Géometrie algébrique et Théorie des modèles

Frank Wagner

Chapitre 1

Les constructibles

1.1 Fermés et ouverts

Définition 1.1.1 Soit K un corps algébriquement clos, et $s < \omega$. Une partie F de K^s est un *fermé principal* si elle consiste des s-uples dans K^s qui annulent un polynôme $f(x_1, \ldots, x_s)$. Donc F consiste des zéros de $f(\bar{x})$; il est défini par l'équation polynomiale $f(\bar{x}) = 0$. Plus généralement, un *fermé* est une intersection finie de fermés principaux ; il est défini par un système (une conjonction) d'équations polynomiales.

Un *ouvert principal* est le complément d'un fermé principal ; il est donc défini par une inéquation $f(\bar{x}) \neq 0$. Un *ouvert* est le complément d'un fermé, il est la réunion des ouvert principaux et est donné par une disjonction d'équations.

Cette définition dépend de l'espace ambiant : le même polynôme $f(\bar{x})$ peut être considéré comme polynôme en variables $\bar{x}$ qui figurent dedans, ou bien en variables $\bar{x}\bar{y}$ pour tout $\bar{y}$; si $\bar{x}$ est de longueur s et $\bar{y}$ est de longueur t, alors $f(\bar{x}) = 0$ définit un fermé F dans K^s, et le fermé $F \times K^t$ dans K^{s+t}.

Nous remarquons que l'intersection d'un nombre fini d'ouverts principaux donnés par des inéquations $f_i(\bar{x}) \neq 0$ (pour $i < n$) est encore principal, et determiné par l'inéquation $\prod_{i<n} f_i(\bar{x}) \neq 0$. Alors, la réunion d'un nombre fini de fermés principaux est aussi un fermé principal ; par distributivité des opération booléennes on voit facilement que la réunion d'un nombre fini de fermés est fermé, et l'intersection d'un nombre fini d'ouverts est ouvert. Nous verrons plus tard que l'intersection d'une famille quelconque des fermés est encore fermée, et est en fait l'intersection d'une sous-famille finie (ce qui

qualifie comme *noethérianité*), et que ce vocabulaire topologique est bien justifié. Il s'agit de la *topologie de Zariski.*

Pour $s = 1$, un fermé est soit K entier, soit un ensemble fini, dont le cardinal est borne par le plus petit des degrés des polynômes dans sa définition. Par dualité, un ouvert est soit vide, soit co-fini (de complément fini) dans K. Par contre, dès que $s \geq 2$, la structure formée dans K^s par les fermés (ou les ouverts) est beaucoup plus riche ; il n'y a pas seulement les produits des fermés de K, mais aussi les diagonales (définies par $x_i = x_j$), les droites, les cercles, les plans, sous-espaces, hyperplans.... On note que dans plusieurs dimensions les points sont toujours fermés, mais ne sont plus des fermés principaux ; en général les fermés principaux sont des ensembles de codimension 1 (donc, des courbes dans K^2, des surfaces dans K^3, etc.).

Lemme 1.1.2

1. *L'inéquation $f(\bar{x}) \neq 0$ définit un ouvert non-vide ssi f n'est pas le polynôme nul.*
2. *L'intersection de deux ouverts non-vides de K^n n'est pas vide ; K^n n'est pas la réunion de deux fermés propres.*

DÉMONSTRATION: Pour la première partie on raisonne par récurrence sur le nombre s de variables. C'est vrai si $s = 0$ et f est constant non-nulle. Soit donc $f(\bar{x}, y) = \sum_{i=0}^{n} f_i(\bar{x})y^i$ où $f_n(\bar{x})$ n'est pas identiquement nul ; par hypothèse d'induction on trouve $\bar{a}$ tel que $f_n(\bar{a}) \neq 0$, et $f(\bar{a}, y)$ n'a pas plus que n zéros. Comme tout corps algébriquement clos est infini, on trouve b tel que $f(\bar{a}, b) \neq 0$.

La deuxième partie suit : si $f(\bar{x})$ et $g(\bar{x})$ ne sont pas identiquement nuls, leur produit $(fg)(\bar{x})$ ne l'est pas non plus. Donc, la réunion de deux fermés principaux propres n'est pas K^s entier. Or, tout fermé propre est contenu dans un fermé principal propre. ■

Définition 1.1.3 Un *constructible* est une combinaison booléenne de fermés.

Donc, un constructible est obtenu à partir des fermés en prenant réunions finies, intersections finies, et compléments. Evidemment, un constructible est aussi une combinaison booléenne d'ouverts.

Lemme 1.1.4 *Tout constructible est réunion d'un nombre fini d'ensembles de la forme $F \cap O$, où F est fermé et O est ouvert principal ; on peut même l'écrire comme une réunion de tels ensembles deux-à-deux disjoints.*

DÉMONSTRATION: En utilisant les lois distibutives booléennes et le loi de de Morgan, on peut exprimer tout constructible en *forme normal disjonctive*, c'est-à-dire comme réunion d'intersections de fermés et d'ouverts. Mais une intersection (finie !) de fermés est encore fermée, et une intersection d'ouverts est ouverte ; tout constructible A s'exprime sous la forme $A = \bigcup_{i<n} F_i \cap \Omega_i$, où les F_i sont fermés et les Ω_i ouverts. Chaque Ω_i est égale à une réunion finie $\bigcup_{j<n_i} O_i^j$ d'ouverts principaux O_i^j, et $A = \bigcup_{i<n} \bigcup_{j<n_i} F_i \cap O_i^j$.

Pour exprimer $A = \bigcup_{i<n} F_i \cap O_i$ comme réunion des intersections deux-à-deux disjointes, on l'écrit d'abord comme

$$A = \bigcup_{i<n} F_i \cap O_i \cap \bigcap_{j<i} (\neg O_j \cup \neg F_j).$$

Si $\bigcap_{j<i}(\neg O_j \cup \neg F_j) = \bigcup_{j<n_i} \Phi_i^j \cap \Omega_i^j$ avec Φ_i^j fermé et Ω_i^j ouvert principal, on obtient

$$\begin{aligned} F_i \cap O_i \cap \bigcap_{j<i} (\neg O_j \cup \neg F_j) &= F_i \cap O_i \cap \bigcup_{j<n_i} \Phi_i^j \cap \Omega_i^j \\ &= \bigcup_{j<n_i} F_i \cap \Phi_i^j \cap O_i \cap \Omega_i^j \\ &= \bigcup_{j<n_i} (F_i \cap \Phi_i^j \cap \bigcap_{k<j} \neg \Omega_i^k) \cap (O_i \cap \Omega_i^j), \end{aligned}$$

ce qui donne la forme requise. ■

Autrement dit, chaque constructible s'exprime comme réunion d'un nombre fini d'ensembles définis chacun par un système de la forme

$$f_1(\bar{x}) = 0 \wedge f_2(\bar{x}) = 0 \wedge \cdots \wedge f_n(\bar{x}) = 0 \wedge g(\bar{x}) \neq 0;$$

bien sûr, il n'y a rien de canonique de cette décomposition !

Pour chaque s nous avons défini les parties constructibles de K^s. Il nous faut maintenant établir des liens entre les constructibles de ces différents espaces. On voit facilement que si $F(\bar{x}, \bar{y})$ est un fermé (principal) de K^{s+t}, alors pour chaque $\bar{a} \in K^t$ on obtient un fermé (principal) $K(\bar{x}, \bar{a})$ en substituant $\bar{a}$ pour $\bar{y}$ dans les équations. De même, pour un ouvert (principal) $O(\bar{x}, \bar{y})$ de K^{s+t} on obtient un ouvert (principal) $O(\bar{x}, \bar{a})$ de K^s ; en substituant dans un constructible $C(\bar{x}, \bar{y})$ on obtient un constructible $C(\bar{x}, \bar{a})$.

Définition 1.1.5 Une famille $\{C_i : i \in I\}$ de constructibles dans K^s est *uniforme* s'il y a un t et un constructible $C(\bar{x}, \bar{y})$ de K^{s+t} tel que chaque C_i s'exprime comme $C(\bar{x}, \bar{a}_i)$ pour un $\bar{a}_i \in K^t$.

Par exemple, les droites du plan K^2 forment une famille uniforme de fermés : on considère le fermé $F(x, y, u, v, w)$ de K^5 défini par $ux+vy = w$; une droite est obtenue en substituant (a, b, c) (avec $a \neq 0$ ou $b \neq 0$) pour (u, v, w).

Proposition 1.1.6

1. *Si $\{F_i : i \in I\}$ est une famille uniforme de fermés dans K, il y a un $n < \omega$ tel que pour chaque $i \in I$ soit $F_i = K$, soit $|F_i| \leq n$.*
2. *Si $\{C_i : i \in I\}$ est une famille uniforme de constructibles dans K, alors il y a un $n\omega$ tel que pour chaque $i \in I$ soit $|C_i| \leq n$, soit $|K - C_i| \leq n$.*

Démonstration: Si $C(x, \bar{y})$ est un constructible dans K^{1+t} et n est la somme des degrés en x de tous les polynômes qui figurent dans une définition de C, alors il est facile de voir que tout ensemble défini par $C(x, \bar{a})$ pour un $\bar{a} \in K^t$ a au plus n éléments, ou bien son complément a au plus n éléments. Mais si $C(x, \bar{a})$ est fermé, la deuxième alternative est impossible sauf si $C(x, \bar{a})$ est K entier. ■

Lemme 1.1.7 *Si ni $F \subseteq K^s$ ni $F' \subseteq K^t$ sont vides, alors $F \times F'$ est fermé dans K^{s+t} ssi F est fermé dans K^s et F' est fermé dans K^t.*

Démonstration: Si F et F' sont fermés, on obtient les équations définissant $F \times F'$ comme réunion des équations définissant F et F' (c'est-à-dire en prenant l'intersection de $F \times K^t$ et $K^s \times F'$). Réciproquement, si $F \times F'$ est fermé, alors $F(\bar{x}) = (F \times F')(\bar{x}, \bar{a})$ pour tout $\bar{a} \in F'$, donc F est fermé. Par symétrie, F' l'est aussi. ■

On voit donc que la topologie de Zariski sur K^{s+t} raffine bien la topologie produit induite par les topologies de Zariski sur K^s et sur K^t. Mais elle est bien plus fine : les diagonales ne sont pas fermées dans la topologie produit !

1.2 Projection d'un constructible

Dans cette section, nous allons démontrer un théorème important qui a été découvert, indépendamment, en algèbre par Chevalley et en logique par

Tarski. Il nous dit qu'en prenant des projections, nous ne sortons pas de l'univers constructible.

Soit $C(\bar{x}, \bar{y})$ un ensemble dans K^{s+t}. Si π dénote la projection de K^{s+t} à K^s, la projection πC est l'ensemble des $\bar{a} \in K^s$ tel qu'il y a un $\bar{b} \in K^t$ avec $(\bar{a}, \bar{b}) \in C$. C'est pour ça qu'on la note aussi $\exists \bar{y}\, C(\bar{x}, \bar{y})$, avec l'avantage que la notation specifie les variables projectées. Il est évident que la projecton par rapport à plusieurs variables s'écrit comme suite de projections par rapport à une seule : $\exists \bar{y} C(\bar{x}, \bar{y})$ définit le même ensemble que $\exists y_1 \ldots \exists y_t\, C(\bar{x}, \bar{y})$, et aussi que $\exists y_t \ldots \exists y_1\, C(\bar{x}, \bar{y})$.

Lemme 1.2.1 *1. La projection d'un ouvert est ouvert.*

2. Si $F(\bar{x}, y)$ est un fermé contenu dans la diagonale $x_s = y$, alors la projection $\exists y\, F(\bar{x}, y)$ est fermé.

Démonstration: Comme la projection d'une réunion est la réunion des projections (mais attention : la projection d'une intersection n'est pas nécessairement l'intersection des projections), il suffit de traiter le cas d'un ouvert principal, défini par une inéquation $g(\bar{x}, y) \neq 0$. Si $g(\bar{x}, y) = \sum_{i<n} g_i(\bar{x}) y^i$, cette projection équivaut l'ouvert défini par $\bigvee_{i<n} g_i(\bar{x}) \neq 0$, car dans un corps infini un polynôme non-nul n'est pas anullé par tous les éléments.

Pour la deuxième partie, il suffit de reécrire les équations en substituant x_n pour y. ■

Proposition 1.2.2 *Si $C \subseteq K^s$ est constructible, il existe un fermé $F(\bar{x}, y)$ de K^{s+1} tel que $C(\bar{x})$ est égal à $\exists y\, F(\bar{x}, y)$; en plus, la projection est une bijection entre $F(\bar{x}, y)$ et $C(\bar{x})$.*

Démonstration: Tout constructible C s'exprime comme une réunion disjointe $\bigcup_{i<n} (F_i \cap O_i)$, ou F_i est fermé et O_i est un ouvert principal défini par une inégalité $g_i(\bar{x}) \neq 0$. Si F_i' dénote le fermé donné par $g_i(\bar{x}) y - 1 = 0$, alors C est la projection du ferme défini par la réunion $\bigcup_{i<n} ((F_i \times K) \cap F_i')$; les composantes de cette réunion étant aussi deux-à-deux disjointes, la projection nous donne bien une bijection. ■

Pour la preuve du théorème principal, nous utiliserons le lemme suivant :

Lemme 1.2.3 *Tout constructible peut s'exprimer comme réunion finie de constructibles, chacun défini par un systeme d'équations et d'inequations polynomiales dont au plus une seule mentionne la dernière variable.*

Démonstration: Considerons d'abord un système de deux équations $f(\bar{x}, y) = 0 \wedge g(\bar{x}, y) = 0$. En developpant par rapport à y on obtient

$$\sum_{i \leq m} f_i(\bar{x}) y^i = 0 \wedge \sum_{j \leq n} g_j(\bar{x}) y^j = 0;$$

où ni f_m ni g_n sont identiquement nuls. Si $m \geq n$, considérons le polynôme

$$r(\bar{x}, y) = g_n(\bar{x}) f(\bar{x}, y) - y^{m-n} f_m(\bar{x}) g(\bar{x}, y),$$

un polynôme de degré en y inférieur à m. Je tiens que $f(\bar{x}, y) = 0 \wedge g(\bar{x}, y) = 0$ est équivalent à

$$[r(\bar{x}, y) = 0 \wedge g(\bar{x}, y) = 0 \wedge g_n(\bar{x}) \neq 0] \vee [f(\bar{x}, y) = 0 \wedge \sum_{j < n} g_j(\bar{x}) y^j = 0 \wedge g_n(\bar{x}) = 0].$$

En effet, on voit facilement que tout $(\bar{a}, b)$ qui satisfait $f(\bar{a}, b) = g(\bar{a}, b) = 0$ aussi satisfait la disjonction. Pour le converse, si $(\bar{a}, b)$ satisfait la disjonction, soit $g_n(\bar{a}) = 0$ et on a aussi $f(\bar{a}, b) = g(\bar{a}, b) = 0$, soit $g_n(\bar{a}) \neq 0$ et le fait que $r(\bar{a}, b) = g(\bar{a}, b) = 0$ implique que $f(\bar{a}, b) = 0$. On note que la somme des degrés en y des polynômes dans chaque conjonction est inférieure à $m + n$, c'est-à-dire inférieure a la somme des degrés en y de f et de g.

