Table des matières

Chapitre 1

Groupes : algèbre

Un groupe, j'espère que vous savez ce que c'est.
Bruno Poizat.

La théorie des modèles d'une classe de structures, en l'occurrence des groupes, se fait fréquemment en suivant deux lignes principales :

- l'étude de classes de structures définies abstraitement par des hypothèses de la théorie des modèles (groupes stables, etc.) ;
- l'étude de classes de structures connues, plus ou moins générales, provenant de divers domaines des mathématiques (groupes algébriques sur une certaine classe de corps commutatifs, anneaux commutatifs, espaces de Hilbert, etc.) en suivant des questions motivées par la théorie des modèles.

La notion de "définissabilité", sous quelque forme qu'elle apparaîsse, est fondamentale à toutes ces études.

L'objectif principal des deux premier chapitres de notre cours est de démontrer des résultats de nature modèle-théorique sur certaines classes de groupes. Le premier chapitre se penche sur des classes de nature algébrique tandis que le deuxième soulignera des aspects combinatoires. Les théorèmes de ce chapitre, simples et démontrés en utilisant des outils algébriques, sont dans leurs fonds modèle-théoriques. Ils ont des thèmes qui reviendront souvent durant le cours. Ils ont été choisis pour motiver certains aspects du cours, d'où le style informel des preuves.

Au début, il y a un rappel non exhaustif des connaissances requises en théorie des groupes. Il y en aura d'autres tout au long du cours en cas de besoin. Ils seront parfois appuyés par des exercices à la fin.

Les exercices ne sont pas seulement destinés à rendre plus robustes des connaissances déjà acquises. Il y en a qui ont l'objectif d'approfondir les nouvelles connaissances. Une bonne compréhension nécessite du cours la capacité de s'attaquer à ces exercices. Vous êtes encouragés à les aborder et à en discuter avec tous les autres acteurs de ce cours.

1.1 Groupes, notations, notions de base

Un groupe est une *structure*, un ensemble sous-jacent dont sont distinguées des parties de ses puissances cartesiennes :

$$\mathcal{G} = (G; ., 1, \ ^{-1}) \ .$$

Un groupe peut appartenir à une plus grande structure :

$$\mathcal{R} = (\mathbb{R}; +, 0, \ ^{-1}, <) \ .$$

Le premier exemple présente l'écriture générale d'une structure de groupe. L'ensemble sous-jacent est G tandis que les parties ditinguées de ses puissances cartésiennes correspondent aux graphes de trois fonctions : une binaire qui est la loi interne de groupe, une unaire qui est l'inversion, une constante dont l'ensemble d'arrivée est l'élément neutre du groupe que nous aurons

tendance à noter 1 ou 0 suivant si la notation est multiplicative ou additive respectivement. Il est bien connu en théorie des groupes que ces deux dernières fonctions sont d'une certaine manière redondantes puisqu'elles peuvent s'exprimer en utilisant des "formules" qui n'utilisent que la loi interne du groupe ambiant.

Le deuxième exemple est une expansion de groupes. Il s'agit du corps ordonné des réels. Parmi les ensembles distingués des puissances cartésiennes de l'ensemble sous-jacent, il y a aussi une relation binaire : l'ordre usuel des réels.

Pour alléger la notation, nous aurons tendance à utiliser la même lettre à la fois pour l'ensemble sous-jacent et pour la structure, sauf quand nous voudrons faire une distinction claire entre les deux entités.

Voici quelques no(ta)tions de la théorie des groupes à retenir :
- ordre d'un élément g ; notation $|g|$; peut être fini (dit aussi élément de "torsion") ou infini ;
- sous-groupe ; notation $<, \leq$;
- sous-groupe distingué (dit aussi "normal") ; notation $\lhd$;
- sous-groupe engendré par une partie X d'un groupe G ; notation $\langle X \rangle$; le groupe engendré est dit *de type fini* si X est de cardinal fini ;
- centre ; notation $Z(G)$;
- centralisateur d'un élément g ; notation $C_G(g)$;
- conjugué d'une partie non vide X par un élément g ; notation X^g ;
- commutateur de deux éléments x, y d'un groupe ; notation $[x, y] = x^{-1}y^{-1}xy$;
- sous-groupe engendré par les commutateurs, dans un groupe G, dont les premières coordonnées appartiennent à X et les deuxièmes à Y ; notation $[X, Y]$; (en général, $[X, Y] \neq \{[x, y] \mid x \in X,\ y \in Y\}$) ;
- le produit de deux sous-ensembles non vides X et Y d'un groupe G ; notation XY ; définition $XY = \{xy \mid x \in X,\ y \in Y\}$;
- centralisateur d'une partie non vide X ; notation $C_G(X)$;
- normalisateur d'une partie non vide X ; notation $N_G(X)$

