour $\xi < \alpha$ satisfaisant

$$(M, a_\xi)_{\xi<\alpha} \equiv (M, a^\alpha_\xi)_{\xi<\alpha}. \qquad (*)$$

(Par exemple, nous pouvons démarrer avec a^α). Nous voulons ajouter un élément a_α à notre suite. Par hypothèse, $(M, a^\alpha_\xi)_{\xi<\alpha} \equiv (M, a^{\alpha+1}_\xi)_{\xi<\alpha}$. Par hypothèse d'induction et par κ-homogénéité, il existe donc $a_\alpha \in M$ tel que $(M, a_\xi)_{\xi\leq\alpha} \equiv (M, a^{\alpha+1}_\xi)_{\xi\leq\alpha}$.

Cela prouve que nous pouvons toujours rajouter un élément à notre suite. On vérifie sans peine que si β est un ordinal limite, et la suite $(a_\xi)_{\xi<\beta}$ a été construite de façon que $(a_\xi)_{\xi<\alpha}$ satisfasse $(*)$ pour tout $\alpha < \beta$, alors , alors $(M, a_\xi)_{\xi<\beta} \equiv (M, a^\beta_\xi)_{\xi<\beta}$. Cela démontre le lemme.

(5.12) **Lemme**. Soient M et N des modèles de T, κ un cardinal tels que:
(i) N est κ-homogène.
(ii) Pour tout $n \in \omega$, tout n-type réalisé dans M est réalisé dans N.
Alors si A est un sous-ensemble de M de taille $\leq \kappa$, il existe un isomorphisme partiel élémentaire $f : M \to N$ de domaine A.

Démonstration. La démonstration est par induction sur la cardinalité λ de A. Si A est fini, c'est évident (par hypothèse, il existe $B \subset N$ réalisant $tp(A/\emptyset)$).

Nous allons donc supposer le résultat montré pour tout sous-ensemble de M de cardinalité inférieure à λ, et en déduire le résultat pour λ. (Attention, les α et ξ ci-dessous sont des ordinaux ; on considère λ aussi en tant qu'ordinal)

Nous savons que N est λ-homogène. Soit $(a_\xi)_{\xi<\lambda}$ une énumération de A. Par hypothèse d'induction, si $\alpha < \lambda$, il existe un isomorphisme partiel élémentaire f_α de M dans N avec domaine $A_\alpha = \{a_\xi \mid \xi < \alpha\}$. Par définition d'un isomorphisme partiel élémentaire, et comme $A_\alpha \subset A_\beta$ si $\alpha < \beta$, les suites b^α pour $\alpha < \lambda$, définies par

$$b^\alpha_\xi = f_\alpha(a_\xi) \qquad \text{pour } \xi < \alpha,$$

satisfont l'hypothèse de (5.11). Il existe donc une suite $b = (b_\xi)_{\xi<\lambda}$ telle que

$$(N, b^\alpha_\xi)_{\xi<\alpha} \equiv (N, b_\xi)_{\xi<\alpha}$$

pour tout $\alpha < \lambda$ et pour tout $\xi < \alpha$. L'application f définie par $f(a_\xi) = b_\xi$ est alors un isomorphisme partiel élémentaire.

(5.13) **Exercice**. (1) Soient M et N des modèles de T qui sont κ-saturés. Montrer que la famille $\mathcal{I}_\kappa(M, N)$ d'isomorphismes partiels élémentaires de domaine de taille $< \kappa$ satisfait la propriété du va-et-vient.

(2) Supposons maintenant que M et N sont κ-homogènes, et que pour tout $n \in \mathbf{N}$, ils réalisent les mêmes types de $S_n(T)$. Montrer qu'ils satisfont aussi la conclusion de (1).

(3) Supposons que M et N satisfont l'hypothèse de (2), et qu'ils sont de cardinalité κ. Montrez qu'ils sont isomorphes.

(4) En déduire que si M est κ-homogène de cardinalité κ, alors tout automorphisme élémentaire partiel de domaine de taille $< \kappa$ s'étend à un automorphisme de M.

(5) Déduire de (3) que deux modèles saturés de T de même cardinalité sont isomorphes.

(5.14) **Construction de modèles κ-saturés**. Soit κ un cardinal infini, que nous supposerons plus grand ou égal à la cardinalité de $\mathcal{L}$. Nous allons montrer que tout modèle M de cardinalité $\leq 2^\kappa$ a une extension élémentaire κ^+-saturée de cardinalité $\leq 2^\kappa$.

Nous allons construire une suite M_ξ, $\xi < 2^\kappa$, telle que

(1) Si $\xi < \lambda < 2^\kappa$, alors $M_\xi \prec M_\lambda$, et $|M_\xi| \leq 2^\kappa$.

(2) Si $\xi < \lambda < 2^\kappa$ et $A \subset M_\xi$ est de taille $\leq \kappa$, alors tout type de $S_1(A)$ est réalisé dans M_λ.

Etape successeur. Supposons M_ξ construit. Alors M_ξ a au plus $|M_\xi|^\kappa \leq (2^\kappa)^\kappa = 2^\kappa$ sous-ensembles A de cardinalité $\leq \kappa$. Pour chaque tel A, $|S_1(A)| \leq 2^{|A|} = 2^\kappa$. Donc M_ξ a une extension élémentaire $M_{\xi+1}$ de taille $\leq 2^\kappa 2^\kappa = 2^\kappa$ satisfaisant (2). [Voici le détail du raisonnement : vous prenez une énumération $\{p_\alpha(x) \mid \alpha < 2^\kappa\}$ de tous les types que nous devons réaliser. Vous rajoutez à $\mathcal{L}(M_\xi)$ une collection de nouvelles constantes c_α pour $\alpha < 2^\kappa$, puis vous considérez la théorie $Diag(M_\xi) \cup \{p_\alpha(c_\alpha) \mid \alpha < 2^\kappa\}$. Comme cette théorie est consistante, elle a un modèle M'. Comme $M' \models Diag(M_\xi)$ on peut supposer que le réduit de M' à $\mathcal{L}$ est une extension élémentaire de M_ξ. D'autre part M' réalise tous les types $p_\alpha(x_\alpha)$. Par le théorème de Löwenheim-Skolem, il existe une sous-structure élémentaire $M_{\xi+1}$ de M' qui contient M_ξ ainsi que les réalisations des types p_α, et qui est de cardinalité $\leq 2^\kappa$.]

Etape limite. Soit λ un ordinal limite, et tous les M_ξ, $\xi < \lambda$ ont déjà été construits, nous définissons $M_\lambda = \bigcup_{\xi<\lambda} M_\xi$. C'est bien une extension élémentaire de chaque M_ξ, $\xi < \lambda$. (2) est évident : si $\xi < \lambda$, et $A \subset M_\xi$ est de cardinalité $\leq \kappa$, alors tout type de $S_1(A)$ est réalisé dans $M_{\xi+1}$, et donc dans M_λ.

Considérons $M^* = M_{2^\kappa}$, et soit $A \subset M^*$ de taille $\leq \kappa$. Comme la cofinalité de 2^κ est plus grande que κ (voir ci-dessous), il existe $\lambda < 2^\kappa$ tel que $A \subset M_\lambda$. Alors tout type sur A est réalisé dans $M_{\lambda+1}$, et donc aussi dans M^*.

(5.15) **Rappels sur les cofinalités d'ordinaux ou de cardinaux**. Soit γ un ordinal. On appelle cofinalité de γ, notée $cf(\gamma)$, le plus petit cardinal λ tel qu'il existe un sous-ensemble X de γ de cardinalité λ qui soit cofinal dans γ, c'est à dire qui satisfasse: pour tout $\alpha < \gamma$, il existe $\beta \in X$, $\beta \geq \alpha$.

Notons tout de suite que la cofinalité d'un ordinal successeur est 1: si $\gamma = \delta + 1$, on prend $X = \{\delta\}$. Donc ça n'a d'intérêt que si γ est un ordinal limite.

Il existe une définition équivalente: $cf(\gamma)$ est le plus petit cardinal λ tel qu'il existe une fonction $f : \lambda \to \gamma$, dont l'image est cofinale dans γ. Pour prouver l'équivalence des deux définitions, on remarque tout simplement qu'un ensemble de cardinalité λ est un ensemble qui est en bijection avec κ.

(5.16) **Exemples**. $cf(\omega) = \omega$; $cf(\omega^2) = \omega$; $cf(\aleph_\alpha) = \aleph_\alpha$ is α est un ordinal successeur, et $cf(\alpha)$ sinon. En fait, si κ est un cardinal infini, alors $cf(\kappa^+) = \kappa^+$. Un cardinal κ satisfaisant $cf(\kappa) = \kappa$ est appelé **régulier**, et sinon il est appelé **singulier**.

Lemme. Soit κ un cardinal infini. Alors $cf(2^\kappa) > \kappa$.

Démonstration. Il suffit de montrer que si λ est un cardinal infini alors $\lambda^{cf(\lambda)} > \lambda$. En effet, supposons que nous ayons montré cette assertion. Alors, prenant $\lambda = 2^\kappa$, on obtient

$(2^\kappa)^{cf(2^\kappa)} > 2^\kappa$. Mais d'autre part nous savons que $(2^\kappa)^\kappa = 2^{\kappa\times\kappa} = 2^\kappa$. Nous ne pouvons donc avoir $cf(2^\kappa) \leq 2^\kappa$, ce qui entraîne $cf(2^\kappa) > \kappa$.

Il nous reste à montrer l'assertion. Fixons une application $f : cf(\lambda) \to \lambda$ dont l'image est cofinale en λ, et soit $g : \lambda \to \lambda^{cf(\lambda)}$ une application injective. Nous pensons à $\lambda^{cf(\lambda)}$ comme à l'ensemble des fonctions $cf(\lambda) \to \lambda$. Nous allons construire une fonction $h : cf(\lambda) \to \lambda$ qui ne peut être de la forme $g(\alpha)$ pour $\alpha < \lambda$. Cela montrera que la fonction g ne peut être surjective, et donc que $\lambda < \lambda^{cf(\lambda)}$. L'argument est un argument de diagonalisation.

Pour chaque $\alpha < cf(\lambda)$, on considère l'ensemble $X(\alpha) = \{g(\gamma)(\alpha) \mid \gamma < f(\alpha)\}$. Comme $\alpha < cf(\lambda)$, on a $|X(\alpha)| < \lambda$, et d'autre part $X(\alpha) \subset \lambda$. C'est donc un sous-ensemble propre de λ, et nous posons $h(\alpha)$ comme étant le plus petit élément de λ qui n'est pas dans $X(\alpha)$.

Nous allons montrer que $h \neq g(\beta)$ pour tout $\beta < \lambda$. Soit $\beta < \lambda$, et prenons $\alpha \in cf(\lambda)$ tel que $f(\alpha) > \beta$. Alors, par définition, $h(\alpha) \notin X(\alpha)$, et d'autre part $g(\beta)(\alpha) \in X(\alpha)$: nous avons donc $h(\alpha) \neq g(\beta)(\alpha)$, c'est à dire $h \neq g(\beta)$.

(5.17) **Constructions de modèles ω-saturés**. Nous supposons que $\mathcal{L}$ est dénombrable. S'il existe n tel que $S_n(T)$ ne soit pas dénombrable, alors nous avons vu que $|S_n(T)| = 2^{\aleph_0}$. Cela entraîne facilement que tout modèle ω-saturé de T est de cardinalité au moins $2^{\aleph_0}$. Et par le résultat précédent il en existe un de cardinalité $2^{\aleph_0}$.

Théorème. Supposons que $S_n(T)$ soit dénombrable pour tout $n \in \omega$. Alors T a un modèle saturé dénombrable.

Démonstration. Nous allons construire une suite M_i, $i \in \omega$, de modèles dénombrables de T, telle que

(1) $M_i \prec M_{i+1}$ pour tout i.

(2) Si $A \subset M_i$ est fini, alors tout type de $S_1(A)$ est réalisé dans M_{i+1}.

On prend pour M_0 un modèle dénombrable de T. Supposons M_i construit. Alors M_i a $\aleph_0$ sous-ensembles finis A. De plus, si A est fini, alors $S_1(A)$ est dénombrable: soit $m = |A|$, et $p(\bar{v})$ le m-type réalisé par A. Alors tout type $q(x) \in S_1(A)$ produit un $(m+1)$-type $p(\bar{v}) \cup q'(\bar{v}, x)$, obtenu en remplaçant les éléments de A par la variable correspondante. Il est clair que l'application $q \mapsto q'$ est injective, et donc $|S_1(A)| \leq |S_{m+1}(T)| \leq \aleph_0$.

Nous avons donc $\aleph_0$ sous-ensembles finis A de M_i, et chacun de ces sous-ensembles finis produit au plus $\aleph_0$-types que nous devons réaliser. Il existe donc une extension élémentaire M_{i+1} de M_i qui les réalise tous et est dénombrable.

Nous prenons maintenant $M_\omega = \bigcup M_i$. Alors M_ω est dénombrable, et l'on prouve facilement qu'il est ω-saturé.

Remarque. La même démonstration montre que si T est κ-stable, si κ est un cardinal régulier tel que l'ensemble $\mathcal{P}_\kappa(\kappa)$ des parties de κ de cardinalité $< \kappa$ soit de cardinalité κ, alors T a un modèle saturé de cardinalité κ.

(5.18) **Théorème**. Supposons que $\mathcal{L}$ est dénombrable, et que la théorie (complète) T n'est pas $\aleph_0$-catégorique. Alors T a au moins 3 modèles dénombrables de T non-isomorphes.

Démonstration. S'il existe n tel que $S_n(T)$ ne soit pas dénombrable, alors T a $2^{\aleph_0}$ modèles dénombrables non-isomorphes (puisqu'un modèle dénombrable ne peut réaliser qu'un nombre dénombrable de types). Nous pouvons donc supposer que $S_n(T)$ est dénombrable pour tout n. Alors T a modèle premier M_0 ((5.4)), et un modèle saturé dénombrable M_1 ((5.17)). Fixons n tel que $S_n(T)$ soit infini (il en existe un puisque T n'est pas $\aleph_0$-catégorique, cf (4.21)). Nous savons que $S_n(T)$ contient un type $p(\bar{v})$ qui n'est pas isolé, et n'est donc pas réalisé dans M_0 (par (5.3)). Donc M_0 et M_1 ne sont pas isomorphes. Nous avons donc montré que si T n'est pas $\aleph_0$-catégorique, alors un modèle premier de T n'est pas ω-saturé.

Soit maintenant un n-uplet $\bar{c}$ de nouvelles constantes, $\mathcal{L}' = \mathcal{L} \cup \{\bar{c}\}$, et $T' = T \cup p(\bar{c})$. Alors T' est complète. De plus $S_m(T')$ est dénombrable pour tout m (car homéomorphe à un fermé de $S_{n+m}(T)$). Comme $S_m(T)$ n'est pas fini pour $m \geq n$, cela entraîne que $S_m(T')$ n'est pas fini non plus, et donc que T' n'est pas $\aleph_0$-catégorique. Puisque M_1 est ω-saturé, il contient une réalisation $\bar{a}$ de $p(\bar{v})$, et nous pouvons donc étendre M_1 en un modèle de T', en interprétant $\bar{c}$ par $\bar{a}$. On vérifie aisément que la $\mathcal{L}'$-structure $(M_1, \bar{a})$ est ω-saturée. Soit N le modèle premier de T' (qui existe par (5.4)). Comme T' n'est pas $\aleph_0$-catégorique, N n'est pas isomorphe à M_1 (en tant que $\mathcal{L}'$-structure) par ce que nous avons montré plus haut. Cela entraîne que le réduit N_0 de N à $\mathcal{L}$ ne peut être isomorphe à M_1 : sinon, on aurait que N est un modèle saturé dénombrable de T' et donc isomorphe à $(M_1, \bar{a})$.

Donc les modèles dénombrables M_0, M_1 et N_0 sont deux-à-deux non-isomorphes.

(5.19) **Clôture algébrique, clôture définissable.** Soit A un sous-ensemble d'un modèle M de T.

(1) Soit $p(\bar{v}) \in S_n(A)$. On dit que $p(\bar{v})$ est **algébrique** si dans toute extension élémentaire N de M, le type $p(\bar{v})$ n'a qu'un nombre fini de réalisations.

(2) Un uplet d'éléments de M est **algébrique** sur A si son type sur A est algébrique. L'ensemble des éléments de M algébriques sur A est noté $acl(A)$.

(3) Soit $p(\bar{v}) \in S_n(A)$. On dit que $p(\bar{v})$ est définissable si dans tout extension élémentaire N de M, le type $p(\bar{v})$ n'a qu'**une** réalisation. Un uplet déléments de M est **définissable** sur A si son type sur A est définissable. L'ensemble des éléments de M qui sont définissables sur A est noté $dcl(A)$.

(5.20) **Remarque**. Soit $\bar{a} = (a_1, \dots, a_n)$. On montre aisément que $\bar{a}$ est algébrique sur A si et seulement si chaque a_i l'est, et de même pour définissable.

(5.21) **Proposition**. Les conditions suivantes sont équivalentes, pour A un sous-ensemble du modèle M de T et $p(\bar{v}) \in S_n(A)$:

(i) $p(\bar{v})$ est algébrique.

(ii) Il existe une extension élémentaire N de M qui est $(|A| + |\mathcal{L}| + \aleph_0)^+$-saturée, et dans laquelle $p(\bar{v})$ n'a qu'un nombre fini de réalisations.

(iii) Il existe une formule $\varphi(\bar{v})$ qui isole $p(\bar{v})$ et un entier m tels que $Diag(A) \models \exists^{\leq m} \bar{v}\, \varphi(\bar{v})$.

(iv) Il existe une formule $\varphi(\bar{v}) \in p(\bar{v})$ et un entier m tels que $Diag(A) \models \exists^{\leq m} \bar{v}\, \varphi(\bar{v})$.

Démonstration. Les implications (i)$\rightarrow$(ii), (iii)$\rightarrow$(iv) et (iv)$\rightarrow$(i) sont immédiates.

Supposons (ii). Soit $\{\bar{c}_i \mid i \in \omega\}$ une collection dénombrable de nouvelles constantes, chaque $\bar{c}_i$ étant un n-uplet. Nous allons montrer que la théorie $Diag(A) \cup \{p(\bar{c}_i) \mid i \in \omega\} \cup \{\bar{c}_i \neq \bar{c}_j \mid i < j < \omega\}$ est inconsistante. Sinon, elle aurait un modèle M_1', que nous pouvons supposer de cardinalité $\leq |A| + \aleph_0$. Le réduit M_1 de M_1' à $\mathcal{L}(A)$ est donc un modèle de $Diag(A)$ contenant une infinité de réalisations distinctes de $p(\bar{v})$. Par l'hypothèse de saturation de N, il existe donc un plongement élémentaire de la $\mathcal{L}(A)$-structure M_1 dans

N. Cela entraîne que N lui aussi contient une infinité de réalisations distinctes de $p(\bar{v})$ et contredit notre hypothèse.

Par compacité, il existe donc un entier m, et une formule $\varphi(\bar{v}) \in p(\bar{v})$ telle que

$$Diag(A) \cup \{\varphi(\bar{c}_0), \ldots, \varphi(\bar{c}_m)\} \vdash \bigvee_{0 \leq i < j \leq m} \bar{c}_i = \bar{c}_j.$$

Donc en particulier,

$$Diag(A) \vdash \exists^{\leq m} \bar{v}\, \varphi(\bar{v}).$$

Nous avons donc montré (iv). Il reste donc à montrer que (iv) entraîne (iii). Par hypothèse, l'ouvert $\langle \varphi(\bar{v}) \rangle$ de $S_n(A)$ ne contient qu'un nombre fini de points (au plus m, puisque $\varphi(\bar{v})$ a au plus m réalisations). Donc tous ses points sont isolés. Comme $p(\bar{v})$ est l'un de ces points, il est isolé par une formule $\psi(\bar{v})$, qui entraîne $\varphi(\bar{v})$, et a donc encore moins de réalisations que $\varphi(\bar{v})$.

(5.22) **Lemme**. Soit A un sous-ensemble d'un modèle M de T. On supposera M suffisamment saturé (c'est à dire: $(|A| + |\mathcal{L}| + \aleph_0|^+$-saturé).

(1) Si $a \in acl(A)$, alors il existe un sous-ensemble fini A_0 de A tel que $a \in acl(A_0)$.

(2) $acl(acl(A)) = acl(A)$, $dcl(dcl(A)) = dcl(A)$.

Démonstration. (1) est clair par la condition (iii) de (5.21). Soit maintenant $b \in acl(acl(A))$. Par (1), il existe un uplet fini $\bar{a}$ d'éléments de $acl(A)$ tel que $b \in acl(\bar{a})$. On montre facilement maintenant que $tp(b, \bar{a}/A)$ n'a qu'un nombre fini de réalisations dans M: en effet, soit $(b', \bar{a}')$ réalisant $tp(b, \bar{a})$. Alors $\bar{a}'$ appartient à l'ensemble fini D des réalisations de $tp(\bar{a}/A)$. De plus il existe un isomorphisme partiel élémentaire f de M qui laisse A fixé et envoie $\bar{a}$ sur $\bar{a}'$. Comme $tp(b/\bar{a})$ n'a qu'un nombre fini de réalisations, de même, l'image q par f de $tp(b/\bar{a})$ n'a qu'un nombre fini de réalisations. Or b' realise q. Cela montre bien que $tp(b, \bar{a})$ est algébrique.

Il existe une autre preuve qui utilise plus (5.21)(iii): soient $\varphi(\bar{v}) \in \mathcal{L}(A)$ la formule isolant $tp(\bar{a}/A)$, et n le nombre de réalisations distinctes de $\varphi(\bar{v})$; soient de plus $\psi(x, \bar{v}) \in \mathcal{L}$ telle que $\psi(x, \bar{a})$ isole $tp(b/\bar{a})$, et m le nombre de ses réalisations. Alors la formule $\varphi(\bar{v}) \wedge \psi(x, \bar{v})$ est réalisée par $(b, \bar{a})$ et a au plus nm réalisations dans M. En fait cette formule isole $tp(b, \bar{a}/A)$.

(5.23) **Retour sur les indiscernables**. Soit $(I, <)$ un ensemble ordonné sans dernier élément, $A \subset M \models T$, et $\bar{a}_i$, $i \in I$ une suite indiscernable au-dessus de A. S'il existe $i(1) < \cdots < i(n)$ tels que $tp(\bar{a}_{i(n)}/A, \bar{a}_{i(1)}, \ldots, \bar{a}_{i(n-1)})$ soit algébrique, alors tous les $\bar{a}_i$ sont égaux.

Démonstration. La formule $\varphi(\bar{x}, \bar{a}, \bar{a}_{i(1)}, \ldots, \bar{a}_{i(n-1)})$ isolant $tp(\bar{a}_{i(n)}/A, \bar{a}_{i(1)}, \ldots, \bar{a}_{i(n-1)})$ est satisfaite par tous les uplets $\bar{a}_j$ avec $j > i(n-1)$, et donc par une infinité d'éléments de la suite $\bar{a}_i$, $i \in I$ (puisque I n'a pas de dernier élément). Comme d'autre part elle est satisfaite seulement par un ensemble fini (puisqu'elle isole un type algébrique), cela entraîne qu'il existe $i \neq j \in J$ tels que $\bar{a}_i = \bar{a}_j$. Mais par indiscernabilité, nous avons alors $\bar{a}_i = \bar{a}_j$ pour tous $i, j \in I$.

(5.24) **Exemple 1**. Considérons la théorie des ordres denses sans extrémités. Puisqu'elle est $\aleph_0$-catégorique, tous ses modèles dénombrables sont premiers et $\aleph_0$-saturés.

Soit $(I,<)$ un modèle quelconque. Puisque T est $\aleph_0$-catégorique, I est ω-saturé (exercice). Cependant, pour qu'il soit $\aleph_1$-satureé, il faut par exemple que si A et B sont des sous-ensembles dénombrables tels que $A < B$ (c'est à dire, pour tout $a \in A$ et $b \in B$, $a < b$) il existe c tel que $A < c < B$. Notez qu'on permet à l'un de A ou B d'être vide.

En particulier $(\mathbf{R},<)$ n'est pas $\aleph_1$-saturé: prenons $A = \{0\}$ et $B = \{1/n \mid n \in \mathbf{N}^{>0}\}$. De même le type $\{x > n \mid n \in \mathbf{N}\}$ n'est pas réalisé.

On montre aussi que si $A \subset I$, alors $acl(A) = A$: en effet, soit $a \in acl(A)$; par (5.22), on peut supposer que A est fini. Ecrivons $A = \{a_1, \dots, a_n\}$ où $a_1 < \cdots < a_n$. Si $a \notin A$, alors a est dans l'un des intervalles $(-\infty, a_1[,]a_1, a_2[, \dots,]a_n, +\infty)$, et tout élément b qui est dans le même intervalle que a réalise $tp(a/A)$.

Soit $C \subset I$ ayant la propriété que si $a \in C$ et $b < a$, alors $b \in C$. (J'appelle C une coupure). A C on associe le type (complet sur I) défini par:

$$Diag(I) \cup \{x < a \mid a \in C\} \cup \{x > b \mid b \notin C\}.$$

Ce type n'est pas réalisé dans I. Si on peut trouver des sous-ensembles C_0 de C et D_0 de $I \setminus C$ de cardinalité $< |I|$ tels que C_0 est cofinal en C, et D_0 est co-initial en $I \setminus C$, alors I ne peut être saturé. En fait la saturation de $(I,<)$ implique des conditions sur sa cardinalité.

(5.25) **Exemple 2**. Soit T la théorie des groupes divisibles abéliens sans torsion. Nous savons qu'elle est catégorique en tout cardinal $> \aleph_0$, et cela implique que ses modèles non-dénombrables sont saturés. (En fait, ceci nécéssite une démonstration, que nous ne donnerons pas. On peut aussi montrer à la main que ses modèles non-dénombrables sont saturés).

Le modèle premier de cette théorie est $\mathbf{Q}$, et son modèle dénombrable saturé est $\mathbf{Q}^{(\aleph_0)}$ (somme directe de $\aleph_0$-copies de $\mathbf{Q}$).

Soit κ un cardinal infini, et M le group $\mathbf{Q}^{(\kappa)}$. Nous savons donc que M est saturé, de cardinalité κ. Soit A un sous-ensemble de M de taille $< \kappa$. Alors $dcl(A)$ contient le sous-groupe $\langle A \rangle$ de M engendré par les éléments de A (ceci est vrai pour tout groupe).

De plus, nous savons que M s'étend uniquement en un espace vectoriel sur $\mathbf{Q}$: en effet, si $a \in M$, et $m \in \mathbf{Z}$, $n \in \mathbf{N}^{>0}$, alors l'élément défini par l'équation $nx = ma$ est unique (parce que M est sans torsion). Cela entraîne que la clôture définissable de A contient en fait le $\mathbf{Q}$-sous-espace vectoriel de M engendré par A. Notons cet ensemble (qui est bien sûr un sous-groupe de M) par $V(A)$.

Nous allons maintenant montrer que $acl(A) = V(A)$. Soit $a \in M$, $a \notin V(A)$, et soit $b \in M$, $b \notin V(A)$. Alors $V(A) \cap V(b) = (0) = V(A) \cap V(a)$. Il existe donc un automorphisme f de l'espace vectoriel M qui fixe $V(A)$ et envoie a sur b. Cet automorphisme est certainement un automorphisme de groupe, et nous avons donc $tp(a/A) = tp(b/A)$. Donc tout élément de $M \setminus V(A)$ réalise le même type sur A que a, ce qui prouve que ce type ne peut être algébrique (puisque $M \setminus V(A)$ est infini).