En itérant ce procédé, on voit par récurrence (sur le maximum des sommes des degrés en y de tous les polynômes dans une conjonction qui contient au moins deux polynômes qui font intervenir y) que tout fermé $F(\bar{x}, y)$ s'exprime comme réunion disjointe de constructibles de la forme $C_i(\bar{x}) \cap F_i(\bar{x}, y)$, où F_i est un fermé principal.

Pour traiter le cas général, il suffit de considerer une intersection d'un fermé avec un ouvert principal, car tout constructible est une réunion finie de tels ensembles. Par le raisonnement précédent, on peut l'écrire comme $C(\bar{x}) \cap F(\bar{x}, y) \cap O(\bar{x}, y)$, où C est constructible, F est fermé principal, et O est ouvert principal. Soit F défini par un équation $f(\bar{x}, y) = \sum_{i \leq m} f_i(\bar{x}) y^i = 0$ et O par une inéquation $g(\bar{x}, y) = \sum_{j \leq n} g_j(\bar{x}) y^j \neq 0$.

Si $n \geq m$, on considère $r(\bar{x}, y) = f_m(\bar{x}) g(\bar{x}, y) - y^{n-m} g_n(\bar{x}) f(\bar{x}, y)$ de degré en y inférieur à n ; on voit comme précédemment que $f(\bar{x}, y) = 0 \wedge g(\bar{x}, y) \neq 0$ équivaut à

$$\begin{aligned} &[f_m(\bar{x}) \neq 0 \ \wedge \ f(\bar{x}, y) = 0 \wedge r(\bar{x}, y) \neq 0] \\ &\qquad \vee \ [f_m(\bar{x}) = 0 \wedge \sum_{i < m} f_i(\bar{x}) y^i = 0 \wedge g(\bar{x}, y) \neq 0]; \end{aligned}$$

la somme des degrés en y des polynômes dans chaque conjonction étant inférieure à $m+n$, on peut raisonner par récurrence.

Si $m > n$, on regarde l'algorithme d'élimination pour la conjonction $f(\bar{x},y)=0 \wedge g(\bar{x},y)=0$. Comme avant, on peut mettre

$$r_1(\bar{x},y) = g_n(\bar{x})f(\bar{x},y) - f_m(\bar{x})y^{m-n}g(\bar{x},y);$$

si le degré m_1 en y de r_1 est inférieur à celui de g, on s'arrète. Sinon, on a

$$r_2(\bar{x},y) = g_n(\bar{x})r_1(\bar{x},y) - r^1(\bar{x})y^{m_1-n}g(\bar{x},y),$$

où $r^1(\bar{x})$ est le coefficient de y^{m_1} dans $r_1(\bar{x},y)$. On repete $k \leq \deg_y(f) - \deg_y(g)$ fois ; à la fin on obtient

$$\begin{aligned} g_n(\bar{x})^k f(\bar{x},y) &= g_n(\bar{x})^{k-1}[f_m(\bar{x})y^{m-n}g(\bar{x},y) + r_1(\bar{x},y)] \\ &= g_n(\bar{x})^{k-1}f_m(\bar{x})y^{m-n}g(\bar{x},y) + g_n(\bar{x})^{k-2}[r^1(\bar{x})y^{m_1-n}g(\bar{x},y) + r_2(\bar{x},y)] \\ &\vdots \\ &= p(\bar{x},y)g(\bar{x},y) + r_k(\bar{x},y), \end{aligned}$$

où le degré en y de p est inférieur à m et celui de r_k est inférieur à n. Si pour un certain $\bar{x}$ un coefficient $r_{k,j}(\bar{x})$ de y^j dans $r_k(\bar{x},y)$ n'est pas nul (avec j maximal possible), on repète en divisant $r_{k,j}(\bar{x})g(\bar{x},y)$ par $r_k(\bar{x},y)$. En conclusion, si on met $C_0(\bar{x}) = \bigwedge_j r_{k,j}(\bar{x}) = 0$ et $h_0(\bar{x},y) = g(\bar{x},y)$, on voit que $f(\bar{x},y)=0 \wedge g(\bar{x},y)=0 \wedge g_n(\bar{x}) \neq 0$ peut s'exprimer sous la forme

$$g_n(\bar{x}) \neq 0 \wedge \bigvee_i [C_i(\bar{x}) \wedge h_i(\bar{x},y)=0],$$

où les $C_i(\bar{x})$ sont constructibles et deux-à-deux disjoints, et le degré en y de chaque polynôme h_i est inférieur à n pour tout $i>0$. En plus, les $C_i(\bar{x})$ recouvrent K^s, car à chaque étape en divise en deux, dépendant si $h(\bar{x})=0$ ou non pour un certain polynôme $h(\bar{x})$. Or, $g_n(\bar{x}) \neq 0 \wedge \neg[f(\bar{x},y)=0 \wedge g(\bar{x},y)=0]$ est équivalent à

$$g_n(\bar{x}) \neq 0 \wedge \bigvee_i [C_i(\bar{x}) \wedge h_i(\bar{x},y) \neq 0].$$

Donc $f(\bar{x},y)=0 \wedge g(\bar{x},y) \neq 0$ équivaut à

$$\begin{aligned} &[f(\bar{x},y)=0 \wedge g_n(\bar{x})=0 \wedge \sum_{j<n} g_j(\bar{x})y^j \neq 0] \\ &\qquad \vee [f(\bar{x},y)=0 \wedge g_n(\bar{x}) \neq 0 \wedge \neg(f(\bar{x},y)=0 \wedge g(\bar{x},y)=0)]; \end{aligned}$$

la deuxième conjonction s'exprime aussi comme

$$\bigvee_i [f(\bar{x}, y) = 0 \wedge g_n(\bar{x}) \neq 0 \wedge C_i(\bar{x}) \wedge h_i(\bar{x}, y) \neq 0].$$

Le seul cas où la somme des degrés en y de f et de h_i n'est pas inférieur à $m + n$ est le cas $i = 0$. Mais

$$C_0(\bar{x}) \wedge g_n(\bar{x}) \neq 0 \wedge f(\bar{x}, y) = 0 \wedge g(\bar{x}, y) \neq 0$$

est équivalent à

$$C_0(\bar{x}) \wedge g_n(\bar{x}) \neq 0 \wedge p(\bar{x}, y) = 0 \wedge g(\bar{x}, y) \neq 0,$$

et la somme des degrés en y de p et de g est inférieur à $m + n$.

Par récurrence sur ce degré, le lemme est démontré. ∎

Voici le théorème principal :

Théorème 1.2.4 *Soit K un corps algébriquement clos. Alors la projection d'un constructible est constructible.*

Démonstration: Par le lemme précédent, et car la projection d'une réunion est la réunion des projections, il suffit de considerer un système de la forme $C(\bar{x}) \wedge f(\bar{x}, y) = 0$ ou $C(\bar{x}) \wedge f(\bar{x}, y) \neq 0$. Si $f(\bar{x}, y) = \sum_{i<n} f_i(\bar{x}) y^i$, la projection du premier cas s'exprime comme

$$C(\bar{x}) \wedge [\bigvee_{0<i<n} f_i(\bar{x}) \neq 0 \vee f_0(\bar{x}) = 0$$

car tout polynôme non-nul a une racine dans un corps algébriquement clos. Dans le second cas, la projection s'écrit

$$C(\bar{x}) \wedge \bigvee_{i<n} f_i(\bar{x}) \neq 0. \quad \blacksquare$$

Pour terminer cette section, on note que si $C(\bar{x}, \bar{y}, \bar{z})$ est un constructible avec une projection constructible $\exists \bar{z} C(\bar{x}, \bar{y}, \bar{z})$, alors on peut substituer $\bar{a}$ pour $\bar{y}$ et ensuite projeter le constructible $C(\bar{x}, \bar{a}, \bar{z})$, ou bien projeter C et ensuite substituer : on obtient le même constructible $\exists \bar{z}\, C(\bar{x}, \bar{a}, \bar{z})$. Donc, les projections d'une famille uniforme donnent une famille uniforme.

Chapitre 2

Logique

2.1 La terminologie

Cette section est plein de définitions de base ; elles sont assez naturelles et je les ai rassemblées ici pour faciliter la référence. J'ai aussi tenté de les illustrer en disant ce que ça signifie dans les cas qui nous interessent en particulier, c'est-à-dire les anneaux et les corps.

D'abord quelques mots sur la notation : je dénoterai par ω l'ensemble des entiers non-négatifs ; plus généralement α, β etc. seront des ordinaux. La somme $\alpha + \beta$ de deux ordinaux est l'ordinal correspondant à l'ordre de la concatenation $\alpha\hat{\ }\beta$; leur produit $\alpha\beta$ est l'ordinal correspondant à des copies de α arrangées en type de β (donc $2 \cdot \omega = \omega$, mais $\omega \cdot 2 = \omega + \omega$). L'exponentiation ordinale est défini récursivement par $\alpha^0 = 1$, $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$ et $\alpha^\delta = \bigcup_{\beta<\delta} \alpha^\beta$ pour ordinal limite δ. (Alors $2^\omega = \lim_{n<\omega} 2^n = \omega$.)

Les cardinaux seront appelés $\kappa, \lambda, \ldots$; un cardinal est identifié avec le plus petit ordinal de sa cardinalité. Le cardinal successeur de κ sera κ^+, qui est bien différent du successeur ordinal $\kappa + 1$, lui aussi de cardinal κ (pour κ infini). Rappelons que la somme et le produit de deux cardinaux infinis est égal à leur maximum, mais la puissance λ^κ est de cardinal strictement supérieur à λ (théorème de Cantor).

Définition 2.1.1 Un *language* $\mathcal{L}$ est l'union (disjointe) d'un ensemble $\mathcal{F}$ de symboles de fonctions, d'un ensemble $\mathcal{R}$ de symboles de relations, et d'un ensemble $\mathcal{C}$ de symboles de constantes. A chaque $f \in \mathcal{F}$ et chaque $R \in \mathcal{R}$ on associe un entier, l'*arité*, qui indique le nombre d'arguments.

En plus, on aura les variables, qui seront notés $x, y, z, \ldots, x_0, x_1, x_2, \ldots$.

Exemple 2.1.2 Le language naturel $\mathcal{L}_R$ pour la théorie des anneaux consiste de trois fonctions binaires (d'arité deux) $+$, $-$ et $*$, une relation binaire $=$, et deux constantes 0 et 1.

Définition 2.1.3 Soit $\mathcal{L}$ un language. La collection des $\mathcal{L}$-*termes* est défini récursivement par :
- toute constante et toute variable est un $\mathcal{L}$-terme.
- si $f \in \mathcal{F}$ est une fonction n-aire et $t_1, \dots, t_n$ sont des $\mathcal{L}$-termes, alors $f(t_1, \dots, t_n)$ est un $\mathcal{L}$-terme.

Une $\mathcal{L}$-*formule atomique* est une expression de la forme $R(t_1, \dots, t_n)$, où $R \in \mathcal{R}$ est une relation n-aire et $t_1, \dots, t_n$ sont des $\mathcal{L}$-termes. La collection des $\mathcal{L}$-*formules* est défini récursivement par :
- une $\mathcal{L}$-formule atomique est une $\mathcal{L}$-formule.
- si φ et ψ sont des $\mathcal{L}$-formules, leurs *combinaisons booleennes* $\varphi \wedge \psi$ (*conjonction, et*), $\varphi \vee \psi$ (*disjonction, ou*) et $\neg\varphi$ (*négation, non*) sont des $\mathcal{L}$-formules.
- si φ est une $\mathcal{L}$-formule et x est une variable, les *quantifications* $\forall x\varphi$ (*universelle, quel que soit*) et $\exists x\varphi$ (*existentielle, il y a*) sont des $\mathcal{L}$-formules. Les occurrences de la variable x dans ces formules sont *liées* à ce quanteur $\forall$ ou $\exists$ (sauf si elles sont déjà liées à un quanteur dans φ). Une variable qui n'est pas liée est *libre*.

Un *énoncé*, ou une *formule close*, est une formule sans variable libre ; une formule *positive* est une formule sans négation.

Exemple 2.1.4 Les termes de $\mathcal{L}_R$ sont les polynômes sur $\mathbb{Z}$ (où n est une abbreviation pour $1+\cdots+1$, somme de n fois 1, et x^n dénote $x*\cdots*x$, produit de n fois x). Les $\mathcal{L}_R$-formules atomiques sont les équations polynomiales.

Définition 2.1.5 Soit $\mathcal{L}$ un language. Une $\mathcal{L}$-structure $\mathfrak{M}$ est un ensemble M, la *domaine* de $\mathfrak{M}$ (souvent confondue avec $\mathfrak{M}$), et
- pour chaque symbole $f \in \mathcal{F}$ d'arité n une fonction $f^{\mathfrak{M}} : M^n \to M$.
- pour chaque symbole $R \in \mathcal{R}$ d'arité n un sous-ensemble $R^{\mathfrak{M}}$ de M^n.
- pour chaque symbole $c \in \mathcal{C}$ un élément $c^{\mathfrak{M}} \in M$.

Définition 2.1.6 Soit $\mathcal{L}$ une language, et $\mathfrak{M}$ une $\mathcal{L}$-structure. Si $\bar{m}$ est un uple d'éléments de M et $\bar{x}$ est un uple de variables (de la même longueur) dans un terme $t(\bar{x})$, on peut substituer $\bar{m}$ pour toutes les occurences de $\bar{x}$ dans t et obtenir un terme $t(\bar{m})$, un terme à *paramètres* $\bar{m}$. Nous allons définir l'*interpretation* $t^{\mathfrak{M}}$ d'un terme t à paramètres dans $\mathfrak{M}$ récursivement par :

– l'interpretation d'une constante c est $c^{\mathfrak{M}}$; l'interpretation d'un paramètre m est m.
– si $f \in \mathcal{F}$ est une fonction n-aire et $t_1, \ldots, t_n$ sont des termes à paramètres, alors $f(t_1, \ldots, t_n)^{\mathfrak{M}} = f^{\mathfrak{M}}(t_1^{\mathfrak{M}}, \ldots, t_n^{\mathfrak{M}})$.