Dans le cours des techniques de construction de groupes à partir d'autres seront utilisées. Deux telles méthodes, déjà connues, sont révisées dans les exercices : produits et sommes directs, produits semi-directs.

1.2 Classes de groupes : point de vue algébrique

Groupes commutatifs (dits aussi "abéliens")

Définition 1.2.1 *Un groupe G est dit abélien s'il satisfait l'une des conditions équivalentes :*

1. *pour tous $x, y \in G$, $[x, y] = 1$;*
2. *$G = Z(G)$;*
3. *pour tout $g \in G$, $G = C_G(g)$.*

Voici quelques exemples :

1. si A est un anneau, alors $(A; +, 0)$ est un groupe commutatif ;
2. si K est un corps commutatif, alors $(K^\times; ., 1)$ est un groupe commutatif où $K^\times = K \setminus \{0\}$;
3. si p est un nombre premier, alors les racines complexes p^ne de l'unité munies de la multiplication usuelle des nombres complexes forment un groupe que nous noterons $\mathbb{Z}_{p^\infty}$;
4. si A est un anneau, alors la structure

$$\left(\left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in A\right\}; +, -, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)$$

est un groupe abélien isomorphe à $(A; +, 0)$.

Groupes nilpotents

Définition 1.2.2 (Série Centrale Ascendante) *Soit G un groupe. La* série centrale ascendante *de G est définie de façon inductive :*

$$Z_0(G) = \{1\}$$

$$\textit{pour tout } \ k \in \mathbb{N}, \quad Z_{k+1}(G)/Z_k(G) = Z(G/Z_k(G)) \ .$$

De façon équivalente pour tout $k \in \mathbb{N}$ est

$$Z_{k+1}(G) = \{g \in G \mid [g, h] \in Z_k(G) \textit{ pour tout } h \in G\} \ .$$

Voici quelques remarques sur les séries centrales ascendantes :

1. La définition d'une série centrale ascendante est cohérente, en d'autres termes que tout $Z_k(G) \lhd G$.
2. En fait, la condition suivante plus forte que le point précédent est satisfaite aussi : chaque $Z_k(G)$ est stable sous l'action de tout automorphisme de G (un tel sous-groupe est dit *caractéristique*).
3. Du point de la théorie des modèles le centre d'un groupe G est l'ensemble des éléments z de G qui satisfont la "formule" suivante :

   $$\forall x(xz = zx) \ ;$$

   de façon équivalente, si on se permet l'usage de l'inversion et de l'élément neutre :

   $$\forall x(x^{-1}z^{-1}xz = 1) \ .$$

   C'est un sous-groupe "définissable". On peut réitérer cette idée pour montrer par récurrence que chaque membre de la série ascendante est définissable.

Définition 1.2.3 (Groupes nilpotents) *Un groupe G est dit* nilpotent *s'il existe $n \in \mathbb{N}$ tel que $G = Z_n(G)$. Le plus petit n safisfaisant cette condition est dit la* classe de nilpotence de G.

De cette définition, il est clair que le centre d'un groupe nilpotent non trivial est non trivial.

Ci-dessous sont quelques exemples de groupes nilpotents. Rappelons que, quand p est un nombre premier, un p-groupe est un groupe dont tous les éléments sont d'ordre une puissance de p.