(5.26) **Exemple 3**. Les corps algébriquement clos de caractéristique fixée. Comme dans l'exemple 2, tous les modèles non-dénombrables sont saturés. Nous regardons maintenant les modèles dénombrables:

Supposons d'abord que la caractéristique soit nulle. Le modèle premier est $\tilde{\mathbf{Q}}$, la clôture algébrique de $\mathbf{Q}$. Le modèle saturé (dénombrable) est isomorphe à la clôture algébrique de $\mathbf{Q}(t_i \mid i \in \mathbf{N})$, où les t_i, $i \in \mathbf{N}$, sont des éléments algébriquement indépendants au-dessus de $\mathbf{Q}$ (donc, pour tout $n \in \mathbf{N}$, $\mathbf{Q}(t_0, \ldots, t_n) \simeq \mathbf{Q}(X_0, \ldots, X_n)$). Un autre façon de décrire ce modèle est de dire qu'il est algébriquement clos de degré de transcendance infini dénombrable.

De même, si la caractéristique est $p > 0$, le modèle premier est $\tilde{\mathbf{F}}_p$, le modèle saturé est la clôture algébrique de $\mathbf{F}_p(t_i \mid i \in \mathbf{N})$, où les éléments t_i, $i \in \mathbf{N}$, sont algébriquement indépendants au dessus de $\mathbf{F}_p$.

Soit A un sous-ensemble du corps algébriquement clos K. Alors le sous-corps B de K engendré par A est contenu dans la clôture définissable de A : en effet, tout élément de l'**anneau** R engendré par A est de la forme $t(\bar{a})$ où $\bar{a}$ est un uplet d'éléments de A et $t(\bar{x})$ est un terme du langage. D'autre part, si $b \in R$, alors l'élément $1/b$ est certainement définissable sur R, ce qui montre que B est bien contenu dans la clôture définissable de A.

Certainement, les éléments de K qui sont algébriques sur B (au sens de la théorie des corps), sont algébriques sur B au sens de la théorie des modèles, puisqu'un polynôme non-nul en une variable n'a qu'un nombre fini de solutions. Soit $\tilde{B}$ l'ensemble de ces éléments. Si a, b sont deux éléments de K qui ne sont pas dans $\tilde{B}$, alors ils sont tous les deux transcendants au-dessus de $\tilde{B}$. Ils réalisent donc le même type au dessus de $\tilde{B}$. Nous avons donc montré que tous les éléments de $K \setminus \tilde{B}$ réalisent le même type au dessus de $\tilde{B}$: ce type ne peut donc être algébrique.

Nous venons donc de montrer que $acl(A) = \tilde{B}$. Nous savons aussi que B est contenu dans $dcl(A)$. Quand la caractéristique de K est nulle, nous allons montrer que $dcl(A) = B$. En effet, si $a \in \tilde{B}$, et $p(X)$ est son polynôme minimal sur B, alors $p'(X)$ est non nul, ce qui entraîne que a est une racine simple de l'équation $p(X) = 0$. Ce polynôme ayant $n = deg(p)$ racines distinctes dans $\tilde{B}$, et étant donné que deux racines distinctes de $p(X)$ ont le même type au-dessus de B, il s'ensuit que, si $n > 1$, alors $a \notin dcl(A)$. Nous avons donc montré que $dcl(A) = B$.

Supposons maintenant que $car(K) = p > 0$. Nous définissons la **clôture parfaite de** B, notée B^{1/p^∞}, comme étant l'ensemble des éléments $a \in \tilde{B}$ tel qu'il existe $n \geq 1$ avec $a^{p^n} \in B$. Tout d'abord, si $a \in B^{1/p^\infty}$, soit n minimal tel que $a^{p^n} = b \in B$. Alors le polynôme $X^{p^n} - b$ n'a qu'une seule racine, car $(X^{p^n} - b) = (X - a)^{p^n}$, puisque nous sommes dans un corps de caractéristique p.

Soit maintenant $a \in \tilde{B}$, et $p(X) = \sum_{i=0}^n a_i X^i$ son polynôme minimal sur B, avec $a_n = 1$, et $n > 1$. Si $p'(X) \neq 0$, alors on raisonne comme dans le cas de la caractéristique nulle pour montrer que $a \notin dcl(A)$. Supposons maintenant que $p'(X) = 0$. Pour tout $i = 1, \ldots, n$ on a alors : ou bien p divise i, ou bien $a_i = 0$. Soit m maximal tel que p^m divise i pour tout i tel que $a_i \neq 0$. Nous pouvons donc écrire $p(X) = \sum_{i=0}^n a_i (X^{p^m})^{i/p^m}$, et l'un des exposants i/p^m avec $a_i \neq 0$ n'est pas divisible par p. Notre polynôme s'écrit donc $p(X) = q(X^{p^m})$ pour un certain polynôme $q(Y)$ tel que $q'(Y) \neq 0$. De plus, ce polynôme $q(Y)$ est le polynôme minimal de $b = a^{p^m}$ au-dessus de B. Si $p^m \neq n$, alors le degré de $q(Y)$ est suérieur à 1, b n'est pas dans $dcl(A)$ (par le cas précédent), et donc a non plus. Cela montre que les seuls éléments de $\tilde{B}$ qui sont définissables sur A sont dans B^{1/p^∞}.

Rappels. Dans un corps K de caractéristique $p > 0$, l'application $x \mapsto x^p$ (appelée le Frobénius) définit un monomorphisme de corps : elle est clairement multiplicative. De plus $a^p = 0$ entraîne $a = 0$. On vérifie, en utilisant les coefficients binomiaux, que $(a + b)^p = a^p + b^p$, car p divise chaque $p!/i!(p - i)!$ pour $0 < i < p$.

Un corps est **parfait** s'il est de caractéristique 0, ou bien s'il est de caractéristique $p > 0$, et chacun de ses éléments est une puissance p-ième. (Ce qui veut dire que le Frobénius est surjectif.)

(5.27) **Rappel sur les bases de transcendance**. Soient $K \subset L$ des corps. Un sous-ensemble B de L est **algébriquement indépendant au-dessus de** K, si pour tout $n \in \mathbf{N}$, et tout n-uplet $(a_1, \ldots, a_n)$ d'éléments distincts de B, et tout polynôme non nul $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, nous avons $f(a_1, \ldots, a_n) \neq 0$.

Une **base de transcendance de** L **sur** K est un sous-ensemble B de L qui est algébriquement indépendant sur K, et maximal avec cette propriété. Il est facile, grâce au lemme de Zorn, de montrer que L possède une base de transcendeance B sur K. Par maximalité de B, nous avons alors que tout élément de L est algébrique sur $K(B)$ (le sous-corps de L engendré au-dessus de K par les éléments de B).

On montre que deux bases de transcendance de L sur K ont nécéssairement la même cardinalité. Pour cela on montre d'abord un

Lemme d'échange. Soient $a_1, \ldots, a_n$ des éléments algébriquement indépendants au-dessus de K, et a un élément algébrique sur $K(a_1, \ldots, a_n)$, qui n'est pas dans la clôture algébrique $\tilde{K}$ de K. Alors il existe i tel que a_i soit algébrique sur $K(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n, a)$.

Ce lemme de l'échange permet alors de raisonner exactement comme dans la preuve que deux bases d'un espace vectoriel ont la même cardinalité, et de montrer le résultat pour les bases de transcendance.

(5.28) **Exemple 4**. Soient $\mathcal{L} = \{+, -, 0, 1\}$ et $T = Th(\mathbf{Z})$. Alors $\mathbf{Z}$ est un modèle premier de T, car il est engendré par la constante 1. Comme nous savons que la théorie T est complète, cela entraîne que l'inclusion de $\mathbf{Z}$ dans un modèle de T est nécéssairement une inclusion élémentaire: si $a_1, \ldots, a_n \in \mathbf{Z}$, alors $a_i = t_i(1)$ pour un terme $t_i(x)$ du langage, et donc on a, pour $\varphi(\bar{x})$ une formule

$$\mathbf{Z} \models \varphi(a_1, \ldots, a_n) \iff T \vdash \varphi(t_1(1), \ldots, t_n(1)).$$

Soit maintenant M un modèle ω-saturé de T, et $D(M) = \bigcap_n nM$. Nous savons que $M/D(M)$ se plonge dans $\hat{\mathbf{Z}}$. Pour chaque $a \in \hat{\mathbf{Z}}$, le type $p_a(x)$ doit être réalisé, et cela entraîne que $M/D(M) \simeq \hat{\mathbf{Z}}$.

De plus, si M est ω-saturé, alors nécéssairement on doit avoir $D(M) = \mathbf{Q}^{(\kappa)}$ avec $\kappa \geq \aleph_0$. En effet, si $A = \{a_1, \ldots, a_n\}$ est un sous-ensemble fini de $D(M)$, soit B le $\mathbf{Q}$-sous-espace vectoriel de $D(M)$ engendré par A. Alors tout élément de B est l'unique réalisation dans M d'une formule $\varphi(x) \in \mathcal{L}(A)$: par définition, si $b \in B$, alors il existe $m, m_1, \ldots, m_n$ tels que $mb = \sum_{i=1}^n m_i a_i$, et b est l'unique élément de M satisfaisant la formule $mx = \sum_{i=1}^n m_i a_i$.

Donc le type $p(x)$ qui dit que x est divisible par n pour tout $n \geq 2$ et n'est pas dans B, est réalisable dans M. Raisonnant de la même façon pour un cardinal non dénombrable, cela nous dit que tout modèle λ-saturé de T est de la forme $\hat{\mathbf{Z}} \oplus \mathbf{Q}^{(\kappa)}$, où $\kappa \geq \lambda$. En fait on peut montrer qu'un tel modèle est en fait κ-saturé.

(5.29) Soient maintenant $\mathcal{L}_0 = \{+, -, 0\}$ et $T_0 = Th(\mathbf{Z})$ (Remarque: nous avons enlevé la constante 1). Alors nous montrerons que $\mathbf{Z}$ n'est pas un modèle premier de T_0!!

Tout d'abord nous allons donner une axiomatisation de T_0 (voir (3.10)). T_0 dit que un modèle M de T est un groupe abélien sans torsion. De plus, pour chaque $n \geq 2$, nous avons un énoncé qui exprime que M/nM a exactement n éléments, et en fait est cyclique d'ordre n :

$$\exists x\, \forall y\, (\bigwedge_{i=1}^{n-1} ny \neq ix) \wedge \exists z \bigvee_{i=0}^{n-1} (y - ix) = nz. \tag{n}$$

On montre que si M est un modèle ω-saturé de T_0, alors T réalise le type $q(x) = \{\forall z,\, nz \neq x \mid n \geq 2\}$. En effet, soit $m \geq 2$; nous voulons montrer qu'il existe un élément $a \in M$ tel que a ne soit pas divisible par $2, \ldots, m$. C'est clair en regardant l'axiome $(m!)$: soit $a \in M$ tel que aucun des ia, $i = 1, \ldots, m! - 1$, ne soit divisible par $m!$. Soit $2 \leq j \leq m$, et soit $i = m!/j$. Comme ia n'est pas divisible par $m!$, cela entraîne que a n'est pas divisible par j.

Donc si M est un modèle ω-saturé, alors M contient une réalisation a de $q(x)$. Si on interprète la constante 1 par cet élément a, on a alors que M est un modèle de T. Cela entraîne que T_0 est complète (pourquoi?).

Alors $\mathbf{Z}$ n'est pas un modèle premier de T_0. En effet, considérons $M = \oplus_{p \text{ premier}} \mathbf{Z}_{(p)}$, où $\mathbf{Z}_{(p)}$ est l'ensemble des nombres rationnels dont le dénominateur (quand le nombre est écrit sous forme réduite) n'est pas divisible par p. Alors si n est un nombre non-divisible par p, tout élément de $\mathbf{Z}_{(p)}$ est divisible par n.

On vérifie que M est un modèle de T_0; cependant M ne réalise pas le type $p(x)$: si $a \in M$, alors $a \in \oplus_S \mathbf{Z}_{(p)}$ pour un ensemble S fini de nombres premiers, et cela entraîne que a est divisible par tout nombre premier qui n'est pas dans S. Donc, bien que M contienne beaucoup de copies de $\mathbf{Z}$, aucune n'est une sous-structure élémentaire de M.

(5.30) **Exercice**. (1) Expliquez pourquoi la théorie T_0 décrite ci-dessus est complète.

Considérons maintenant le langage $\mathcal{L}' = \mathcal{L}_0 \cup \{\equiv_n \mid n \geq 2\}$, et la théorie T' obtenue en rajoutant à T_0 les axiomes

$$x \equiv_n y \iff \exists z\, (x - y) = nz.$$

Alors tout modèle de T_0 s'étend en un modèle de T' de façon **unique**.

(2) Si Γ est un sous-groupe d'un groupe abélien G sans torsion, on définit l'**enveloppe pure** de Γ (dans G) comme étant l'ensemble $EP(\Gamma) = \{a \in G \mid \exists n \geq 1, na \in \Gamma\}$. Montrez que c'est bien un sous-groupe de G. (Si $\Gamma = EP(\Gamma)$, on dit que Γ est **pur dans** G).

(3) Soient M et N des modèles de T', et f un isomorphisme partiel entre les $\mathcal{L}'$-structures M et N. Montrez que f s'étend uniquement en un isomorphisme partiel f' défini sur l'enveloppe pure du sous-groupe de M engendré par $dom(f)$. Montrez que $Im(f')$ est aussi un sous-groupe pur de N.

(4) Soient M et N des modèles $\aleph_1$-saturés de T'. Supposons que nous ayons montré que la famille $\mathcal{I}(M, N)$ des isomorphismes partiels de domaine un **sous-groupe dénombrable et pur** de M, a la propriété du va-et-vient. En déduire que T' élimine les quantificateurs.

(5) Montrez que si A est un sous-groupe pur de M, alors A s'écrit $(D(M) \cap A) \oplus A_0$, pour un sous-groupe A_0 de A qui est pur dans M, et que $D(M) \cap A$ est divisible.

(6) Nous allons montrer que la famille $\mathcal{I}(M, N)$ d'isomorphismes partiels décrite en (4) a la propriété du va-et-vient. [Vous n'avez pas le droit d'utiliser la conclusion de (4)].

Soit $f \in \mathcal{I}(M, N)$ de domaine A, d'image B, et écrivons $A = (D(M) \cap A) \oplus A_0$. Soient $B_0 = f(A_0)$, et $a \in M$. Nous voulons prolonger f en une fonction $f' \in \mathcal{I}(M, N)$ ayant a dans son domaine. Nous avons trois cas à considérer, et je vous demande de montrer l'existence de f' dans chacun de ces cas:

(a) Il existe $b \in A$ tel que $(b - a) \in D(M)$.

(b) Pour tout $n \geq 2$ il existe $b_n \in A$ tel que $(b_n - a) \in nM$, mais il n'existe pas de $b \in A$ tel que $(b - a) \in D(M)$.

(c) Nous supposons maintenant que ni (a), ni (b) ne sont vrais. La preuve se décompose en plusieurs étapes, que vous devriez être capables de faire :

(c1) Montrez que la pureté de A_0 dans M entraîne que pour tout nombre premier p :

– ou bien pour tout $n \geq 1$, $A_0/p^n A_0 \simeq \mathbf{Z}/p^n\mathbf{Z}$,

– ou bien pour tout $n \geq 1$, $A_0 = p^n A_0$ (c'est à dire que A_0 est p-divisible).

(c2) Montrez que si $b \in N$ satisfait les conditions suivantes :

– Pour chaque premier p tel que A_0 est p-divisible, pour tout $n \geq 1$, le sous-groupe de $N/p^n N$ engendré par l'image de b est de même taille que le sous-groupe de $M/p^n M$ engendré par l'image de a.

– Pour chaque premier p tel que A_0 n'est pas p-divisible, pour tout $n \geq 1$ nous savons qu'il existe un élément $a_n \in A$ tel que $(a - a_n) \in p^n M$ (par (c1)), et nous avons $(b - f(a_n)) \in p^n N$ pour tout $n \geq 1$.

Alors l'application f' définie en posant $f'(a' + na) = f(a') + nb$ pour $a' \in A$ et $n \in \mathbf{Z}$, est bien un homomorphisme de groupe qui respecte les relations $\equiv_n$.

(c3) Montrez l'existence d'un tel b (ce qui finit la preuve du cas (c)) [Il faut utiliser la $\aleph_1$-saturation de N].

6. Produits réduits et ultraproduits

(6.1) **Filtres et ultrafiltres**. Soit I un ensemble. Un **filtre sur** I est un sous-ensemble $\mathcal{F}$ de $\mathcal{P}(I)$ satisfaisant aux conditions suivantes :

(i) $I \in \mathcal{F}$, $\emptyset \notin \mathcal{F}$.

(ii) Si $U \in \mathcal{F}$ et $V \supset U$ alors $V \in \mathcal{F}$.

(iii) Si U et V sont dans $\mathcal{F}$ alors $U \cap V \in \mathcal{F}$.

Un **ultrafiltre sur** I est un filtre sur I qui est maximal (pour l'inclusion).

(6.2) **Remarques**. (1) Soit $\mathcal{G}$ un sous-ensemble non-vide de $\mathcal{P}(I)$ ne contenant pas $\emptyset$ et satisfaisant la condition (iii). Soit $\mathcal{F}$ l'ensemble des sous-ensembles de I qui contiennent un élément de $\mathcal{G}$. Alors cette famille satisfait (i) et (ii) (clairement), et satisfait encore (iii). Donc $\mathcal{F}$ est un filtre.

(2) Plus généralement, soit $\mathcal{G}$ un sous-ensemble de $\mathcal{P}(I)$ ayant la propriété que toute intersection finie de ses éléments est non-vide (cette propriété est appelée **la propriété de l'intersection finie**). On définit alors le **filtre engendré par** $\mathcal{G}$ comme étant l'ensemble des sous-ensembles de I qui contiennent une intersection finie d'éléments de $\mathcal{G}$. On vérifie facilement que c'est bien un filtre.

(6.3) **Lemme**. Soit $\mathcal{F}$ un filtre sur I. Alors $\mathcal{F}$ est un ultrafiltre si et seulement si pour tout sous-ensemble U de I, nous avons $U \in \mathcal{F} \iff I \setminus U \notin \mathcal{F}$.

Démonstration. Supposons d'abord que $U \in \mathcal{F}$, et que $I \setminus U \in \mathcal{F}$. Alors, par l'axiome (iii) nous avons $\emptyset = U \cap (I \setminus U) \in \mathcal{F}$, ce qui contredit l'axiome (i).

Supposons maintenant que $I \setminus U \notin \mathcal{F}$. Soit $\mathcal{G} = \{V \cap U \mid V \in \mathcal{F}\}$. Nous prétendons que $\emptyset \notin \mathcal{G}$. Sinon, il existerait $V \in \mathcal{F}$ tel que $U \cap V = \emptyset$, c'est à dire, $V \subset I \setminus U$, et nous aurions donc que $I \setminus U \in \mathcal{F}$, contrairement à notre hypothèse. La famille $\mathcal{G}$ satisfait donc aux conditions énoncées dans (6.2)(1) ; donc l'ensemble $\mathcal{F}'$ des sous-ensembles de I qui contiennent $U \cap V$ pour un $V \in \mathcal{F}$, est un filtre qui contient $\mathcal{F}$. Par maximalité de $\mathcal{F}$, nous avons $\mathcal{F}' = \mathcal{F}$, c'est à dire, $U \in \mathcal{F}$.

(6.4) **Définition**. Un filtre $\mathcal{F}$ est **principal** s'il existe $U \in \mathcal{F}$ tel que $\mathcal{F} = \{V \subseteq I \mid V \supseteq U\}$.

Un ultrafiltre principal est forcément de la forme $\{V \subseteq I \mid i \in V\}$ pour un élément $i \in I$. En effet, supposons que $\mathcal{F}$ soit un ultrafiltre principal, et U soit tel que $\mathcal{F} = \{V \subseteq I \mid V \supseteq U\}$. Si U contient deux éléments $i \neq j$, alors ni $I \setminus \{i\}$ ni $\{i\}$ ne contiennent U, ce qui contredit la maximalité de $\mathcal{F}$.

(6.5) **Exercice**. Soient I un ensemble et $\mathcal{F}$ un filtre sur I.

(1) Montrez que l'ensemble $\{I \setminus U \mid U \in \mathcal{F}\}$ est un idéal de l'algèbre de Boole $\mathcal{P}(I)$. Nous l'appellerons l'idéal associé à $\mathcal{F}$.

(2) Montrez que réciproquement, si I est un idéal (propre) de $\mathcal{P}(I)$, alors $\{I \setminus U \mid U \in I\}$ est un filtre sur I.

(3) Montrez que $\mathcal{F}$ est un ultrafiltre si et seulement si l'idéal I associé est maximal.

(4) Montrez que $\mathcal{F}$ est principal si et seulement si l'idéal associé est principal.

(5) Montrez que si I est fini alors tout filtre sur I est principal.

(6.6) **Filtre de Fréchet**. Soit I un ensemble infini. Le filtre de Fréchet sur I est le filtre engendré par la famille $\{I \setminus \{i\} \mid i \in I\}$. Notons que comme I est infini, cette famille satisfait bien que toute intersection finie de ses membres est non-vide. C'est donc le filtre des parties co-finies de I. Notons aussi qu'un ultrafiltre sur I est non-principal si et seulement s'il contient le filtre de Fréchet sur I : en effet, un ultrafiltre est non-principal si et seulement s'il ne contient aucun singleton, si et seulement s'il contient les complémentaires des singletons, si et seulement s'il contient le filtre de Fréchet.

(6.7) **Produits réduits de $\mathcal{L}$-structures**. Soit I un ensemble, $\mathcal{D}$ un filtre sur I, et $(M_i)_{i\in I}$ une famille de $\mathcal{L}$-structures.

Nous avions déjà défini une $\mathcal{L}$-structure sur le produit $\prod_{i\in I} M_i$. Nous définissons le **produit réduit des M_i sur le filtre $\mathcal{D}$**, noté $\prod_{i\in I} M_i/\mathcal{D}$, comme étant la $\mathcal{L}$-structure suivante :

L'univers de $\prod_{i\in I} M_i/\mathcal{D}$ est le quotient de $\prod_{i\in I} M_i$ par la relation d'équivalence $\equiv_\mathcal{D}$ définie par

$$(a_i) \equiv_\mathcal{D} (b_i) \iff \{i \in I \mid a_i = b_i\} \in \mathcal{D}.$$

Notons que

$$\{i \in I \mid a_i = b_i\} \cap \{i \in I \mid b_i = c_i\} \subseteq \{i \in I \mid a_i = c_i\},$$

ce qui montre la transitivité de $\equiv_\mathcal{D}$. La réfléxivité et la symétrie de $\equiv_\mathcal{D}$ sont évidentes. Nous notons $(a_i)_\mathcal{D}$ la classe d'équivalence de (a_i) pour la relation $\equiv_\mathcal{D}$.

Pour c un symbole de constante, l'interprétation de c dans $\prod_{i\in I} M_i/\mathcal{D}$ est tout simplement $(c_i)_\mathcal{D}$, où chaque c_i est l'interprétation de c dans M_i.

Si f est un symbole de fonction n-aire du langage, et $(a_i^1), \dots, a^n(i) \in \prod_{i\in I} M_i$, nous posons

$$f((a_i^1)_\mathcal{D}, \dots, (a_i^n)_\mathcal{D}) = (f(a_i^1, \dots, a_i^n))_\mathcal{D}.$$

Notons que si $(b_i^j)_\mathcal{D} = (a_i^j)_\mathcal{D}$ pour $j = 1, \dots, n$, alors $\{i \in I \mid b_i^j = a_i^j \text{ pour } j = 1, \dots, n\}$ est dans $\mathcal{D}$, ce qui montre que f est bien définie.

Si R est un symbole de relation n-aire du langage, et $(a_i^1), \dots, (a_i^n) \in \prod_{i\in I} M_i$, alors nous posons

$$\prod_{i\in I} M_i/\mathcal{D} \models R((a_i^1)\mathcal{D}, \dots, (a_i^n)_\mathcal{D}) \iff \{i \in I \mid M_i \models R(a_i^1, \dots, a_i^n)\} \in \mathcal{D}.$$

(6.8) **Définitions**. S'il existe une $\mathcal{L}$-structure M telle que tous les M_i sont égaux à M, alors on écrit $M^I/\mathcal{D}$ au lieu de $\prod_{i\in I} M_i/\mathcal{D}$, et on parle de **puissance réduite de** M. Elle est aussi parfois notée $M^\mathcal{D}$.

Si le filtre $\mathcal{D}$ est un ultrafiltre, alors $\prod_{i\in I} M_i/\mathcal{D}$ est appelé un **ultraproduit des structures** M_i, et $M^I/\mathcal{D}$ est appelée une **ultrapuissance de** M.

(6.9) **Remarques**. Soient $\mathcal{D} \subseteq \mathcal{D}'$ des filtres sur I. Alors l'application $\prod_{i\in I} M_i/\mathcal{D} \to \prod_{i\in I} M_i/\mathcal{D}'$ définie par $(a_i)_\mathcal{D} \mapsto (a_i)_{\mathcal{D}'}$, est un homomorphisme de $\mathcal{L}$-structures.

Notons aussi que le produit est un cas particulier de produit réduit : on prend le filtre $\{I\}$.

(6.10) **Théorème de Łos.** Soit I un ensemble, $\mathcal{D}$ un ultrafiltre sur I, et $(M_i)_{i\in I}$ une famille de $\mathcal{L}$-structures, $M^* = \prod_{i\in I} M_i/\mathcal{D}$.

(1) Si $t(x_1, \ldots, x_n)$ est un terme du langage, et $(a_i^1), \ldots, (a_i^n) \in \prod_{i \in I} M_i$, alors

$$t((a_i^1)_\mathcal{D}, \ldots, (a_i^n)_\mathcal{D}) = (t(a_i^1, \ldots, a_i^n))_\mathcal{D}.$$

(En fait, ceci est vrai aussi dans un produit réduit.)

(2) Soient $\varphi(x_1, \ldots, x_n)$ une formule, et $(a_i^1), \ldots, (a_i^n) \in \prod_{i \in I} M_i$. Alors

$$M^* \models \varphi((a_i^1)_\mathcal{D}, \ldots, (a_i^n)_\mathcal{D}) \iff \{i \in I \mid M_i \models \varphi(a_i^1, \ldots, a_i^n)\} \in \mathcal{D}.$$

(3) Soit φ un énoncé. Alors

$$M^* \models \varphi \iff \{i \in I \mid M_i \models \varphi\} \in \mathcal{D}.$$

Démonstration. (1) est clair par la définition de la $\mathcal{L}$-structure de M^*, et (3) est un cas particulier de (2). Il suffit donc de montrer (2). C'est fait par induction sur la complexité des formules : nous allons d'abord montrer que c'est vrai pour les formules atomiques.

Les formules atomiques sont de la forme $R(t_1(\bar{x}), \ldots, t_n(\bar{x}))$, où $\bar{x}$ est un uplet de variables, chaque $t_i(\bar{x})$ est un terme du langage, et R est une symbole de relation n-aire, ou bien le graphe de l'égalité. L'équivalence suit de la définition de la $\mathcal{L}$-structure M^*. Remarquons qu'ici nous utilisons seulement le fait que $\mathcal{D}$ est un filtre.

Supposons que l'équivalence soit vraie pour les formules $\varphi(\bar{x})$ et $\psi(\bar{x})$. Elle est alors vraie pour la formule $\varphi(\bar{x}) \wedge \psi(\bar{x})$. De même, si elle est vraie pour la formule $\theta(\bar{x}, y)$, alors elle est vraie pour la formule $\exists y\, \theta(\bar{x}, y)$. Encore une fois, nous utilisons seulement le fait que $\mathcal{D}$ est un filtre.