De même, pour une formule $\varphi(\bar{x})$, on peut substituer $\bar{m}$ pour toutes les occurences libres de $\bar{x}$ dans φ et obtenir une formule $\varphi(\bar{m})$ à paramètres. Nous allons définir la *satisfaction* d'une formule à paramètres dans $\mathfrak{M}$ récursivement par :

– si $\varphi(\bar{m}) = R(t_1(\bar{m}), \ldots, t_n(\bar{m}))$ est une formule atomique, où $R \in \mathcal{R}$ est une relation n-aire et $t_1, \ldots, t_n$ sont des termes, alors $\varphi(\bar{m})$ est satisfaite dans $\mathfrak{M}$ si $(t_1(\bar{m})^{\mathfrak{M}}, \ldots, t_n(\bar{m})^{\mathfrak{M}}) \in R^{\mathfrak{M}}$.
– si $\varphi = \varphi_1 \wedge \varphi_2$, alors φ est satisfaite dans $\mathfrak{M}$ si φ_1 et φ_2 sont satisfaites dans $\mathfrak{M}$.
– si $\varphi = \varphi_1 \vee \varphi_2$, alors φ est satisfaite dans $\mathfrak{M}$ si φ_1 ou φ_2 (ou bien les deux) est satisfaite dans $\mathfrak{M}$.
– si $\varphi = \neg\psi$, alors φ est satisfaite dans $\mathfrak{M}$ si ψ n'est pas satisfaite dans $\mathfrak{M}$.
– si $\varphi = \forall x \psi(x)$, alors φ est satisfaite dans $\mathfrak{M}$ si pour tout $m \in M$ la formule $\psi(m)$ est satisfaite dans $\mathfrak{M}$.
– si $\varphi = \exists x \psi(x)$, alors φ est satisfaite dans $\mathfrak{M}$ s'il y a un $m \in M$ tel que $\psi(m)$ est satisfaite dans $\mathfrak{M}$.

Si φ est satisfaite dans $\mathfrak{M}$, on le dénote par $\mathfrak{M} \models \varphi$.

On peut aussi voir les choses de l'autre coté : si $\mathfrak{M} \models \varphi(\bar{m})$, on dit également que $\bar{m}$ satisfait $\varphi(\bar{x})$ dans $\mathfrak{M}$, et on écrit $\bar{m} \models_{\mathfrak{M}} \varphi(\bar{x})$.

Exemple 2.1.7 Un anneau est un exemple naturel d'une $\mathcal{L}_R$-structure (mais on pourrait aussi interpreter les symboles de $\mathcal{L}_R$ par autre chose). Souvent on confond f et $f^{\mathfrak{M}}$, R et $R^{\mathfrak{M}}$, et c et $c^{\mathfrak{M}}$. Donc, dans un anneau R, on parlera de $+$, $-$, $*$, et pas de $+^R$, $-^R$, $*^R$. L'égalité $=$ est dans la plupart des languages, et sera toujour interpreté par la vrai égalité.

Si Φ est un ensemble d'énoncés et $\mathfrak{M}$ une $\mathcal{L}$-structure, on écrit $\mathfrak{M} \models \Phi$ si $\mathfrak{M} \models \varphi$ pour tout $\varphi \in \Phi$; on dit que $\mathfrak{M}$ satisfait Φ, ou bien que $\mathfrak{M}$ est un *modèle* de Φ.

Définition 2.1.8 Deux formules $\varphi(\bar{x})$ et $\psi(\bar{x})$ sont *équivalentes* si pour toute $\mathcal{L}$-structure $\mathfrak{M}$ et pour tout $\bar{m} \in M$ on a $\mathfrak{M} \models \varphi(\bar{m})$ si et seulement si $\mathfrak{M} \models \psi(\bar{m})$.

Exemple 2.1.9 Il est facile de vérifier que pour tout φ et ψ les formules suivantes sont équivalentes :

- φ et $\neg\neg\varphi$.
- $\neg(\varphi \wedge \psi)$ et $\neg\varphi \vee \neg\psi$.
- $\neg(\varphi \vee \psi)$ et $\neg\varphi \wedge \neg\psi$.
- $\forall x \neg\varphi$ et $\neg\exists x\varphi$.
- $\exists x \neg\varphi$ et $\neg\forall x\varphi$.

En particulier, on peut remplacer une formule quelconque par une formule équivalente qui ne contient ni $\vee$ ni $\forall$.

Démonstration: Par exemple, pour tout $\mathcal{L}$-structure $\mathfrak{M}$ et tout $\bar{m}$ dans $\mathfrak{M}$ on a

$$\begin{aligned} \mathfrak{M} \models \neg\neg\varphi(\bar{m}) &\Leftrightarrow \mathfrak{M} \not\models \neg\varphi(\bar{m}) \\ &\Leftrightarrow \text{ il n'est pas vrai que } \mathfrak{M} \models ! \neg\varphi(\bar{m}) \\ &\Leftrightarrow \text{ il n'est pas vrai que } \mathfrak{M} \not\models \varphi(\bar{m}) \\ &\Leftrightarrow \mathfrak{M} \models \varphi(\bar{m}). \quad \blacksquare \end{aligned}$$

Nous utiliserons aussi les abbreviations suivantes : $\varphi \to \psi$ pour $\neg\varphi \vee \psi$, et $\varphi \leftrightarrow \psi$ pour $(\varphi \to \psi) \wedge (\psi \to \varphi)$. On doit faire attention : ces connectifs cachent des négations, et sont interdits dans les formules positives.

Exercice 2.1.10 Deux formules $\varphi(\bar{x})$ et $\psi(\bar{x})$ sont équivalentes si et seulement si $\forall\bar{x}\ \varphi(\bar{x}) \leftrightarrow \psi(\bar{x})$ est vrai dans toute $\mathcal{L}$-structure.

Définition 2.1.11 Une *théorie* T est un ensemble d'énoncés consistant (qui a un modèle) ; elle est *complète* si pour chaque énoncé φ soit tout modèle de T satisfait φ, soit tout modèle satisfait $\neg\varphi$.

Si $\mathfrak{M}$ est une $\mathcal{L}$-structure et A un ensemble d'éléments dans M, le $\mathcal{L}(A)$-*théorie de* $\mathfrak{M}$, noté $\mathrm{Th}(\mathfrak{M}, A)$, est l'ensemble de tous les énoncés à paramètres dans A qui sont satisfaits par $\mathfrak{M}$. Il est évident que c'est une théorie complète.

Nous verrons plus tard que sauf si $\mathfrak{M}$ est fini, il est impossible qu'une théorie caractérise un modèle à isomorphisme près. Donc, on définit :

Définition 2.1.12 Deux $\mathcal{L}$-structures $\mathfrak{M}$ et $\mathfrak{N}$ sont élémentairement équivalentes si elles satisfont les mêmes énoncés.

Exemple 2.1.13 La théorie des corps algébriquement clos de caractéristique p fixe est une théorie complète ; elle est donnée par les énoncés suivants :

1. l'additon est un groupe abélien, avec $-$ comme inverse et 0 comme élément neutre.
2. la multiplication est un groupe abélien sur tous les éléments sauf 0, avec 1 comme élément neutre.
3. la loi distributive.
4. soit $p = 0$, en caractéristique $p > 0$, soit $n \neq 0$ pour tout $n \in \omega$, en caractéristique 0.
5. $\forall x_0 \ldots \forall x_n \exists y \sum_{i \leq n} x_i y^i = 0$, pour tout $n \in \omega$.

On notera que les axiomes 1, 2 et 3 s'expriment par un seul énoncé, qui axiomatise le théorie des corps. Si on ajoute 4, on obtien la théorie des corps de caractéristique p, qui est axiomatisable par un seul axiome si et seulement si $p > 0$. Les axiomes 1, 2, 3 et 5 forment la théorie ACF des corps algébriquement clos ; 5 ne s'exprime pas par un nombre fini d'énoncés. Finalement, 1–5 donnent la théorie ACF_p des corps algébriquement clos de caractéristique p.

Nous verrons plus tard que tous les corps algébriquement clos de même caractéristique sont élémentairement équivalents, et ACF_p est une théorie complète. En plus, un modèle de ACF_p est déterminé à isomorphisme près par une seule invariante, le degré de transcendance.

2.2 La compacité

Nous allons construire ici, à partir d'une famille $\{\mathfrak{M}_i : i \in I\}$ de $\mathcal{L}$-structures, une $\mathcal{L}$-structure qui est une sorte de limite, ou moyenne, des structures dans la famille.

Définition 2.2.1 Soit I un ensemble quelconque. Un ensemble $\mathcal{U}$ de sous-ensembles de I est un *filtre* sur I si
- $\emptyset \notin \mathcal{U}$.
- si $X \in \mathcal{U}$ et $Y \in \mathcal{U}$, alors $X \cap Y \in \mathcal{U}$.
- si $X \in \mathcal{U}$ et $X \subseteq Y \subseteq I$, alors $Y \in \mathcal{U}$.

Un filtre $\mathcal{U}$ est un *ultrafiltre* si pour chaque $X \subseteq I$ soit $X \in \mathcal{U}$, soit $I - X \in \mathcal{U}$.

Pour tout $i \in I$ il y a l'ultrafiltre *principal* sur i, qui est l'ensemble $\{X \subseteq I : i \in X\}$. Par contre, l'existence des ultrafiltres non-principaux est plus délicat.

Lemme 2.2.2 *Tout filtre sur I est contenu dans un ultrafiltre.*

Démonstration: On voit facilement que la réunion d'une chaîne croissante de filtres sur I est toujours un filtre sur I ; c'est une propriété *inductive*. Or, le lemme de Zorn (oui, nous supposerons l'axiome du choix) nous assure que tout filtre est contenu dans un filtre maximal. Vérifions qu'un filtre maximal est un ultrafiltre.

Soit donc $\mathcal{U}$ un filtre maximal, et $X \notin \mathcal{U}$ un sous-ensemble de I. On pose $\mathcal{U}' = \{Y \subseteq I : \exists F \in \mathcal{U}\ F - X \subseteq Y\}$. C'est un ensemble clos par intersection (car $\mathcal{U}$ l'est) et agrandissement; si $\emptyset \in \mathcal{U}'$, on aurait $F - X = \emptyset$ pour un $F \in \mathcal{U}$, d'où $F \subseteq X$ et $X \in \mathcal{U}$, contradiction. Donc $\mathcal{U}'$ est un filtre qui étend $\mathcal{U}$ et contient $I - X$; par maximalité $I - X \in \mathcal{U}$. ■

Définition 2.2.3 Soit $\{\mathfrak{M}_i : i \in I\}$ une famille de $\mathcal{L}$-structures, et $\mathcal{U}$ un filtre sur I. Le *produit réduit* $\prod_I \mathfrak{M}_i/\mathcal{U}$ est la structure $\mathfrak{M}$ suivante :

– la domaine de $\mathfrak{M}$ est le produit $\times_I M_i$, modulo la relation $\sim$ d'équivalence suivante :

$$(m_i : i \in I) \sim (n_i : i \in I) \Leftrightarrow \{i \in I : m_i = n_i\} \in \mathcal{U}.$$

On dénotera la classe de $(x_i : i \in I)$ modulo $\sim$ par $[x_i : i \in I]$.

– pour tout $c \in \mathcal{C}$ on pose $c^{\mathfrak{M}} = [c^{\mathfrak{M}_i} : i \in I]$.

– pour tout $f \in \mathcal{F}$ d'arité n on pose

$$f^{\mathfrak{M}} : ([m_i^1 : i \in I], \dots, [m_i^n : i \in I]) \mapsto [f^{\mathfrak{M}_i}(m_i^1, \dots, m_i^n) : i \in I].$$

– pour tout $R \in \mathcal{R}$ d'arité n on pose

$$R^{\mathfrak{M}} = \{([m_i^1 : i \in I], \dots, [m_i^n : i \in I]) \in \mathfrak{M}^n : \{i \in I : (m_i^1, \dots, m_i^n) \in R^{\mathfrak{M}_i}\} \in \mathcal{U}\}.$$

Il nous faut vérifier que c'est une bonne définition, qui définit vraiment une $\mathcal{L}$-structure.

D'abord, supposons que $(m_i : i \in I) \sim (n_i : i \in I)$ et $(n_i : i \in I) \sim (k_i : i \in I)$. Alors

$$\{i \in I : m_i = k_i\} \supseteq \{i \in I : m_i = n_i\} \cap \{i \in I : n_i = k_i\} \in \mathcal{U},$$

parce que $\mathcal{U}$ est clos par intersection et agrandissement. Donc $(m_i : i \in I) \sim (k_i : i \in I)$; car reflexivité et symétrie sont évidentes, $\sim$ est bien une relation d'équivalence.

Ensuite, si $[m_i^j : i \in I] = [n_i^j : i \in I]$ pour $j = 1, 2, \ldots, n$, alors par clôture de $\mathcal{U}$ par intersections finies,

$$J = \{i \in I : m_i^j = n_i^j \text{ pour tout } j = 1, 2, \ldots, n\} \in \mathcal{U}.$$

Mais si $f \in \mathcal{F}$ est une fonction n-aire, J est contenu dans

$$\{i \in I : f^{\mathfrak{M}_i}(m_i^1, \ldots, m_i^n) = f^{\mathfrak{M}_i}(n_i^1, \ldots, n_i^n)\},$$

et la définition de $f^{\mathfrak{M}}$ ne dépend pas du choix des représentants modulo $\sim$. De même, si $R \in \mathcal{R}$ est une relation n-aire, alors J est contenu dans

$$\{i \in I : (m_i^1, \ldots, m_i^n) \in R^{\mathfrak{M}_i} \Leftrightarrow (n_i^1, \ldots, n_i^n) \in R^{\mathfrak{M}_i}\},$$

et la définition de $R^{\mathfrak{M}}$ ne dépend pas du choix des représentants modulo $\sim$ non plus.

Théorème 2.2.4 Critère de Łos *Soit $\mathcal{U}$ un ultrafiltre sur un ensemble I, et $\{\mathfrak{M}_i : i \in I\}$ une famille de $\mathcal{L}$-structures. Si $\bar{m} = ([m_i^1 : i \in I], \ldots, [m_i^n : i \in I])$ est un n-uple dans le produit réduit $\mathfrak{M} = \prod_I \mathfrak{M}_i/\mathcal{U}$ et $\varphi(\bar{x})$ est une $\mathcal{L}$-formule, alors $\mathfrak{M} \models \varphi(\bar{m})$ si et seulement si*

$$\{i \in I : \mathfrak{M}_i \models \varphi(m_i^1, \ldots, m_i^n)\} \in \mathcal{U}.$$

Démonstration: D'abord, nous démontrons par récurrence sur la longueur d'un terme $t(\bar{x})$ que

$$\{i \in I : \mathfrak{M}_i \models t(m_i^1, \ldots, m_i^n) = n_i\} \in \mathcal{U}$$

si et seulement si $\mathfrak{M} \models t(\bar{m}) = [n_i : i \in I]$.