1. Les groupes abéliens sont nilpotents de classe 1.
2. Un p-groupe *fini* est nilpotent.
3. Soient $n \in \mathbb{N}^*$ et K un corps commutatif. Alors la structure

   $$\left(\left\{ \left(\begin{array}{ccccc} 1 & a_{1,2} & & \dots & a_{1,n+1} \\ 0 & 1 & a_{2,3} & \dots & a_{2,n+1} \\ \vdots & 0 & 1 & & \\ & & & \ddots & \\ 0 & & & \dots & 1 \end{array} \right) \mid a_{i,j} \in K \right\} ; ., \ ^{-1}, \left(\begin{array}{cccc} 1 & 0 & & \dots \ 0 \\ 0 & 1 & 0 & \dots \ 0 \\ \vdots & 0 & 1 & \\ & & & \ddots \\ 0 & & & \dots \ 1 \end{array} \right) \right)$$

   où . est la multiplication usuelle des matrices est un groupe nilpotent. En fait, c'est un groupe n-nilpotent. Nous noterons ce groupe $U(n + 1, K)$.

Maintenant démontrons un théorème :

Théorème 1.1 *Soit K un corps commutatif. Alors le corps K est "définissable" dans $U(3,K)$.*

Preuve. Fixons d'abord la notation que nous utiliserons. Nous commençons avec certains sous-groupes que ceux qui ont trempé leurs plumes dans les algèbres de Lie ou les groupes algébriques reconnaîtront comme des sous-groupes de racine :

$$X = \left\{ \begin{pmatrix} 1 & t & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \ : \ t \in K \right\}$$

$$Y = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} \ : \ t \in K \right\}$$

$$Z = Z(U(3,K)) = \left\{ \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \ : \ t \in K \right\}$$

Nous noterons les éléments de X, Y et Z $x(t)$, $y(t)$ et $z(t)$ respectivement, suivant la valeur du paramètre. Ces trois ensembles, munis de la multiplication usuelle des matrices, forment des sous-groupes abéliens qui sont en fait isomorphes au groupe additif $(K,+,0)$ du corps K.

Voici un calcul pour ceux qui aiment multiplier les matrices :

$$(+) \qquad \left[\begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & a_1b_2 - a_2b_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

La formule suivante est une conséquence de cette égalité :

$$(*) \qquad \text{pour tout } t,u \in K,\ [x(t),y(u)] = z(tu) .$$

En utilisant ces identités, nous concluons que

$$Z = \{[x(t),y(u)] \ : \ t,u \in K\} .$$

Remarquons que ce que nous venons d'écrire est plus fort que de dire que $Z = [X,Y]$.

Nous définirons deux fonctions binaires sur l'ensemble Z qui donneront à cet ensemble une structure de corps. Pour ce faire, nous ne ferons usage que de la loi interne du groupe Z. Définissons d'abord "l'addition" :

$$\begin{array}{rccc} + & : & Z \times Z & \longrightarrow & Z \\ & & (z_1,z_2) & \longmapsto & z_1z_2 . \end{array}$$

En d'autres termes, le graphe de la fonction + est l'ensemble suivant :

$$\{(z_1,z_2,z_3) \in Z^3 \mid \text{le triplet } (z_1,z_2,z_3) \text{ satisfait la formule } z_1z_2 = z_3\} .$$

La multiplication, quoique l'idée sous-jacente soit déjà visible dans la formule (*), nécessite une préparation plus longue. Si z_1 et z_2 sont deux éléments de Z alors d'après la formule (*), il existe, dans les sous-groupes $XZ = \{xz \mid x \in X,\ z \in Z\}$ et $YZ = \{xz \mid x \in X,\ z \in Z\}$ (voyez-vous pourquoi ce sont des sous-groupes ?), x_1 et y_2 respectivement tels que $[x_1,y(1)] = z_1$ et $[x(1),y_2] = z_2$. Notons qu'il existe plusieurs candidats pour x_1 et y_2. Néanmoins, d'après la formule (+), les candidats pour x_1 (resp. pour y_2) diffèrent entre eux d'un élément de Z. Par conséquent, le choix de x_1 ni de y_2 n'a aucune influence sur la valeur du commutateur $[x_1,y_2]$. Nous pouvons maintenant définir la "multiplication" :

$$\begin{array}{rccc} \bullet & : & Z \times Z & \longrightarrow & Z \\ & & (z_1,z_2) & \longmapsto & [x_1,y_2] . \end{array}$$