Il reste maintenant à montrer que si le résultat est vrai pour $\varphi(\bar{x})$, alors il est vrai pour $\neg\varphi(\bar{x})$, et c'est là enfin que nous utiliserons le fait que $\mathcal{D}$ est un ultrafiltre. Nous avons par hypothèse :

$$M^* \models \neg\varphi((a_i^1)_\mathcal{D}, \ldots, (a_i^n)_\mathcal{D}) \iff \{i \in I \mid M_i \models \varphi(a_i^1, \ldots, a_i^n)\} \notin \mathcal{D}.$$

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

$$\{i \in I \mid M_i \models \varphi(a_i^1, \ldots, a_i^n)\} \notin \mathcal{D} \iff \{i \in I \mid M_i \models \neg\varphi(a_i^1, \ldots, a_i^n)\} \in \mathcal{D},$$

ce qui nous donne que la formule $\neg\varphi(\bar{x})$ satisfait aussi l'équivalence.

(6.11) Soient I un ensemble, M une $\mathcal{L}$-structure, et $\mathcal{D}$ un filtre sur I. Nous avons alors une inclusion $M \to M^I/\mathcal{D}$, donnée en envoyant $a \in M$ sur la classe d'équivalence de l'élément $(a)_{i \in I}$ (la suite constante égale à a). Il est clair que c'est un plongement de $\mathcal{L}$-structures. Nous avons aussi

Corollaire. Supposons que $\mathcal{D}$ soit un ultrafiltre. Alors l'inclusion $M \to M^I/\mathcal{D}$ est une inclusion élémentaire.

Démonstration. Immédiat par (6.10).

(6.12) **Théorème de compacité, revisité**. Soit T une théorie dans un langage $\mathcal{L}$, et supposons que tout sous-ensemble fini Σ de T ait un modèle M_Σ. Alors il existe un ultrafiltre $\mathcal{D}$ sur l'ensemble I des parties finies de T, tel que $\prod_{\Sigma\in I} M_\Sigma/\mathcal{D} \models T$.

Démonstration. Nous allons construire un ultrafiltre $\mathcal{D}$ sur I tel que $M^* = \prod_{\Sigma\in I} M_\Sigma/\mathcal{D} \models T$. Pour cela il suffit de faire en sorte que pour chaque $\varphi \in T$, $\{\Sigma \in I \mid \varphi \in \Sigma\}$ appartienne à $\mathcal{D}$. [En effet, nous appliquerons alors le théorème de Łos.]

Définissons donc, pour $\varphi \in T$, $S(\varphi) = \{\Sigma \in I \mid \varphi \in \Sigma\}$, et soit $\mathcal{G} = \{S(\varphi) \mid \varphi \in T\}$. Notons que $S(\varphi_1 \wedge \varphi_2) = S(\varphi_1) \cap S(\varphi_2)$, ce qui entraîne que notre famille $\mathcal{G}$ a la propriété de l'intersection finie. Le filtre (sur I) engendré par $\mathcal{G}$ est donc propre, et est contenu dans un ultrafiltre $\mathcal{D}$.

(6.13) **Groupes ordonnés et ordonnables**. Un **groupe ordonné** est une groupe $(G, \cdot, ^{-1}, 1)$, muni d'un ordre total $<$ satisfaisant la relation de compatibilité suivante :

$$\forall x, y, z\,(x < y) \to (xz < yz).$$

Notons que cela entraîne que en fait on a une équivalence : $(x < y) \leftrightarrow (xz < yz)$, et que de plus on a $(x > 1) \leftrightarrow (x^{-1} < 1)$, et que connaître l'ensemble des éléments > 1 (appelé le **cône positif de** G), c'est connaître l'ordre sur le groupe : en effet on a $x < y \leftrightarrow xy^{-1} < 1$. Notons aussi qu'un groupe ordonné est nécéssairement sans torsion : si $a > 1$ alors

$$1 < a < a^2 < \cdots < a^n \cdots$$

Un groupe G est **ordonnable**, s'il existe un ordre total sur G qui satisfait à l'axiome de compatibilité ci-dessus.

Rappelons aussi qu'un groupe de **type fini** est un groupe ayant un ensemble fini de générateurs.

(6.14) **Applications aux groupes ordonnables**. **Théorème**. Un groupe G est ordonnable si et seulement si tout sous-groupe de G de type fini est ordonnable.

Démonstration. Il faut remarquer que si G est un groupe ordonné, et si H est un sous-groupe de G, alors la restriction de l'ordre de G à H en fait un groupe ordonné : c'est parce que les axiomes nécéssaires pour exprimer qu'un groupe est ordonné sont des axiomes universels. La nécéssité de l'ordonnabilité de tous les sous-groupes de type fini de G est donc évidente.

Supposons maintenant que tout sous-groupe de G de type fini soit ordonnable, et soit I l'ensemble des parties finies de G. Pour chaque $\Sigma \in I$, soit G_Σ, le sous-groupe de G engendré par les éléments de Σ, et fixons un ordre sur ce groupe (qui en fasse un groupe ordonné). Nous considérons donc $(G_\Sigma, \cdot, ^{-1}, 1, <)$.

Pour chaque $g \in G$, soit $S(g) = \{\Sigma \in I \mid g \in \Sigma\}$. Alors l'ensemble $\{S(g) \mid g \in G\}$ a la propriété de l'intersection finie, et donc est contenu dans un ultrafiltre $\mathcal{D}$ sur I.

Nous allons définir une application $f : G \to G^* = \prod_{\Sigma\in I} G_\Sigma/\mathcal{D}$, qui sera un plongement de groupe. Nous définissons f de la façon suivante, pour $g \in G$:

$$f(g) = (g_\Sigma)_\mathcal{D}, \text{ et } g_\Sigma = \begin{cases} g & \text{si } g \in G_\Sigma, \\ 1 & \text{sinon.} \end{cases}$$

Alors f est injective, car pour chaque $g \in G$, l'ensemble $S(g)$ est dans $\mathcal{D}$. Donc, si $g \neq h$, on aura $g_\Sigma \neq h_\Sigma$ pour tout $\Sigma \in S(g) \cap S(h) \in \mathcal{D}$. De même, cette injection respecte la loi de groupe : si $g, h \in G$, alors $S(g) \cap S(h)$ est contenu dans l'ensemble des $\Sigma \in I$ tels que $g_\Sigma h_\Sigma = f(g \cdot h)_\Sigma$, et f est donc un plongement de groupe. L'ultraproduit G^* des groupes ordonnés $(G_\Sigma, <)$ est aussi un groupe ordonné, avec sous-groupe G, ce qui montre bien que G est ordonnable.

(6.15) **Application des ultraproduits aux classes élémentaires**. Rappelons qu'une classe $\mathcal{K}$ de $\mathcal{L}$-structures est appelée une **classe élémentaire** s'il existe une théorie T telle que $\mathcal{K}$ est l'ensemble des modèles de T, noté $\mathcal{K} = Mod(T)$. Notons que nécéssairement nous aurons alors $T = Th(\mathcal{K})$ (= l'ensemble des énoncés vrais dans tous les membres de $\mathcal{K}$). Nous avons le résultat suivant :

Proposition. Soit $\mathcal{K}$ une classe de $\mathcal{L}$-structures, $T = Th(\mathcal{K})$.

(1) $\mathcal{K} = Mod(T)$ si et seulement si la classe $\mathcal{K}$ est close par équivalence élémentaire et par ultraproduits.

(2) $\mathcal{K} = Mod(\varphi)$ pour un énoncé φ si et seulement si $\mathcal{K}$ et son complément $\mathcal{K}^c$ sont closes par équivalence élémentaire et par ultraproduits.

Démonstration. (1) Supposons d'abord que $\mathcal{K} = Mod(T)$. Alors, si $M \in \mathcal{K}$ et $M' \equiv M$, nous avons $M' \models T$, et $M' \in \mathcal{K}$. De même, si chaque M_i est dans $\mathcal{K}$, alors chaque M_i est un modèle de T, donc leur ultraproduit est un modèle de T, qui est donc dans $\mathcal{K}$. Cela montre une direction.

Pour la réciproque, montrons que si $\mathcal{K}$ est close par équivalence élémentaire et ultraproduits, alors elle est élémentaire. Soit donc $M \models T$, nous voulons montrer que $M \in \mathcal{K}$. Pour cela, il suffit de montrer qu'il existe un ultraproduit M^* d'éléments de $\mathcal{K}$ qui est élémentairement équivalent à M.

Pour cela, utilisant (6.12), il suffit de montrer que pour tout sous-ensemble fini Σ de $Th(M)$, il existe $M_\Sigma \in \mathcal{K}$ qui est modèle de Σ. Soit un tel Σ, et θ la conjonction des énoncés de Σ. Par hypothèse, $T \not\models \neg\varphi$, car $M \models T$ et $M \models \varphi$. Par définition de T, cela signifie qu'il existe $M_\Sigma \in \mathcal{K}$ qui ne satisfait pas $\neg\varphi$, c'est à dire que $M_\Sigma \models \Sigma$. Cqfd.

(2) $\mathcal{K} = Mod(\varphi)$ implique que $\mathcal{K}$ et son complément sont des classes élémentaires ($\mathcal{K}^c = Mod(\neg\varphi)$). Réciproquement, si $\mathcal{K}$ et $\mathcal{K}^c$ sont des classes élémentaires, posons $T_1 = Th(\mathcal{K}^c)$. Alors $T \cup T_1$ est inconsistante puisqu'elle n'a pas de modèle. Par compacité, il existe donc des énoncés $\varphi \in T$ et $\varphi_1 \in T_1$ tels que $\varphi \wedge \varphi_1$ soit inconsistante. Nous avons alors $\mathcal{K} = Mod(\varphi)$, $\mathcal{K}^c = Mod(\varphi_1)$. En effet, si $M \models \varphi$, alors $M \not\models \varphi_1$, donc $M \not\models T_1$, $M \notin \mathcal{K}^c$, c'est à dire, $M \in \mathcal{K}$. De même si $M \models \varphi_1$, alors $M \in \mathcal{K}^c$.

(6.16) **Théorème**. Soit I un ensemble dénombrable, $\mathcal{D}$ un ultrafiltre non-principal sur I, et $(M_i)_{i \in I}$ une famille de $\mathcal{L}$-structures, où $\mathcal{L}$ est un langage dénombrable. Alors $M^* = \prod_{i \in I} M_i/\mathcal{D}$ est ω_1-saturé.

Démonstration. Nous pouvons supposer que $I = \mathbf{N}$. Soit A un sous-ensemble dénombrable de M^*, et $p(x) \in S_1(A)$. [Le type $p(x)$ contient donc le diagramme élémentaire de A dans M^*.] Il nous faut trouver dans M^* une réalisation de $p(x)$. Nous fixons une énumération $\{\varphi_n(x, \bar{a}^n) \mid n \in \mathbf{N}\}$ des formules de $p(x)$; ici les formules $\varphi_n(x, \bar{y})$ sont des formules de $\mathcal{L}$, la longueur du uplet $\bar{y}$ dépendant de n, et les uplets $\bar{a}^n$ sont des uplets de A (qui dépendent eux aussi de n), que nous écrivons $\bar{a}^n = (\bar{a}^n_i)_\mathcal{D}$. Puisque $\mathcal{L}$ et A sont dénombrables, nous savons que l'ensemble des formules de $\mathcal{L}(A)$ en une variable libre est dénombrable, et il existe bien une telle énumération de $p(x)$.

Pour chaque $n \in \mathbf{N}$, soit

$$S(n) = \{i \in \mathbf{N} \mid M_i \models \exists x \bigwedge_{k=0}^{n} \varphi_k(x, \bar{a}_i^k)\}.$$

Puisque $p(x)$ est un type consistant, nous savons que $M^* \models \exists x \bigwedge_{k=0}^{n} \varphi_k(x, \bar{a}^k)$, et par le théorème fondamental (6.10), cela entraîne que chaque $S(n)$ est dans $\mathcal{D}$. Notons aussi que $S(n)$ contient $S(n+1)$ pour tout $n \in \mathbf{N}$. Nous allons maitenant exhiber une réalisation $b = (b_i)_{\mathcal{D}}$ de $p(x)$ dans M^*.

Pour $i \in \mathbf{N}$, nous définissons b_i de la façon suivante :

(a) Si $i \notin S(0)$, alors nous prenons pour b_i n'importe quel élément de M_i.

(b) Si $i \in \bigcap_{m \in \mathbf{N}} S(m)$, alors nous choisissons $b_i \in M_i$ satisfaisant $\bigwedge_{k=0}^{i} \varphi_k(x, \bar{a}^k)$.

(c) Sinon, soit $m \in \mathbf{N}$ maximal tel que $i \in S(m)$, et prenons $b_i \in M_i$ satisfaisant $\bigwedge_{k=0}^{m} \varphi_k(x, \bar{a}^k)$.

Soit maintenant $n \in \mathbf{N}$. Nous voulons montrer que l'ensemble $T(n) = \{i \in \mathbf{N} \mid M_i \models \bigwedge_{k=0}^{n} \varphi_k(b_i, \bar{a}_i^k)\}$ appartient à $\mathcal{D}$. Nout allons montrer que $T(n) \supseteq S(n) \cap \{i \mid i \geq n\}$. En effet, soit $i \in S(n)$, $i \geq n$. Si $i \in \bigcap_m S(m)$, alors par construction $M_i \models \bigwedge_{k=0}^{i} \varphi_i(b_i, \bar{a}_i^k)$, et comme $i \geq n$, nous avons bien que $i \in T(n)$. Supposons maintenant que $i \notin \bigcap_m S(m)$, et soit m défini comme dans (c). Puisque $i \in S(n)$, nous avons $m \geq n$, et donc $i \in T(m) \supseteq T(n)$.

Cela finit la démonstration : puisque $\mathcal{D}$ est non-principal, l'ensemble $\{i \mid i \geq n\}$ est bien dans $\mathcal{D}$; donc son intersection avec $S(n)$ aussi, et aussi $T(n)$. Par le théorème fondamental, nous obtenons que $M^* \models \varphi_k((b_i)_{\mathcal{D}}, \bar{a}^k)$ pour tout $k \in \mathbf{N}$, et donc que $(b_i)_{\mathcal{D}}$ réalise $p(x)$ dans M^*.

(6.17) **Deux résultats importants que nous ne montrerons pas**. La démonstration de ces deux résultats peut être trouvée par exemple dans le Chang et Keisler. Le premier est difficile à montrer (la preuve est très combinatoire), le deuxième est plus facile (mais aussi plus faible).

Théorème 1. (Shelah) Soient M et N des $\mathcal{L}$-structures. Alors $M \equiv N$ si et seulement s'il existe un ensemble I et un ultrafiltre $\mathcal{D}$ sur I tels que $M^I/\mathcal{D} \simeq N^I/\mathcal{D}$.

Théorème 2. Soient M et N des $\mathcal{L}$-structures. Alors $M \equiv N$ si et seulement s'il existe un ensemble I, un ultrafiltre $\mathcal{D}$ sur I, et un plongement élémentaire $f : M \to N^I/\mathcal{D}$.

(6.18) **Remarques**. (1) Ces résultats peuvent être appliqués à n'importe quel langage. Par exemple, M est une extension élémentaire de N si et seulement s'il existe I, $\mathcal{D}$ et un plongement élémentaire f de M dans $N^I/\mathcal{D}$ qui prolonge l'inclusion naturelle $N \to N^I/\mathcal{D}$ définie en (6.11).

(2) Une classe $\mathcal{K}$ de $\mathcal{L}$-structures est élémentaire si et seulement si elle est close par ultraproduits et par sous-structures élémentaires.

(6.19) **Exercice**. Soit $\mathcal{D}$ un ultrafiltre principal sur l'ensemble I, et soit $(M_i)_{i \in I}$ une famille de $\mathcal{L}$-structures. Montrez que $\prod_{i \in I} M_i/\mathcal{D} \simeq M_j$ pour un $j \in I$.

(6.20) **Exercice**. Soit I un ensemble, $\mathcal{D}$ un filtre sur I, et $J \in \mathcal{D}$. Posons $\mathcal{U} = \{U \cap J \mid U \in \mathcal{D}\} = \mathcal{D} \cap \mathcal{P}(J)$. Si $(M_i)_{i \in I}$ est une famille de $\mathcal{L}$-structures, montrez que

$$\prod_{i \in I} M_i/\mathcal{D} \simeq \prod_{i \in J} M_i/\mathcal{U}.$$

(6.21) **Exercice**. Soit I un ensemble, $\mathcal{D}$ un ultrafiltre sur I, et soient $(M_i)_{i \in I}$ et $(N_i)_{i \in I}$ deux familles de $\mathcal{L}$-structures telles que $M_i \prec N_i$ pour tout $i \in I$. Les inclusions $M_i \to N_i$ induisent une inclusion $\prod_{i \in I} M_i \to \prod_{i \in I} N_i$. Montrez que cette inclusion est élémentaire.

(6.22) **Exercice**. Soient $\mathcal{K}_1$ et $\mathcal{K}_2$ des classes de $\mathcal{L}$-structures, et $T_1 = Th(\mathcal{K}_1)$ et $T_2 = Th(\mathcal{K}_2)$. Montrez que $T_1 \cup T_2$ est consistante si et seulement s'il existe un ultraproduit déléments de $\mathcal{K}_1$ qui est élémentairement équivalent à un ultraproduit déléments de $\mathcal{K}_2$.

(6.23) **Exercice**. Soit I un ensemble, $\mathcal{D}$ un filtre sur I, et $(K_i)_{i \in I}$ une famille de corps. Nous savons que $R = \prod_{i \in I} K_i$ a une structure d'anneau. Nous identifions $\mathcal{P}(I)$ avec l'algèbre de Boole $\mathcal{B}(R)$ des idempotents de R de la faqn suivante : à $J \subset I$ nous faisons correspondre l'idempotent e_J qui prend la valeur 0 sur J et 1 sur $I \setminus J$. [La structure d'algèbre de Boole sur $\mathcal{B}(R)$ est donnée par : $a \cap b = ab$, $a \cup b = a + b - ab$]. Montrez que $\{e_J \mid J \in \mathcal{D}\}$ est un idéal de $\mathcal{B}(R)$. De plus, si M est l'idéal de l'anneau R engendré par $\{e_J \mid J \in \mathcal{D}\}$, montrez que

$$\prod_{i \in I} K_i/\mathcal{D} \simeq R/M.$$

(6.24) **Exercice** (Itérations). Soient I et J des ensembles, $\mathcal{D}$ un filtre sur I et $\mathcal{F}$ un filtre sur J. Définissons $\mathcal{D} \times \mathcal{F}$ comme étant l'ensemble des $Y \in \mathcal{P}(I \times J)$ tels que

$$\{j \in J \mid \{i \in I \mid (i,j) \in Y\} \in \mathcal{D}\} \in \mathcal{F}.$$

(1) Montrez que $\mathcal{D} \times \mathcal{F}$ est bien un filtre sur $I \times J$.

(2) Montrez que si $\mathcal{D}$ et $\mathcal{F}$ sont des ultrafiltres, alors $\mathcal{D} \times \mathcal{F}$ est aussi un ultrafiltre.

(3) Soit $(M_{(i,j)})$, $(i,j) \in I \times J$, une famille de $\mathcal{L}$-structures. Pour $j \in J$ définissons $M_j^* = \prod_{i \in I} M_{(i,j)}/\mathcal{D}$. Montrez que

$$\prod_{(i,j) \in I \times J} M_{(i,j)}/\mathcal{D} \times \mathcal{F} \simeq \prod_{j \in J} M_j^*/\mathcal{F}.$$

(6.25) **Exercice** (difficile). Soit I un ensemble dénombrable, et $\mathcal{D}$ un ultrafiltre sur I. Pour chaque $i \in I$, soit M_i une $\mathcal{L}$-structure **finie**, et soit $M^* = \prod_{i \in I} M_i/\mathcal{D}$. Montrez que $|M^*|$ est finie, ou bien égale $2^{\aleph_0}$.

7. 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.

(7.1) 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:

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

(7.2) **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**.

Soient $I, J \subseteq K[\bar{X}]$. Alors $V(I) \cap V(J) = V(I, J)$: c'est évident. En fait, si I_j, $j \in J$, est une famille de sous-ensembles de $K[\bar{X}]$ alors $\bigcap_{j \in J} V(I_j) = V(\bigcup_{j \in J} I_j)$. De plus, $V(I) \cup V(J) = V(I \cdot J)$, où $I \cdot J = \{f(\bar{X})g(\bar{X}) \mid f(\bar{X}) \in I, \, g(\bar{X}) \in J\}$. En effet, tout d'abord l'inclusion $V(I) \cup V(J) \subseteq V(I \cdot J)$ est évidente. Ensuite, soit $\bar{a} \in V(I \cdot J)$, et supposons que $\bar{a} \notin V(I)$. Par définition, il existe donc $f(\bar{X}) \in I$ tel que $f(\bar{a}) \neq 0$. Par hypothèse, $f(\bar{a})g(\bar{a}) = 0$ pour tout $g(\bar{X}) \in J$, ce qui entraîne (car K est un corps) que $g(\bar{a}) = 0$ pour tout $g(\bar{X}) \in J$, c'est à dire, $\bar{a} \in V(J)$. Nous avons donc montré :

Proposition. La famille des sous-ensembles algébriques de K^n est close par intersection (arbitraire) et union finie. C'est donc l'ensemble des fermés d'une topologie sur K^n, appelée la **topologie 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.

Si $I \subseteq F[\bar{X}]$, alors l'ensemble $V(I) \cap F^n$ sera aussi appelé un **fermé de Zariski de** F^n. La proposition ci-dessous (ou plutôt, sa démonstration) montre que ces ensembles sont aussi les fermés d'une topologie sur F^n, qui sera aussi appelée la topologie de Zariski sur F. Nous verrons qu'il n'y a pas de confusion à craindre.

(7.3) **Noetherianité de la topologie de Zariski**. 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. La classe des anneaux noethériens est aussi close par quotient. L'anneau de polynômes $K[\bar{X}]$ est donc noethérien (Attention, ce n'est plus vrai quand $\bar{X}$ est un uplet infini de variables).

Soient $I \subseteq J \subset K[\bar{X}]$. On voit tout d'abord qu'on peut supposer que I et J sont des idéaux : en effet, si $f_1(\bar{X}), \ldots, f_m(\bar{X})$ s'annulent en un point $\bar{a}$, alors toute $K[\bar{X}]$-combinaison linéaire de $f_1(\bar{X}), \ldots, f_m(\bar{X})$ s'annulera aussi en $\bar{a}$. Nous savons que $V(I) \supseteq V(J)$. Si $V(I) \neq V(J)$, alors il existera forcément un élément $f(\bar{X}) \in J$, $f(\bar{X}) \notin I$. Ce qui veut dire que **à une inclusion stricte** de fermés de K^n correspond une contenance stricte d'idéaux de $K[\bar{X}]$.

Mais nous savons qu'il n'existe pas de chaîne croissante infinie d'idéaux de $K[\bar{X}]$. Cela entraîne donc qu'il n'existe pas de chaîne décroissante infinie de fermés de K^n.

(7.4) **Remarques sur la compacité**. **Définition**. Un espace topologique satisfaisant que toute suite décroissante de fermés est finie, est appelé **noethérien**.

Remarquons tout de suite que la noethérianité entraîne que tout recouvrement par des ouverts de K^n contient un sous-recouvrement fini : en effet, en passant au complémentaire, on a une famille de fermés dont l'intersection est vide, et par noethérianité, l'intersection de cette famille est égale à une intersection finie d'éléments de la famille.

Cependant, notre espace K^n n'est pas compact au sens français : en effet il n'est pas Hausdorff. Pire, on montre que l'intersection de deux ouverts non-vide est forcément non-vide. En effet, passant au complémentaire, il suffit de montrer que si $V(I)$ et $V(J)$ sont des fermés propres de K^n, alors $V(I) \cup V(J) \neq K^n$. Soit F un sous-corps de K tel que $I, J \subseteq F[\bar{X}]$. Si $\bar{a} \in V(I) \cup V(J)$, cela veut dire que le uplet $\bar{a}$ satisfait une équation non triviale à coefficients dans F. C'est à dire nous aurons $tr.deg(\bar{a}/F) < n$. De même si $\bar{a} \in V(J)$. Donc $V(I) \cup V(J)$ ne contient aucun n-uplet d'éléments algébriquement indépendants sur F. Puisque F peut être choisi de degré de transcendance fini, et que K est "gros", il contient des n-uplets d'éléments algébriquement indépendants au-dessus de F, qui ne sont donc pas dans $V(I) \cup V(J)$. Cela montre que $V(I) \cup V(J) \neq K^n$, et donc que l'intersection de leurs complémentaires est non-vide.

Le même raisonnement nous donne que dans F^n, toute suite décroissante de fermés est non-vide. De plus, on peut montrer que, si F est **infini**, alors l'intersection de deux ouverts non-vides de F^n est non-vide (Voir exercice (7.14)).

(7.5) **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 $V = V_0 \cup V_1$ où V_0 et V_1 sont des fermés contenus strictement dans V. Si V_0 est irréductible, on ne fait rien, sinon on trouve des fermés V_{00} et V_{01} contenus strictement dans V_o et tels que $V_0 = V_{00} \cup V_{01}$; on fait de même pour V_1, pour V_{00}, 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. Cet arbre est donc un arbre fini, et ses noeuds terminaux sont des fermés irréductibles contenus dans V.

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.

(7.6) 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 $L = K[X]/M$ contient naturellement K comme sous-corps, et sa clôture algébrique $\tilde{L}$ est une extension élémentaire de K. Soient $f_1(\bar{X}), \ldots, f_m(\bar{X})$ 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 $\tilde{L}$, $K \models \exists \bar{x}\, f_1(\bar{x}) = f_2(\bar{x}) = \cdots = f_m(\bar{x}) = 0$, ce qui montre $V(I) \neq \emptyset$.

(7.7) **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 $V(J) = \emptyset$: en effet, 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 $g(\bar{X}, Y), g_1(\bar{X}, Y), \ldots, g_m(\bar{X}, Y) \in K[\bar{X}, Y]$, et $f_1(\bar{X}), \ldots, f_m(\bar{X}) \in I$ 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.

(7.8) **Remarque**. Ce résultat est faux lorsque K n'est pas algébriquement clos. Le problème vient en fait du lemme précédent : si F est un corps quelconque, et I un idéal propre de $F[\bar{X}]$, il se peut très bien que $V(I) \cap F^n$ soit vide.

Par exemple, soit $F = \mathbf{Q}$, ou même $F = \mathbf{R}$, et prenons pour I l'idéal engendré par $X^2 + Y^2 + 1$. Alors $V(I) \cap \mathbf{R}^2 = \emptyset$. Pourtant, dans $\mathbf{C}$, $V(I)$ est assez "gros": pour tout $a \in \mathbf{C}$, il existe $b \in \mathbf{C}$ tel que $(a, b) \in V(I)$: on prend tout simplement $b = \sqrt{1 - a^2}$.

(7.9) 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. 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 $I(V)$ ne soit 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: 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.

(7.10) **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 $I \cap F[\bar{X}]$. 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 $f_1(\bar{X}), \dots, f_r(\bar{X}) \in K_1[\bar{X}]$ 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 $g_1(\bar{X}), \dots, g_r(\bar{X}) \in K[\bar{X}]$ 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 $\bar{b} = (b_{im})_{m\in S, i=1,\dots,r}$ et $c_m(\bar{Y}) \in K_1[\bar{Y}]$ est une K_1-combinaison linéaire des variables Y_{im}, $(m \in S,\ 1 \le i \le r)$. 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 nous donne le résultat suivant:
Tout élément de $I(V) \subset K[\bar{X}]$ est une K-combinaison linéaire de polynômes $m - A_m$, $m \in M \setminus B$.

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

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

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.

(7.11) Supposons maintenant que $F_1 \subseteq F_2$ soient des sous-corps de K, et soient $\mathcal{T}_1$ la topologie de Zariski sur F_1^n, $\mathcal{T}_2$ celle de F_2^n. Les fermés de $\mathcal{T}_1$ seront donc les ensembles $V(I) \cap F_1^n$, où $I \subset F_1[\bar{X}]$. Il est clair qu'un fermé de $\mathcal{T}_1$ est l'intersection avec F_1^n d'un fermé de $\mathcal{T}_2$. La réciproque, qui montre que la topologie $\mathcal{T}_1$ coïncide avec la topologie induite par $\mathcal{T}_2$ sur F_1^n ($\subseteq F_2^n$) est vraie.