C'est évident si $t(\bar{x}) = f(\bar{x})$ pour une fonction n-aire $f \in \mathcal{F}$, par définition de $f^{\mathfrak{M}}$. Soient donc $t_1(\bar{x}), \ldots, t_k(\bar{x})$ des termes de longueur inférieur à celle de t, et $f \in \mathcal{F}$ une fonction k-aire, tels que $t(\bar{x}) = f(t_1(\bar{x}), \ldots, t_k(\bar{x}))$. Si $n_i^j = t_j(m_i^1, \ldots, m_i^n)$ pour $j = 1, 2, \ldots, k$, par hypothèse de récurrence $\mathfrak{M} \models [n_i^j : i \in I] = t_j(\bar{m})$, pour tout $j = 1, 2, \ldots, k$. Ensuite

$$\mathfrak{M} \models f([n_i^1 : i \in I], \ldots, [n_i^k : i \in I]) = [n_i : i \in I]$$

si et seulement si $\{i \in I : \mathfrak{M}_i \models f(n_i^1, \ldots, n_i^k) = n_i\} \in \mathcal{U}$ par définition de $f^{\mathfrak{M}}$; le résultat suit par substitution.

Maintenant on peut démontrer le théorème par récurrence sur la longueur de $\varphi(\bar{x})$; pour l'économie de l'effort supposera qu'on a remplacé toutes les formules par des formules équivalentes qui ne contiennent ni $\vee$ ni $\forall$ (et la récursion reste bien dans cette classe).

Si $\varphi(\bar{x}) = R(\bar{x})$ pour un $R \in \mathcal{R}$, la proposition suit de la définition de $R^{\mathfrak{M}}$; si $\varphi(\bar{x}) = R(t_1(\bar{x}), \dots, t_k(\bar{x}))$ est atomique, on utilise le paragraphe précédent. Si $\varphi(\bar{m}) = \neg\psi(\bar{m})$, on a

$$\begin{aligned} \mathfrak{M} \models \varphi(\bar{m}) &\Leftrightarrow \mathfrak{M} \not\models \psi(\bar{m}) \\ &\Leftrightarrow \{i \in I : \mathfrak{M}_i \models \psi(m_i^1, \dots, m_i^n)\} \notin \mathcal{U} \\ &\Leftrightarrow \{i \in I : \mathfrak{M}_i \not\models \psi(m_i^1, \dots, m_i^n)\} \in \mathcal{U} \\ &\Leftrightarrow \{i \in I : \mathfrak{M}_i \models \varphi(m_i^1, \dots, m_i^n)\} \in \mathcal{U}, \end{aligned}$$

car le complément d'un ensemble $J \subseteq I$ est dans $\mathcal{U}$ si et seulement si $J \notin \mathcal{U}$.

Si $\varphi(\bar{x}) = \varphi_1(\bar{x}) \wedge \varphi_2(\bar{x})$, on a pour $j = 1, 2$ que

$$\{i \in I : \mathfrak{M}_i \models \varphi_j(m_i^1, \dots, m_i^n)\} \supseteq \{i \in I : \mathfrak{M}_i \models \varphi(m_i^1, \dots, m_i^n)\}. \qquad (\dagger)$$

Donc si le dernier est dans $\mathcal{U}$, ainsi sont les premiers, et par hypothèse de récurrence $\mathfrak{M} \models \varphi_j(\bar{m})$ pour $j = 1, 2$, d'où $\mathfrak{M} \models \varphi(\bar{m})$. Réciproquement, si $\mathfrak{M}$ satisfait $\varphi(\bar{m})$, il satisfait $\varphi_1(\bar{m})$ et $\varphi_2(\bar{m})$, donc les deux premiers ensembles dans (†) sont dans $\mathcal{U}$, ainsi que leur intersection, qui est le troisième.

Finalement, si $\varphi(\bar{m}) = \exists x\, \psi(x, \bar{m})$, soit $J = \{i \in I : \mathfrak{M}_i \models \varphi(m_i^1, \dots, m_i^n)\}$. Pour chaque $i \in J$ soit $n_i \in \mathfrak{M}_i$ tel que $\mathfrak{M}_i \models \psi(n_i, m_i^1, \dots, m_i^n)$; pour $i \notin J$ on choisit $n_i \in \mathfrak{M}_i$ quelconque. Si $n = [n_i : i \in I]$, alors par hypothèse de récurrence $i \in I$ implique $\mathfrak{M} \models \psi(n, \bar{m})$, d'où $\mathfrak{M} \models \varphi(\bar{m})$. Réciproquement, si $\mathfrak{M} \models \varphi(\bar{x})$, il y a un $n = [n_i : i \in I] \in \mathfrak{M}$ tel que $\mathfrak{M} \models \psi(n, \bar{m})$; par hypothèse de récurrence $\{i \in I : \mathfrak{M}_i \models \psi(n_i, m_i^1, \dots, m_i^n)\} \in \mathcal{U}$, et $\{i \in I : \mathfrak{M}_i \models \varphi(m_i^1, \dots, m_i^n)\} \in \mathcal{U}$. ■

Remarque 2.2.5 On n'a utilisé le fait que $\mathcal{U}$ est un ultrafiltre que pour la négation. Ainsi, un produit réduit modulo un filtre $\mathcal{U}$ satisfait une formule $\varphi(\bar{m})$ sans $\neg$, $\vee$ ou $\forall$ si et seulement si $\{i \in I : \mathfrak{M}_i \models \varphi(m_i^1, \dots, m_i^n)\} \in \mathcal{U}$.

Comme simple corollaire, on obtient un des théorèmes le plus fondamentaux de la théorie des modèles.

Théorème 2.2.6 COMPACITÉ *Soit Σ un ensmble d'énoncés tel que tout sous-ensemble fini de Σ a un modèle. Alors Σ a un modèle.*

Démonstration: Soit I la collection de sous-ensembles finis de Σ, et pour $i \in I$ soit I_i l'ensemble des sous-ensembles finis de Σ qui étendent i. Si $\mathcal{U}_0 = \{X \subseteq I : \text{ il y a } i \in I \text{ tel que } X \supseteq I_i\}$, alors pour $X \supseteq I_i$ et $Y \supseteq I_j$ on a $X \cap Y \supseteq I_{i\cup j} \in \mathcal{U}_0$; en plus $X \supseteq I_i \ni i$, et $\mathcal{U}_0$ est un filtre. Soit $\mathcal{U}$ un ultrafiltre contenant $\mathcal{U}_0$.

Pour $i \in I$ soit $\mathfrak{M}_i$ un modèle de i, et $\mathfrak{M} = \prod_I \mathfrak{M}_i/\mathcal{U}$. Donc pour tout $\sigma \in \Sigma$ on a

$$\{i \in I : \mathfrak{M}_i \models \sigma\} \supseteq I_{\{\sigma\}} \in \mathcal{U}_0 \subseteq \mathcal{U}.$$

Par le théorème de Łos, $\mathfrak{M} \models \sigma$. ■

Le réciproque est bien sûr évident.

Exercice 2.2.7 Démontrer que si tous les $\mathfrak{M}_i$ sont élémentairement équivalents, alors un ultraproduit $\prod_I \mathfrak{M}_i/\mathcal{U}$ est élémentairement équivalent aux $\mathfrak{M}_i$.

Exercice 2.2.8 Démontrer qu'il n'y a pas d'ensemble Σ d'énoncés de $\mathcal{L}_R$ tel que les modèles de Σ sont précisement les corps finis.

2.3 Sous-structures élémentaires

Définition 2.3.1 Soit $\mathfrak{N}$ une $\mathcal{L}$-structure. Une *sous-structure* de $\mathfrak{N}$ est un ensemble M de $\mathfrak{N}$ qui contient toutes les constantes et qui est clos par toutes les fonctions ; les réstrictions à M des relations de $\mathfrak{N}$ y induiseront une $\mathcal{L}$-structure $\mathfrak{M}$.

$\mathfrak{M}$ est une sous-structure *élémentaire* de $\mathfrak{N}$ si pour tout formule $\varphi(\bar{m})$ à paramètres dans $\mathfrak{M}$ on a $\mathfrak{M} \models \varphi(\bar{m})$ si et seulement si $\mathfrak{N} \models \varphi(\bar{m})$. On dénote cette condition par $\mathfrak{M} \prec \mathfrak{N}$.

Un $\mathcal{L}$-morphisme de $\mathcal{L}$-structures est une application qui preserve les constantes, les fonctions, et les relations. Un $\mathcal{L}$-morphisme $\sigma : \mathfrak{M} \to \mathfrak{N}$ est *élémentaire* si pour tout $\bar{m} \in \mathfrak{M}$ on a $\mathfrak{M} \models \varphi(\bar{m})$ si et seulement si $\mathfrak{N} \models \varphi(\sigma(\bar{m}))$.

Exercice 2.3.2 Soit $\mathfrak{M}$ une sous-structure de $\mathfrak{N}$. Les trois conditions suivantes sont équivalentes :
- $\mathfrak{M} \prec \mathfrak{N}$.
- $\mathrm{Th}(\mathfrak{M}, M) = \mathrm{Th}(\mathfrak{N}, M)$.
- l'inclusion $\mathfrak{M} \to \mathfrak{N}$ est un $\mathcal{L}$-morphisme élémentaire.

Exercice 2.3.3 Soient $\mathfrak{M} \prec \mathfrak{N} \prec \mathfrak{N}'$ des $\mathcal{L}$-structures. Alors $\mathfrak{M} \prec \mathfrak{N}'$.

Exercice 2.3.4 Soit $(\mathfrak{M}_i : i < \alpha)$ une chaîne élémentaire de $\mathcal{L}$-structures ($\mathfrak{M}_i \prec \mathfrak{M}_j$ pour tout $i < j$). Alors la réunion $\mathfrak{M} = \bigcup_{i<\alpha} \mathfrak{M}_i$ est une $\mathcal{L}$-structure qui satisfait $\mathfrak{M}_i \prec \mathfrak{M}$ pour tout $i < \alpha$.

Exercice 2.3.5 Soit $\mathcal{U}$ un ultrafiltre sur un ensemble I, et $\mathfrak{M}$ une $\mathcal{L}$-structure. Alors on peut considérer l'ultraproduit où tous les $\mathfrak{M}_i$ sont égaux à $\mathfrak{M}$; on l'appèle une *ultrapuissance* de $\mathfrak{M}$, et on le dénote $\prod_I \mathfrak{M}/\mathcal{U}$.

1. Vérifier que l'application diagonale $m \mapsto [m : i \in I]$ est un $\mathcal{L}$-morphisme, l'*inclusion canonique*.
2. Démontrer que l'inclusion canonique est élémentaire.

Maintenant nous allons voir que l'équivalence élémentaire ne peut pas determiner le cardinal d'une $\mathcal{L}$-structure, sauf s'il est fini.

Lemme 2.3.6 *Soit $\mathfrak{M}$ une $\mathcal{L}$-structure infini. Alors il y a $\mathfrak{N} \succ \mathfrak{M}$ arbitrairement large.*

Démonstration: Soit λ un cardinal arbitraire, $\{c_i : i < \lambda\}$ des nouvelles constantes, et
$$\Sigma = \mathrm{Th}(\mathfrak{M}, M) \cup \{c_i \neq c_j : i \neq j\}.$$
Alors chaque sous-ensemble fini de Σ ne mentionne qu'un nombre fini de constantes, qu'on peut réaliser dans $\mathfrak{M}$. Donc Σ est finiment réalisable, et ainsi réalisable par compacité ; soit $\mathfrak{N}$ un modèle de Σ. Evidemment $|\mathfrak{N}| \geq \lambda$. En plus, on a une injection canonique de $\mathfrak{M}$ dans $\mathfrak{N}$, qui envoie un élément $m \in \mathfrak{M}$ à la réalisation $m^{\mathfrak{N}}$ de sa constante dans $\mathfrak{N}$.

Soit maintenant $\varphi(\bar{m}) \in \mathcal{L}(\bar{m})$ pour un $\bar{m} \in \mathfrak{M}$. Alors
$$\mathfrak{M} \models \varphi(\bar{m}) \Leftrightarrow \varphi(\bar{m}) \in \mathrm{Th}(\mathfrak{M}, M) \Leftrightarrow \mathfrak{N} \models \varphi(\bar{m}),$$
donc l'inclusion est élémentaire. ■

Voici un critère utile pour que une sous-structure soit élémentaire :

Proposition 2.3.7 Crtitère de Tarski *Soit $\mathfrak{M}$ une sous-structure de $\mathfrak{N}$. Alors $\mathfrak{M} \prec \mathfrak{N}$ si et seulement si pour tout formule $\varphi(x)$ à paramètres dans $\mathfrak{M}$, si $\mathfrak{N} \models \exists x\, \varphi(x)$, alors il y a $m \in \mathfrak{M}$ tel que $\mathfrak{N} \models \varphi(m)$.*

On notera que ce critère ne mentionne plus la satisfaction dans $\mathfrak{M}$.

DÉMONSTRATION: Nous démontrons par induction sur la longueur d'un énoncé φ à paramètres dans $\mathfrak{M}$ que $\mathfrak{M} \models \varphi$ si et seulement $\mathfrak{N} \models \varphi$. Si φ est atomique, ça suit du fait que $\mathfrak{M}$ est une sous-structure de $\mathfrak{N}$, et donc les interpretations des constantes sont les mêmes, et les fonctions et relations sont les restrictions à $\mathfrak{M}$ des fonctions et relations de $\mathfrak{N}$.

Si φ est une combinaison booléenne, on peut facilement appliquer l'hypothèse de récurrence. Par exemple, si $\varphi = \neg\psi$, alors

$$\mathfrak{M} \models \varphi \Leftrightarrow \mathfrak{M} \not\models \psi \Leftrightarrow \mathfrak{N} \not\models \psi \Leftrightarrow \mathfrak{N} \models \varphi.$$

On notera que ceci démontre aussi que tout sous-structure $\mathfrak{M} \subseteq \mathfrak{N}$ satisfait les mêmes énoncés sans quantificateurs que $\mathfrak{N}$, sans aucun hypothèse sur l'inclusion.

Maintenant, si $\varphi = \exists x\, \psi(x)$ et $\mathfrak{M} \models \varphi(x)$, alors il y a $m \in \mathfrak{M}$ tel que $\mathfrak{M} \models \psi(m)$. Par hypothèse de récurrence $\mathfrak{N} \models \psi(m)$, d'où $\mathfrak{N} \models \varphi$. Réciproquement, si $\mathfrak{N} \models \varphi$, alors par hypothèse il y a $m \in \mathfrak{M}$ tel que $\mathfrak{N} \models \psi(m)$. Par hypothèse de récurrence $\mathfrak{M} \models \psi(m)$, et $\mathfrak{M} \models \varphi$. ■

Corollaire 2.3.8 LÖWENHEIM-SKOLEM *Soit $\mathfrak{N}$ une $\mathcal{L}$-structure infini. Alors pour tout $A \subseteq \mathfrak{N}$ et tout λ infini tel que $|\mathcal{L}| + |A| \leq \lambda \leq |\mathfrak{N}|$, il y a une sous-structure élémentaire $\mathfrak{M} \prec \mathfrak{N}$ contenant A.*

Pour tout $\lambda \geq |\mathcal{L}| + |\mathfrak{N}|$ il a une sur-structure élémentaire $\mathfrak{M}' \succ \mathfrak{N}$ de cardinal λ.