En d'autres termes, le graphe de la fonction $\bullet$ est l'ensemble suivant :

$$\{(z_1, z_2, z_3) \in Z^3 \mid \text{le triplet } (z_1, z_2, z_3) \text{ satisfait la formule}$$
$$\exists x_1 y_2 (\ [x_1, x(1)] = 1 \ \wedge \ [y_2, y(1)] = 1 \wedge \ [x_1, y(1)] = z_1 \ \wedge \ [x(1), y_2] = z_2 \ \wedge \ [x_1, y_2] = z_3 \ )\}$$

Nous avons déjà constaté que l'existence suffit pour conclure que ce graphe est celui d'une fonction déterminée par les deux premières coordonnées. Une autre remarque qu'il importe de bien souligner est notre choix de sous-groupes pour le lieu de x_1 et y_2. Nous avons préféré XZ et YZ à X et Y parce queXZ et YZ sont aussi les centralisateurs de $x(1)$ et $y(1)$ respectivement, ce qui nous a permis d'écrire la formule de définition ci-dessus.

Il reste maintenant à vérifier que la structure $(Z; +, \bullet, z(0), z(1))$ est un corps isomorphe à $(K; +, ., 0, 1)$. C'est un exercice.

Nous avons montré que le corps K est "définissable" à partir de la "pure" structure de groupe de $U(3, K)$ en utilisant les "paramètres" $x(1)$, $y(1)$, $z(1)$. En effet, en décrivant les graphes des deux fonctions binaires $+$ et $\bullet$, outre les paramètres, nous n'avons utilisé que la loi interne de groupe et l'inversion (qui n'est pas inévitable)... et certaines règles d'écriture.

Nous pouvons aller plus loin. La représentation matricielle de $U(3, K)$ est définissable à partir du groupe $U(3, K)$ en utilisant la copie isomorphe de K que nous venons de construire. En d'autres termes, nous pouvons la reproduire dans les puissances cartésiennes de $Z(U(3, K))$ accompagné d'un tel isomorphisme que le graphe de celui-ci soit définissable à partir de la pure structure de groupe de $U(3, K)$. □

Groupes résolubles

Définissons la série dérivée d'un groupe G.

Définition 1.2.4 (Série Dérivée) *Soit G un groupe. La* série dérivée *de G est définie de façon inductive :*

$$G^{(0)} = G$$

$$\textit{pour tout} \quad k \in \mathbb{N}, \quad G^{(k+1)} = [G^{(k)}, G^{(k)}] \ .$$

Contrairement à ce qui était dans la troisième remarque après la définition de la série centrale ascendante, il n'est pas clair s'il existe une "formule" générale pour "définir" chaque membre de la série dérivée. En fait, comme nous en verrons des exemples, il n'en existe pas.

Définition 1.2.5 (Groupes Résolubles) *Un groupe G est dit résoluble s'il existe $k \in \mathbb{N}$ tel que $G^{(k)} = \{1\}$. Si k est le plus petit nombre naturel ayant cette propriété, alors G est dit d'être résoluble de classe k, ou k-résoluble.*

Voici quelques exemples de groupes résolubles :

1. Tout groupe nilpotent est résoluble.
2. Soit K un corps commutatif. Alors la structure

$$\left(\left\{ \begin{pmatrix} t & u \\ 0 & 1 \end{pmatrix} \ : \ t \in K^\times, \ u \in K \right\}; ., \ ^{-1}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

où . est la multiplication usuelle des matrices est un groupe résoluble. Sauf quand K contient au plus deux éléments, c'est un groupe 2-résoluble et non nilpotent.

Ce groupe est isomorphe au produit semidirect $K_+ \rtimes K^\times$ où l'action du groupe multiplicatif sur le groupe additif est donné par la multiplication par les éléments de $K^\times$.