Une démonstration très élégante de cette réciproque m'a été indiquée par W. Hodges. Soit $I \subseteq F_2[\bar{X}]$; nous allons trouver $J \subseteq F_1[\bar{X}]$ tel que

$$V(I) \cap F_1^n = V(J) \cap F_1^n,$$

ce qui montrera le résultat.

Choisissons une base B du F_1-espace vectoriel F_2; alors tout élément de $F_2[\bar{X}]$ s'écrit comme une $F_1[\bar{X}]$-combinaison linéaire d'éléments de B. Soit $f_1(\bar{X}), \dots, f_m(\bar{X})$ un système de générateurs de I, et écrivons pour chaque $i = 1, \dots, m$,

$$f_i(\bar{X}) = \sum_{b \in B} g_{i,b}(\bar{X}) b,$$

où les $g_{i,b}(\bar{X}) \in F_1[\bar{X}]$ sont presque tous nuls. Nous avons alors, pour $\bar{a} \in F_1^n$:

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

ce qui montre le résultat. Ici nous avons utilisé le fait que les éléments de B sont F_1-linéairement indépendants pour passer de la deuxième ligne à la troisième.

(7.12) **Remarque**. Cela montre donc que nous aurions pu définir les fermés de Zariski de F^n directement dans F, sans passer pr K.

(7.13) **Exercice**. Montrez les inclusions énoncées dans (7.1).

(7.14) **Exercice**. Soit F un corps infini, et F^* une extension élémentaire de F, qui contient proprement F.

(1) Montrez que tout élément de $F^* \setminus F$ est transcendant sur F.

(2) Supposons maintenant que F^* soit de cardinalité $|F|^+$. Montrer que le degré de transcendance de F^* sur F égale $|F|^+$.

(3) En déduire que si U et V sont des ouverts de Zariski non vides de F^n, alors $U \cap V \neq \emptyset$.

(7.15) 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 $F[V]$.

Pourquoi parle-t-on de "fonctions rationnelles"? Voici une explication. Si $f(\bar{X}) \in K[\bar{X}]$, alors $f(\bar{X})$ définit une fonction $\tilde{f} : V \to K$, en posant tout simplement $\tilde{f}(\bar{a}) = f(\bar{a})$ pour $\bar{a} \in V$. On montre immédiatement que $\tilde{f} = \tilde{g}$ si et seuelement si $f(\bar{X}) - g(\bar{X}) \in I(V)$. La fonction $f(\bar{X}) \mapsto \tilde{f}$ définit donc un homomorphisme d'anneau, avec noyau $I(V)$, qui envoie $K[\bar{X}]$ dans l'anneau des fonctions de V dans K. Cela établit un isomorphisme entre $K[V]$ et un anneau de fonctions sur V. On peut donc considérer les éléments de $K[V]$ comme des fonctions définies sur K.

Si maintenant $f(\bar{X}), g(\bar{X}) \in K[\bar{X}]$, et $g(\bar{X}) \notin I(V)$, l'élément $\tilde{f}/\tilde{g}$ est une fonction (partielle) définie sur l'ouvert de Zariski $U = \{\bar{a} \in V \mid g(\bar{a}) \neq 0\}$ de V. Nous pensons donc aux éléments de $K(V)$ comme à des fonctions définies sur des ouverts de V.

(7.16) **Dimension, points génériques, etc.** 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.

(7.17) **Quelques exemples de dimension**.

(1) Soit $V = K^n = \mathbf{A}^n(K)$, $(V) = (0)$, $K[V] = K[\bar{X}]$, $K(V) = K(\bar{X})$ et donc $dim(V) = n$.

(2) Soit $f(\bar{X}) \in K[\bar{X}]$, non nul, et soit $V = V(f)$. Alors $dim(V(f)) = n - 1$.

(3) En fait plus généralement, soit V une variété, $f(\bar{X}) \in K[\bar{X}] \backslash I(V)$ et $W = V \cap V(f)$. Alors $dim(W) = dim(V) - 1$.

(7.18) Soient $\bar{a}$ et F comme ci-dessus. L'idéal $I(\bar{a}/F)$ définit alors un fermé de Zariski $((V(I(\bar{a}/F)))$, appelé le **locus** de $\bar{a}$ sur F. Par définition, ce fermé V est F-irréductible, et $\bar{a}$ est un générique de V sur F. Nous allons donner un critère d'irréductibilité de V :

Fait. Le fermé V est une variété si et seulement si $F(\bar{a}) \cap F^s = F$.

Nous n'allons pas montrer ce résultat, mais seulement montrer sa nécéssité. Supposons que $\alpha \in F(\bar{a})$ soit dans $F^s \setminus F$, et soient $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ l'ensemble des conjugués de α au-dessus de F. Soient maintenant $f(\bar{X}), g(\bar{X}) \in F[\bar{X}]$ des polynømes relativement premiers tels que $g(\bar{a}) \neq 0$ et $f(\bar{a})/g(\bar{a}) = \alpha$. Si $p(T)$ est le polynôme minimal de α au-dessus de F, alors une équation de la forme $g(\bar{X})^k p((f(\bar{X})/g(\bar{X}))$ est dans $I(\bar{a}/F)$. Si maintenant on regarde un idéal premier P de $K[\bar{X}]$ minimal contenant $I(\bar{a}/F)$, il devra nécéssairement contenir $g(\bar{X})\alpha_i - f(\bar{X})$ pour un indice i, puisque le polynôme $p(T)$ se factorise en facteurs linéaires sur K. On peut montrer que si $i \neq j$, alors l'idéal $(I(\bar{a}/F), g(\bar{X})\alpha_i - f(\bar{X}), g(\bar{X})\alpha_j - f(\bar{X}))$ de $K[\bar{X}]$ égale 1.

(7.19) **Fait**. Les discussions précédentes montrent en particulier les choses suivantes. Soit $\bar{a}$ un uplet de K, et F un sous-corps de K, $I = I(\bar{a}/F)$.

(1) Si F est algébriquement clos, alors I engendre dans $K[\bar{X}]$ un idéal premier. Le locus de $\bar{a}$ sur F est donc une **variété**.

(2) Supposons maintenant que F soit séparablement clos. Alors l'idéal J de $K[\bar{X}]$ engendré par I n'est pas nécéssairement premier, mais son radical le sera. De plus le locus de $\bar{a}$ au-dessus de F est aussi une variété.

(7.20) **Quelques remarques additionnelles**. Pour se souvenir des différents cas, il est bon de se rappeler le cas algébrique. En effet, considérons un polynôme en une variable $p(T)$, irréductible sur F. Alors l'ensemble $V(p)$ est un ensemble fini de points (de $\tilde{F}$), et chacun de ces points est une composante irréductible de $V(p)$. Si $p(T)$ a des racines distinctes, alors $V(p)$ contient plusieurs points, n'est pas irréductible, et ses composantes sont définies sur l'extension de F obtenues en rajoutant à F les racines de $p(T)$.

Si maintenant F est séparablement clos, alors le polynôme irréductible $p(T)$ n'a qu'une seule racine. Nous avons donc que $V(p)$ consiste d'un point et est irréductible. Si le degré de $p(T)$ est > 1 et $p(a) = 0$, alors $p(T) = (T - a)^{deg(p)}$, $I(V(p))$ est engendré par $T - a$, et le radical de l'idéal de $K[T]$ engendré par $p(T)$ est précisément $I(V(p))$.

Et finalement, si F est algébriquement clos, alors tout polynôme irréductible sur F est linéaire, et donc définit une variété.

(7.21) **Variétés projectives**. Dans les paragraphes précédents, nous avons étudié des sous-ensemble algébriques de K^n. La variété K^n est ausi appelée l'**espace affine de dimension** n et est notée $\mathbf{A}^n(K)$. (La notation $\mathbf{A}$ est une notation fonctorielle). De la même façon, les variétés projectives sont des sous ensemble de l'**espace projectif** $\mathbf{P}^n(K)$ de dimension n sur K.

$\mathbf{P}^n(K)$ est construit de la façon suivante. On prend le quotient de $K^{n+1} \setminus \{0\}$ par la relation d'équivalence $\sim$ "être proportionnel à", c'est à dire $(a_0, \dots, a_n) \sim (b_0, \dots, b_n)$ si et seulement s'il existe $\lambda \in K$ tel que $a_i = \lambda b_i$ pour $i = 0, \dots, m$. Notons qu'un tel λ est forcément non-nul, puisque l'un des a_i doit être non nul.

La classe d'équivalence de $(a_o, \dots, a_n)$ est alors notée $(a_0 : \dots : a_n)$. L'ensemble des classes d'équivalence est l'espace projectif. D'après notre définition il est évident que $\mathbf{P}^n(K)$ peut être aussi décrit comme l'ensemble des droites de $\mathbf{A}^{n+1}(K)$.

On peut aussi exprimer $\mathbf{P}^n(K)$ comme une réunion d'espace affines de dimension n. En effet, pour chaque $i = 0, \dots, n$, soit

$$U_i = \{(a_0 : \dots : a_n) \in \mathbf{P}^n(K) \mid a_i \neq 0\}.$$

Alors certainement $\mathbf{P}^n(K) = \bigcup_{i=0}^m U_i$. De plus chaque U_i est en bijection avec $\mathbf{A}^n(K)$: notons que tout élément de U_i peut s'écrire $(b_0 : \dots : b_n)$ avec $b_i = 1$: en effet, $(1/a_i)(a_0, \dots, a_n) = (b_0, \dots, b_n)$. Nous avons donc une bijection $f_i : U_i \to \mathbf{A}^n(K)$, obtenue à partir de l'application

$$(a_0, \dots, a_n) \mapsto (a_0/a_i, \dots, \widehat{a_i/a_i}, \dots, a_n/a_i).$$

Un sous ensemble S de $\mathbf{P}^n(K)$ est un **fermé de Zariski** si pour tout $i = 0, \dots, m$, $f_i(S)$ est un fermé de Zariski de $\mathbf{A}^n(K)$. On vérifie que cela définit bien une topologie noethérienne sur $\mathbf{P}^n(K)$, où les ensembles U_i sont des ouverts. En fait quand on travaille dans $\mathbf{P}^n(K)$, on travaille très souvent localement, c'est à dire, dans un des U_i, et on peut alors utiliser les résultats sur les espaces affines. Une sous-variété de $\mathbf{P}^n(K)$ est un fermé irréductible S, et on vérifie que c'est le cas si et seulement si $f_i(S \cap U_i)$ est une variété de l'espace affine pour tout i.

Si maintenant $S \subset \mathbf{P}^n(K)$ est un fermé, on peut aussi regarder l'idéal $I(S)$ des polynômes $f(X_0, \dots, X_n) \in K[X_0, \dots, X_n]$ tel que pour tout $(a_0, \dots, a_n) \in \mathbf{A}^{n+1}(K) \setminus \{0\}$ avec $(a_0 : \dots : a_n) \in S$, on ait $f(a_0, \dots, a_n) = 0$. On vérifie que c'est un idéal **homogène**, c'est à dire engendré par des polynômes $f(\bar{X})$ où tous les monômes apparaissant avec un coefficient non nul ont le même degré (rappelons que le degré du monôme $X_0^{i(0)} \cdots X_n^{i(n)}$ est $i(0) + \dots + i(n)$).

8. Types définissables, héritiers.

Nous fixons une théorie complète T dans un langage $\mathcal{L}$ (dénombrable), et un modèle M^* de T suffisamment saturé, infini, dans lequel nous travaillerons. Tous les ensembles de paramètres sont des sous-ensembles de M^*, les modèles de T sont des sous-structures élémentaires de M^*.

(8.1) **Définitions**. Soit $p(\bar{x}) \in S_n(A)$, et $B \subseteq A$.

(1) Nous disons que p est définissable sur B si pour toute formule $\varphi(\bar{x}, \bar{y}) \in \mathcal{L}$, il existe une formule $d_\varphi(\bar{y}) \in \mathcal{L}(B)$ telle que pour tout $\bar{b} \in A$,

$$\varphi(\bar{x}, \bar{b}) \in p(\bar{x}) \iff M^* \models d_\varphi(\bar{b}).$$

(2) Si p est définissable sur A, on dit tout simplement que p est définissable.

(3) L'ensemble des formules d_φ est appelé un schéma de définition de p.

(8.2) **Remarques**. (1) Dire qu'un type $p \in S_n(A)$ est définissable, c'est dire que l'ensemble $\{\bar{a} \in A^{\ell(\bar{y})} \mid \varphi(\bar{x}, \bar{a}) \in p(\bar{x})\}$ est l'intersection avec $A^{\ell(\bar{y})}$ d'un ensemble $\mathcal{L}(A)$-définissable dans M.

(2) Donc en particulier, si $p(\bar{x})$ est définissable, et si $\varphi_1(\bar{x}, \bar{y}_1)$ et $\varphi_2(\bar{x}, \bar{y}_2)$ sont des formules, avec définitions $d_{\varphi_1}(\bar{y}_1)$ et $d_{\varphi_2}(\bar{y}_2)$ respectives, alors la formule $d_{\varphi_1}(\bar{y}_1) \wedge d_{\varphi_2}(\bar{y}_2)$ sera une définition pour la formule $\varphi_1(\bar{x}, \bar{y}_1) \wedge \varphi_2(\bar{x}, \bar{y}_2)$. On raisonne de même pour les autres opérations booléennes.

Si notre type $p(\bar{x})$ est axiomatisé (modulo T) par des combinaison booléennes de formules de la forme $\varphi(\bar{x}, \bar{a})$, avec $\varphi(\bar{x}, \bar{y}) \in \Delta$ (un ensemble de formules), il suffira donc, pour montrer que $p(\bar{x})$ est définissable, de montrer que d_φ eziste pour chacune des formules de Δ. En particulier, si notre théorie T élimine les quantificateurs, pour vérifier qu'un type $p(\bar{x})$ est définissable, il suffira donc de vérifier que toutes les formules sans quantificateurs ont une définition.

(8.3) **Exemple 1**. Un type isolé est toujours définisssable. En effet, soit $\psi(\bar{x}, \bar{a})$ une formule isolant $p(\bar{x}) \in S_n(A)$. Alors $d_\varphi(\bar{y})$ est la formule $\forall \bar{x}(\psi(\bar{x}, \bar{a}) \to \varphi(\bar{x}, \bar{y}))$.

(8.4) **Exemple 2**. Soit T la théorie de l'ordre dense sans extrémités, et soient $A = \mathbf{Q}$, $a \in A$ et $r \in \mathbf{R} \setminus \mathbf{Q}$.

Soit $p_{a^+}(x)$ le type (sur A) défini par $\{x < b \mid b \in \mathbf{Q},\ b > a\} \cup \{x > a\}$. Alors $p_{a^+}(x)$ est définissable. En effet $d_{x<y}(y) = y > a$, $d_{x>y}(y) = y \leq a$, and $d_{x=x}(y) = y \neq y$.

Soit maintenant $q_r(x) = tp(r/\mathbf{Q})$. Alors on peut montrer que $q_r(x)$ n'est pas définissable. Rappelons que $q_r(x)$ est donné par la coupure $C = \{s \in \mathbf{Q} \mid s < r\}$. En effet (par élimination des quantificateurs) $q_r(x)$ est axiomatisé par les formules $\{x > s \mid s \in C\} \cup \{x < s \mid s \in \mathbf{Q} \setminus C\}$. Si $q_r(x)$ était définissable, alors la formule $d_{x<y}(y)$ définirait l'ensemble C. Cependant, si $a_1 < \ldots < a_m$ sont des rationnels, on sait que deux éléments quelconques de (a_i, a_{i+1}) réalisent le même type sur $\bar{a} = (a_1, \ldots, a_n)$. Donc, si $r \in (a_i, a_{i+1})$, il existe des éléments de C et de $\mathbf{Q} \setminus C$ qui réalisent le même type sur $\bar{a}$: C ne peut donc être définissable.

(8.5) **Exemple 3**. Soit $\mathcal{L}$ le langage de l'egalité, T la théorie d'un ensemble infini. Nous savons que T est complète, et élimine les quantificateurs. Si $p(\bar{x})$ est un type sur A, alors

$p(\bar{x})$ est une combinaison booléenne de formules de la forme $x_i = a$ pour $a \in A$. Il est clair que les formules $d_{x_i=y}(y)$ existent.

(8.6) **Définition**. Soit $p(\bar{x}) \in S_n(A)$, et supposons que $p(\bar{x})$ soit définissable par un schéma (d_φ). Soit $B \supset A$. On définit alors $p(B)(\bar{x})$ comme étant l'ensemble $\{\varphi(\bar{x}, \bar{b}) \mid M^* \models d_\varphi(\bar{b})\}$.

Attention : $p(B)(\bar{x})$ est un ensemble de formules de $\mathcal{L}(B)$. Mais nous n'avons pas dit qu'il est consistant, encore moins qu'il est complet.

Lemme. Le schéma (d_φ) définit un type sur B pour tout $B \supset A$ si et seulement si les conditions suivantes sont satisfaites (dans M^*) :

(a) Pour toute formule $\varphi(\bar{x}, \bar{y}) \in \mathcal{L}$,

$$M^* \models \forall \bar{y}\, (\neg d_\varphi(\bar{y}) \iff d_{\neg\varphi}(\bar{y})).$$

(b) Pour toutes formules $\varphi_1(\bar{x}, \bar{y}_1), \ldots, \varphi_m(\bar{x}, \bar{y}_m)$,

$$M^* \models d_{\varphi_1}(\bar{y}_1) \wedge \cdots \wedge d_{\varphi_m}(\bar{y}_m) \to \exists \bar{x} \bigwedge_{i=1}^{m} \varphi_i(\bar{x}, \bar{y}_i).$$

Démonstration. Soit $B \supset A$. Tout d'abord, la condition (a) nous dit que si $p(B)(\bar{x})$ est consistant, alors il est complet. Mais sa consistance est impliquée par la condition (b).

Corollaire. Soit $M \prec M^*$, et $p(\bar{x}) \in S_n(M)$ un type définissable, avec schéma de définition (d_φ). Alors pour tout $B \supset M$, $p(B)(\bar{x})$ est un type (complet) sur B, qui prolonge $p(\bar{x})$.

Démonstration. Que $p(B)(\bar{x})$ prolonge $p(\bar{x})$ est évident car (d_φ) est un schéma de définition de $p(\bar{x})$. Que le schéma (d_φ) satisfasse les conditions du lemme précédent est aussi évident, puisque $M \prec M^*$.

(8.7) **Proposition**. Soit $p(\bar{x}) \in S_n(M)$, $M \prec M^*$, et soient (d_φ) et (d'_φ) deux schémas de définitions de $p(\bar{x})$. Alors $M^* \models \forall \bar{y}(d_\varphi(\bar{y}) \leftrightarrow d'_\varphi(\bar{y}))$ pour toute $\varphi(\bar{x}, \bar{y}) \in \mathcal{L}$.

Démonstration. Pour tout $\bar{a}$ dans M, nous avons

$$M \models d_\varphi(\bar{a}) \iff \varphi(\bar{x}, \bar{a}) \in p(\bar{x}) \iff M \models d'_\varphi(\bar{a}).$$

Comme $M \prec M^*$, cela montre le résultat.

(8.8) Ces deux résultats nous disent donc que si $p(\bar{x})$ est un type sur $M \prec M^*$ qui est définissable, alors pour tout $A \supset M$, $p(\bar{x})$ a une extension privilégiée $p(A)(\bar{x})$ à un type sur A, et ce type ne dépend pas du schéma de définition de $p(\bar{x})$ choisi. Notons que le type $p(A)(\bar{x})$ est certainement défini sur M.

(8.9) **Définition**. Soit $\varphi(\bar{x}, \bar{y}) \in \mathcal{L}$. Nous disons que $\varphi(\bar{x}, \bar{y})$ est **stable** si on ne peut trouver dans M^* de suites $(\bar{a}_i)$ et $(\bar{b}_i)$, $i \in \mathbf{N}$, telles que pour tous $i, j \in \mathbf{N}$,

$$M^* \models \varphi(\bar{a}_i, \bar{b}_j) \iff \mathbf{N} \models i < j.$$

Sinon, on dira que $\varphi(\bar{x}, \bar{y})$ est **instable**.

(8.10) **Remarques**. (1) La définition dépend de la partition $(\bar{x}, \bar{y})$ des variables de φ. Elle dépend aussi bien entendu de la théorie T, puisqu'on travaille dans M^*.

(2) Supposons que $\varphi(\bar{x}, \bar{y})$ soit instable, et soit $(I, <)$ un ordre (de cardinalité $< |M^*|$). Par compacité et saturation de M^*, il existe des suites $(\bar{a}_i)$, $(\bar{b}_i)$, $i \in I$, de uplets de M^* telles que pour tous $i, j \in I$,

$$M^* \models \varphi(\bar{a}_i, \bar{b}_j) \iff I \models i < j.$$

En effet, nous enrichissons le langage avec des nouveaux symboles de constantes, groupés en uplets $\bar{c}_i$, $\bar{d}_i$, $i \in I$, $\ell(\bar{c}_i) = \ell(\bar{x})$, $\ell(\bar{b}_i) = \ell(\bar{y})$, puis nous considérons la théorie T' obtenue en rajoutant à $Th(M^*)$ les énoncés (du nouveau langage)

$$\{\varphi(\bar{c}_i, \bar{d}_j) \mid i < j \in I\} \cup \{\neg\varphi(\bar{c}_i, \bar{d}_j) \mid j \leq i \in I\}.$$

Tout fragment fini de cette théorie T' est satisfaisable dans M^*, car il ne met en jeu qu'un sous-ensemble fini I_0 d'éléments de I, et que tout ordre linéaire fini se plonge dans $(\mathbf{N}, <)$.

(3) Si $\varphi(\bar{x}, \bar{y})$ est stable, alors il existe $n \in \mathbf{N}$, tel qu'il n'existe pas de suite $(\bar{a}_i)$, $(\bar{b}_i)$, $0 \leq i \leq n$, telles que pour tous i, j

$$M^* \models \varphi(\bar{a}_i, \bar{b}_j) \iff \mathbf{N} \models i < j.$$

(4) Si $\varphi(\bar{x}, \bar{y})$ est stable, alors $\neg\varphi(\bar{x}, \bar{y})$ aussi.

(5) Si $\varphi_1(\bar{x}, \bar{y}_1)$ et $\varphi_2(\bar{x}, \bar{y}_2)$ sont stables, alors $\varphi_1(\bar{x}, \bar{y}_1) \wedge \varphi_2(\bar{x}, \bar{y}_2)$ aussi. Donc aussi toute combinaison booléenne de $\varphi_1(\bar{x}, \bar{y}_1)$ et de $\varphi_2(\bar{x}, \bar{y}_2)$.

(6) Il est clair que si $<$ définit un ordre total sur un sous-ensemble infini de M^*, alors la formule $x < y$ n'est pas stable : on prend tout simplement une suite infinie $(a_i)_{i \in \mathbf{N}}$ d'éléments de M^* telle que $a_i < a_j$ si et seulement si $i < j$, et prenant $b_i = a_i$, on voit que la formule est instable.

(8.11) Rappelons d'abord le théorème de Ramsey : Soit I un ensemble infini (avec un ordre), et soit $[I]^n$ l'ensemble des suites $i(1) < \ldots < i(n)$ d'éléments de I. Si $F : [I]^n \to \{0, 1\}$ est une fonction, alors il existe un sous-ensemble infini J de I tel que F soit constante sur $[J]^n$.

Exercice. Montrez les items (3) – (5) de la remarque ci-dessus.

(8.12) **Théorème**. Les conditions suivantes sont équivalentes :
(1) Pour tous $M \prec M^*$, et $p(\bar{x}) \in S_n(M)$, alors $p(\bar{x})$ est définissable.
(2) T est κ-stable pour tout $\kappa = \kappa^{\aleph_0}$.
(3) Toute formule de $\mathcal{L}$ est stable.

Démonstration. (1)$\to$(2). Soit $M \prec M^*$. Il existe au plus $|M|$-formules de $\mathcal{L}(M)$, et donc (comme $\mathcal{L}$ est dénombrable) au plus $|M|^{\aleph_0}$ schémas de définition. Cela entraîne que $|S_n(M)| \leq |M|^{\aleph_0}$. Soit maintenant $A \subset M^*$ un ensemble de cardinalité $\lambda = \lambda^{\aleph_0}$. Alors il existe $M \prec M^*$ de cardinalité λ et contenant A. Nous avons alors

$$|S_n(A)| \leq |S_n(M)| \leq \lambda^{\aleph_0} = |M|,$$

ce qui montre que T est λ-stable pour tout cardinal $\lambda = \lambda^{\aleph_0}$.

(2)$\to$(3). Soit $\varphi(\bar{x}, \bar{y}) \in \mathcal{L}$. Nous allons montrer que $\varphi(\bar{x}, \bar{y})$ est nécéssairement stable. En effet, soit κ un cardinal. En utilisant des resultats de théorie des ensembles, on montre qu'il existe un ordre dense sans extrémités I de cardinalité κ, tel que $|S_1(I)| > \kappa$ (pour la théorie $Diag(I)$). Soient $(\bar{a}_i)$ et $(\bar{b}_i)$, $i \in I$, des suites comme dans la remarque (8.10)(2), et $B = \bigcup\{\bar{b}_i \mid i \in I\}$. Chaque type sur I est (uniquement) déterminé par une coupure C de I (car I est un ordre dense), et chaque coupure C de I donne un type partiel $\Sigma_C(\bar{x})$ sur B : $\{\neg\varphi(\bar{x}, \bar{b}_i) \mid i \in C\} \cup \{\varphi(\bar{x}, \bar{b}_i) \mid i \in C\}$.

(3)$\to$(1). Soient $M \prec M^*$, $p \in S_n(M)$. Nous voulons montrer que $p(\bar{x})$ est définissable. Soit $\bar{c}^*$ une réalisation de $p(\bar{x})$ dans M^*, et soit N un entier satisfaisant la conclusion de (8.10)(4) pour les formules $\varphi(\bar{x}, \bar{y})$ et $\neg\varphi(\bar{x}, \bar{y})$. Nous allons définir par induction des sous-ensembles finis A_i et B_i de $M^{\ell(\bar{y})}$, et des $\ell(\bar{x})$-uplets $\bar{c}_i$ de M, pour $i \in \mathbf{N}$, tels que, pour tout $k \in \mathbf{N}$:

(a) Si $W \subseteq \{0, \dots, k-1\}$ est tel qu'il existe $\bar{b} \in M$ satisfaisant $\{\varphi(\bar{c}_i, \bar{y}) \mid i \in W\}$, mais cependant $M^* \models \neg\varphi(\bar{c}^*, \bar{b})$, alors il existe un tel $\bar{b}$ dans A_k.

(b) Si $W \subseteq \{0, \dots, k-1\}$ est tel qu'il existe $\bar{b} \in M$ satisfaisant $\{\neg\varphi(\bar{c}_i, \bar{y}) \mid i \in W\}$, mais cependant $M^* \models \varphi(\bar{c}^*, \bar{b})$, alors il existe un tel $\bar{b}$ dans B_k.

(c) Si $\bar{b} \in A_k$ alors $M^* \models \neg\varphi(\bar{c}^*, \bar{b})$; si $\bar{b} \in B_k$ alors $M^* \models \varphi(\bar{c}^*, \bar{b})$.

(d) Si $\bar{b}$ est un uplet de $\bigcup_{i=0}^{k} A_i \cup B_i$, alors $M \models \varphi(\bar{c}_k, \bar{b}) \iff M^* \models \varphi(\bar{c}_k, \bar{b})$.