DÉMONSTRATION: Nous définissons une suite ascendante $(A_i : i \in \omega)$ de sous-ensembles de $\mathfrak{N}$, tel que $|A_i| = \lambda$ pour tout $i \in \omega$, et $\bigcup_{i\in\omega} A_i$ est une sous-structure $\mathfrak{M}$ de $\mathfrak{N}$ qui satisfait le critère de Tarski. Alors $\lambda \leq |\mathfrak{M}| \leq \lambda \cdot \omega = \lambda$, et nous aurions trouvé la structure requise.

Soit A_0 un ensemble de cardinal λ qui contient A, et $(\varphi_i(x) : i < \lambda)$ une énumération des formules à paramètres dans A_0 et à une variable libre x. Notons d'abord qu'il n'y en a pas plus que λ, car une telle formule est un mot de longueur fini n dans l'alphabet

$$\mathcal{L} \cup A_0 \cup \{x_i : i \in \omega\} \cup \{\neg, \vee, \wedge, \exists, \forall, (,)\}$$

de cardinal λ, dont il y a au plus

$$\bigcup_{n\in\omega} \lambda^n = \bigcup_{n<\omega} \lambda = \lambda \cdot \omega = \lambda.$$

Pour chaque $i < \lambda$ on choisit un $a_i \in \mathfrak{N}$ tel que $\mathfrak{N} \models \exists x\, \varphi(x)$ implique $\mathfrak{N} \models \varphi(a_i)$, et on met $A_1 = A_0 \cup \{a_i : i \in I\}$. Donc $|\mathfrak{A}_1| = \lambda$; en remplaçant A_0 par A_1 on obtienda A_2, puis A_3, etc. Il est évident de la construction que tout A_i est de cardinal λ, et que $\bigcup_{i\in\omega} A_i$ satisfait le critère de Tarski, car une formule ne peut utiliser que des paramètres dans un des A_i, pour i suffisament grand.

En plus, car les énumerations $(\varphi_i(x) : i < \lambda)$ contiennent toutes les formules $x = c$, où $c \in \mathcal{C}$, et $x = f(\bar{a})$, où $f \in \mathcal{F}$ et $\bar{a} \in A_i$ pour un $i \in \omega$, on voit que $\bigcup_{i\in\omega} A_i$ est en fait une sous-structure de $\mathfrak{N}$.

Pour la deuxième partie, on construira d'abord par compacité une surstructure élémentaire $\mathfrak{N}' \succ \mathfrak{N}$ de cardinal au moins λ, et ensuite une sous-structure élémentaire $\mathfrak{M}' \prec \mathfrak{N}'$ contenant $\mathfrak{N}$ de cardinal λ. Alors $\mathfrak{N} \prec \mathfrak{M}'$. ■

2.4 Elimination des quantificateurs

Définition 2.4.1 Une théorie T *élimine les quantificateurs* si toute formule $\varphi(\bar{x})$ est équivalente à une formule sans quantificateurs.

L'élimination des quantificateurs a une conséquence bien importante.

Définition 2.4.2 Une théorie T est *modèle-complète* si tout inclusion de modèles de T est élémentaire.

Proposition 2.4.3 *Une théorie qui élimine les quantificateurs est modèle-complète.*

Démonstration: Soient $\mathfrak{M}$ et $\mathfrak{N}$ des modèles de T avec $\mathfrak{M} \subseteq \mathfrak{N}$, et $\varphi(\bar{m})$ un énoncé à paramètres dans $\mathfrak{M}$. Alors $\varphi(\bar{x})$ est équivalent dans tout modèle de T à une formule $\psi(\bar{x})$ sans quantificateurs, et

$$\mathfrak{M} \models \varphi(\bar{m}) \Leftrightarrow \mathfrak{M} \models \psi(\bar{m}) \Leftrightarrow \mathfrak{N} \models \psi(\bar{m}) \Leftrightarrow \mathfrak{N} \models \varphi(\bar{m}). \quad ■$$

Dans cette section, nous allons démontrer un critère pour qu'une théorie élimine les quantificateurs, et ensuite vérifier que ce critère est satisfait par la théorie des corps algébriquement clos. Cela nous donnera une deuxième démonstration du fait que la projection d'un constructible est constructible.

Lemme 2.4.4 *Soit T une théorie telle que si $\mathfrak{M}$ et $\mathfrak{N}$ sont des modèles de T, et $\bar{a} \in \mathfrak{M}$ et $\bar{b} \in \mathfrak{N}$ deux uples qui satisfont les mêmes formules atomiques (dans leurs modèles respectifs), alors $\bar{a}$ et $\bar{b}$ satisfont les mêmes formules de la forme $\exists x\, \varphi(x, \bar{y})$, où φ est sans quantificateurs. Alors deux tels uples $\bar{a} \in \mathfrak{M}$ et $\bar{b} \in \mathfrak{N}$ satisfont les mêmes formules.*

Il est nécessaire que l'hypothèse du lemme soit satisfaite pour tous modèles $\mathfrak{M}$, $\mathfrak{N}$ de T, et tous $\bar{a} \in \mathfrak{M}$, $\bar{b} \in \mathfrak{N}$.

Démonstration: On raisonne par récurrence sur la longueur des formules. le cas des combinaisons booléennes étant évidant, il suffit de traîter le cas où $\mathfrak{N} \models \forall x\, \varphi(x, \bar{b})$. Soit donc $a \in \mathfrak{M}$, et mettons

$$\Sigma = \mathrm{Th}(\mathfrak{N}, N) \cup \{\psi(c, \bar{b}) : \psi \text{ atomique tel que } \mathfrak{M} \models \psi(a, \bar{a})\},$$

où c est une nouvelle constante. Pour chaque partie finie $\Sigma_0 \subset \Sigma$ soient $\psi_1(c, \bar{b}), \ldots, \psi_n(c, \bar{b})$ les formules de Σ_0 qui mentionnent c. Alors $\mathfrak{M} \models \exists x \bigwedge_{i=1}^n \psi_i(x, \bar{a})$, donc $\mathfrak{N} \models \exists x \bigwedge_{i=1}^n \psi_i(x, \bar{b})$ par hypothèse du lemme ; on voit qu'on peut choisir une interpretation convenable $c^{\mathfrak{N}}$ de c telle que $\mathfrak{N}$ satisfasse même $\mathrm{Th}(\mathfrak{N}, N) \cup \Sigma_0$. Par compacité, Σ a un modèle $\mathfrak{N}'$, et l'inclusion canonique $\mathfrak{N} \to \mathfrak{N}'$ est élémentaire. Donc $\mathfrak{N}' \models \forall x\, \varphi(x, \bar{b})$; en particulier $\mathfrak{N}' \models \varphi(c, \bar{b})$. Or, $a\hat{\ }\bar{a}$ et $c^{\mathfrak{N}'}\hat{\ }\bar{b}$ satisfont les mêmes formules atomiques ; par hypothèse de récurrence $\mathfrak{M} \models \varphi(a, \bar{a})$. Car $a \in \mathfrak{M}$ était arbitraire, $\mathfrak{M} \models \forall x\, \varphi(x, \bar{a})$. L'autre direction, et le cas d'un quantificateur existentiel, suit par symétrie. ∎

Théorème 2.4.5 *Une théorie T élimine les quantificateurs si et seulement si pour tous modèles $\mathfrak{M}$ et $\mathfrak{N}$ de T deux uples $\bar{a} \in \mathfrak{M}$ et $\bar{b} \in \mathfrak{N}$ qui satisfont les mêmes formules atomiques (dans leurs modèles respectifs) satisfont les mêmes formules de la forme $\exists x\, \varphi(x, \bar{y})$, où φ est sans quantificateurs.*

Démonstration: Si T élimine les quantificateurs, une formule de la forme $\exists x\, \varphi(x, \bar{y})$ est équivalente à une formule $\psi(\bar{y})$ sans quantificateurs. Soit A la sous-structure de $\mathfrak{M}$ engendré par $\bar{a}$ et B la sous-structure de $\mathfrak{N}$ engendré par $\bar{b}$; on voit facilement qu'on peut continuer l'application $\bar{a} \mapsto \bar{b}$ à un isomorphisme entre A et B. Donc

$$\begin{aligned} \mathfrak{M} \models \exists x\, \varphi(x, \bar{a}) \quad &\Leftrightarrow \quad \mathfrak{M} \models \psi(\bar{a}) \Leftrightarrow A \models \psi(\bar{a}) \\ &\Leftrightarrow \quad B \models \psi(\bar{b}) \Leftrightarrow \mathfrak{N} \models \psi(\bar{b}) \Leftrightarrow \mathfrak{N} \models \exists x\, \varphi(x, \bar{b}), \end{aligned}$$

car les sous-structures préservent les formules sans quantificateurs.

Réciproquement, supposons que le critère soit satisfait, et qu'une formule $\varphi(\bar{x})$ n'est pas équivalente modulo T à une formule sans quantificateurs. Soient $\bar{c}, \bar{d}$ des nouvelles variables, et considérons

$$\Sigma := T \cup \{\psi(\bar{c}) \leftrightarrow \psi(\bar{d}) : \psi \text{ atomique}\} \cup \{\varphi(\bar{c}), \neg\varphi(\bar{d})\}.$$

Si Σ est finiment satisfaisable, on peut trouver un modèle $\mathfrak{M}$ de Σ entier, dans lequel $\bar{c}^{\mathfrak{M}}$ et $\bar{d}^{\mathfrak{M}}$ satisfont les mêmes formules atomiques, mais pas les mêmes formules, en contradiction avec le lemme précédent. Donc il y a une partie finie $T_0 \cup \{\psi_i(\bar{c}) \leftrightarrow \psi_i(\bar{d}) : i < n\} \cup \{\varphi(\bar{c}), \neg\varphi(\bar{d})\}$ qui n'a pas de modèle, où $T_0 \subseteq T$. Il suit que dans chaque modèle $\mathfrak{M} \models T$ la formule φ est équivalente à une des 2^{2^n} combinaisons booléennes des $\{\psi_i : i < n\}$.

Si $\mathfrak{M}$ et $\mathfrak{N}$ sont deux modèles de T qui satisfont les mêmes énoncés atomiques, alors par le critère ils satisfont les mêmes énonces ; en particulier φ est équivalente dans $\mathfrak{M}$ à la même combinaison booléenne des ψ_i que dans $\mathfrak{N}$. Par compacité, un nombre fini d'énoncés atomiques vrais dans $\mathfrak{M}$ suffit à impliquer, modulo T, que φ est équivalente à une combinaison booléenne particulière ; soit $\sigma_{\mathfrak{M}}$ leur conjonction.

Car il n'y a que $|\mathcal{L}| + \omega$ énoncés sans paramètres, par compacité il y en a un nombre fini $\sigma_{\mathfrak{M}_1}, \ldots, \sigma_{\mathfrak{M}_k}$ tels que tout modèle en satisfait un ; si $\vartheta_1, \ldots, \vartheta_k$ sont le combinaisons booléennes des $\{\psi_i : i < n\}$ correspondantes, alors $\varphi(\bar{x})$ est équivalent modulo T à $\bigvee_{i<k}[\vartheta_i(\bar{x}) \wedge \sigma_i]$. ■

Corollaire 2.4.6 *La théorie des corps algébriquement clos élimine les quantificateurs.*

Démonstration: Soient K et L deux corps algébriquement clos, et $\bar{a} \in K$ et $\bar{b} \in L$ deux uples qui satisfont les mêmes formules atomiques. Alors $\bar{a}$ et $\bar{b}$ engendrent des sous-corps A et B isomorphes. Considérons une formule $\varphi(x, \bar{y})$ sans quantificateurs ; c'est une disjonction finie de formules de la forme $\bigwedge_i f_i(x, \bar{y}) = 0 \wedge g(x, \bar{y}) \neq 0$, où les f_i et g sont des polynômes à coefficients dans $\mathbb{Z}$.

Si $\bigwedge_i f_i(x, \bar{a}) = 0$ définit un ensemble fini dans $\mathcal{K}$ (possiblement vide), il est contenu dans la clôture algébrique $\tilde{A}$ de A, ainsi que toutes les solutions de $\varphi(x, \bar{a})$. Or, l'isomorphie de A et B implique l'isomorphie de leurs clôtures algébriques ; on voit que $\varphi(x, \bar{a})$ a une solution dans $\tilde{A}$ (c'est-à-dire dans K) si et seulement si $\varphi(x, \bar{b})$ a une solution dans $\tilde{B}$ (c'est-à-dire dans L).

Si $\bigwedge_i f_i(x, \bar{a}) = 0$ définit un ensemble infini dans K (ce sont des équations polynomiales triviales), c'est K entier, et $\varphi(x, \bar{a})$ définit un ensemble co-fini.

La clôture algébrique étant infini, $\varphi(x, \bar{a})$ a une solution dans $\tilde{A}$, et $\varphi(x, \bar{b})$ a une solution dans $\tilde{B}$ par isomorphie, donc dans L.

En tout cas, $K \models \exists x\, \varphi(x, \bar{a})$ si et seulement si $L \models \exists x\, \varphi(x, \bar{b})$. ■

Chapitre 3

Conséquences de l'élimination des quantificateurs dans la théorie des corps algébriquement clos

La modèle-complétude nous donne par un court raisonnement algébrique le fameux théorème des zéros de Hilbert.

Proposition 3.0.7 *Si K est un corps algébriquement clos, alors tout système fini $\varphi(\bar{x})$ d'équations et d'inéquations à coefficients dans K qui a une solution dans un corps L extension de K a déjà une solution dans K lui-même.*

DÉMONSTRATION: Soit $\tilde{L}$ la clôture algébrique de L. Alors $\varphi(\bar{x})$ a une solution dans $\tilde{L}$; car $K \prec \tilde{L}$ par modèle-complétude, $K \models \exists \bar{x}\, \varphi(\bar{x})$. ■

Théorème 3.0.8 NULLSTELLENSATZ *Soit K un corps algébriquement clos, et $f_1(\bar{x}), \ldots, f_m(\bar{x}), g(\bar{x})$ des polynômes sur K. Si tout zéro commun de $f_1, \ldots, f_m$ est aussi un zéro de g, alors il y a k tel que g^k est dans l'idéal engendré par $f_1, \ldots, f_m$.*

DÉMONSTRATION: On met $f_0(\bar{x}, z) = 1 - g(\bar{x})z$, et considère l'idéal I dans $K[\bar{x}, z]$ engendré par $f_0, f_1, \ldots, f_m$.