3. Soient $n \in \mathbb{N} \setminus \{0,1\}$ et K un corps commutatif. Alors la structure

$$\left(\left\{ \left(\begin{array}{ccccc} t_1 & a_{1,2} & & \dots & a_{1,n} \\ 0 & t_2 & a_{2,3} & \dots & a_{2,n} \\ \vdots & 0 & t_3 & & \\ & & & \ddots & \\ 0 & & & \dots & t_n \end{array} \right) \mid a_{i,j} \in K \right\}; ., {}^{-1}, \left(\begin{array}{ccccc} 1 & 0 & & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & 1 & 0 & \\ & & & \ddots & \\ 0 & & & \dots & 1 \end{array} \right) \right)$$

où . est la multiplication usuelle des matrices est un groupe résoluble. En fait, c'est un groupe n-résoluble non nilpotent sauf quand le corps K a au plus 2 éléments. Nous noterons ce groupe $B(n, K)$.

Démontrons notre deuxième théorème.

Théorème 1.2 *Soit K un corps commutatif. Soit G le groupe formé par les matrices*

$$\left\{ \left(\begin{array}{cc} t & u \\ 0 & 1 \end{array} \right) \; : \; t \in K^\times, \; u \in K \right\}$$

munies de la multiplication usuelle des matrices. Alors le corps K est définissable *dans G.*

Preuve. Comme dans la preuve du théorème 1.1, nous commençons en fixant la notation. D'abord deux sous-groupes :

$$T = \left\{ \left(\begin{array}{cc} t & 0 \\ 0 & 1 \end{array} \right) \; : \; t \in K^\times \right\}$$

$$U = \left\{ \left(\begin{array}{cc} 1 & u \\ 0 & 1 \end{array} \right) \; : \; u \in K \right\}$$

Notons que T est isomorphe au groupe multiplicatif du corps K tandis que U est isomorphe au groupe additif de K. Nous utiliserons le sous-groupe U pour définir une copie isomorphe de K en n'utilisant que la loi interne de groupe de G. Il est possible de faire une définition en utilisant T (exercice).

Une remarque algébrique importante est que T agit sur U par conjugaison. L'action est transitive sur $U^\times$ et pour tout $x \in U^\times$, $\mathrm{Stab}_T(x) = \{1\}$. Une telle action est dite *régulière*. Ces conlusions découlent de l'identité suivante :

$$(C) \qquad \text{pour tout } t \in K^\times \text{ et } u \in K, \; \left(\begin{array}{cc} t & 0 \\ 0 & 1 \end{array} \right) \left(\begin{array}{cc} 1 & u \\ 0 & 1 \end{array} \right) \left(\begin{array}{cc} t^{-1} & 0 \\ 0 & 1 \end{array} \right) = \left(\begin{array}{cc} 1 & tu \\ 0 & 1 \end{array} \right) \; .$$

Comme dans la preuve du théorème 1.1, nous définirons deux fonctions binaires, cette fois-ci sur l'ensemble U qui muniront cet ensemble d'une structure de corps. Encore une fois, nous ne ferons usage que de la loi interne de groupe, cette fois-ci celle de G. La définition de "l'addition" est similaire à ce que nous avons fait en démontrant le théorème 1.1 :

$$\begin{array}{rccc} + \; : & U \times U & \longrightarrow & U \\ & (u_1, u_2) & \longmapsto & u_1 u_2 \; . \end{array}$$

La multiplication sera définie en utilisant l'action de T sur U. Nous fixons d'abord un élément quelconque u_0 de U différent de l'élément neutre du groupe G. Soient maintenant u_1 et u_2 deux éléments arbitraires de U différents de l'élément neutre. D'après l'identité (C), il existe t_1 et t_2 dans T tels que $u_0^{t_1} = u_1$ et $u_1^{t_2} = u_2$. En plus t_1 et t_2 sont uniques pour leurs tâches respectives. Alors, le produit u_3 de u_1 et u_2 dans la multiplication que nous sommes en train de définir sera l'élément $(u_0^{t_1})^{t_2} = u_0^{t_1 t_2}$.