On construit ces ensembles par induction sur k. On commence avec A_0 : alors nous nous intéréssons à $W = \emptyset \subseteq \emptyset$. S'il existe $\bar{b} \in M$ tel que $M^* \models \neg\varphi(\bar{c}^*, \bar{b})$, alors on met ce $\bar{b}$ dans A_0 ; et sinon on ne fait rien. De même, s'il existe $\bar{b} \in M$ tel que $M^* \models \varphi(\bar{c}^*, \bar{b})$, alors on en met un dans B_0, et sinon on ne fait rien. Il est clair que (c) est satisfait. Maintenant pour $\bar{c}_0$, il faut remarquer la chose suivante :

Assertion. Si $B \subset M^{\ell(\bar{y})}$ est un ensemble fini, alors il existe $\bar{c} \in M$ tel que pour tout $\bar{b} \in B$ on ait :

$$M \models \varphi(\bar{c}, \bar{b}) \iff M^* \models \varphi(\bar{c}^*, \bar{b}).$$

En effet, puisque B est fini, l'ensemble

$$\{\varphi(\bar{x}, \bar{b}) \mid \bar{b} \in B,\ M^* \models \varphi(\bar{c}^*, \bar{b})\} \cup \{\neg\varphi(\bar{x}, \bar{b}) \mid \bar{b} \in B,\ M^* \models \neg\varphi(\bar{c}^*, \bar{b})\}$$

est un ensemble fini de formules, dont la conjonction est satisfaite par c^*, et donc est aussi satisfaite dans M, puisque $M \prec M^*$.

Nous pouvons donc trouver $\bar{c}_0 \in M$ satisfaisant (d). Pour un k arbitraire, la démonstration est similaire : on énumère les sous-ensembles W de $\{0, 1, \dots, k-1\}$, on regarde si (a) nous dit de faire quelque chose : si oui, on met un uplet $\bar{b}$ dans A_k ; sinon, on n'en met pas. par construction, A_k satisfera (a) et (c). De même pour construire B_k, et enfin, on utilise le "fait" pour trouver $\bar{c}_k$ satisfaisant (d).

Nous allons d'abord montrer que si $0 \leq i(0) < i(1) < \ldots < i(m) \in \mathbf{N}$ et $\bar{b} \in M$ sont tels que

$$M^* \models \bigwedge_{j=0}^{m} \varphi(\bar{c}_{i(j)}, \bar{b}) \wedge \neg\varphi(\bar{c}^*, \bar{b}),$$

alors il existe $\bar{b}_0, \ldots, \bar{b}_m \in M$ tels que pour tous $j, r \leq m$,

$$M \models \varphi(\bar{c}_{i(j)}, \bar{b}_r) \iff j < r.$$

En effet, appliquant (a) à $W = \emptyset$, il existe $\bar{b}_0 \in B_{i(0)}$ tel que $M^* \models \neg\varphi(\bar{c}^*, \bar{b}_0)$. Par (c), nous avons alors $M \models \neg\varphi(\bar{c}_{i(j)})$ pour $j \geq 0$.

Soit maintenant $0 \leq k < m$, et supposons que nous ayons construit $\bar{b}_0, \ldots, \bar{b}_k$ satisfaisant les conditions requises. Nous voulons donc trouver $\bar{b}_{k+1} \in M$ tel que

$$M \models \bigwedge_{0 \leq j \leq k} \varphi(\bar{c}_{i(j)}, \bar{b}_{k+1}) \wedge \bigwedge_{k < j \leq m} \neg\varphi(\bar{c}_{i(j)}, \bar{b}_{k+1}).$$

Par (a) appliqué à $W = \{i(0), \ldots, i(k)\}$, il existe $\bar{b}_{k+1} \in B_{i(k)+1}$ tel que $M^* \models \neg\varphi(\bar{c}^*, \bar{b}_{k+1}) \wedge \bigwedge_{j=0}^{k} \varphi(\bar{c}_{i(j)}, \bar{b}_{k+1})$. Par (c), nous avons alors $M \models \neg\varphi(\bar{c}_{i(j)}, \bar{b}_{k+1})$ pout $j \geq k+1$.

Notons que par hypothèse (de stabilité de $\varphi(\bar{x}, \bar{y})$), et par notre choix de N, nous avons nécéssairement que $m \leq N$. De même, on montre que si $0 \leq i(0) < i(1) < \ldots < i(m) \in \mathbf{N}$ et $\bar{b} \in M$ sont tels que

$$M^* \models \bigwedge_{j=0}^{m} \neg\varphi(\bar{c}_{i(j)}, \bar{b}) \wedge \varphi(\bar{c}^*, \bar{b}),$$

alors il existe $\bar{b}_0, \ldots, \bar{b}_m \in M$ tels que pour tous $j, r \leq m$,

$$M \models \varphi(\bar{c}_{i(j)}, \bar{b}_r) \iff j < r.$$

Nous avons donc montré :

(I) Si $\bar{b} \in M$ et il existe un sous-ensemble W de $\{0, \ldots, 2N\}$ de cardinalité $N+1$ tel que $M \models \bigwedge_{i \in W} \varphi(\bar{c}_i, \bar{b})$, alors $M^* \models \varphi(\bar{a}, \bar{c}^*)$.

(II) Si $\bar{b} \in M$ et il existe un sous-ensemble W de $\{0, \ldots, 2N\}$ de cardinalité $N+1$ tel que $M \models \bigwedge_{i \in W} \neg\varphi(\bar{c}_i, \bar{b})$, alors $M^* \models \neg\varphi(\bar{a}, \bar{c}^*)$.

Notons que pour tout uplet $\bar{b}$ de M, les ensembles $\{i \in \{0, \ldots, 2N\} \mid M^* \models \varphi(\bar{c}^*, \bar{b})\}$ et $\{i \in \{0, \ldots, 2N\} \mid M^* \models \neg\varphi(\bar{c}^*, \bar{b})\}$ forment une partition de $\{0, \ldots, 2N\}$, et donc l'un des deux (mais pas les deux) doit être de taille $\geq N+1$.

Les propriétés (I) et (II) entraînent que pour tout uplet $\bar{b}$ de M, nous avons $\varphi(\bar{x}, \bar{b}) \in p(\bar{x})$ si et seulement s'il existe un sous-ensemble W de $\{0, \ldots, 2N\}$ de taille $N+1$, et tel que $M \models \bigwedge_{j \in W} \varphi(\bar{c}_j, \bar{b})$. Cela nous donne la définition $d_\varphi(\bar{y})$:

$$d_\varphi(\bar{y}) = \bigvee_{W \subset \{0, \ldots, 2N\}, |W| = N+1} \bigwedge_{j \in W} \varphi(\bar{c}_j, \bar{y}).$$

(8.13) **Remarques et discussion**. Soit $\varphi(\bar{x}, \bar{y})$ une formule, et $A \subset M^*$. Un φ-type partiel sur A est un ensemble de formules, qui sont équivalentes (modulo $Diag(A)$), à une combinaison booléenne de formules de la forme $\varphi(\bar{x}, \bar{a})$ pour un uplet $\bar{a}$ de A. Un φ-type sur A est un φ-type maximal consistant, l'ensemble de φ-types sur A est noté $S_\varphi(A)$. On remarque qu'il existe une application $S_n(A) \to S_\varphi(A)$, donnée en associant à un type $p(\bar{x})$ le type

$$p|_{\varphi}(\bar{x}) = Diag(A) \cup \{\varphi(\bar{x}, \bar{a}) \mid \varphi(\bar{x}, \bar{a}) \in p(\bar{x})\} \cup \{\neg\varphi(\bar{x}, \bar{a}) \mid \neg\varphi(\bar{x}, \bar{a}) \in p(\bar{x})\}.$$

Il est facile de voir que cette application est surjective. On peut donner des définitions analogues pour des ensembles Δ de formules.

Nous avons en fait montré bien plus. Supposons la formule $\varphi(\bar{x}, \bar{y})$ stable.

(1) Tous les φ-types sur des sous-structures élémentaires de M^* sont définissables, c'est à dire, d_φ existe.

(2) De plus nous avons montré que la définition $d_\varphi(\bar{y})$ est de forme spéciale : c'est une combinaison booléenne de formules de la forme $\varphi(\bar{c}_i, \bar{y})$, $i \in \{0, \ldots, 2N\}$.

(3) De plus, la démonstration de (8.12) nous montre que si $\varphi(\bar{x}, \bar{y})$ est instable, alors pour tout cardinal infini κ il existe un sous-ensemble B de M^* de cardinalité κ tel que $|S_\varphi(B)| > \kappa$: tout simplement parce que les types partiels $\Sigma_C(\bar{x})$ exhibés dans la démonstration de (2)$\to$(3) sont en fait des φ-types partiels.

D'autre part, si $\varphi(\bar{x}, \bar{y})$ est stable, alors puisque tout φ-type sur une sous-structure élémentaire M de M^* est définissable, et que connaître d_φ est suffisant pour connaître la définition d'un φ-type, il s'ensuit que

$$|S_\varphi(M)| \leq |M|.$$

Nous avons donc montré l'équivalence suivante :

$$\varphi(\bar{x}, \bar{y}) \text{ est stable } \iff \text{ pour tout } A \subset M^*,\ |S_\varphi(A)| \leq |A| + \aleph_0.$$

(3) Il existe des théories instables qui ont quand même beaucoup de formules stables. Par exemple, on peut montrer que si K est un corps (peut-être avec d'autre stucture), si $T = Th(K)$ et $\varphi(\bar{x}, \bar{y})$ est une formule **sans quantificateurs** du langage de corps $(\{+, -, \cdot, 0, 1\})$, alors $\varphi(\bar{x}, \bar{y})$ est stable. On réduit la preuve de cette assertion aux formules atomiques, c'est à dire aux formules

$$\varphi(\bar{x}, \bar{y}) : f(\bar{x}, \bar{y}) = 0,$$

où $f(\bar{X}, \bar{Y}) \in \mathbf{Z}[\bar{X}, \bar{Y}]$. La démonstration utilise la noethérianité de $K[\bar{X}]$, et est laissée en exercice.

Cependant, le corps ordonné $\mathbf{R}$ n'est certainement pas stable, puisqu'un ordre total y est définissable.

(8.14) **Formules représentées dans un type, héritiers**. Soient $A \subset M^*$ et $p(\bar{x}) \in S_n(A)$, $\varphi(\bar{x}, \bar{y}) \in \mathcal{L}(A)$. On dit que $\varphi(\bar{x}, \bar{y})$ est **représentée dans** $p(\bar{x})$ s'il existe un uplet $\bar{a}$ dans A tel que $\varphi(\bar{x}, \bar{a}) \in p(\bar{x})$.

Soient $M \subseteq A \subseteq M^*$, avec $M \prec M^*$, et $p(\bar{x}) \in S_n(M)$, $q(\bar{x}) \in S_n(A)$. On dit que $q(\bar{x})$ **hérite de** $p(\bar{x})$, ou bien **est un héritier de** $p(\bar{x})$ **sur** A si $q(\bar{x}) \supseteq p(\bar{x})$ et toute formule de $\mathcal{L}(M)$ représentée dans $q(\bar{x})$ est représentée dans $p(\bar{x})$.

Il existe une notion duale, celle de **cohéritier**, que nous n'utiliserons pas mais que je voudrais mentionner. Si M et A, $p(\bar{x})$ et $q(\bar{x})$ sont comme-ci dessus, on dira que $q(\bar{x})$ est un cohéritier de $p(\bar{x})$ si $q(\bar{x}) \supset p(\bar{x})$ et toute formule $\varphi(\bar{x}) \in q(\bar{x})$ est satisfaite dans M par un uplet $\bar{a}$. On dit aussi que $q(\bar{x})$ est **finiment satisfaisable dans** M. On vérifie facilement que si $\bar{a}$ et $\bar{b}$ sont des uplets de M^* alors $tp(\bar{a}/M, \bar{b})$ hérite de sa restriction à A si et seulement si $tp(\bar{b}/A, \bar{a})$ cohérite de sa restriction à A.

(8.15) **Proposition**. Soient $M \prec M^*$, $A \supseteq M$, et $p(\bar{x}) \in S_n(M)$. Alors $p(\bar{x})$ a un héritier sur A.

Démonstration. Soit Γ l'ensemble des formules $\varphi(\bar{x}, \bar{y})$ de $\mathcal{L}(M)$ qui ne sont **pas** représentées dans $p(\bar{x})$. Il nous faut montrer que le type partiel $\Sigma(\bar{x})$ (sur A) suivant est consistant :

$$p(\bar{x}) \cup Diag(A) \cup \{\neg\varphi(\bar{x}, \bar{a}) \mid \varphi(\bar{x}, \bar{y}) \in \Gamma,\ \bar{a} \in A^{\ell(\bar{y})}\}.$$

Il suffit donc de montrer qu'il est finiment consistant : soient $\psi(\bar{x}, \bar{m}) \in p(\bar{x})$, $\theta(\bar{m}, \bar{a}) \in Diag(A)$ et $\varphi_1(\bar{x}, \bar{m}, \bar{a}), \dots, \varphi_m(\bar{x}, \bar{m}, \bar{a})$ des formules de l'ensemble de droite. Nous supposons que $\bar{m}$ est un uplet de M, que $\bar{a}$ est un uplet de $A \setminus M$, et que toutes les formules considérées sont dans $\mathcal{L}$ (ie, tous les paramètres sont dans $\bar{a} \cup \bar{m}$). (Remarquons que si $\bar{y} = (\bar{y}_1, \bar{y}_2)$ et $\bar{m}_1$ est un uplet de M, alors si la formule $\varphi(\bar{x}, \bar{m}_1, \bar{y})$ est représentée dans M, la formule $\varphi(\bar{x}, \bar{y})$ le sera aussi. Donc, $\varphi(\bar{x}, \bar{y}) \in \Gamma$ implique $\varphi(\bar{x}, \bar{m}_1, \bar{y}_2) \in \Gamma$: c'est pourquoi nous avons pu nous ramener au cas $\bar{a} \in A \setminus M$.) Nous voulons montrer que

$$\psi(\bar{x}, \bar{m}) \wedge \theta(\bar{m}, \bar{a}) \wedge \bigwedge_{i=1}^{m} \neg\varphi_i(\bar{x}, \bar{m}, \bar{a})$$

est consistante. Sinon, on aurait (puisque $\bar{a} \subset A \setminus M$)

$$\psi(\bar{x}, \bar{m}) \vdash (\neg\theta(\bar{m}, \bar{y}) \vee \bigvee_{i=0}^{m} \varphi_i(\bar{x}, \bar{m}, \bar{y}).$$

D'autre part, commme $M \prec M^*$, il existe $\bar{a}' \in M$ tel que $M \models \theta(\bar{a}', \bar{m})$. Puisque les formules $\varphi_i(\bar{x}, \bar{y})$ sont dans Γ, nous avons donc

$$p(\bar{x}) \vdash \psi(\bar{x}, \bar{m}) \wedge \theta(\bar{m}, \bar{a}') \wedge \bigwedge_{i=0}^{m} \neg\varphi_i(\bar{x}, \bar{m}, \bar{a}').$$

Cela montre la consistance de $\Sigma(\bar{x})$. Si $q(\bar{x}) \in S_n(A)$ est un type contenant $\Sigma(\bar{x})$ alors $q(\bar{x}) \supset p(\bar{x})$, et toute formule représentée dans $q(\bar{x})$ l'est déjà dans $p(\bar{x})$: $q(\bar{x})$ est bien un héritier de $p(\bar{x})$ sur A.

(8.16) **Proposition**. Soit $M \prec M^*$, $A \supset M$. Si $p(\bar{x}) \in S_n(M)$ est définissable, alors $p(A)(\bar{x})$ est l'unique héritier de $p(\bar{x})$ sur A.

Démonstration. Il y a deux choses à montrer : que $p(A)(\bar{x})$ hérite, et qu'il est l'unique héritier.

Soit $\varphi(\bar{x}, \bar{y}, \bar{z}) \in \mathcal{L}$, $\bar{m} \in M$, et supposons que $\varphi(\bar{x}, \bar{y}, \bar{m})$ ne soit pas représentée dans $p(\bar{x})$. Puisque $p(\bar{x})$ est définissable, si $d_\varphi(\bar{y}, \bar{z})$ est la définition de φ dans $p(\bar{x})$, nous avons alors $M \models \forall \bar{y}\ \neg d_\varphi(\bar{y}, \bar{m})$. Comme $M \prec M^*$, cela entraîne que $\varphi(\bar{x}, \bar{y}, \bar{m})$ n'est pas représentée dans $p(A)(\bar{x})$.

Soit maintenant $q(\bar{x})$ un héritier de $p(\bar{x})$ sur A, et soit $\varphi(\bar{x}, \bar{y})$ une formule de $\mathcal{L}$, et $d_\varphi(\bar{y}) \in \mathcal{L}(M)$ sa définition (pour p). Alors la formule

$$\varphi^*(\bar{x}, \bar{y}) : \neg(\varphi(\bar{x}, \bar{y}) \leftrightarrow d_\varphi(\bar{y}))$$

n'est pas représentée dans $p(\bar{x})$, puisqu'elle contredit le fait que la formule $d_\varphi(\bar{y})$ définit dans M l'ensemble des $\bar{b}$ tels que $\varphi(\bar{x}, \bar{b})$ appartienne à $p(\bar{x})$. Remarquons que $\varphi^*(\bar{x}, \bar{y}) \in \mathcal{L}(M)$, car la formule $d_\varphi(\bar{y}) \in \mathcal{L}(M)$. Puisque $q(\bar{x})$ est un héritier de $p(\bar{x})$, la formule $\varphi^*(\bar{x}, \bar{y})$ n'est pas représentée dans $q(\bar{x})$, ce qui dit précisément que $q(\bar{x}) = p(A)(\bar{x})$.

(8.17) **Attention**. Que se passe-t-il si nous ne sommes plus au-dessus d'un modèle? Les choses ne se passent pas nécéssairement bien. En effet, soient $A \subset B \subset M^*$, et $p(\bar{x}) \in S_n(A)$. Nous voulons étendre $p(\bar{x})$ à un type sur B qui représente les même formules que $p(\bar{x})$. Mais maintenant, puisque A n'est pas un modèle, il est très possible que nous ayons des $\mathcal{L}(A)$-formules $\varphi_i(\bar{x}, \bar{y}_i)$, $i = 1, \ldots, m$, qui ne sont pas représentées dans $p(\bar{x})$, et des uplets $\bar{b}_1, \ldots, \bar{b}_m$ de B tels que

$$p(\bar{x}) \cup Diag(B) \vdash \bigvee_{i=1}^{m} \varphi_i(\bar{x}, \bar{b}_i).$$

On ne peut donc définir un héritier de cette façon la. Voici un exemple simple :

Soit K un corps algébriquement clos, F un sous-corps de K non-algébriquement clos. Soit $f(T) \in F[T]$ un polynôme irréductible sur F, et considérons le type $p(x) \in S_1(F)$: $f(x) = 0$. Comme $f(T)$ est irréductible, cela donne un type complet. Il est cependant clair que si $\tilde{F}$ dénote la clôture algébrique de F, et si $a_1, \ldots, a_m$ sont les racines de $f(T)$, alors

$$Diag(\tilde{F}) \cup f(x) = 0 \vdash \bigvee_{i=1}^{m} (x = a_i).$$

Cependant, la formule $x = y$ n'est pas représentée dans $p(x)$.

(8.18) **Définition des héritiers dans le cas général, mais quand $Th(M^*)$ est stable**. Dans le cas général, la définition d'héritier est plus compliquée. Elle s'appuie aussi sur le fait de "représenter le moins de formules possibles", mais contrairement au cas d'un modèle, nous ne considèrons que des $\mathcal{L}$-formules.

Je vous donne la formulation d'abord dans le cas $A \subset M \prec M^*$, $q(\bar{x}) \in S_n(M)$ étendant $p(\bar{x}) \in S_n(A)$: $q(\bar{x})$ hérite de $p(\bar{x})$ si et seulement si l'ensemble des $\mathcal{L}$-formules $\varphi(\bar{x}, \bar{y})$ représentées dans $q(\bar{x})$ est minimal possible (relatif à la condition d'être un type sur M étendant $p(\bar{x})$). Notons que, puisque notre théorie est **stable**, le type $q(\bar{x})$ est définissable, et nous aurons donc que $q(M^*)(\bar{x})$ est aussi un héritier de $p(\bar{x})$

Si maintenant $A \subseteq B \subset M^*$, et $p(\bar{x}) \in S_n(A)$, $q(\bar{x}) \in S_n(B)$ étend $p(\bar{x})$, $q(\bar{x})$ hérite de $p(\bar{x})$ si et seulement s'il existe $M \prec M^*$ contenant B et un type $r(\bar{x}) \in S_n(M)$ qui hérite de $p(\bar{x})$ et de $q(\bar{x})$.

On vérifie que si $A \prec M$, alors les deux notions d'héritiers coïncident, et que si $A \subset B \subset C \subset M^*$ et $r(\bar{x}) \in S_n(C)$, alors $r(\bar{x})$ hérite de sa restriction à A si et seulement si $r(\bar{x})$ hérite de sa restriction $q(\bar{x})$ à B, et $q(\bar{x})$ hérite de sa restriction à A.

(8.19) **Définition de l'indépendance dans le cas des théories stables.** Soient $\bar{a} \in M^*$, et $A \subseteq B \subset M^*$. On dit que $\bar{a}$ est indépendant de B sur A, si $tp(\bar{a}/B)$ hérite de $tp(\bar{a}/A)$. Cette notion est symétrique, et s'étend aux ensembles infinis : C est indṕendant de B sur A si et seulement si tout uplet fini de C est indépendant de B sur A. Nous ne montrerons pas ces propriétés.

(8.20) **Exemple 1**. M^* est un modèle de la théorie des ordres denses sans extrémités, et on prend $M = \mathbf{Q}$. Soit $a \in \mathbf{Q}$, et $p_{a^+}(x)$ le type (sur M) axiomatisé par $\{x > a\} \cup \{x < b \mid b > a\}$. Ce type est bien définissable, et donc aura un unique héritier à tout ensemble A contenant $\mathbf{Q}$.

Regardons maintenant $\mathbf{Q}$ comme un sous-modèle de $\mathbf{R}$, et soit $r \in \mathbf{R} \backslash \mathbf{Q}$. On considère le type $q_r(x) = \{x > a \mid a \in \mathbf{Q}, a < r\} \cup \{x < a \mid a \in \mathbf{Q},\ a > r\}$, et nous savons qu'il n'est pas définissable. Soit $A = \mathbf{Q} \cup \{r\}$, et considérons les extensions de $q_r(x)$ à A. Il y a trois possibilités pour une extension $q(x)$ de $q_r(x)$ à A : ou bien elle contient $x = r$, ou bien elle contient $x < r$, ou bien elle contient $x > r$. Ces extensions nous donnent donc le type réalisé, le type $p_{r^-}(x)$ et le type $p_{r^+}(x)$. Les deux derniers sont des héritiers de $q_r(x)$. En effet, soit $\varphi(x, \bar{m}, r)$ une formule sans quantificateurs ($\bar{m} \in M$). Nous savons qu'elle est impliquée par une formule qui nous dit où est placé x par rapport aux éléments du uplet $(\bar{m}, r)$. Considérons par exemple $q_{r^+}(x)$. Alors $\varphi(x, \bar{m}, r)$ sera impliquée par la formule $m_j < r < x < m_i$, où m_i est le plus petit élément du uplet $\bar{m}$ qui soit plus grand que r, et m_j le plus grand élément du uplet $\bar{m}$ qui soit plus petit que r. Comme les rationnels sont denses, il existe certainement un rationnel m entre m_j et r, et donc la formule $m_j < m < x < m_i$ est dans $q_r(x)$.

Remarquez une chose curieuse : les deux héritiers de $q_r(x)$ à A sont définissables (alors que $q_r(x)$ ne l'était pas). On peut montrer aussi, de la même façon, que si l'on prend $B \prec M^*$ contenant M, alors toute extension non réalisée de $q_r(x)$ à B est un héritier de $q_r(x)$.

(8.21) **Exemple 2**. Nous supposons que M^* est un corps algébriquement clos. Soit A un sous-corps de M^*. Par élimination des quantificateurs de $Th(M^*)$, nous savons que tout type $p(\bar{x}) \in S_n(A)$ est uniquement déterminé par l'idéal

$$I(p) = \{f(\bar{X}) \in A[\bar{X}] \mid f(\bar{x}) = 0 \in p(\bar{x})\}.$$

En effet, étant donné $I(p)$, le type $p(\bar{x})$ est tout simplement axiomatisé par

$$\{f(\bar{x}) = 0 \mid f(\bar{X}) \in I(p)\} \cup \{f(\bar{x}) \neq 0 \mid f(\bar{X}) \notin I(p)\}.$$

L'idéal $I(p)$ est premier, et $\bar{a}$ est une réalisation de $p(\bar{x})$ si et seulement si $I(\bar{a}/A) = I(p)$.

Remarquons que l'ensemble de gauche peut être remplacé par un ensemble fini d'équations : si $f_1(\bar{X}), \ldots, f_m(\bar{X})$ engendrent l'idéal $I(p)$, il suffit de dire que $f_1(\bar{x}) = \cdots = f_m(\bar{x}) = 0$.

Supposons maintenant que A soit un sous-corps algébriquement clos de M^*, et donc $A \prec M^*$. Soit $B \supseteq A$ un sous-corps de M^*, et $q(\bar{x})$ une extension de $p(\bar{x})$ à B. Nous avons alors $I(q) \supseteq I(p)B[\bar{X}]$ (puisque $q(\bar{x})$ étend $p(\bar{x})$). De plus, nous savons que $I(p)B[\bar{X}]$ est un idéal premier de $B[\bar{X}]$ (C'est ici que nous utilisons l'hypothèse que A est algébriquement clos, voir (7.19)). Nous avons donc une extension privilégiée de $p(\bar{x})$ à B : celle avec idéal associé $I(p)B[\bar{X}]$. Nous allons montrer que c'est bien le seul héritier de $p(\bar{x})$ à B. C'est-à-dire, nous allons montrer qu'aucun des autres types n'hérite de p.

Soit donc $q(\bar{x}) \in S_n(B)$ étendant $p(\bar{x})$, avec $I(q)$ contenant strictement $I(p)B[\bar{X}]$. Considérons la variété V définie par $I(p)$, et la sous-variété W de V définie par $I(q)$. Comme W est contenue strictement dans V, nous avons que $dim(W) < dim(V)$ (voir (7.17)). Soit $\bar{a}$ une réalisation de $q(\bar{x})$. Alors $\bar{a}$ est un point générique de W sur B, et de V sur A (mais pas de V sur B). Nous avons donc $tr.deg(A(\bar{a})/A) = dim(V) > tr.deg(B(\bar{a})/B) = dim(W)$. Il existe alors des indices $i(1) < \ldots < i(d)$ tels que $a_{i(1)}, \ldots, a_{i(d)}$ sont algébriquement indépendants sur A dans $B(V)$, mais ne le sont pas sur B. Il existe donc un polynôme non nul $f(\bar{X}) \in I(q) \cap B[X_{i(1)}, \ldots, X_{i(d)}]$ qui s'annule sur $(a_{i(1)}, \ldots, a_{i(d)})$. Soient $g(\bar{X}, \bar{Y}) \in \mathbf{Z}[\bar{X}, \bar{Y}]$ et $\bar{b} \in B$ tels que $f(\bar{X}) = g(\bar{X}, \bar{b})$, et tels que le coefficient d'un monôme en X soit dans $\mathbf{Z}$. Alors la formule $f(\bar{x}, \bar{y}) = 0$ n'est pas représentée dans $p(\bar{x})$: en effet, comme $a_{i(1)}, \ldots, a_{i(d)}$ sont algébriquement indépendants sur A, nous avons $I(p) \cap A[X_{i(1)}, \ldots, X_{i(d)}] = (0)$. D'autre part, par notre choix de $g(\bar{X}, \bar{Y})$, nous savons que si $\bar{c}$ est un uplet quelconque de M^*, nous avons $g(\bar{X}, \bar{c}) \neq 0$.