Supposons que $I < K[\bar{x}, z]$. Alors I est contenu dans un idéal propre maximal M, et $K[\bar{x}, z]/M$ est un corps L. Car M ne peut contenir aucun élément invertible de l'anneau, K s'injecte canoniquement dans L par $a \mapsto a + M$; ceci induit une injection $\sigma : K[\bar{X}, Z] \to L[\bar{X}, Z]$ des anneaux polynômiaux en $\bar{X}Z$.

On voit facilement que les polynômes $f_0(\bar{X}, Z), \ldots, f_m(\bar{X}, Z)$ ont un zéro commun $(x_0 + M, \ldots, x_n + M, z + M)$, car

$$f_i(x_0 + M, \ldots, x_n + M, z + M) = f_i(x_0, \ldots, x_n, z) + M \in M.$$

Donc $f_0, \ldots, f_m$ ont un zéro commun dans K, qui est impossible, car tout zéro commun $\bar{x}_0$ de $f_1, \ldots, f_m$ annule g, d'où $f_0(\bar{x}_0, z) = 1$.

Alors $I = K[\bar{x}, z]$, et il y a des polynômes $p_i(x, z) \in K[\bar{x}, z]$ pour $i \leq m$ tels que $\sum_{i=0}^m p_i f_i = 1$; en mettant $z = 1/g(\bar{x})$ et en multipliant par une large puissance g^d de g, on obtient polynômes $\tilde{p}_i(\bar{x}) = g^d(\bar{x}) p_i(\bar{x}, 1/g(\bar{x})) \in K[\bar{x}]$ tels que

$$g^d(\bar{x}) = \sum_{i=1}^m \tilde{p}_i(\bar{x}) f_i(\bar{x}). \quad \blacksquare$$

Maintenant, nous allons étudier les fonctions définissables (c'est-à-dire constructibles) dans un corps algébriquement clos :

Définition 3.0.9 Soit $\mathfrak{M}$ une $\mathcal{L}$-structure. Une fonction $f : M^m \to M^n$ est *définissable* si son graphe est un sous-ensemble définissable de M^{m+n}.

Définition 3.0.10 Soit K un corps. Une fonction $f : K^n \to K$ est *rationelle par morceaux constructibles* s'il y a une partition de K^n en un nombre fini $C_0, \ldots, C_m$ de parties constructibles, telles que pour chaque $i \leq m$ la restricton de $f(\bar{x})$ à C_i s'exprime comme $f_i(\bar{x})/g_i(\bar{x})$, où f_i et g_i sont des polynômes tels que $g_i(\bar{x})$ ne s'annule pas sur C_i.

Théorème 3.0.11 *Soit K un corps algébriquement clos de caractéristique nulle. Alors toute fonction $f : K^n \to K$ définissable est rationelle par morceaux constructibles.*

Remarque 3.0.12 Si f n'est défini que sur une partie constructible C de K^n, on peut la prolonger à K^n entier en mettant $f(\bar{x}) = 0$ pour tout $\bar{x} \notin C$.

Si $f(\bar{x}) = (f_1(\bar{x}), \ldots, f_k(\bar{x}))$ est une fonction à valeurs vectorielles, le théorème s'applique bien sur aux coordonnées $f_i(\bar{x})$.

DÉMONSTRATION: Si f est défini en utilisant des paramètres $\bar{b}$, et si $\bar{a} \in K^n$, alors $f(\bar{a})$ est fixé par tout automorphisme de K qui fixe $\bar{a}\bar{b}$. Mais l'ensemble des tels éléments est le corps L engendré par $\bar{a}$ et $\bar{b}$: si $c \in L$, évidemment c est fixé par tout automorphisme qui fixe $\bar{a}\bar{b}$; réciproquement, si $c \notin L$ est algébrique sur L, on peut l'envoyer par un automorphisme de la clôture algébrique $\tilde{L}$ de L à n'importe quelle racine de son polynôme minimal (dont il y a pluseronsieurs car en caractéristique nulle c engendre une extension séparable de L), et étendre cet automorphisme à K en fixant une base de transcendence de K sur L ; si c est transcendant sur L, on peut l'envoyer à $c+1$ par un automorphisme de K qui fixe $\tilde{L}$ et les autres éléments d'une base de transcendence de K sur L qui contient c.

Mais tout élément de L s'exprime comme fonction rationelle en $\bar{a}\bar{b}$: pour tout $\bar{a} \in K^n$ il y a une fonction rationelle sans paramètres $f_{\bar{a}}(\bar{x}, \bar{y})$ telle que $f(\bar{a}) = f_{\bar{a}}(\bar{a}, \bar{b})$. Il n'y a qu'un nombre dénombrable de fonctions rationelles sans paramètres, disons $(f_i(\bar{x}, \bar{y}) : i \in \omega)$; pour tout $i \in \omega$ l'ensemble $C_i(\bar{x}) = \{\bar{x} \in K^n : f(\bar{x}) = f_i(\bar{x}, \bar{b})\}$ est constructible. Soient $\bar{c}$ des nouvelles constantes ; on met

$$\Sigma(\bar{c}) = \mathrm{Th}(K, K) \cup \{\neg C_i(\bar{c}) : i \in \omega\}.$$

Si Σ a un modèle K_1, on a l'inclusion canonique $x \mapsto x^{K_1}$ de K dans K_1 ; car $K_1 \models \mathrm{Th}(K, K)$, l'inclusion est élémentaire. Or, dans K_1 il y a un uple $\bar{c}^{K_1}$ tel que $f(\bar{c})$ ne s'exprime pas comme fonction rationelle en $\bar{c}^{\mathcal{K}_1}\bar{b}$; ceci contredit l'argument précédent, qui marche aussi bien dans K_1 que dans K.

Donc il y a une partie finie de $\Sigma(\bar{c})$ qui n'a pas de modèle. Alors il y a $m \in \omega$ et $i_0, \ldots, i_m$ tels que $\mathrm{Th}(K, K)$ implique $\bigvee_{j=0}^{m} C_{i_j}(\bar{c})$; on voit que f est rationelle sur chaque partie de la partition $C_{i_0}, C_{i_1} - C_{i_0}, \ldots, C_{i_m} - \bigcup_{j<m} C_{i_j}$. ■

En caractéristique $p > 0$ il y a une légère complication, c'est que l'application $x \mapsto x^p$ est un endomorphisme, dit le *Frobenius*. En fait, évidemment $(xy)^p = x^p y^p$, mais car un nombre premier p divise tous le coefficients binomiales $\binom{p}{i}$ pour $0 < i < p$, on a aussi $(x+y)^p = x^p + y^p$. En plus, car $x^p - a^p = (x-a)^p$, le Frobenius est clairement injectif, et surjectif car dans un corps algébriquement clos tout élément a une racine $p$me. Donc l'inverse du Frobenius est une fonction définissable qui n'est pas linéaire, même par morceaux.

Définition 3.0.13 Soit K un corps de caractéristique $p > 0$. Une fonction est *pseudo-rationelle* si elle est obtenue en composant une fonction rationelle avec une puissance de l'inverse du Frobenius.

Une fonction $f : K^n \to K$ est *pseudo-rationelle par morceaux constructibles* s'il y a une partition de K^n en un nombre fini de parties constructibles telle que sur chaque partie f coïncide avec une fonction pseudo-rationelle.

Théorème 3.0.14 *Soit K un corps algébriquement clos de caractéristique $p > 0$. Alors toute fonction définissable est pseudo-rationelle par morceaux.*

DÉMONSTRATION: On raisonne comme précédemment, sauf que l'ensemble des éléments de K qui sont fixés par tout automorphisme de K qui fixe $\bar{a}$ et $\bar{b}$ n'est plus le sous-corps L engendré par $\bar{a}\bar{b}$. Ce qu'on doit prendre à sa place, c'est la clôture inséparable L^{insep} de L, obtenue en ajoutant toutes les racines p^m-mes des éléments de L, pour tout $m \in \omega$: car tout élément de L n'a qu'une seule racine p^m-me, c'est un corps fixé par les automorphismes de K qui fixent $\bar{a}\bar{b}$; réciproquement, tout élément de L^{insep} ayant une racine $p$me, L^{insep} est parfait, et tout polynôme non-linéaire irreductible sur L^{insep} a plusieurs racines.

Donc $f(\bar{a})^{p^m}$ est une fonction rationelle de $\bar{a}\bar{b}$ pour un $m \in \omega$ assez large, c'est-à-dire $f(\bar{a})$ est pseudo-rationelle, et on finit comme avant. ∎

Exercice 3.0.15 Démontrer les deux théorèmes précédents directement (sans compacité) en utilisant le lemme principal de l'algorithe d'élimination.

Voici une proposition qui connecte la théorie d'un corps algébriquement clos de caractéristique nulle avec celles des corps de caractéristique $p > 0$:

Proposition 3.0.16
1. *La théorie d'un corps algébriquement clos de caractéristique donné p est complète : tout énoncé φ sans paramètres est soit vrai dans tout corps algébriquement clos de caractéristique p, soit faux dans tout corps algébriquement clos de caractéristique p. Le même est vrai pour les énoncés à paramètres $\bar{a}$, pourvu que les corps contiennent le corps engendré par $\bar{a}$.*
2. *Soit φ un énonce sans paramètres. Alors φ est vrai dans tout corps algébriquement clos de caractéristique nulle si et seulement si φ est vrai dans tout corps algebriquement clos de caractéristique $p > 0$, pour tout p premier sauf un nombre fini.*

DÉMONSTRATION:

1. La première partie suit de la deuxième, car tout corps de caractéristique donné contient le sous-corps engendré par 0 et 1 (le corps premier). Soit donc $\varphi(\bar{a})$ un énoncé à paramètres $\bar{a}$, et K et L deux corps algébriquement clos contenant le corps A engendré par $\bar{a}$. Alors $\bar{a}$ satisfait les mêmes formules sans quantificateurs dans K, dans A et dans L, et donc les mêmes formules ; en particulier $K \models \varphi(\bar{a}) \Leftrightarrow L \models \varphi(\bar{a})$.
2. Soit I un ensemble infini de nombres premiers $p > 0$ tel qu'il y a un corps K_p algébriquement clos de caractéristique p avec $K_p \models \varphi$, et soit $\mathcal{U}$ un ultrafiltre non-principal sur I. On met $K = \prod_I K_p/\mathcal{U}$; car tout K_p satisfait la théorie des corps algébriquement clos, le théorème de Łos nous dit que K aussi est un corps algébriquement clos. En plus, pour tout $n \in \omega$ tout K_p sauf au plus un seul satisfait $n \neq 0$; car $\mathcal{U}$ n'est pas principal, K est de caractéristique nulle. Et le fait que $K_p \models \varphi$ pour tout $p \in I$ implique que $K \models \varphi$.

   Le réciproque suit en regardant la négation de φ. ■

En particulier, tout énoncé est soit vrai dans tous les corps algébriquement clos sauf un nombre fini, soit faux dans tous les corps algébriquement clos sauf un nombre fini.

Corollaire 3.0.17 Principe d'Ax *Si K est un corps algébriquement clos et $C \subseteq K^n$ est constructible, toute application constructible injective de A dans A est surjective.*

Démonstration: Soit K un corps avec une fonction constuctible $f : A \to A$ qui est injective mais pas surjective. Si $\bar{a}$ sont les paramètres utilisés pour définir f et A, ce fait s'exprime par une formule $\varphi(\bar{a})$, et $K \models \exists\bar{x}\,\varphi(\bar{x})$. Donc cet énonce est vrai dans les corps algébriquement clos de toute caractéristique sauf un nombre fini ; en particulier il y a un nombre premier p tel que la clôture algébrique K_p de $\mathbb{F}_p$ satisfait $\exists\bar{x}\,\varphi(\bar{x})$.

Soit $\bar{b} \in K_p$ tel que $K_p \models \varphi(\bar{b})$. Donc il y a un sous-ensemble constructible B de K_p^n et une application constructible $g : B \to B$ qui est injective mais pas surjective, où B et g se définissent à partir de $\bar{b}$ comme A et f se définissent à partir de $\bar{a}$. Il y a une partition constructible de B en un nombre fini de parties constructibles $B_0, \ldots, B_m$ telles que g est équivalent à une fonction pseudo-rationelle g_i sur chaque B_i. Soit C l'ensemble fini des paramètres qui figurent dans la définition des B_i et des g_i, et F un sous-corps fini de K_p qui contient C. Alors les valeurs de g sur $F^n \cap B$ sont des valeurs des fonctions pseudo-rationelles à paramètres dans F, et donc toujours dans $F^n \cap B$: la restriction de g à $F^n \cap B$ est une fonction injective de $F^n \cap B$ dans lui-même. Mais une fonction injective sur une domaine fini est surjective : g atteint tous les points dans $F^n \cap B$, pour tout sous-corps fini F de K_p assez grand. Or, la réunion de ces sous-corps est K_p lui même, g est bien surjective sur B, ce qui contredit nos hypothèses. ■

Chapitre 4

Ensembles fortement minimaux

4.1 La dimension

Dans ce chapitre nous allons introduire une dimension qui dans le cas d'un corps algébriquement clos devient la dimension géometrique.

Définition 4.1.1 Soit $\mathfrak{M}$ une structure. Pour les sous-ensembles A définissables de $\mathfrak{M}^s$ nous allons définir par récurrence la condition "$\dim(A) \geq n$" par

– $\dim(A) \geq 0$ si A n'est pas vide.
– $\dim(A) \geq n+1$ s'il y a une famille infinie $A_0, A_1, \ldots$ de sous-ensembles définissables disjoints de A tel que $\dim(A_i) \geq n$ pour chaque $i \in \omega$.

Nous posons $\dim(A) = n$ si $\dim(A) \geq n$ mais $\dim(A) \not\geq n+1$.

Il est évident que $A \subseteq B$ implique $\dim(A) \leq \dim(B)$. On voit facilement qu'un ensemble définissable est de dimension au moins 1 si et seulement s'il est infini ; il est de dimension au moins 2 s'il contient une famille infinie d'ensembles disjoints infinis, etc.

Lemme 4.1.2 *Si* $\dim(A) \geq n+1$, *alors* $\dim(A) \geq n$.

DÉMONSTRATION: Par récurrence sur n. Pour $n = 0$ on sait que A contient une infinité d'ensembles non-vides, donc A n'est pas vide et $\dim(A) \geq 0$. Supposons donc que $\dim(A) \geq n+2$ et considérons une famille $A_0, A_1, \ldots$ de sous-ensembles définissable disjoints de A avec $\dim(A_i) \geq n+1$ pour tout $i \in \omega$. Par hypothèse de récurrence $\dim(A_i) \geq n$ pour tout $i \in \omega$, doncc $\dim(A) \geq n+1$. ■

Donc la définition de la dimension est raisonnable ; dans la prochaine section on va rencontrer une condition sous laquelle la dimension de tout ensemble définissable est finie. En fait, on peut prolonger la définition et définir une dimension à valeurs ordinales, appellé *rang de Morley*, par la condition "$\dim(A) \geq \delta$ si $\dim(A) \geq^\alpha$ pour tout $\alpha < \delta$", où δ est un ordinal limite.