Nous pouvons préciser la définition de la "multiplication" :

$$\begin{array}{rccc} \bullet & : & U\setminus\{1\}\times U\setminus\{1\} & \longrightarrow & U\setminus\{1\} \\ & & (u_0^{t_1},u_0^{t_2}) & \longmapsto & u_0^{t_1t_2}\ . \end{array}$$

Comme les éléments t_1 et t_2 proviennent de T, il nous faut exprimer T en utilisant la structure de groupe. Or, un calcul similaire à celui représenté par l'identité (C) montre que pour tout $t\in T\setminus\{1\}$, $C_G(t)=T$. Alors, le graphe de la fonction $\bullet$ est décrit de la façon suivante :

$$\{(u_1,u_2,u_3)\in U^3 \mid \text{le triplet } (u_1,u_2,u_3) \text{ satisfait la formule}$$
$$\exists t_1t_2(\ [t_1,t_0]=1\ \wedge\ [t_2,t_0]=1\wedge\ u_0^{t_1}=u_1\ \wedge\ u_0^{t_2}=u_2\ \wedge\ u_0^{t_1t_2}=u_3\ )\}$$

Il reste à vérifier que la structure $(U;.,\bullet,1,u_0)$ est un corps isomorphe à $(K;+,.,0,1)$. C'est un exercice.

Comme dans la preuve du théorème 1.1, nous pouvons reconstruire la représentation linéaire de G de "définissablement à partir de la structure de groupe de G". □

Groupes simples

Définition 1.2.6 *Un groupe G est dit* simple *s'il n'a pas de sous-groupe distingué autre que $\{1\}$ et lui-même.*

Voici une caractérisation de la simplicité en théorie des groupes :

Lemme 1.2.7 *Un groupe G est simple si et seulement si pour tout x et y dans G, il existe $n\in\mathbb{N}^*$ tel que si $x\neq 1$ alors il existe $z_1\dots z_n\in G$ tels que*

$$\bigvee_{(\epsilon_1,\dots,\epsilon_n)\ \in\ \{-1,1\}^n} (y=(x^{\epsilon_1})^{z_1}\dots(x^{\epsilon_n})^{z_n})\ .$$

Preuve. Exercice. □

La "formule" du lemme 1.2.7 est de taille finie. Néanmoins, le nombre n dépend du choix de x et de y et n'a aucune raison d'être borné. L'existence d'une telle borne est un phénomène suffisamment exceptionnel pour mériter un nom particulier : un groupe simple pour lequel n ne dépend pas de la paire d'éléments x et y est dit d'être *de simplicité bornée.*

Le dernier théorème de cette séance concerne un résultat négatif sur la simplicité bornée. Nous définissons d'abord le *groupe alterné sur* $\mathbb{N}$: c'est l'ensemble de permutations de $\mathbb{N}$ à supports finis et pairs (au sens des groupes de permutation finis) muni de la composition des fonctions. Nous noterons ce groupe $\mathrm{Alt}(\mathbb{N})$.

Théorème 1.3 *1. Le groupe* $\mathrm{Alt}(\mathbb{N})$ *est simple.*

2. Le groupe $\mathrm{Alt}(\mathbb{N})$ *n'est pas de simplicité bornée.*

Preuve. Pour le premier point, il suffit de se rappeler le théorème sur la simplicité des groupes alternés finis. Pour le deuxième, il faudra remanier des permutations convenables. □

Exercices

Exercice 1.1 Soit A un groupe abélien sans torsion. Montrer qu'il existe un corps K tel que A se plonge dans $(K, +)$.

Exercice 1.2 (Produits et sommes directs)
Soient I un ensemble non vide et $\{(G_i, i_i, 1_i) \mid i \in I\}$ une famille de groupes. Le *produit direct externe* des G_i noté

$$\prod_{i\in I} G_i \text{ ou } \times_{i\in I} G_i$$

est l'ensemble des fonctions

$$f : I \longrightarrow \bigcup_{i\in I} G_i$$

telles que pour tout $i \in I$, $f(i) \in G_i$.

1. Vérifier que la loi de composition suivante donne une structure de groupe à cet ensemble :

   pour toutes f et $g \in \prod_{i\in I} G_i$ $f.g$ est la fonction définie par $(f.g)(i) = f(i).{}_i g(i)$ pour tout $i \in I$.