9. Rang de Morley, ensembles fortements minimaux

(9.1) **Rang de Morley**. Le rang de Morley, noté RM, est une fonction de l'ensemble des formules de $\mathcal{L}(M^*)$ dans $Ord \cup \{\infty\}$, où Ord dénote la classe des ordinaux. Nous étendons l'ordre sur les ordinaux en posant $\infty > \alpha$ pour tout $\alpha \in Ord$. Soit $\varphi(\bar{x})$ une formule (de $\mathcal{L}(M^*)$) définissant un ensemble X dans M^*. On définit par induction le rang de Morley $RM(X) \geq \alpha$, ou bien $RM(\varphi) \geq \alpha$, pour $\alpha \in Ord$, de la façon suivante :

– $RM(X) \geq 0$ si et seulement $X \neq \emptyset$.

– (α limite) $RM(X) \geq \alpha$ si et seulement si $RM(X) \geq \beta$ pour tout $\beta < \alpha$.

– ($\alpha = \beta + 1$) $RM(X) \geq \beta + 1$ si et seulement s'il existe une famille $(X_i)_{i \in \mathbf{N}}$ de sous-ensembles définissables **disjoints** de X tels que $RM(X_i) \geq \beta$ pour tout $i \in \mathbf{N}$.

(9.2) **Lemme 1**. Soient $X \subset Y$ des sous-ensembles définissables de M^{*n}, et $\beta < \alpha$ des ordinaux.

(1) $RM(X) \geq \alpha$ implique $RM(Y) \geq \alpha$.

(2) $RM(X) \geq \alpha$ implique $RM(X) \geq \beta$.

Démonstration. (1) Pour $\alpha = 0$ et pour α limite, c'est évident. Pour $\alpha = \gamma + 1$, la famille $(X_i)_{i \in \mathbf{N}}$ de sous-ensembles définissables disjoints de X et de rang $\geq \gamma$ nous donne $RM(Y) \geq \gamma + 1$.

(2) Pour α limite, c'est par définition du rang. Supposons le montré pour α et montrons-le pour $\alpha+1$. Par hypothèse, l'ensemble X contient un sous-ensemble définissable X_0 avec $RM(X_0) \geq \alpha$. Par hypothèse d'induction, on a $RM(X_0) \geq \beta$. Mais comme $X_0 \subseteq X$, cela donne $RM(X) \geq \beta$.

(9.3) **Définition du rang de Morley**. Soit φ une formule, définissant un sous-ensemble X de M^{*n}. S'il existe un ordinal α tel que $RM(X) \geq \alpha$, $RM(X) \not\geq \alpha+1$, on pose $RM(X) = RM(\varphi) = \alpha$. S'il n'existe pas de tel ordinal, alors on pose $RM(X) = RM(\varphi) = \infty$. Nous avons donc défini une fonction de l'ensemble des formules de $\mathcal{L}(M^*)$ dans $Ord \cup \{\infty\}$.

(9.4) **Lemme**. Soient X et Y des sous-ensembles définissables de M^{*n}. Alors $RM(X \cup Y) = \max\{RM(X), RM(Y)\}$.

Démonstration. Il est clair que $RM(X \cup Y) \geq RM(X), RM(Y)$. Nous supposerons $RM(X) \geq RM(Y)$. Montrons par induction sur α que $RM(X \cup Y) \geq \alpha$ implique $RM(X) \geq \alpha$. Si $\alpha = 0$ ou α est limite, c'est clair. Supposons $RM(X \cup Y) \geq \alpha + 1$, et soit Z_i, $i \in \mathbf{N}$, une famille de sous-ensembles définissables disjoints de $X \cup Y$ de rang $\geq \alpha$. Par hypothèse d'induction, pour tout i, l'un de $X \cap Z_i$ ou $Y \cap Z_i$ est de rang $\geq \alpha$. Soient $I = \{i \in \mathbf{N} \mid RM(Z_i \cap X) \geq \alpha\}$, $J = \{i \in \mathbf{N} \mid RM(Z_i \cap Y) \geq \alpha\}$. Alors $I \cup J = \mathbf{N}$, et donc l'un des deux est infini. Si par exemple I est infini, la famille $(Z_i \cap X)_{i \in I}$ montre que $RM(X) \geq \alpha + 1$.

(9.5) **Lemme**. Soient X un sous-ensemble définissable de M^{*n}, de rang $\alpha < \infty$. Alors X est une réunion finie d'ensembles disjoints X_i de rang α et ayant la propriété suivante : $(*)$ si Y est un sous-ensemble définissable de X_i, alors $RM(X_i) < \alpha$ ou bien $RM(X_i \setminus Y) < \alpha$.

Démonstration. Si notre ensemble X n'a pas la propriété $(*)$, alors il existe un sous ensemble définissable X_0 de X tel que $RM(X_0) = RM(X \setminus X_0) = \alpha$. C'est à dire qu'un ensemble qui ne satisfait pas $(*)$ peut être coupé en deux ensembles de même rang. On repète la procédure en l'appliquant à X_0 et à $X \setminus X_0$, etc., pour construire un arbre dont les feuilles (à chaque étape de la construction) nous donnent une partition de X en ensembles de rang α. Comme $RM(X) \not\geq \alpha + 1$, cette construction doit s'arrêter, c'est à dire qu'a partir d'un certain moment toutes les feuilles de l'arbre doivent satisfaire $(*)$.

Définition du degré de Morley. Supposons que $RM(X) = \alpha < \infty$. Nous définissons alors le degré de Morley de X, noté $DM(X)$, comme étant le plus grand entier n tel qu'il existe des sous-ensembles définissables disjoints $X_1, \ldots, X_n$ de M avec $RM(X_i) = \alpha$.

Le lemme précédent nous montre qu'un tel n existe. En effet, être de degré de Morley 1 correspond exactement à notre condition $(*)$ du lemme.

(9.6) **Remarques**. (1) Soit X un ensemble définissable non vide. Nous avons alors $RM(X) \geq 0$. Si X est infini, alors les sous-ensembles de X définis par les formules $\bar{x} = \bar{a}$ pour $\bar{a} \in X$, forment une partition de X, et nous aurons donc $RM(X) \geq 1$. Réciproquement, le fait que $RM(X)$ soit ≥ 1 entraîne qu'il contient une infinité de sous-ensembles non-vides et disjoints, ce qui entraîne que X est infini. Nous avons donc montré:

$$RM(X) = 0 \iff X \text{est fini.}$$

De plus, si $RM(X) = 0$, nous aurons $DM(X) = |X|$.

(2) Il est clair que RM et DM sont préservés par les automorphismes de M^*.

(3) Si $RM(X) = \alpha$ et $RM(Y) < \alpha$, alors $RM(X \cup Y) = RM(X)$ et $DM(X \cup Y) = DM(X)$.

(4) Si $RM(X) = RM(Y) = \alpha$ alors $RM(X \cup Y) = \alpha$ et $DM(X \cup Y) \leq DM(X) + DM(Y)$. Nous aurons $DM(X \cup Y) = DM(X) + DM(Y)$ si et seulement si $RM(X \cap Y) < \alpha$.

(5) Si $f : X \to Y$ est une bijection définissable, alors $RM(X) = RM(Y)$.

(9.7) **Exemple 1 - Ordres denses**. Considérons l'ordre dense sans extrémités, des point $a < b \in M^*$, et la formule $a < x < b$. Nous savons que si $c < d$ sont des éléments de M^* alors il existe un automorphisme de M^* qui envoie a sur c et b sur d. Les formules $a < x < b$ et $c < x < d$ auront donc le même rang. Mais, tout intervalle ouvert de M^* contient une infinité d'intervalles ouverts disjoints. Nous aurons donc $RM(a < x < b) \geq RM(a < x < b)) + 1$, ce qui ne peut arriver que si $RM(a < x < b) = \infty$.

(9.8) **Exemple 2 - Groupes divisibles**. Les groupes divisibles abéliens sans torsion. Nous savons que leur théorie élimine les quantificateurs. Un sous-ensemble définissable de M^{*n} sera donc une combinaison booléenne d'ensembles de la forme

$$A\bar{x} = \bar{b}$$

où A est une matrice $(m \times n)$, and $\bar{x}$, $\bar{b}$ sont des vecteurs (colonne) de longueur n. La dimension d'un tel ensemble X est égale à $n-$rang(A), et notée $dim(X)$. Nous allons montrer que $RM(X) = dim(X)$, par induction sur $dim(X)$.

Pour $dim(X) = 0$, c'est clair, car X est alors réduit à un point. Supposons le résultat montré pour tous les entiers $< dim(X) = d$. En appliquant une application linéaire (à coefficients dans $\mathbf{Q}$), et en utilisant (5) de la remarque ci-dessus, nous pouvons supposer que notre matrice A s'écrit $(I_m|B)$, où I_m est la $(m \times m)$ matrice identité. Nous avons donc $d = n - m$. Pour chaque $a \in M^*$, nous rajoutons l'équation $x_n = a$, et obtenons un sous-ensemble X_a de X, de dimension $d-1$, et les ensembles X_a sont certainement disjoints. Nous avons donc $dim(X) \geq d$. Nous voulons maintenant montrer que X ne contient pas une infinité de sous-ensembles définissable disjoints de rang $\geq d$. Pour cela nous allons étudier d'un peu plus près les sous-ensembles définissables de X.

Soit Y un sous-ensemble définissable propre de X. Par élimination des quantificateurs, Y s'écrit donc comme une combinaison booléenne d'ensembles de base, et en fait on peut l'écrire comme une union $Y = \bigcup_{i=1}^{r} Y_i \setminus Z_i$, où chaque Y_i est un sous-ensemble de base, et chaque Z_i est une union **finie** d'ensembles de base strictement contenus dans Y_i. De plus nous pouvons supposer que les ensembles Y_i sont distincts. Nous avons donc que chacun des ensembles de base apparaissant dans Z_i est de dimension inférieure à celle de Y_i, et donc (par hypothèse d'induction) que $RM(Z_i) < RM(Y_i)$. Nous avons alors $RM(Y) = \sup_i RM(Y_i)$.

Si $RM(Y) \geq d$, cela entraîne que l'un des Y_i est égale à X. Dans ce cas, nous avons $X \setminus Y \subseteq Z_i$. Par hypothèse d'induction, $RM(Z_i) < d$, et donc Z_i ne peut contenir une infinité de sous-ensembles disjoints de dimension $\geq d-1$, en particulier de rang d.

Cela montre que toute famille infinie de sous-ensembles définissables disjoints de X ne peut contenir une infinité d'éléments de rang $\geq d$. Et donc que $RM(X) = d$. En fait, notre preuve montre aussi que $DM(X) = 1$.

(9.9) **Exemple 3 - Corps algébriquement clos**. Soit $V \subseteq M^{*n}$ une variété, de dimension d. Nous allons montrer par induction sur d, que $RM(V) = d$. Pour $d = 0$, c'est clair car V est réduite à un point. Supposons le résultat montré pour tous les entiers $< d$. Nous allons d'abord montrer que $RM(V) \geq d$. Soit F le corps de définition de la variété V, et $\bar{a}$ un générique de V sur F. Puisque $dim(V) > 0$, l'un des éléments du uplet $\bar{a}$ est transcendant sur F, et nous supposerons que c'est a_1. L'équation $x_1 = a_1$ coupe alors V en un ensemble algébrique $V(a_1)$ de dimension $d-1$; par induction, nous avons donvc $RM(V(a_1) = d-1$, car les composantes irréductibles de $V(a_1)$ sont de dimension $d-1$.

Soient maintenant b_n, $n \geq 0$, des éléments distincts de M^* qui sont transcendants sur F. Pour chaque n il existe un F-automorphisme de M^* qui envoie a_1 sur b_n. L'ensemble $V(b_n)$ défini par $\bar{x} \in V \wedge x_1 = b_n$ est donc de rang $d-1$. Ces ensembles sont disjoints, contenus dans V, et cela montre que $RM(V) \geq d$.

Nous allons maintenant montrer que $RM(V) \leq d$, et pour cela nous avons besoin de regarder les sous-ensembles définissables de V. Nous savons que tout sous-ensemble définissable X de M^{*n} est une combinaison booléenne de sous-variétés de M^{*n}. Nous pouvons donc écrire

$$X = \bigcup_{i=1}^{m} V_i \setminus F_i$$

ou chaque V_i est une variété (contenue dans la clôture de Zariski $\tilde{X}$ de X) et chaque F_i est un fermé (propre) de V_i. Prenons un tel X contenu dans V. Remarquons que comme les V_i et V sont des variétés, nous avons $dim(F_i) < dim(V_i)$, et que si $dim(V_i) = d$ alors $V_i = V$.

Si $dim(V_i) = d$, alors par hypothèse d'induction nous avons $RM(F_i) < d$, et donc $RM(V_i \setminus F_i) = RM(V_i) = RM(V)$. Comme $V \setminus X \subseteq F_i$, nous en déduisons que $RM(X) =$

$RM(V)$. Si pour tout i nous avons $dim(V_i) < d$, alors par hypothèse d'induction, $RM(V_i) < d$, ce qui entraîne que $RM(X) < d$.

Nous avons donc montré la chose suivante : si X est un sous-ensemble définissable de V, alors $RM(X) < d$ ou bien $RM(V \setminus X) < d$. Comme nous savons que $RM(V) \geq d$, cela entraîne que $RM(V) = d$ et $DM(V) = 1$.

Cela nous donne maintenant très facilement le résultat suivant : soit $X \subset M^{*n}$ un ensemble définissable, et $\tilde{X}$ sa clôture de Zariski. Alors $RM(X) = dim(\tilde{X})$, et $DM(X)$ est le nombre de composantes irréductibles de $\tilde{X}$ de dimension maximale (en effet, celles de dimension inférieure sont aussi de rang inférieur). Ceci utilise que si V_1 et V_2 sont deux variétés distinctes de même dimension, alors $dim(V_1 \cap V_2) < dim(V_1)$.

(9.10) **Quelques remarques sur le rang de Morley**. On peut montrer que toute formule a un rang de Morley $< \infty$ si et seulement T ($= Th(M^*)$, dans un langage dénombrable) est ω-stable.

Je vous rappelle que l'ω-stabilité entraîne la λ-stabilité pour tout cardimal infini λ. De plus, on montre que si T est ω-stable, alors le rang d'une formule sera $< \omega_1$.

On vérifie facilement (en comptant les types) que les théories des exemples 2 et 3 ci-dessus sont ω-stables, et donc il est normal que le rang de Morley soit fini.

Nous avons aussi vu que $Th(\mathbf{Z}, +)$ n'est pas ω-stable, car il existe $2^{\aleph_0}$ types sur $\{1\}$. En fait on peut voir directement que $RM(x = x) = \infty$. En effet nous avons des bijections définissables entre M^* et $2M^*$, M^* et $2M^* + 1$ (données par $x \mapsto 2x$ et $x \mapsto 2x + 1$). Supposons $RM(M^*) = \alpha < \infty$. Alors nous avons $RM(2M^*) = RM(2M^* + 1) = \alpha$, et $DM(M^*) = DM(2M^*) = DM(2M^* + 1)$. Mais $2M^* \cap (2M^* + 1) = \emptyset$, et cela nous donne une contradiction. Donc $RM(M^*) = \infty$. Nous verrons plus tard qu'il existe un rang plus approprié à l'étude de ce groupe.

(9.11) **Rang de Morley de types**. Soit $A \subset M^*$, $p(\bar{x}) \in S_n(A)$ et $\bar{a}$ une réalisation de $p(\bar{x})$ dans M^*. On définit

$$RM(p) = RM(\bar{a}/A) = \inf\{RM(\varphi(\bar{x}) \mid \varphi(\bar{x}) \in p(\bar{x})\}.$$

C'est bien défini car toute suite décroissante d'ordinaux se stabilise.

(9.12) **Ensembles fortements mininaux**. Soit X un sous-ensemble définissable de M^{*n}. On dit que X est **fortement minimal** si et seulement si $RM(X) = DM(X) = 1$. Remarquons que cela veut dire que si Y est un sous-ensemble définissable de X, alors Y ou $X \setminus Y$ est cofini.

Si M^* est un corps algébriquement clos (sans autre structure), alors M^* est fortement minimal. De même les espaces vectoriels sur un corps K sont fortement minimaux (s'ils sont infinis). Je rappelle que ce sont des groupes abéliens (dans le langage $\{+, -.0\}$) avec des symboles de multiplications scalaire λ_c pour chaque $c \in K$. Ces deux exemples vérifient des propriétés plus fortes : leur théorie est $\aleph_1$-catégorique. En fait on peut montrer que si la formule $(x = x)$ définit un ensemble fortement minimal dans un modèle saturé de T, alors T est $\aleph_1$-catégorique si le langage est dénombrable, voir en fin de chapitre.

(9.13) **Prégéométrie sur les ensembles fortement minimaux**. Soit $X \subseteq M^{*n}$ un ensemble fortement minimal. En ajoutant quelques symboles de constantes au langage nous pouvons donc supposer que X est défini sur $\emptyset$. Pour simplifier la notation, nous ne mettrons pas de barre au dessus des éléments de X, mais la reserverons aux uplets d'éléments de X. Nous définissons une opération de clôture dans X, notée cl, de la façon suivante : si $A \subset X$, alors $cl(A) = acl(A) \cap X$. Remarquons tout de suite que $cl(cl(A)) = cl(A)$, et que si $a, b \in X, \notin cl(A)$, alors $tp(a/A) = tp(b/A)$: en effet, soit $\varphi(x) \in \mathcal{L}(A)$, et soit Y l'ensemble qu'elle définit sur X. Nous savons que Y est fini ou cofini dans X. S'il est fini, alors $Y \subset cl(A)$, s'il est infini, alors $X \setminus Y \subset cl(A)$. Dans tous les cas, nous avons $M^* \models \varphi(a) \leftrightarrow \varphi(b)$, ce qui montre que $tp(a/A) = tp(b/A)$.

(9.14) **Lemme d'échange**. Soit $A \subset X$, et $a, b \in X$. Si $b \in cl(A, a) \setminus cl(A)$, alors $a \in cl(A, b) \setminus cl(A)$.

Démonstration. En incorporant les éléments de A au langage, nous pouvons supposer que $A = \emptyset$. Nous avons alors $b \in cl(a)$, $b \notin cl(\emptyset)$. Tout d'abord nous ne pouvons avoir $a \in cl(\emptyset)$, car sinon nous aurions $cl(a) = cl(\emptyset)$, et $b \in cl(\emptyset)$. Nous allons supposer que $a \notin cl(b)$ et obtenir une contradiction. Soit $\varphi(x, a)$ la formule isolant $tp(b/a)$, et $n \geq 1$ tel que $M \models \exists^{=n} x\, \varphi(x, a)$. Par forte minimalité, et comme $a \notin cl(b)$, il existe un sous-ensemble cofini X_1 de X tel que pour tout $a' \in X_1$ on ait

$$M \models \varphi(b, a') \wedge \exists^{=n} x\, \varphi(x, a').$$

Comme $b \notin cl(\emptyset)$, il existe un sous-ensemble cofini Y de X tel que pour tout $b' \in Y$, il existe au plus $|X \setminus X_1|$ éléments a' de X qui ne satisfont pas la formule

$$(\varphi(b', y) \wedge \exists^{=n} x\, \varphi(x, y)).$$

Soient $b_0, \ldots, b_n$ des éléments distincts de Y. Alors pour chaque i, l'ensemble Y_i des éléments a' de X qui ne satisfont pas la formule

$$(\varphi(b_i, y) \wedge \exists^{=n} x\, \varphi(x, y))$$

est de cardinalité au plus $|X \setminus X_1|$, et est donc fini. Une union finie d'ensembles finis est finis, et nous pouvons donc trouver un élément a' dans le complémentaire de $\bigcup Y_i$. Nous avons alors

$$M \models \bigwedge_{i=0}^{n} \varphi(b_i, a') \wedge \exists^{=n} x\, \varphi(x, a'),$$

ce qui est absurde.

(9.15) **Définitions**. Soit $X \subset M^{*n}$ un ensemble fortement minimal (défini sur $\emptyset$). Nous disons que $a \in X$ est **indépendant** de $A \subset X$ si $a \notin cl(A)$. Un sous-ensemble A de X est **indépendant** si tout uplet $a \in A$ est indépendant de $A \setminus \{a\}$. Un sous-ensemble B de A est une **base de** A si B est independant et $cl(A) = cl(B)$.

Remarquons qu'une base de A peut être aussi définie comme étant un sous-ensemble de A maximal indépendant.

(9.16) **Corollaire**. Soit $X \subset M^{*n}$ un ensemble fortement minimal (défini sur $\emptyset$).

(1) Soit $A \subset X$. Les propriétés suivantes sont équivalentes pour un sous-ensemble B de A :

(i) B est une base de A.

(ii) $cl(B) = cl(A)$ et si $C \subseteq B$ et $cl(C) = cl(B)$ alors $C = B$.

(2) Si $A \subset B \subset X$, alors toute base de A s'étend en une base de B.

(3) Soit $A \subset X$. Alors deux bases de A ont la même cardinalité.

Démonstration. (1) (i) $\to$ (ii) : $cl(B) = cl(A)$ par définition. Supposons $C \subset B$ et $cl(C) = cl(B)$. Si $b \in B \setminus C$, nous avons alors $b \in cl(C)$, ce qui contredit le fait que B soit indépendant. (ii) $\to$ (i) : tout d'abord comme $cl(B) = cl(A)$, un sous-ensemble de $cl(A)$ contenant strictement B ne peut être indépendant. Il suffit donc de montrer que B est indépendant. Mais sinon, il existe $b \in B$, tel que $b \in cl(B \setminus \{b\})$, ce qui entraîne $cl(B) = cl(B \setminus \{b\})$ et contredit notre hypthèse.

(2) Une base de A est un sous-ensemble indépendant de B, et est donc contenue dans un sous-ensemble maximal indépendant de B, c'est à dire dans une base de B.

(3) Nous allons d'abord montrer cela dans le cas où A a une base finie. Nous prenons alors pour B une base finie de A de cardinalité n minimale, et allons montrer que si $C = \{c_\alpha \mid \alpha < \kappa\}$ (κ un cardinal) est une autre base de A alors $\kappa = n$. La démonstration est par induction (inverse) sur $|B \cap C|$. Si $|B \cap C| = n$, alors $B \subseteq C$, et donc $B = C$. Soit $c \in C \setminus B$. Par hypothèse, $c \in cl(B)$. Prenons $B' \subseteq B$ minimal tel que $c \in cl(B')$, et soit $b \in B'$. Par minimalité de B', nous avons alors $c \in cl(B')$, $c \notin cl(B' \setminus \{b\})$. Par le lemme d'échange, $b \in cl(B' \setminus \{b\}, c)$. Cela entraîne que $cl(B \setminus \{b\}, c) = cl(A)$, et donc que $B_1 = B \setminus \{b\} \cup \{c\}$ est une base de A (par minimalité de n). Nous avons $|B_1 \cap C| = |B \cap C| + 1$, et par hypothèse d'induction cela entraîne que $\kappa = n$.

Supposons maintenant que A n'ait pas de base finie, et soient $B = \{b_\alpha \mid \alpha < \kappa\}$ et $C = \{c_\alpha \mid \alpha < \lambda\}$ des bases de A. Nous allons définir une fonction $f : \lambda \to \mathcal{P}_\omega(B)$ de la façon suivante : pour chaque $\alpha < \lambda$ nous choisissons un sous-ensemble fini B_α de B tel que $c_\alpha \in cl(B_\alpha)$, et nous posons $f(\alpha) = B_\alpha$. Alors, pour tout sous-ensemble fini B' de B, l'ensemble $f^{-1}(B')$ est fini : en effet, $cl(B')$ a une base finie (B'), et les éléments $c_\alpha \in cl(B')$ sont indépendants. Par le cas fini, nous savons qu'il y en a au plus $|B'|$, c'est à dire que $|f^{-1}(B')| \leq |B'|$. Nous avons alors $\lambda \leq |\mathcal{P}_\omega(B)|\aleph_0 = \kappa$ car κ est infini. Cela montre que $\lambda \leq \kappa$, et par symétrie on obtient $\kappa = \lambda$.

(9.17) Proposition. Soit $X \subseteq M^{*n}$ un ensemble fortement minimal défini sur $\emptyset$, et $A \subseteq X$ un ensemble infini. Alors les uplets de A forment une suite totalement indiscernable (sur $\emptyset$) si et seulement s'ils sont indépendants.

Démonstration. Supposons d'abord que A soit indépendant. Comme A est infini, nous savons en particulier qu'aucun de ses éléments n'est dans $cl(\emptyset)$ (si $a \neq b \in A$, alors $a \notin cl(b)$). Nous allons montrer que si $a_1, \ldots, a_n$ et $b_1, \ldots, b_n$ sont des uplets de X, avec les a_i deux à deux distincts et $\{a_1, \ldots, a_n\}$ indépendant, et les b_i deux à deux distincts et $\{b_1, \ldots, b_n\}$ indépendant, alors $tp(a_1, \ldots, a_n) = tp(b_1, \ldots, b_n)$. Par (9.13), le résultat est vrai pour $n = 1$. Supposons le montré pour $n - 1$. Par (9.13), $tp(a_n/a_1, \ldots, a_{n-1})$ est axiomatisé par les formules exprimant que $x_n \in X$, $x_n \notin cl(a_1, \ldots, a_n)$. Par hypothèse d'induction, $tp(a_1, \ldots, a_{n-1})$ est axiomatisé par les formules exprimant que $x_1, \ldots, x_{n-1} \in D$, $x_1, \ldots, x_{n-1}$ forment un ensemble indépendant. Donc, $tp(a_1, \ldots, a_n)$ est axiomatisé par les formules disant que $x_1, \ldots, x_n$ sont des éléments de X qui forment un ensemble indépendant. Comme $b_1, \ldots, b_n$ satisfont aussi ces formules, nous avons que $tp(a_1, \ldots, a_n) = tp(b_1, \ldots, b_n)$. En particulier, puisque A est indépendant, nous obtenons que A est un ensemble totalement indiscernable.

Pour la réciproque, supposons que A soit totalement indiscernable, et supposons que A ne soit pas indépendant. Il existe alors $a_1, \ldots, a_n \in A$, $a \in A$ tel que $a \in cl(a_1, \ldots, a_n)$, $a \notin \{a_1, \ldots, a_n\}$. Soit $\varphi(x, a_1, \ldots, a_n)$ la formule isolant $tp(a/a_1, \ldots, a_n)$. Puisque A est totalement indiscernable, cette formule est alors satisfaite par tous les éléments de $A \setminus \{a_1, \ldots, a_n\}$. Mais A est infini, et $\varphi(x, a_1, \ldots, a_n)$ n'a qu'un nombre fini de réalisations, ce qui nous donne une contradiction.

(9.18) **Lemme**. Soit $X \subset M^{*m}$ un ensemble fortement minimal. Pour simplifier la notation, nous noterons les éléments de X sans barre, et réserverons la barre aux uplets d'éléments de X. Soit $\varphi(x, \bar{y})$ une formule de $\mathcal{L}$. Alors l'ensemble

$$\{\bar{b} \mid M^* \models \exists^{<\infty} x\, x \in X \wedge \varphi(x, \bar{b})\}$$

est définissable.

Démonstration. Nous allons montrer qu'il existe un entier N tel que pour tout uplet $\bar{b}$ de M^*,

$$|\{a \in X \mid M^* \models \varphi(a, \bar{b})\}| \leq N \text{ ou bien } |\{a \in X \mid M^* \models \neg\varphi(a, \bar{b})\}| \leq N.$$

Notons que comme ces deux ensembles recouvrent X la disjonction est exclusive. C'est évident : sinon, par compacité il existerait un uplet $\bar{b}$ de M^* tel que les sous-ensembles de X définis par les formules $\varphi(x, \bar{b})$ et $\neg\varphi(x, \bar{b})$ sont tous deux infinis, ce qui contredit la minimalité forte de X. Nous avons donc montré que l'ensemble $\{a \in X \mid M^* \models \varphi(a, \bar{b})\}$ est fini si et seulement s'il est de cardinalité $\leq N$. La formule désirée (en $\bar{y}$) est donc

$$\exists^{\leq N} x\, x \in X \wedge \varphi(x, \bar{y}).$$

(9.19) **Proposition**. Supposons que M^* soit fortement minimal. Si $A \subseteq M^*$ est tel que $acl(A)$ est infini, alors $acl(A) \prec M^*$.