Lemme 4.1.3 $\dim(A \cup B) = \max\{\dim(A), \dim(B)\}$.

DÉMONSTRATION: $A \cup B$ contient A et B, donc $\dim(A \cup B) \geq \dim(A)$ et $\dim(A \cup B) \geq B$. Pour le réciproque, nous démontrons par récurrence sur n que $\dim(A \cup B) \geq n$ implique $\dim(A) \geq n$ ou $\dim(B) \geq n$. Pour $n = 0$ c'est claire : si $A \cup B$ ets non-vide, soit A, soit B ets non-vide. Soit donc $\dim(A \cup B) \geq n + 1$ et $C_0, C_1, \ldots$ une famille infinie de sous-ensembles définissables disjoints de $A \cup B$ tel que $\dim(C_i) \geq n$ pour chaque i. On pose $I = \{i \in \omega : \dim(A \cap C_i) \geq n\}$ et $J = \{i \in \omega : \dim(B \cap C_i) \geq n\}$; comme $A_i \cup B_i = C_i$, l'hypothèse de récurrence implique que $I \cup J = \omega$. Si I est infini, on obtient une famille infini disjointe de sous-ensembles définissables de A de dimension au moins n, et $\dim(A) \geq n+1$, sinon $\dim(B) \geq n+1$. ■

Alors la dimension d'une réunion finie $\bigcup_{i=1}^n A_i$ est le maximum des $\dim(A_i)$.

Proposition 4.1.4 $\dim(A) \geq n + 1$ *si pour tout* $k \in \omega$ *il y a une famille* $A_0, \ldots, A_k$ *de sous-ensembles définissables disjoints de* A *avec* $\dim(A_i) \geq n$ *pour tout* $i \geq k$*.*

Remarquons que le réciproque est évident.

DÉMONSTRATION: Supposons que nous avons trouvé une partition de A en un nombre fini d'ensembles $X_0, \ldots, X_k$ d'ensembles de dimension au moins n (ensembles disjoints, avec $\bigcup_{i \leq k} X_k = A$). Nous allons voir qu'on peut raffiner cette partition. Par hypothèse il y a une famille $A_0, \ldots, A_{k+1}$ de sous-ensembles définissables disjoints de A de dimension au moins n ; car $\bigcup_{i \leq k} X_i \cap A_j = A_j$ pour chaque $j \geq k+1$, on trouve $i(j)$ tel que $\dim(X_i \cap A_j) \geq n$. Il y a donc $j \neq j'$ tel que $i(j) = i(j') = i_0$; on divise X_{i_0} en deux parties $X_{i_0} \cap A_j$ et $X_{i_0} - A_j \supseteq X_{i_0} \cap A_{j'}$, chaqu'une de dimension au moins n.

On obtient un arbre infini de sous-ensembles définissables de A à branchement fini (en effet, chaque sommet non-final a deux successeurs) ; par le Lemme de König il y a une branche infinie, disons $A \supseteq Y_0 \supseteq Y_1 \supseteq Y_2 \supseteq \cdots$. Si Z_i est l'autre successeur de Y_i (différent de Y_{i+1}), on voit que les Z_i forment une famille infinie de sous-ensembles définissables disjoints de A de dimension au moins n. Or, $\dim(A) \geq n + 1$. ■

Définition 4.1.5 Le *degré* $\deg(A)$ d'un sous-ensemble définissable A de $\mathfrak{M}^s$ est le cardinal d'une famille maximale de sous-ensembles définissables disjoints de A de même dimension.

Par la proposition précédente, le degré d'un ensemble de dimension finie existe. Tout ensemble A de dimension finie se décompose en $\deg(A)$ ensembles de même dimension et de degré 1 ; cette décomposition est unique à ensembles de dimension $< \dim(A)$ près.

Exercice 4.1.6 Si $\dim(B) < \dim(A)$, alors A et $A \cup B$ ont même dimension et degré.

Exercice 4.1.7 Si A et B ont même dimension n, alors $\deg(A \cup B) \leq \deg(A) + \deg(B)$, avec égalité si et seulement si $\dim(A \cap B) < n$.

Exercice 4.1.8 Si A, B et $A \cap B$ ont même dimension, alors $\deg(A \cup B) + \deg(A \cap B) = \deg(A) + \deg(B)$.

Ile st évident qu'une bijection définissable préserve la dimension et le dergé, comme elle échange les sous-ensembles définissables de sa domaine et de son image. Plus généralement, nous avons :

Proposition 4.1.9 *Soit* $f : A \to B$ *une surjection définissable. Alors* $\dim(A) \geq \dim(B)$ *; si en outre* $|f^{-1}(b)| \leq d$ *pour tout* $b \in B$*, alors* $\dim(A) = \dim(B)$ *et* $\deg(B) \leq \deg(A) \leq d \cdot \deg(B)$.

Démonstration: Toute famille de sous-ensembles disjointes définissables de B se relève en une telle famille de sous-ensembles de A ; la première partie suit par récurrence sur la dimension.

Pour la deuxième partie supposons que les fibres $f^{-1}(b)$ sont toutes de cardinal au plus d. Si $\dim(A) \geq n+1$, alors par récurrence $\dim(B) \geq n$. Supposons donc que $\dim(B) = n$ et $\deg(B) = k$, et choisissons une famille $A_0, \ldots, A_{dk}$ de sous-ensembles disjoints de A de dimension au moins n. Par récurrence $\dim(f(A_i) \geq n$ pour tout $i \leq dk$. Soit $B_1, \ldots, B_k$ une partition de B en ensembles disjoints de dimension n et degré 1. Alors pour tout $i \leq dk$ il y a un $j(i)$ tel que $\dim(f(A_i) \cap B_{j(i)}) = n$. Donc $\dim(B_{j(i)} - f(A_i)) < n$. Mais il y a une valeur j_0 qui est pris au moins $d+1$ fois par les $j(i)$, disons $j_0 = j(i_0) = \cdots = j(i_d)$. Or

$$\begin{aligned}\dim(B_{j_0} - \bigcap_{s=0}^{d} f(A_{i_s})) &= \dim(\bigcup_{s=0}^{d} [B_{j_0} - f(A_{i_s})]) \\ &= \max_{s=0}^{d} \dim(B_{j_0} - f(A_{i_s}) < n,\end{aligned}$$

d'où $\dim(B_{j_0} \cap \bigcap_{s=0}^d f(A_{i_s})) = n \geq 0$. En particulier, c'est un ensemble non-vide. Mais chaque $b \in B_{j_0} \cap \bigcap_{s=0}^d f(A_{i_s})$ a un préimage dans chaque A_{i_s} pour $s = 0, \ldots, d$, et donc $|f - -1(b)| \geq d + 1$, contradiction. Donc $\dim(A) = \dim(B)$.

Une famille disjointe de sous-ensembles de B de dimension n se relevant en une famille disjointe de sous-ensembles de A de dimension n, on voit que $\deg(A) \geq \deg(B)$. Mais si $\dim(A) = n$ et $\deg(A) > d \cdot \deg(B)$, on obtient une contradiction comme dans le paragraphe précédent, d'où $\dim(A) \leq d \cdot \deg(B)$. ■

4.2 La minimalité forte

Définition 4.2.1 Une structure $\mathfrak{M}$ est *minimale* si tout sous-ensemble définissable $X \subseteq \mathfrak{M}$ est soit fini, soit co-fini.
$\mathfrak{M}$ ets *fortement minimale* si tout $\mathfrak{N} \cong \mathfrak{M}$ est minimale.

Exercice 4.2.2 Démontrer qu'une structure $\mathfrak{M}$ est fortement minimale si et seulement si pour chque formule $\varphi(x, \bar{y})$ il y a un $n \in \omega$ tel que pour chaque $\bar{m} \in \mathfrak{M}$ soit $|\{x \in \mathfrak{M} : \mathfrak{M} \models \varphi(x, \bar{m})\}| \leq n$, soit $|\{x \in \mathfrak{M} : \mathfrak{M} \models \neg\varphi(x, \bar{m})\}| \leq n$ (on dit que φ est *uniformement* fini ou co-fini).

Exemple 4.2.3 On a déjà vu qu'un corps algébriquement clos est fortement minimal.

Remarquons qu'un ensemble est minimal si et seulement s'il est de dimension 1 et de degré 1.

Théorème 4.2.4 *Soit $\mathfrak{M}$ une structure fortement minimale, $n > 0$ un entier, et $C(\bar{x}, \bar{y})$ une partie définissable de $\mathfrak{M}^{n+m}$. Alors*

1. $\dim(\mathfrak{M}^1) = n$ *et* $\deg(\mathfrak{M}^n) = 1$.
2. *pour tout entier k l'ensemble* $\{\bar{a} \in \mathfrak{M}^m : \dim(C(\bar{x}, \bar{a})) = k\}$ *est définissable.*
3. *il existe un entier d tel que* $\deg(C(\bar{x}, \bar{a})) \leq d$ *pour tout* $\bar{a} \in \mathfrak{M}^m$.

DÉMONSTRATION: Nous allons démontrer les parties 1.–3. simultanément par récurrence sur n. Si $n = 1$, la minimalité de $\mathfrak{M}$ implique que $\dim(\mathfrak{M}) = 1$ et $\deg(\mathfrak{M}) = 1$. La minimalité forte implique que pour chaque $C(x, \bar{y})$ il y a un k tel que pour tout $\bar{a}$ soit $C(x,\bar{a})$, soit $\mathfrak{M} - C(x,\bar{a})$ a au plus k éléments, donc on peut définir $\{\bar{a} : \dim(C(x,\bar{a}) = 1\}$ par

$$\exists\, x_0,\ldots,x_k \bigwedge_{i\neq j} x_i = x_j \wedge \bigwedge_i C(x_i,\bar{a}),$$

et $\{\bar{a} : \dim(C(x,\bar{a}) = 0\}$ par le complément. En plus, ce k borne aussi la multiplicité de $C(x,\bar{a})$, qui vaut $|C(x,\bar{a})|$ si $C(x,\bar{a})$ est fini, et 1 sinon.

Considérons donc une partie $C(\bar{x},x,\bar{a})$ définissable de $\mathfrak{M}^{n+1}$. Notons $A_\emptyset$ l'ensemble des $(a,\bar{a}) \in \mathfrak{M}^{1+m}$ pour lesquels le fibre $C(\bar{x},a,\bar{a}) \subseteq \mathfrak{M}^n$ est vide, et A_k l'ensemble des $(a,\bar{a}) \in \mathfrak{M}^{1+m}$ tels que $\dim(C(\bar{x},a,\bar{a})) = k$ pour tout $k \leq n$; par hypothèse de récurrence ça forme une partition définissable de $\mathfrak{M}^{1+m}$. On pose

$$C_i(\bar{x},x,\bar{y}) = C(\bar{x},x,\bar{y}) \wedge A_i(x,\bar{y});$$

on obtient ainsi une partition de $C(\bar{x},x,\bar{a})$ en ensembles définissables $C_i(\bar{x},x,\bar{a})$.

Si $A_i(x,\bar{a})$ est fini, son cardinal est borné indépendemment de $\bar{a}$ par un entier d' ; si $a_1,\ldots,a_{d'}$ sont ses éléments, on a bien

$$\begin{aligned}\dim(C_i(\bar{x},x,\bar{a})) &= \dim(\bigvee_{j=1}^{d'}[C_i(\bar{x},x,\bar{a}) \wedge x = a_j]) \\ &= \max_{j=1}^{d'}\dim(C_i(\bar{x},x,\bar{a}) \wedge x = a_j) = i.\end{aligned}$$

En plus, si $f : (\bar{x},x) \mapsto \bar{x}$ dénote la projection, qui a des fibres de taille bornée par d', on obtient

$$\deg(C_i(\bar{x},x,\bar{a})) \leq d' \cdot \deg(\exists x\, C_i(\bar{x},x,\bar{a})),$$

ce qui est borné indépendemment de $\bar{a}$ par hypothèse d'induction.

Si $A_i(x,\bar{a})$ est infini, par définition $\dim(C_i(\bar{x},x,\bar{a})) \geq i+1$ (on peut le décomposer en une infinité d'ensembles disjoints de dimension au moins i en spécifiant la dernière variable). Nous allons démontrer que $\dim(C_i(\bar{x},x,\bar{a}) = i+1$, et que $\deg(C_i(\bar{x},x,\bar{a}))$ est borné par $\max\{\deg(C_i(\bar{x},a,\bar{a}) : A_i(a,\bar{a})\}$ (qui est borné indépendemment de $\bar{a}$, disons par d').

Pour $i=0$ la projection $g : (\bar{x},x) \mapsto x$ a des fibres finies sur $C_i(\bar{x},x,\bar{a})$, de taille bornée par d' ; par la section précédente on obtient $\dim(C_i(\bar{x},x,\bar{a})) = \dim(\exists \bar{x}\, C_i(\bar{x},x,\bar{a})) = 1$ et $\deg(C_i(\bar{x},x,\bar{a})) \leq d' \cdot \deg(\exists \bar{x}\, C_i(\bar{x},x,\bar{a})) = d'$. Pour $i>0$ supposons quil y a une famille $B_0,\ldots,B_{d'}$ de sous-ensembles disjoints de $C_i(\bar{x},x,\bar{a})$ avec $\dim(B_j) \geq i+1$ pour tout $0 \leq j \leq d'$. Les fibres

$B_j(\bar{x}, a, \bar{a})$ étant de dimension majorée par i pour tout $(a, \bar{a}) \in A_i$, il faut que les ensembles $\{a \in \mathfrak{M} : \dim(B_j(\bar{x}, a, \bar{a})) = i\}$ (qui sont définissables par hypothèse de récurrence)soient cofinies dans $\mathfrak{M}$. On trouve donc $a \in \mathfrak{M}$ tel que $\dim(B_j(\bar{x}, a, \bar{a})) = i$ pour tout $0 \leq i \leq d'$, ce qui contredit $\deg(C_i(\bar{x}, a, \bar{a})) \leq d'$.