Démonstration. Soit $\varphi(x, \bar{y})$ une formule, $\bar{a} \in acl(A)$, et supposons qu'il existe $b \in M^*$ tel que $M^* \models \varphi(b, \bar{a})$. Regardons l'ensemble X défini par la formule $\varphi(x, \bar{a})$. S'il est fini, alors il est contenu dans $acl(A)$, et $b \in acl(A)$. S'il est infini, alors son complémentaire est fini (par forte minimlité), et X coupe l'ensemble infini $acl(A)$. Nous avons donc montré qu'il existe $b \in acl(A)$ tel que $M^* \models \varphi(b, \bar{a})$. Par le test de Tarski-Vaught, cela montre que $acl(A) \prec M^*$.

(9.20) **Proposition**. Supposons que M^* soit fortement minimal. Alors $T = Th(M^*)$ est $\aleph_1$-catégorique.

Démonstration. Rappelons que le langage est dénombrable) Soient M et N deux modèles de T de cardinalité $\kappa \geq \aleph_1$. Prenons des bases B_1 de M et B_2 de N. Comme le langage est dénombrable, nous savons que $|acl(B_1)| = |B_1| + \aleph_0$, et donc, puisque $|M| = |N| = \kappa$, nous avons $|B_1| = |B_2| = \kappa$. Fixons une bijection $f : B_1 \to B_2$. Par (9.13), cette bijection est un isomorphisme partiel élémentaire. Nous allons montrer qu'elle se prolonge en un isomorphisme entre $M = acl(B_1)$ et $N = acl(B_2)$. En effet, considérons l'ensembles des isomorphismes partiels élémentaires entre M et N étendant f, ordonné par l'inclusion. Cet ensemble satisfait les hypothèse du Lemme de Zorn, et adonc un élément maximal g. Nous allons montrer que $dom(g) = M$. Sinon, il existe $a \in M$, $a \notin dom(g)$. Comme $a \in acl(B_1)$, nous savons que $tp(a/dom(g)$ est algébrique. Soit $\varphi(x, \bar{b})$ la formule isolant $tp(a/dom(g))$ ($\varphi \in \mathcal{L}$, $\bar{b} \in dom(g)$). Comme g est élémentaire, la formule $\varphi(x, g(\bar{b})$ isole un type (complet) sur $Im(g)$, et a donc une réalisation $c \in N$. Nous étendons g en posant $g'(a) = c$, $g' \supset g$, et obtenons un isomorphisme partiel élémentaire prolongeant g, ce qui nous donne la contradiction désirée. Nous avons montré que $dom(g) = M$, on montre de la même façon que $Im(g) = N$, et nous avons donc montré que deux modèles de T de même cardinalité non dénombrable sont isomorphes.

10. Corps différentiellement clos

Dans cette section nous allons étudier la modèle complétion de la théorie des corps différentiels (de caractéristique 0). Tous nos anneaux seront commutatifs unitaires.

(10.1) Une **dérivation sur un anneau** R est un homomorphisme additif $D : R \to R$ satisfaisant

$$D(xy) = xDy + yDx$$

pour tous $x, y \in R$. Les dérivations satisfont les règles usuelles satisfaites par les dérivées de fonctions, et en particulier la loi pour la composition. Les anneaux différentiels sont des structures du langage $\mathcal{L}_D = \{+, -, \cdot, D, 0, 1\}$. Une inclusion d'anneaux différentiels correspond à une inclusion de $\mathcal{L}_D$-structures, et pareil pour les morphismes.

Exemples. (1) La dérivation triviale sur R : $D = 0$.

(2) Soit $C^\infty((0,1))$ l'anneau des fonctions de domaine l'intervalle ouvert $(0,1)$ et à valeurs réelles qui sont infiniment différentiables. On prend pour D la dérivation usuelle.

(3) Soit U un sous-ensemble ouvert et connexe de $\mathbf{C}$, soit $\mathcal{O}_U$ l'anneau des fonctions holomorphes sur U, et D la dérivation usuelle.

(4) Soit $a \in R$ (R un anneau), X une indéterminée. La fonction $D(\sum_{i=0}^m a_i X^i) = a \sum_{i=1}^m i a_i X^{i-1}$ est alors une dérivation sur $R[X]$. Notons que si $a = 1$, alors D coïncide avec la dérivation usuelle $\frac{d}{dX}$ sur $R[X]$ et que D est 0 sur R. On peut généraliser cette construction à $R[X_1, \ldots, X_n]$ en considérant maintenant $D_i = \frac{\partial}{\partial X_i}$.

(5) Soit $D_0 : R \to R$ une dérivation. Nous formons l'anneau de polynômes différentiels en $\bar{X} = (X_1, \ldots, X_n)$ de la façon suivante: Nous posons $X_i^{(0)} = X_i$ pour $i = 1, \ldots, n$, et considérons l'anneau $R\{\bar{X}\} = R[X_i^{(j)} \mid i = 1, \ldots, n,\ j \in \mathbf{N}]$ en une infinité de variables. Pour $j \in \mathbf{N}$ et $i = 1, \ldots, n$, nous posons $D(X_i^{(j)}) = X_i^{(j+1)}$, et pour $a \in R$, $D(a) = D_0(a)$. Il existe alors une seule façon d'étendre D à une dérivation de $R\{\bar{X}\}$, en posant

$$D(f(X)) = D(f)(\bar{X}) + \sum_{i,j} \frac{\partial f}{\partial X_i^{(j)}}(\bar{X}) X_i^{(j+1)}$$

Ici, $D(f)(\bar{X})$ est l'élément de $R\{\bar{X}\}$ obtenu en appliquant D aux coefficients de $f(\bar{X})$, et $\frac{\partial f}{\partial X_i^{(j)}}(\bar{X})$ est la dérivée partielle de $f(\bar{X})$ considérée comme un polynôme en les variables

$X_i^{(m)}$, $i = 1, \dots, n$, $m \in \mathbf{N}$, par rapport à la variable $X_i^{(j)}$. Vous montrerez en exercice que cela définit bien une dérivation. [**Attention**, j'utiliserai indifféremment la notation $g(X)$ pour l'élément de $R\{X\}$ et pour le polynôme en $X, X', X^{(2)}, \dots, X^{(n)}, \dots$ le représentant. J'espère que cela ne créera pas de confusion].

(10.2) **Lemme**. Soit D une dérivation sur R.
(1) $D(1) = D(0) = 0$.
(2) Pour tous $n \in \mathbf{N}$ et $a \in R$, $D(a^n) = na^{n-1}D(a)$.
(3) Si b est inversible dans R, et $n \in \mathbf{Z}$ alors $D(b^n) = nb^{n-1}D(b)$.

Démonstration. (1) $D(1) = D(1 \cdot 1) = D(1) + D(1)$, donc $D(1) = 0$. $D(0) = D(0 + 0) = D(0) + D(0)$, donc $D(0) = 0$.

(2) Par induction sur n. Pour $n = 0$ c'est clair par (1). $D(x^{n+1}) = D(x^n \cdot x) = D(x^n)x + x^n D(x) = nx^{n-1}D(x)x + x^n D(x) = (n+1)x^n D(x)$.

(3) Si $n \geq 0$, c'est (1). Supposons $n = -1$. Alors $D(1) = 0 = D(b \cdot \frac{1}{b}) = bD(\frac{1}{b}) + D(b)\frac{1}{b}$, d'où $D(\frac{1}{b}) = -D(b)b^{-2}$. Si maintenant $n < 0$, on applique le résultat à $c^{-1} = b^n$ (et donc $c = b^{-n}$) et on obtient

$$D(b^n) = -D(c)\frac{1}{b^{2n}} = -((-nb^{-n-1}D(b))\frac{1}{b^{-2n}} = nD(b)b^{n-1}.$$

(10.3) **Exercice 1**. Montrez que si R est un anneau intègre différentiel, il existe une et une seule façon d'étendre la dérivation D de R à une dérivation sur le corps K des fractions de R.

Considérons la dérivée logarithmique définie par $LogD(a) = \frac{D(a)}{a}$ pour $a \in K$. Montrez que $LogD(ab) = LogD(a) + LogD(b)$, et que $LogD(a^{-1}) = -LogD(a)$.

(10.4) **Exercice 2**. Soit R un anneau différentiel (la dérivation est notée D).
(1) Montrez que si $f(\bar{X}) \in R[\bar{X}]$, $\bar{X} = (X_1, \dots, X_n)$, et $\bar{a} = (a_1, \dots, a_n) \in K^n$ alors

$$D(f(\bar{a})) = D(f)(\bar{a}) + \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(\bar{a})D(a_i).$$

(2) Vérifiez que la dérivation sur $R\{\bar{X}\}$ définie en (10.1)(5) définit bien une dérivation de $R\{\bar{X}\}$.

(10.5) **Définition**. Soit D une dérivation sur R. Alors l'ensemble $C_R = \{a \in R \mid D(a) = 0\}$ est appelé l'anneau des constantes de R. Nous omettrons en général l'indice R.

(10.6) **Exercice 3**. (1) Vérifiez que C_R est bien un sous-anneau de R. Montrez que si $a \in R$, alors aD est aussi une dérivation sur R.

(2) Montrez que si R est un anneau de caractéristique $p > 0$, alors C_R contient nécéssairement toutes les puissances p-ièmes d'éléments de R. En particulier, si K est un corps parfait de caractéristique positive, alors toute dérivation sur K est triviale.

(10.7) **Idéaux différentiels**. Si R est un anneau différentiel (avec dérivation D), un **idéal différentiel** de R est un idéal I de R satisfaisant $D(I) \subseteq I$. Si $S \subseteq R$, nous noterons par $\langle S \rangle$ l'idéal différentiel de R engendré par S.

(10.8) **Exercice 4**. Montrez que si I est un idéal différentiel de R, alors R/I a une structure naturelle d'anneau différentiel.

(10.9) Nous allons maintenant étudier l'anneau $R\{X\}$ d'un peu plus près (X une seule variable, R un anneau différentiel). Soit $f(X) \in R\{X\}$. Alors l'**ordre** de $f(X)$ est le plus grand entier n tel que $X^{(n)}$ apparaisse dans $f(X)$ de façon non triviale (si $f(X) \in R$, son ordre est par définition -1). Nous pouvons alors écrire

$$f(X) = \sum_{i=0}^{m} g_i(X) {X^{(n)}}^i$$

où les $g_i(X)$ sont d'ordre $\leq n-1$ (et $m \geq 1$, $g_m \neq 0$). On dit alors que $f(X)$ est de **degré** m.

Nous définissons un préordre $\ll$ sur $R\{X\}$ en posant $f(X) \ll g(X)$ si l'ordre de $f(X)$ est inférieur à celui de $g(X)$, ou bien si ces ordres sont égaux et le degré de $f(X)$ est inférieur ou égal à celui de $g(X)$. Si l'on quotiente par la relation d'équivalence $(f(X) \ll g(X)) \wedge (g(X) \ll f(X))$, on obtient l'ordre lexicographique sur les paires $(ordre(f), deg(f))$. Notons que ce préordre est bien-ordonné, c'est à dire que tout ensemble a un élément minimal.

(10.10) **La séparante.** Soit $f(X) \in R\{X\}$, d'ordre $n \geq 0$. On définit la **séparante** de $f(X)$ par

$$s(X) = \frac{\partial f}{\partial X^{(n)}}(X).$$

Attention, ici nous considérons $f(X)$ comme un polynôme en les variables $X, X', \ldots, X^{(n)}$, et nous prenons sa dérivée partielle par rapport à la variable $X^{(n)}$. Si $f(X) = \sum_{i=0}^{m} g_i(X) {X^{(n)}}^i$, alors

$$s(X) = \sum_{i=0}^{m-1} (i+1) g_{i+1}(X) {X^{(n)}}^i$$

car les polynômes $g_i(X)$ sont des constantes pour la dérivation $\frac{\partial}{\partial X^{(n)}}$. Notons que $s(X) \ll f(X)$, car le degré de $s(X)$ est inférieur à celui de $f(X)$.

Exemple. Soit $f(X) = (X^{(2)})^2 - 2X'$, alors l'ordre de $f(X)$ est 2, ainsi que son degré, et sa séparante est $s(X) = 2X^{(2)}$.

(10.11) **Définition**. Soit $f(X) \in R\{X\}$, et posons $I(f) = \{g(X) \in R\{X\} \mid \exists k \in \mathbf{N}\ s^k(X) g(X) \in \langle f(X) \rangle\}$.

Nous montrerons que si R est un corps et $f(X) \in R\{X\}$ est irréductible, alors $I(f)$ est un idéal différentiel premier de $R\{X\}$, et de plus, que tous les idéaux premiers différentiels de $R\{X\}$ sont de cette forme. Pour l'instant, nous montrerons déjà :

Lemme. $I(f)$ est un idéal différentiel.

Démonstration. C'est certainement un idéal (car $\langle f \rangle$ est un idéal). Supposons que $s^n g \in \langle f \rangle$. Alors $s^{n+1} g \in \langle f \rangle$, donc $D(s^{n+1} g) \in \langle f \rangle$ (car $\langle f \rangle$ est un idéal différentiel), et $D(s^{n+1} g) = (n+1) s^n D(s) g + s^{n+1} D(g)$. Comme $s^n g \in \langle f \rangle$, on en déduit que $s^{n+1} D(g) \in \langle f \rangle$.

A partir de maintenant, nous supposerons que R est un corps K de caractéristique 0. Le lemme ci-dessous est faux en caractéristique $p > 0$.

(10.12) **Lemme**. Soit $f(X) \in K\{X\}$ un polynôme différentiel irréductible d'ordre n et de degré m. Si $g \in \langle f \rangle \setminus 0$, alors l'ordre de $g(X)$ est au moins n, et s'il égale n alors f divise g.

Démonstration. [Rappelons qu'un élément f d'un anneau R est irréductible si pour tous $g, h \in R$ tels que $f = gh$, un des éléments g, h est inversible dans R.] Soit $s(X)$ la séparante de $f(X)$.

Assertion. Si $\ell \geq 1$, alors $D^\ell(f(X)) = s(X)X^{(n+\ell)} + f_\ell(X)$, où $f_\ell(X)$ est d'ordre $\leq n + \ell - 1$.

Ecrivons $f(X) = \sum_{i=0}^m g_i(X)(X^{(n)})^i$, où les $g_i(X)$ sont d'ordre $\leq n - 1$. Alors

$$\begin{aligned} D(f) &= \sum_{i=0}^m D(g_i(X))(X^{(n)})^i + g_i(X)i(X^{(n)})^{i-1}X^{(n+1)} \\ &= s(X)X^{(n+1)} + f_1(X) \end{aligned}$$

où $f_1(X) = \sum_{i=0}^m D(g_i)(X)$ est d'ordre $\leq n$ (car chaque $g_i(X)$ est d'ordre $\leq n - 1$). Ceci montre le cas $\ell = 1$. Le cas général se montre par induction (exercice).

Soit $g \in \langle f \rangle$, et écrivons $g = a_0 f + a_1 D(f) + \cdots + a_k D^k(f)$, où les $a_i \in K\{X\}$. Si $k = 0$ ou bien l'ordre de g est supérieur à n, il n'y a rien à montrer. Nous supposerons donc $k > 0$, et que l'ordre de g est au plus n.

Nous savons que $X^{(n+k)}$ apparaît dans $D^k(f)$ avec coefficient s, et qu'il n'apparaît pas dans g ou dans $f, D(f), \ldots, D^{k-1}(f)$ (car leurs ordres sont $\leq n$). Nous allons remplacer toutes les occurrences de $X^{(n+k)}$ par la fonction rationnelle $-\frac{f_k}{s}$. Rappelons que $D^k(f) = sX^{(n+k)} + f_k$, et en multipliant tout par une puissance de s appropriée, nous obtenons

$$s^m g = b_0 f + b_1 D(f) + \cdots + b_{k-1} D^{k-1}(f).$$

(En effet la substitution n'affecte pas $g, f, \ldots, D^{k-1}(f)$, car $X^{(k+n)}$ n'y apparaît pas). Nous avons donc prouvé que si g appartient à l'idéal de $K\{X\}$ engendré par $f, D(f), \ldots, D^k(f)$, alors il existe m tel que $s^m g$ appartienne à l'idéal de $K\{X\}$ engendré par $f, D(f), \ldots, D^{k-1}(f)$. Par induction, il existe donc M tel que $s^M g = cf$. Mais le degré de s est inférieur à celui de f, et f est irréductible. Donc f divise g, ce qui prouve le lemme.

(10.13) **Corollaire**. Soit $f \in K\{X\}$ irréductible d'ordre n, et soit $g \in I(f) \setminus \{0\}$. Alors l'ordre de g est au moins n, et s'il égale n alors f divise g.

Démonstration. Soit m tel que $s^m g \in \langle f \rangle$. Par le lemme précédent, l'ordre de $s^m g$ est au moins n. S'il est supérieur à n, alors l'ordre de g est supérieur à n. S'il égale n, alors f divise $s^M g$ pour un entier $M \geq m$, ce qui entraîne (comme précédemment) que f divise g.

(10.14) **Exercice 5**. Soit K un corps différentiel, contenu dans un grand corps algébriquement clos Ω, et $\bar{a} = (a_i)_{i \in I}$ un uplet (peut-être infini) d'éléments de Ω. Nous considérons l'idéal (premier) $I(\bar{a}/K) \subseteq K[\bar{X}] = K[X_i \mid i \in I]$, et prenons un système $\{f_\alpha(\bar{X}), \alpha \in J\}$ de générateurs de cet idéal. Supposons que nous ayons une famille $(u_i)_{i\in I}$ d'éléments de $K(\bar a)$ satisfaisant pour tout $\alpha \in J$:

$$0 = D(f_\alpha)(\bar a) + \sum_{i\in I} \frac{\partial f_\alpha}{X_i}(\bar a)u_i.$$

Nous étendons D^* à $K(\bar a)$ en posant, pour $g(\bar X) \in K(\bar X)$ qui soit définie en $\bar a$,

$$D^*(g(\bar a)) = D(g)(\bar a) \sum_{i\in I} \frac{\partial g}{\partial X_i}(\bar a)u_i.$$

(1) Montrez que si $g(\bar X) \in I(\bar a/K) \subseteq K[\bar X]$, alors $D^*(g(\bar a)) = 0$. En déduire que D^* est bien définie, c'est à dire que si $g(\bar a) = h(\bar a)$ pour des éléments $g(\bar X), h(\bar X)$ de $K(\bar X)$, alors $D^*(g(\bar a)) = D^*(h(\bar a))$.

(2) Vérifiez que D^* définit bien une dérivation de $K(\bar a)$.

(3) Soit D' une autre dérivation de $K(\bar a)$ étendant D et satisfaisant $D'(a_i) = u_i$ pour $i \in I$. Montrez que $D = D'$.

(10.15) **Exercice 6**. Soit k un corps différentiel et $a \in \tilde k$, $f(X) = \sum_{i=0}^n a_i X^i$ son polynôme minimal (unitaire) sur k. Utilisant le fait que $f(a) = 0 = D(f(a))$, montrez qu'il existe une seule extension de la dérivation D au corps $k(a)$. Si $b = \sum_{i=0}^{n-1} a^i$, où les $a_i \in k$, calculez $D(b)$.

(10.16) **Lemme** (Division). Soit $f \in K\{X\}$ irréductible d'ordre n, et soit $g \in K\{X\}$. Il existe $g_1 \in K\{X\}$ d'ordre au plus n et $m \in \mathbf{N}$ tel que $s^m g - g_1 \in \langle f\rangle$.

Démonstration. Supposons que g ait ordre $k+n$ avec $k > 0$, et que le lemme soit vrai pour tous les $h \in K\{X\}$ satisfaisant $h \ll g$. Par l'assertion du lemme (10.12), nous pouvons écrire $D^k(f) = sX^{(n+k)} + f_k$, où l'ordre de f_k est au plus $n+k-1$. Supposons que g soit de degré m, et écrivons le $g = \sum_{i=0}^m h_i(X){X^{(n+k)}}^i$, où les h_i sont d'ordre $< n+k$. Soit maintenant $g_1 = s^m g - D^k(f)^m h_m$. Alors g_1 est d'ordre $\leq n+k$ et de degré $< m$. De plus $s^m g - g_1 \in \langle f\rangle$. Par hypothèse d'induction, il existe ℓ et $g_2 \in K\{X\}$ d'ordre $\leq n$ tels que $s^\ell g_1 - g_2 \in \langle f\rangle$. Nous avons alors $s^{\ell+m} g - g_2 \in \langle f\rangle$.

Corollaire. Si $f \in K\{X\}$ est irréductible et d'ordre n, alors $I(f)$ est un idéal différentiel premier.

Démonstration. Soient $u, v \in K\{X\}$ tels que $uv \in I(f)$, et soient u', v' d'ordre $\leq n$ et $m \in \mathbf{N}$ tels que $s^m u - u', s^m v - v' \in \langle f\rangle$. Alors $s^{2m} uv - u'v' \in \langle f\rangle$. Nous avons donc que f divise $u'v'$, ce qui entraîne qu'il divise l'un des deux, disons u'. Mais alors $s^m u \in \langle f\rangle$, ce qui montre que $u \in I(f)$.

(10.17) **Lemma**. Tout idéal différentiel premier I de $K\{X\}$ est de la forme $I(f)$.

Démonstration. Choisissons $f \in I \setminus \{0\}$ minimal pour $\ll$. Nous dirons que f est un **polynôme minimal pour** I. Nous allons montrer que $I = I(f)$. Tout d'abord, $\langle f\rangle \subseteq I$, et $s \notin I$ car $s \ll f$. Donc, si $s^m g \in I$ alors $g \in I$ car I est premier, et cela montre que $I(f) \subseteq I$.

Soit $g \in I$, et prenons $g_1 \in \langle f\rangle$ et $m \in \mathbf{N}$ tels que $s^m g - g_1 \in \langle f\rangle$, et tel que l'ordre de g_1 soit au plus égal à l'ordre n de f (lemme (10.16)). Notons que comme

$g_1 \in I$, l'ordre de g_1 égale n. Soit d le degré de f. En utilisant l'algorithme d'Euclide dans l'anneau $K(X,\ldots,X^{(n-1)})[X^{(n)}]$, nous pouvons écrire $g_1 = af + r_1$, où $a, r_1 \in K(X,\ldots,X^{(n-1)})[X^{(n)}]$, et r_1 est de degré $< d$ en $X^{(n)}$. En chassant les dénominateurs, il existe $a_1, a_2, r_2 \in K[X,\ldots,X^{(n)}]$ tels que $a_1 g_1 = a_2 f + r_2$, avec a_1, a_2 d'ordre $< n$ et r_2 d'ordre n et de degré $< d$. Alors $r_2 \in I$, et $r_2 \ll f$, donc $r_2 = 0$. Cela entraîne que $a_1 g_1 = a_2 f$, et donc que f divise g_1. Nous avons donc : $g_1 \in I(f)$, $s^m g - g_1 \in I(f)$, ce qui entraîne que $g \in I(f)$.

(10.18) **Le rang différentiel**. Si I est un idéal différentiel premier de $K\{X\}$, nous posons $RD(I)$ comme étant l'ordre d'un polynôme minimal de I si $I \neq (0)$, et ω si $I = (0)$.

Soit L un corps différentiel contenant K, et $a \in L$. On définit $I_D(a/K) = \{f(X) \in K\{X\} \mid f(a) = 0\}$. Il est clair que $I_D(a/K)$ est un idéal différentiel premier. De plus, notons par $K\langle a\rangle$ le sous-corps différentiel de L engendré par a au-dessus de K (donc $K\langle a\rangle = K(a, D(a), \ldots, D^k(a), \ldots))$. On montre alors facilement que $tr.deg(K\langle a\rangle/K) = RD(I_D(a/K))$, car $K\langle a\rangle$ est K-isomorphe au corps de fractions de $K\{X\}/I_D(a/K)$ (l'isomorphisme est celui qui envoie a sur la classe $X/I_D(a/K)$, et $D^m(a)$ sur la classe $X^{(m)})/I_D(a/K))$ pour $m \geq 1$).

(10.19) **Corollaire**. Soient $I \subset J \subset K\{X\}$ des idéaux premiers, avec $I \neq J$. Alors $RD(I) > RD(J)$.

Démonstration. Soient f, $g \in K\{X\}$ des polynômes différentiels irréductibles tels que $I(f) = I$ et $I(g) = J$. Nous savons que $RD(I)$ égale l'ordre de f, et $RD(J)$ égale celui de g. Puisque l' ordre de f est minimal parmi les éléments non nuls de I, et que $I \subset J$, nous savons que $RD(I) \geq RD(J)$. Supposons qu'ils soient égaux. Comme $f \in I(g)$, nous avons alors (par (10.13)) que g divise f. Mais cela entraîne que f et g engendrent les même idéaux dans $K\{X\}$ (car f est irréductible), et donc que $I(f) = I(g)$. Ceci contredit notre hypothèse, et l'ordre de f est supérieur à celui de g. Donc $RD(J) > RD(I)$.

(10.20) **Eléments différentiellement algébriques, trasncendants, bases de transcendance différentielle**. Soit $k \subset K$ des corps différentiels. On dit que $a \in K$ est **différentiellement transcendant** sur k si $I_D(a/k) = (0)$. Sinon, on dira que a est **différentiellement algébrique** sur k. Un élément différentiellement algébrique sur k est donc un élément de K qui annule un polynôme différentiel non nul à coefficients dans k. Si $\bar{a}$ est un n-uplet d'éléments de K, on dit que $\bar{a}$ est **différentiellement indépendant** au-dessus de k si $I_D(\bar{a}/k) = (0)$, c'est-à-dire si le n-uplet $\bar{a}$ ne satisfait aucune équation différentielle à coefficients dans k.

Un sous-ensemble B de K est **différentiellement indépendant** au-dessus de k si tout uple fini de B est différentiellement indépendant au-dessus de k. Le sous-enesmble B de K est une **base de transcendance diférentielle** de K sur k si B est différentiellement indépendant sur k, et tout élément de K est différentiellement algébrique sur $k\langle B\rangle$. De façon équivalente, si B est un sous-ensemble de K différentiellement indépendant sur k et maximal pour cette propriété.

(10.21) **Remarque**. Soient $k \subset K$ des corps différentiels, et $a \in K$. Alors a est différentiellement transcendant sur k si et seulement si $tr.deg(k\langle a\rangle/k) = \infty$. Il est clair que si $I_D(a/k) = (0)$ alors $tr.deg(k\langle a\rangle/k) = \infty$. Réciproquement, supposons que $I_D(a/k)$ soit non nul, et soit $f \in k\{X\}$ irréductible et tel que $I_D(a/k) = I(f)$. Soit n l'ordre de f et s sa séparante. Alors $s \notin I(f)$. De plus, par le lemme de division (10.16), si $N > n$, alors il existe g_1 d'ordre au plus n et un entier m tel que $s^m X^{(N)} - g_1 \in \langle f \rangle$. Ceci nous dit exactement que $s^m(a)D^N(a) = g_1(a)$, et donc que $D^N(a) \in k[a, D(a), \dots, D^n(a), s(a)^{-1}] \subset k(a, \dots, D^n(a))$. Le corps $k(a, \dots, D^n(a))$ est donc un corps différentiel, de degré de transcendance n au-dessus de k. [Puisque a ne satisfait aucune équation différentielle d'ordre $n-1$ et à coefficients dans k, les éléments $a, D(a), \dots, D^{n-1}(a)$ sont algébriquement indépendants au-dessus de k ; puisque a satisfait $f(a) = 0$, $D^n(a)$ est algébrique sur $k(a, D(a), \dots, D^{n-1}(a))$.]

(10.22) **Lemme d'échange**. Soient $k \subset K$ des corps différentiels, $A \subset K$, et $a, b \in K$. Supposons que b soit différentiellement algébrique sur $k\langle A, a\rangle$, mais ne soit pas différentiellement algébrique sur $k\langle A\rangle$. Alors a est différentiellement transcendant sur $k\langle A\rangle$, et est différentiellement algébrique sur $k\langle A, b\rangle$.

Démonstration. Nous pouvons supposer que $k = k\langle A\rangle$. Puisque b n'est pas différentiellement transcendental sur $k\langle a\rangle$, nous savons qu'il existe $f(X,Y) \in k\{X,Y\}$ non nul tel que $f(a,b) = 0$. Nous le choisissons d'ordre et de degré minimal en tant que polynôme différentiel en Y. Puisque b n'est pas différentiellement algébrique sur k, nous savons que $f(X,Y) \notin k\{Y\}$, et que le polynôme différentiel $f(X,b) \notin k$, c'est à dire que a est différentiellement algébrique sur $k\langle b\rangle$. D'autre part, a ne peut être différentiellement algébrique sur k, sinon non aurait

$$\begin{aligned} tr.deg(k\langle a,b\rangle/k) &= tr.deg(k\langle a,b\rangle/k\langle b\rangle) + tr.deg(k\langle b\rangle/k) = \infty \\ &= tr.deg(k\langle a,b\rangle/k\langle a\rangle) + tr.deg(k\langle a\rangle/k) < \infty \end{aligned}$$

ce qui nous donnerait une contradiction.

Grâce au lemme d'échange nous obtenons que deux bases de transcendance différentielles de K sur k ont la même cardinalité.

(10.23) **Corps différentiellement clos**. Nous travaillons dans le langage $\mathcal{L}_D$. Soit DCF la théorie dont les modèles sont les $\mathcal{L}_D$-structures K satisfaisant les axiomes suivants:

(i) Les axiomes pour les corps algébriquement clos de caractéristique 0.
(ii) Les axiomes pour les corps différentiels.
(iii) Pour tous $f(X), g(X) \in K\{X\}$ tels que l'ordre de g est inférieur à l'ordre de g, l'axiome $\exists x\, f(x) = 0 \wedge g(x) \neq 0$.

Les modèle de DCF seront appelés des **corps différentiellement clos**.

(10.24) **Théorème**. Tout corps différentiel k se plonge dans un corps différentiellement clos.

Démonstration. Soit $f(X), g(X) \in k\{X\}$, avec $f(X)$ d'ordre n, $g(X)$ d'ordre $< n$ (si $n = 0$, on ne prend pas de g. Le cas $n = 0$ nous permet donc de montrer que k se plongera dans un corps différentiel algébriquement clos). Remplaçant $f(X)$ par un de ses facteurs irréductibles d'ordre n, nous pouvons supposer que f est irréductible. Soit R l'anneau différentiel $k\{X\}/I(f)$. L'élément $a = X/I(f)$ satisfait $f(x) = 0 \wedge g(x) \neq 0$, car $f(X) \in I(f)$, et $g \notin I(f)$ par (10.16). De plus, R est intègre (Corollaire (10.16)), D s'étend au corps F des fractions de R, et F est un corps différentiel contenant k.

Nous avons donc montré les deux choses suivantes :

– si $f(X) \in k[X]$, est un polynôme irréductible, alors k est contenu dans un corps différentiel contenant une racine de $f(X) = 0$. Par un argument limite, nous voyons que tout corps différentiel se plonge dans un corps différentiel algébriquement clos.

– Tout instance de l'axiome (iii) est satisfaite dans un corps différentiel contenant k. De même, un argument standard montre que k se plonge dans un corps différentiellement clos. [On plonge d'abord k dans un corps différentiel k_1 algébriquement clos et satisfaisant toutes les instances de l'axiome (iii) à coefficients dans k, puis on fait de même avec k_1, pour obtenir k_2. Finalement on prend $K = \bigcup k_n$, où chaque k_{n+1} est un corps différentiel algébriquement clos dans lequel toutes les instances de l'axiome (iii) à coefficients dans k_n sont satisfaites. On aura alosr $K \models$DCF.]

(10.25) **Proposition**. Soient K et L des corps différentiels ω-saturés. Alors la famille $\mathcal{I}$ des isomorphismes partiels entre K et L a la propriété du va-et-vient.

Démonstration. Tout d'abord $\mathcal{I}$ n'est pas vide, car l'isomorphisme $\emptyset$ est dans $\mathcal{I}$. Soit $f \in \mathcal{I}$, $\bar{a} = dom(f)$, $\bar{b} = f(\bar{a})$, et soient $k = \mathbf{Q}\langle\bar{a}\rangle$, $\ell = \mathbf{Q}\langle\bar{b}\rangle$. Alors f s'étend de façon unique à un isomorphisme de corps différentiels $f : k \to \ell$. En effet tous les éléments de k sont de la forme $t(\bar{a})u(\bar{a})^{-1}$, où $t(\bar{x}), u(\bar{x})$ sont des termes de $\mathcal{L}_D$, et de même pour ℓ.

Soit g un polynôme minimal de $I(a/k)$, et n son ordre. Nous avons alors $I(a/k) = I(g)$. Par ω-saturation de L et l'axiome (iii), il existe $b \in L$ satisfaisant le type (partiel) suivant:

$$\{f(g)(x) = 0\} \cup \{h(x) \neq 0 \mid h(X) \in l\{X\}, \text{ ordre de } h(X) < n\}.$$

Nous affirmons que nécéssairement $I(b/\ell) = I(f(g))$. Nous savons que $I(b/\ell)$ est un idéal premier différentiel de $l\{X\}$, qui contient le polynôme irréductible $f(g)$ (puisque g est irréductible, $f(g)$ l'est aussi), et qui ne contient pas d'éléments d'ordre inférieur à n. Par le corollaire (10.19), nous avons donc $I(b/\ell) = I(f(g))$, et cela entraîne que $l\langle b\rangle$ est ℓ-isomorphe (comme corps différentiel) au corps des fractions de $l\{X\}/I(f(g))$. L'application f se prolonge donc à un isomorphisme de corps différentiels entre $k\langle a\rangle$ et $l\langle b\rangle$ qui envoie a sur b.

Si maintenant $I(a/\tilde{k}) = (0)$, alors par ω-saturation de L, il existe $b \in L$ tel que b soit différentiellement transcendental sur $\tilde{\ell}$, et nous pouvons prolonger f en envoyant a sur b.

(10.26) **Théorème**. DCF élimine les quantificateurs, est complète et modèle complète .

Démonstration. C'est un corollaire de la proposition (10.25).

(10.27) **Corollaire** (Nullstellensatz différentiel). Si k est un corps différentiel, et Σ est un système fini d'équations différentielles qui a une solution dans un corps différentiel contenant k, alors Σ a une solution dans tout corps différentiellement clos contenant k.

Démonstration. Soit L un corps différentiel contenant k, dans lequel Σ a une solution. Par (10.24), L se plonge dans un corps différentiellement clos K dans lequel Σ a aussi une solution. Par (10.26), DCF $\cup\, \Delta(k)$ est complète, et nous savons aussi que L en est un modèle, qui satisfait la formule $\exists\bar{x}\ \Sigma(\bar{x}) = 0$. Donc DCF $\cup\, \Delta(k) \vdash \exists\bar{x}\ \Sigma(\bar{x}) = 0$. Or, tout corps différentiellement clos contenant k est un modèle de cette théorie.

(10.28) **Thérème** DCF est ω-stable.

Démonstration. Soit K un corps différentiellement clos, et $A \subset K$ de cardinalité $\leq \aleph_0$. Nous pouvons supposer que A est un sous-corps diférentiel de K. Alors l'application qui à un type $p(x) \in S_1(A)$ associe l'idéal différentiel $I_D(p)$ des polynômes différentiels $f(X) \in A\{X\}$ tels que $f(x) = 0 \in p(x)$, établit une correspondance entre les 1-types sur A et les idéaux premiers différentiels de $A\{X\}$. Ces derniers sont ou bien (0), ou bien de la forme $I(f)$ pour un $f \in A\{X\}$. Cela montre que $|S_1(A)| \leq |A\{X\}| = |A|$.

(10.29) **Clôture différentielle**. Je vous ai dit que dans une théorie ω-stable, les modèles premiers au-dessus d'ensembles quelconques existent, et sont uniques à isomorphisme près (au-dessus de l'ensemble considéré). Traduit dans notre cas, cela donne:

Soit K un corps différentiellement clos, et A un sous-corps différentiel de K. Alors il existe une sous-structure élémentaire B de K contenant A qui se plonge dans tout corps différentiellement clos contenant A comme sous-corps différentiel. De plus, cette propriété détermine B à A-isomorphisme près. Nous appellerons ce corps différentiel B la **clôture différentielle de** A.

On peut montrer que B est nécéssairement atomique au-dessus de A, c'est à dire que le type sur A de tout uplet fini d'éléments de B est isolé.

(10.30) **Corollaire**. Soit k un corps différentiel, et K la clôture différentielle de k. Alors le corps C_K des constantes de K est la clôture algébrique du corps C_k des constantes de k.

Démonstration. Soit $a \in \tilde{C}_k$, et $f(X) = \sum_{i=0}^m a_i X^i$ son polynôme minimal sur C_k. Alors $D(a_i) = 0$ pour tout i, et donc $D(f(a)) = 0 = \sum_{i=0}^m a_i i a^{i-1} D(a)$. Comme $\sum_{i=0}^m a_i i a^{i-1} \neq 0$, nous avons $D(a) = 0$.

Soit $a \in C_K$, et $I = I_D(a/k)$. Nous savons que I détermine $tp(a/k)$, et nous savons aussi que $tp(a/k)$ est isolé. Supposons que a ne soit pas algébrique sur k. Alors a est transcendant sur k, et son type sur k est axiomatisé par

$$D(x) = 0 \cup \{f(x) \neq 0 \mid f(X) \in k[X] \setminus 0\}.$$

Il existe donc $g(X) \in k[X]$ tel que $D(x) = 0 \cup g(X) \neq 0$ axiomatise $tp(a/k)$: mais c'est impossible, car cette formule a une réalisation dans $\tilde{C}_k$. Cela entraîne que a est algébrique sur k. Nous avons vu que si b est un conjugué de a au-dessus de k, alors le k-isomorphisme entre $k(a)$ et $k(b)$ qui envoie a sur b est un isomorphisme de corps différentiels (cf exercice 6). Nous avons donc que tous les conjugués de a au-dessus de k sont dans C_K. Si $p(T) \in k[T]$ est le polynôme minimal (unitaire) de a sur k, et $a = a_1, \ldots, a_n$ sont ses racines, alors $p(T) = \prod_{i-1}^n (T - a_i)$, ce qui entraîne que les coefficients de $p(T)$ sont dans C_K. Ils sont donc dans $C_K \cap k = C_k$, ce qui montre que $a \in \tilde{k}$.

(10.31) **Clôture algébrique, clôture définissable**. Soit k un sous-corps différentiel du corps différentiellement clos K. Alors $k = dcl(k)$ et $acl(k) = \tilde{k}$.

Montrons d'abord la deuxième assertion. Si $a \in \tilde{k}$, alors certainement $a \in acl(k)$. Supposons maintenant que $a \in K \setminus \tilde{k}$ et considérons $I_D(a/\tilde{k})$. Si a est algébrique au-dessus de $\tilde{k}$, alors l'ensemble A des $b \in K$ tels que $I_D(b/\tilde{k}) = I_D(a/\tilde{k})$ est fini. Nous savons que $I_D(a/\tilde{k})$ est un idéal différentiel premier de $\tilde{k}\{X\}$, qui est de la forme $I(f)$ pour un polynôme irréductible $f(X) \in \tilde{k}\{X\}$, et donc engendre dans $K\{X\}$ un idéal premier différentiel que nous noterons J.

Soit L le corps des fractions de $K\{X\}/J$, et $c = X/J$. Le corps L se plonge dans un corps différentiellement clos M, et nous avons alors $K \prec M$. Comme l'élément c satisfait $I_D(c/\tilde{k}) = I_D(a/\tilde{k})$, nous avons nécéssairement que $c \in K$. Cela entraîne que J est un idéal maximal de $K\{X\}$, c'est à dire que $f(X) = X - a$, et que $a \in \tilde{k}$.

Soit maintenant $a \in \tilde{k}$, et b un conjugué de a au dessus de k, avec $b \neq a$. Le k-isomorphisme $k(a) \to k(b)$ qui envoie a sur b, est alors un isomorphisme de corps différentiels (cf exercice 6). Par élimination des quantificateurs nous avons $tp(a/k) = tp(b/k)$, et donc $a \notin dcl(k)$.

(10.32) **Rang de Morley**. Puisque la théorie DCF est ω-stable, nous savons que toutes les formules ont un rang de Morley, et donc tous les types aussi. Vous montrerez que $RM(x = x) = \omega$, ici nous allons faire une observation facile, je vous laisse les plus difficiles pour l'examen.

Lemme/Remarque Soient K un modèle de DCF, $f(X) \in K\{X\}$ un polynôme différentiel irréductible d'ordre 1, $s(X)$ sa séparante, et soit $D = \{a \in K \mid f(a) = 0,\ s(a) \neq 0\}$. Alors D est fortement minimal.

Démonstration. Nous allons montrer que tout sous-ensemble définissable de D est fini ou co-fini. Considérons d'abord un sous-ensemble Y de D défini par $x \in D \wedge g_1(x) = \ldots = g_m(x) = 0$, où les $g_i(X) \in K\{X\}$. Tout d'abord, par le lemme de division (10.16), nous pouvons supposer que les ordres des $g_i(X)$ sont sont inférieurs à 1 : en effet pour chaque i il existe $g_i'(X)$ d'ordre inférieur à 1 et un entier m tel que $s^m g_i - g_i' \in \langle f \rangle$. Si $a \in D$, nous aurons alors $s(a) \neq 0$, et donc $g_i(a) = 0 \iff g_i'(a) = 0$. Nous supposerons donc que chaque $g_i(X)$ s'écrit $G_i(X, X')$, où $G_i \in K[X, X']$. De même, nous savons que $f(X) = F(X, X')$ pour $F \in k[X, X']$. Soit $C \subset K^2$ l'ensemble algébrique défini par l'équation $F(X, X') = 0$. Par (7.17), c'est un ensemble de dimension 1, et parce que f est irréductible, F est irréductible, et C est en fait une variété. Alors $C \cap V(G_1, \ldots, G_m)$ est un sous-ensemble fermé de C, qui est ou bien de dimension inférieure à $dim(C) = 1$ (c'est une conséquence de (7.17)(3)), et donc fini, ou alors contient C. Si $a \in Y$, alors $(a, D(a)) \in C \cap V(G_1, \ldots, G_m)$. Dans le cas où $C \cap V(G_1, \ldots, G_m)$ est fini, cela nous donne que Y est fini. Dans le cas où $C \cap V(G_1, \ldots, G_m)$ contient C, nous avons que F divise chacun des G_i, c'est à dire que $f(a) = 0$ implique $g_1(a) = \cdots = g_m(a) = 0$, et $Y = D$.

Soit maintenant Y un sous-ensemble définissable quelconque de D. Par élimination des quantificateurs, nous pouvons écrire Y comme une union finie d'ensembles de la forme $Y_i \setminus Z_i$, où les Y_i et Z_i sont définis par des équations différentielles. Par le premier cas, nous savons que les Y_i ou Z_i sont ou bien finis, ou bien contiennent D. Cela nous donne que Y est fini ou cofini, et montre que D est fortement minimal.

(10.33) **Non minimalité de la clôture différentielle**. Nous allons montrer que la clôture différentielle K de $\mathbf{Q}$ n'est pas minimale, c'est à dire qu'elle a une sous-structure élémentaire propre.

Lemme. Soit T une théorie ω-stable, et soit M un modèle de T premier au-dessus de A.

Supposons que M soit minimal au-dessus de A, c'est à dire, que si M' est une sous-structure élémentaire de M contenant A alors $M = M'$.

Si $\bar{a}_i$, $i \in I$, est une suite totalement indiscernable au-dessus de A, alors I est fini.

Démonstration. Supposons que $\bar{a}_i$, $i \in \mathbf{N}$, soit une suite infinie totalement indiscernable sur A (voir définition (5.6)). Soit $B = \{\bar{a}_i \mid i \in \mathbf{N}\}$, et $C = \{\bar{a}_i \mid i \geq 1\}$. Soit N le modèle premier de T au-dessus de $A \cup C$. Alors N se plonge élémentairement dans M, et nous pouvons supposer que $N \prec M$. Nous allons montrer que $\bar{a}_0 \notin N$, ce qui montrera bien que M est non-minimal. Supposons que $\bar{a}_0 \in N$. Nous savons que N est atomique sur $A \cup C$, ce qui implique que $tp(\bar{a}_0/A \cup C)$ est isolé. Soit $\varphi(\bar{x}, \bar{a}, \bar{c})$ la formule l'isolant ($\varphi \in \mathcal{L}$, $\bar{a} \in A$ et $\bar{c} \in C$). Par indiscernabilité totale au-dessus de A, la formule $\varphi(\bar{x}, \bar{a}, \bar{c})$ est satisfaite par tous les éléments de $C \setminus \bar{c}$. Fixons $i > 0$ avec $\bar{a}_i \notin C$. La formule $\varphi(\bar{x}, \bar{a}, \bar{c})$ ne peut donc isoler $tp(\bar{a}_0/A \cup C)$, puisqu'elle n'implique pas la formule $\bar{x} \neq \bar{a}_i$ qui appartient à $tp(\bar{a}_0/A \cup C)$, et nous obtenons une contradiction. Donc $\bar{a}_0 \notin N$, et M n'est pas minimal.

Remarque. En fait la réciproque de ce lemme est vraie aussi : si toute suite d'indiscernables au-dessus de A est finie, alors M est minimal au-dessus de A.

(10.34) **Stratégie pour montrer que la clôture différentielle n'est pas nécéssairement minimale.** Nous travaillons dans un modèle K de DCF. Nous allons exhiber un sous-corps différentiel k de K, et un ensemble fortement minimal D défini sur k, et tel que les éléments de D sont indépendants au-dessus de k (au sens de la prégéometrie sur D ; en fait cela coïncide aussi avec le sens "stable"). Si K_0 est la clôture différentielle de K, alors $D \cap K_0$ est infini, et ses éléments forment une suite totalement indiscernable au-dessus de k (voir (9.17)). Par le lemme (10.33), K_0 ne peut être minimal au-dessus de k.

(10.35) **Théorème** (Rosenlicht) Soient $k \subset K$ des corps différentiels, avec même corps de constantes, noté C. Soient $f(X) \in C(X)$, $c_1, \ldots, c_n \in C$, $u_1, \ldots, u_n \in C(X)$, et

$$\frac{1}{f(X)} = \sum_{i=1}^{n} c_i \frac{\frac{\partial u_i}{\partial X}}{u_i} + \frac{\partial v}{\partial X}.$$

Soient $x_1, x_2 \in K$ des solutions de $X' = a_1 f(X)$ et $X' = a_2 f(X)$ respectivement, avec $a_1, a_2 \in k$. Si $x_2 \in acl(k, x_1)$ alors $x_2 \in \tilde{k}$, ou bien $a_2 D(v(x_1)) = a_1 D(v(x_2))$.

(10.36) **Exemples**

(1) Soit $f(X) = \frac{X}{1+X}$. Alors

$$\frac{1}{f(X)} = \frac{1}{X} + 1$$

est de la forme requise : on prend $u_1 = v = X$, $c_1 = 1$.

(2) Soit $f(X) = X^3 - X^2$. Prenons $u_1(X) = \frac{X-1}{X}$ et $v(X) = \frac{1}{X}$. Alors $\frac{\partial u}{\partial X} = \frac{1}{X^2}$, et

$$\frac{\frac{\partial u}{\partial X}}{u} = \frac{1}{X(X-1)} = \frac{1}{X-1} - \frac{1}{X},$$

et

$$\frac{1}{f(X)} = \frac{1}{X^2(X-1)} = \frac{1}{X_1} - \frac{1}{X} - \frac{1}{X^2} = \frac{\frac{\partial u}{\partial X}}{u} + \frac{\partial v}{\partial X}.$$

(10.37) **Corollaire**. Soit C le corps des constantes, K sa clôture différentielle, et soit $f(X) = \frac{X}{X+1}$ ou $f(X) = X^3 - X^2$. Soient $x_1, \ldots, x_n$ des solutions distinctes de $X' = f(X)$. Alors $x_1, \ldots, x_n$ sont algébriquement indépendants au-dessus de C.

Démonstration. Nous savons que $C_K = \tilde{C}$, et nous pouvons supposer que C est algébriquement clos. Prenons d'abord le cas où $f(X) = \frac{X}{X+1}$. Alors $v(X) = X$. La démonstration est par induction sur n. Si $n = 1$, il n'y a rien prouver. Supposons que nous ayons montré que $x_1, \ldots, x_{n-1}$ sont algébriquement indépendants au-dessus de C, et soit $k = C(x_1, \ldots, x_{n-2})$. Notons que k est un sous-corps différentiel de K. Supposons maintenant que $x_{n-1} \in acl(k(x_n))$. Par hypothèse d'induction, nous savons que $x_{n-1} \notin \tilde{k}$, et par (10.35), cela entraîne que $D(x_{n-1}) = D(x_n)$. Donc, nous avons

$$\frac{x_{n-1}}{x_{n-1}+1} = \frac{x_n}{x_n+1},$$

ce qui entraîne $x_{n-1} = x_n$. Cela n'est pas possible, et $x_{n-1} \notin acl(k, x_n)$. Comme $RD(x_{n-1}/k) = RD(x_n/k) = 1$, cela entraîne que x_{n-1} et x_n sont indépendants au-dessus de k, et donc que $x_1, \ldots, x_n$ sont indépendants au-dessus de k.

La démonstration est similaire pour $f(X) = X^3 - X^2$.

(10.38) **Corollaire**. La clôture différentielle de $\mathbf{Q}$ n'est pas minimale.

Démonstration. Soit K la clôture différentielle de $\mathbf{Q}$. Elle contient donc une infinité de solutions de l'équation $X' = \frac{X}{X+1}$, et ces solutions sont algébriquement indépendantes au-dessus de $\mathbf{Q}$. De plus, elles réalisent toutes le même type, et forment une suite indiscernable au-dessus de $\mathbf{Q}$, car la formule $X' = \frac{X}{X+1}$ est fortement minimale.

(10.39) **Définition de l'indépendance**. Soit K un corps différentiellement clos, k un sous-corps différentiel de K, et A, B des sous-ensembles de K. Nous dirons que A et B sont **indépendants au-dessus de** k (ou bien que A est **indépendant de** B **au-dessus de** k) si les corps $k\langle A\rangle$ et $k\langle B\rangle$ sont algébriquement indépendants sur k (c'est à dire des éléments de $k\langle A\rangle$ qui sont algébriquement indépendants sur k le sont aussi sur $k\langle B\rangle$.)

(10.40) **Remarques**. (1) Remarquons tout de suite que si k est algébriquement clos, et B est un sous-corps différentiel de K contenant k, $\bar{a}$ un uplet de K, alors $I_D(\bar{a}/k)$ engendre un idéal premier dans $B\{\bar{X}\}$. Il est clair que $\bar{a}$ et B sont indépendants sur k si et seulement si $I_D(\bar{a}/B)$ est l'idéal $I_D(\bar{a}/k)B\{\bar{X}\}$.

(2) Il est clair que si $\bar{a}$ est indépendant de B sur $k = \tilde{k}$, alors l'ensemble de formules représentées par $tp(\bar{a}/B)$ est minimal parmi les ensembles de formules représentées par des extensions de $tp(\bar{a}/k)$ à B. Donc notre notion d'indépendance coïncide avec celle introduite précédemment : si $\bar{a}$ et B sont indépendants au-dessus de k, alors $tp(\bar{a}/B)$ hérite de sa restriction à k.

(3) Il est clair que si A et B sont indépendants sur k, alors $acl(k, A)$ et $acl(k, B)$ sont indépendants sur k (car $acl(k, A) = \widetilde{k\langle A\rangle}$, $acl(k, B) = \widetilde{k\langle B\rangle}$)

(4) On peut étendre cette définition à des sous-ensembles quelconques de K: soient A, B, C des sous-ensembles de K. Nous dirons que A et B sont **indépendants sur** C si les corps $acl(A, C)$ et $acl(B, C)$ sont algébriquement indépendants au-dessus de $acl(C)$.

(10.41) **Définition du rang U**. Nous allons définir un nouveau rang, sur les types d'abord puis sur les formules. Ce rang est aussi appelé le rang de Lascar (son inventeur), et je le trouve plus intuitif et pratique que le rang de Morley.

Soit $A \subset K$, $\bar{a} \in K$, et $p = tp(\bar{a}/A)$. On définit par induction sur les ordinaux la relation $U(p) \geq \alpha$, de la façon suivante :

– $U(p) \geq 0$.

– Si α est limite, alors $U(p) \geq \alpha$ si et seulement si pour tout $\beta < \alpha$, $U(p) \geq \beta$.

– Si $\alpha = \beta + 1$, alors $U(p) \geq \alpha$ si et seulement s'il existe B contenant A tel que $U(tp(\bar{a}/B)) \geq \beta$, et $\bar{a}$ et B ne sont pas indépendants au-dessus de A.

On définit alors $U(p) = U(\bar{a}/A)$ comme étant le plus petit ordinal α s'il existe, tel que $U(p) \geq \alpha$, $U(p) \not\geq \alpha + 1$, et $U(p) = \infty$ si $U(p) \geq \alpha$ pour tout ordinal α.

On montre que cette notion est bien définie. On montre aussi que si $A \subset B$ alors $U(\bar{a}/A) \geq U(\bar{a}/B)$, que si $\bar{a}$ et B sont indépendants sur A, alors $U(\bar{a}/B) = U(\bar{a}/A)$, et que $U(\bar{a}/A) < \infty$. On a bien sûr $U(\bar{a}/A) = U(\bar{a}/acl(A))$ (par notre définition de l'indépendance), et de plus le rang U satisfait une jolie formule additive

$$U(\bar{a}/A\bar{b}) + U(\bar{b}/A) \leq U(\bar{a}, \bar{b}/A) \leq U(\bar{a}/A\bar{b}) \oplus U(\bar{b}/A).$$

Ici, $+$ est la somme des ordinaux, et $\oplus$ est la somme naturelle sur les ordinaux (qui est commutative ; par exemple, $\omega \oplus 1 = 1 \oplus \omega = \omega + 1$). Les deux cas sont possibles : si $\bar{a}$ et $\bar{b}$ sont indépendants sur A, alors $U(\bar{a}, \bar{b}/A) = U(\bar{a}/A) \oplus U(\bar{b}/A)$. Cependant, considérons un élément a différentiellement transcendental sur le corps différentiel A, et soit $b = D(a)$. On peut montrer que $U(a/A) = \omega$ ($= U(b/A)$ car b est aussi différentiellement transcendental sur A), $U(a/Ab) = 1$, et donc $\omega = U(a, b/A) < U(a/Ab) \oplus U(b/A) = 1 \oplus \omega = \omega + 1$. [J'utilise cet exemple pour me rappeler dans quel ordre mettre les éléments $U(\bar{a}/A\bar{b})$ et $U(\bar{b}/A)$].

On peut aussi montrer que $U(p) \leq RM(p)$. Pour finir, on définit le rang U d'une formule $\varphi(\bar{x})$ (à paramètres dans A) par

$$U(\varphi) = \sup\{U(p) \mid p \in S_n(A),\ \varphi(\bar{x}) \in p\}.$$

Il est clair que la définition du rang U s'étend à une théorie stable quelconque, en utilisant la notion d'indépendance correspondant à l'héritage.