En particulier, on est dans ce cas pout $\mathfrak{M}^{n+1}$, qui est donc de dimension $\dim(\mathfrak{M}^n) + 1 = n + 1$ et degré $1 \cdot \deg(\mathfrak{M}^n) = 1$. ■

Nous retirons de la preuve :

Corollaire 4.2.5 *Si $\mathfrak{M}$ est une structure fortement minimale, $A \subseteq \mathfrak{M}^n$, et $f : A \to \mathfrak{M}$ est une application définissables telle que les fibres non-vides sont de dimension k et de multiplicité d, alors :*

- *soit l'image $f(A)$ est fini,* $\dim(A) = k$ *et* $\deg(A) \leq d \cdot |f(A)|$,
- *soit l'image $f(A)$ est infini,* $\dim(A) = k + 1$ *et* $\deg(A) \leq d$. ■

4.3 Relations d'équivalence

Soit $f : A \to B$ une application définissable. Dans cette section, nous allons démontrer une formule d'additivité qui lie $\dim(A)$ a la somme de $\dim(f(A))$ et la dimension des fibres de f. Plus généralement, on peut considerer une relation d'équivalence E sur un ensemble A (elle serait $f(x) = f(y)$ dans le cas ci-desus) et essayer de définir une dimension pour l'ensemble A/E de classes modulo E, telle que $\dim(A)$ est la somme de $\dim(A/E)$ et la dimension des classes. Evidemment, ça nécessite que toutes les classes ont la même dimension.

Lemme 4.3.1 *Soit E une relation d'équivalence définissable sur un ensemble A définissable. Si toutes les classes de E sont de taille bornée par d, alors tout sous-ensemble définissable B de A a la même dimension que l'ensemble $B^* = \{a \in A : \exists\, b \in B \;\; E(a, b)\}$.*

DÉMONSTRATION: $B^* \supseteq B$, donc $\dim(B^*) \geq \dim(B)$, et il suffit de démontrer inductivement sur n que $\dim(B^*) \geq n$ implique $\dim(B) \geq n$, ce qui est évident pour $n = 0$. Supposons donc que $\dim(B^*) \geq n + 1$, et considerons une famille $B_0, B_1, \ldots$ de sous-ensembles définissables disjoints de B^* de dimension au moins n. Posons $C_i = B_i^* \cap B$; on a $B_i^* = C_i^*$, et par hypothèse de récurrence $\dim(B_i^*) \geq n$ implique $\dim(C_i) \geq n$ pour tout i. Or, si

$\dim(B) \not\geq n+1$, il y a une infinité des C_i qui ont un point a commun, qui est aussi dans les B_i^* correspondants. Comme il n'y a que d point équivalents à a, on trouve a' équivalent à a qui est dans une infinité des B_i, ce qui contredit leur disjonction. ■

Proposition 4.3.2 *Soit $\mathfrak{M}$ une structure fortement minimale, $A \subseteq \mathfrak{M}^n$ un ensemble définissable, et E une relation d'équivalence définissable sur A tel que chaque classe modulo E est de dimension $d+1$. Alors il existe un sous-ensemble définissable B de A qui coupe chaque classe modulo E en un ensemble de dimension d.*

DÉMONSTRATION: Soit C une classe modulo E, et considérons les projections f_i de C sur la $i$me coordonnée. Comme $\dim(C) = d+1$, s'il n'y a qu'un nombre fini de points a tels que $f_1^{-1}(a) \cap C$ est de dimension d, il y a un point a dans cette projection tel que la fibre $f_1^{-1}(a) \cap C$ est de dimension $d+1$, et je peux projeter sur la deuxième coordonnée, etc. Je fixe donc une coordonnée après l'autre ; eventuellement je dois en trouver une telle qu'il y a une infinité de fibres de dimension d ; a fortiori la projection de C sur cette coordonnée a une infinité de fibres de dimension d. En partitionant A en un nombre fini de sous-ensembles E-invariants, je peux donc supposer que la projection de chaque classe modulo E sur la première coordonnée a une infinité de points dont la fibre est de dimension d. Or, pour chaque $\bar{a} \in A$ l'ensemble

$$B(\bar{a}) = \{a \in \mathfrak{M} : \dim(E(\bar{a}, a\bar{x})) = d\}$$

(où $\bar{x}$ est de longueur $n-1$) est définissable uniformément en paramètres, et donc uniformément cofini ; il y a un k et $a_0, \ldots, a_k \in \mathfrak{M}$ tel que $B(\bar{a}) \cap \{a_0, \ldots, a_k\} \neq \emptyset$ pour tout $\bar{a} \in A$. L'ensemble B est donc

$$\{\bar{a} \in A : \bigvee_{s=0}^{k} [f_1(\bar{a}) = a_s \wedge a_s \in B(\bar{a})]\}. \quad ■$$

Définition 4.3.3 Soit E une relation d'équivalence sur un ensemble A. Un ensemble de *choix multiples* pour E dans A est une partie B de A qui coupe chaque classe modulo E en un nombre fini (non-nulle) de points.

Corollaire 4.3.4 *Soit $\mathfrak{M}$ une structure fortement minimale, $A \subseteq \mathfrak{M}^n$ et E une relation d'équivalence définissable sur A. Alors il y a un ensemble de choix multiples définissables pour E dans A.*

Démonstration: A se partitionne définissablement comme $A = A_0 \cup \cdots \cup A_n$, où A_i est l'ensemble des points de A dont la classe modulo E est de dimension i. Le corollaire suit par i applications de la proposition précédente à chaque A_i. ■

Théorème 4.3.5 *Soit $\mathfrak{M}$ une structure fortement minimale, et $f : A \to B$ une application définissable surjective, telle que toutes les fibres ont la même dimension d. Alors* $\dim(A) = \dim(f(A)) + d$.

Démonstration: Par induction sur d. Si $d = 0$, la taille d'une classe est son degré, qui est donc borné. On voit facilement par récurrence sur n que $\dim(f(A)) \geq n$ implique $\dim(A) \geq n$; pour le réciproque, on utilise le Lemme 4.3.1, et une récurrence sur la dimension.

Pour le cas général, on trouve un ensemble (définissable) $C_0 \subseteq A$ qui coupe chaque classe modulo la relation d'équivalence définissable $f(\bar{x}) = f(\bar{y})$ en un ensemble de dimension $d-1$; par hypothèse de récurrence $\dim(C_0) = \dim(B) + (d-1)$. Comme chaque classe modulo E de $A - C_0$ est toujours de dimension d, on peut repeter ; à la fin on aura trouvé une famille infinie $C_0, C_1, \dots$ de sous-ensembles disjointes définissables de A de dimension $\dim(B) + (d-1)$, ce qui montre $\dim(A) \geq \dim(B) + d$.

Pour l'autre sens de l'inégalité, supposons que $A_0, A_1, \dots$ est une famille de sous-ensembles disjoints de A de dimension au moins n. Chaque A_i se divise en un nombre fini d'ensembles

$$A_i^j = \{a \in A_i : \dim(f^{-1}(f(a)) \cap A_i) = j\},$$

où $0 \leq j \leq d$. Par récurrence $\dim(A_i^j) \geq n$ implique $\dim(f(A_i^j)) + j \geq n$. Comme $\dim(f(A_i^j)) + j \leq \dim(B) + j$, si $\dim(B) + d \not\geq n + 1$, on obtient $\dim(f(A_i^d) = \dim(B)$ pour tout i. On trouve donc $b \in B$ tel que $f^{-1}(b)$ contient un nombre arbitrairement large de sous-ensembles disjoints de dimension d (dans autant des A_i^d qu'on veut), ce qui contredit le degré borné de $f^{-1}(b)$. ■

Un (élément) *imaginaire*, c'est une classe modulo une relation d'équivalence définissable.

Théorème 4.3.6 *Dans une structure fortement minimale $\mathfrak{M}$, toute relation d'équivalence définissable E sur un ensemble définissable $A \subseteq \mathfrak{M}^n$ est de la forme $f\bar{x}) = f(\bar{y})$, où f est une fonction définissable de A dans un quotient C/F, où C est définissable et F est une relation d'équivalence sur C à classes finies.*

Démonstration: Soit C un ensemble de choix multiples pour E dans A, et F la restriction de E à C ; la fonction f associe à chaque $a \in A$ la classe modulo F des $c \in C$ qui lui sont congrus modulo E. ■

Ce phénomène s'appèle aussi *élimination faible des imaginaires.* Dans un corps algébriquement clos, en a plus :

Théorème 4.3.7 *Soit K un corps algébriquement clos, $A \subseteq K^n$ définissable, et E une relation d'équivalence définissable sur A. Alors il y a une fonction $f : A \to \mathcal{K}^m$ telle que $E(a, b)$ si et seulement si $f(a) = f(b)$.*

On peut donc remplacer les imaginaires dans A/E par leurs images dans $f(A)$.

Démonstration: D'après le théorème précédent, on peut supposer que les classes modulo E sont finies, et en fait de taille borné (par une borne sur leur degré). En partitionnant A, on peut même supposer qu'elles sont toutes de taille k.

Si A est un sous-ensemble de K, on peut facilement coder l'*ensemble* $\{a_1, \ldots, a_k\}$ par la *suite* $(\sigma_1(a_1, \ldots, a_k), \ldots, \sigma_k(a_0, \ldots, a_k))$, où les σ_i sont les fonctions élémentaires symétriques (donc les coefficients du polynm̂e normé $(x - a_1) \cdots (x - a_k)$, à signe près).

Pour le cas général où les a_i sont de longueur n, on considère l'extension galoisienne $\mathbb{Q}(\bar{x})$ de $\mathbb{Q}(\sigma_1(\bar{x}), \sigma_{kn}(\bar{x}))$, où $\bar{x} = (x_1, \ldots, x_{kn}$ sont des éléments trancendents indépendents sur $\mathbb{Q}$, avec groupe de Galois G. Si H est le sous-groupe des automorphismes dans G qui permutent les blocs $(x_1, \ldots, x_n), (x_{n+1}, \ldots, x_{2n}), \ldots, (x_{kn-k+1}, \ldots, x_{kn})$ entre eux, et si K est le corps fixe de H, on peut trouver un générateur de $\mathbb{Q}(\bar{x})$ sur K tel que les coefficients de son polynôme minmal sur K s'expriment comme polynomes $\tau_1(\bar{x}), \tau_2(\bar{x}), \ldots$. L'ensemble $\{a_1, \ldots, a_k\}$ est codé par l'uple

$$(\tau_1(a_1 \ldots a_k), \tau_2(a_1 \ldots a_k) \ldots). \quad ■$$

Exercice 4.3.8 Trouver explicitement des polynômes τ_1, τ_2, etc.

4.4 Sous-structures

D'abord, nous allons généraliser la notion de clôture algébrique.

Définition 4.4.1 Soit $\mathfrak{M}$ und structure, et $A \subseteq \mathfrak{M}$ un ensemble de paramètres. Un élément $a \in \mathfrak{M}$ est *ahgébrique* sur A s'il y a un ensemle fini X, définissable à paramétres dans A, qui contient a. La *clôture algébrique* $\mathrm{acl(A)}$ est l'ensemble de tous les éléments de $\mathfrak{M}$ algébriques sur A.

Un élément $a \in \mathfrak{M}$ est *définissable* sur A si l'ensemble $\{a\}$ est définissable à paramètres dans A. La *clôture définissable* $\mathrm{dcl(A)}$ est l'ensemble des éléments définissables sur A.

Evidemment $\{a\}$ est un ensemble définissable (par la formule $x = a$) fini qui contient a ; l'i,porance c'est qu'on peut prendre des paramètres dans A.

Exemple 4.4.2 Si $\mathfrak{M} = K$ est un corps algébriquement clos, $\mathrm{acl(A)}$ est la clôture algébrique (dans le sens corporal) et $\mathrm{dcl(A)}$ est la clôture inséparable du corps engendré par A. Donc $\mathrm{acl(A)} = \langle\tilde{\mathrm{A}}\rangle$ et $\mathrm{dcl(A)} = \langle\mathrm{A}\rangle^{\mathrm{insep}}$.

Lemme 4.4.3 *Les clôtures algébriques et définissables sont des operateurs finitaires, positifs et idempotens. En effet,*

1. $\mathrm{acl(A)} = \bigcup_{\mathrm{A_0 \subseteq A}\ \mathit{fini}} \mathrm{acl(A_0)}$ *et* $\mathrm{dcl(A)} = \bigcup_{\mathrm{A_0 \subseteq A}\ \mathit{fini}} \mathrm{dcl(A_0)}$.
2. $A \subseteq \mathrm{dcl(A)} \subseteq \mathrm{acl(A)}$, *et*
3. $\mathrm{acl(acl(A))} = \mathrm{acl(A)}$ *et* $\mathrm{dcl(dcl(A))} = \mathrm{dcl(A)}$.

Démonstration: Comme une formule n'utilise qu'un nombre fini de paramètres, tout $a \in \mathrm{acl(A)}$ est algébrique, et tout $a \in \mathrm{dcl(A)}$ est définissable, sur un sous-ensemble fini $A_0 \subseteq A$; cei démontre 1. La partie 2. est évident de la définition, comme $\{a\}$ est définissable à paramètre a.

Pour 3., considérons une formule $\varphi(x, a_0, \ldots, a_k)$ à paramètres dans $\mathrm{acl(A)}$ qui définit un ensemble fini, disons à n éléments. Pour $i \leq k$ soit $\psi_i(x, \bar{a}_i)$ une formule à paramètres dans A qui définit un ensemble fini contenant a_i. Soit $|\varphi(x, \bar{y})| \leq n$ la formule

$$\forall\, x_0, \ldots, x_n\, [\bigwedge_{i \leq n} \varphi(x_i, \bar{y}) \to \bigvee_{i<j} x_i = x_j].$$

Alors

$$\exists\, y_0, \ldots, y_k\, [\bigwedge_{i \leq k} \psi_i(y_i, \bar{a}_i) \wedge \varphi(x, y_0, \ldots, y_k) \wedge |\varphi(x, y_0, \ldots, y_k)| \leq n$$

est une formule à paramètres dans A qui définit un ensemble fini contenant les réalisations de $\varphi(x, a_0, \ldots, a_k)$. Donc acl(acl(A) $\subseteq$ acl(A) ; on a égalité par la partie 2. Pour la clôture définissable, on considère la même démonstration, sauf que $n = 1$ et toutes les formules définissent des ensembles à un élément. ∎

Théorème 4.4.4 *Soit $\mathfrak{M}$ une structure fortement minimale, et $A \subseteq \mathfrak{M}$ un sous-ensemble infini algébriquement clos. Alors $A \prec \mathfrak{M}$.*

Démonstration: Comme A est algébriquement clos, il contient les constantes et est clos par les fonctions. Donc, avec la structure induite c'est bien une sous-structure de $\mathfrak{M}$. Vérifions qu'elle est élémentaire. Soit alors $\varphi(x)$ une formule a paramètres dans A qui définit un ensemble non-vide dans $\mathfrak{M}$. Par minimalité forte, soit φ définit un ensemble fini, qui est inclus dans la clôture algébrique de A, et donc dans A, soit φ définit un ensemble co-fini dans $\mathfrak{M}$, qui doit coupe A en un ensemble infini. En tout cas, on trouve $a \in A$ tel que $\mathfrak{M} \models \varphi(a)$; par le critère de Tarski $A \prec \mathfrak{M}$. ∎