   La notation $.{}_i$ est utilisée pour la loi interne du groupe G_i.
2. Vérifier que
   $$\{f \in \prod_{i\in I} \mid f(i) = 1_i \text{ pour tout } i \in I \text{ sauf un nombre fini}\}$$
   est un sous-groupe distingué de $\prod_{i\in I} G_i$. C'est la *somme directe externe* des G_i, notée $\oplus_{i\in I} G_i$.
3. Soient G un groupe et $\{N_i \mid i \in I\}$ une famille de sous-groupes distingués de G tels que
   – $G = \langle \bigcup_{i\in I} N_i \rangle$;
   – pour tout $j \in I$, $N_j \cap \langle \bigcup_{i\in I} N_i \rangle = \{1\}$.
   Montrer que $G \cong \oplus_{i\in I} N_i$. Le groupe G est dit la *somme directe interne* des N_i. Si I est un ensemble fini, alors G est aussi isomorphe au produit externe direct des N_i.
   Il est important et pratique de noter que l'isomorphisme dans le paragraphe précédent nous permet de ne pas se faire de soucis inutiles sur la distinction entre les sommes externes et ceux qui sont internes.
4. Soient $\{G_i \mid i \in I\}$ et $\{H_i \mid i \in I\}$ deux familles de groupes et $\{\Phi_i : G_i \longrightarrow H_i \mid i \in I\}$ une famille d'homomorphismes. Soit l'application
   $$\begin{array}{rccc} \Phi & : & \prod_{i\in I} G_i & \longrightarrow & \prod_{i\in I} H_i \\ & & f & \longrightarrow & \Phi(f) \end{array}$$
   où $\Phi(f)$ est définie de la façon suivante :
   $$\begin{array}{rccc} \Phi(f) & : & I & \longrightarrow & \bigcup_{i\in I} G_i \\ & & i & \longrightarrow & \Phi_i(f(i)) \end{array}$$
   Montrer que $\Phi(\oplus_{i\in I}(G_i)) \subset \oplus_{i\in I} H_i$. Montrer que $\ker(\Phi) = \prod_{i\in I} \ker(\Phi_i)$. En déduire que Φ est injectif si et seulement si chaque Φ_i l'est.
5. Soient $\{G_i \mid i \in I\}$ une famille de groupes et $\{N_i \mid i \in I\}$ une famille de sous-groupes distingués des G_i respectivement. Montrer que
   – $\prod_{i\in I}(G_i/N_i) \cong \prod_{i\in I} G_i / \prod_{i\in I} N_i$;
   – $\oplus_{i\in I}(G_i/N_i) \cong \oplus_{i\in I} G_i / \prod_{i\in I} N_i$;

Exercice 1.3 (Produits semidirects)
Soient G et H deux groupes tels qu'il existe un homomorphisme ϕ de H vers $\mathrm{Aut}(G)$. Nous définissons alors sur l'ensemble $G \times H$ la loi interne suivante. Soient $g_1,\ g_2 \in G$ et $h_1,\ h_2 \in H$.

$$(g_1, h_1)(g_2, h_2) = (g_1\phi(h_1)(g_2), h_1h_2)\ .$$

1. Montrer que l'ensemble $G \times H$ muni de la loi décrite ci-dessus est un groupe. C'est le *produit semidirect externe* $G \rtimes_\phi H$. Nous n'utiliserons pas l'indice ϕ quand l'action de H sur G est claire du contexte.
2. Montrer que le produit semidirect externe devient un produit direct externe si et seulement si l'image de ϕ est $\{1\}$.
3. Montrer que le sous-groupe $G \times \{1\}$ est distingué dans $G \rtimes_\phi H$. Montrer que $\{1\} \times H$ est un sous-groupe distingué de $G \rtimes_\phi H$ si et seulement si le produit semidirect est direct.
4. Montrer l'identité suivante
$$(g,1)^{(1,h)^{-1}} = (\phi(h)(g),1) \ .$$
5. Soient G un groupe N et H deux sous-groupes de G tels que $G = NH$, $N \lhd G$, $N \cap H = \{1\}$. Montrer alors que $G \cong N \rtimes_\phi H$, où pour tous $h \in H$ et $n \in N$
$$\phi(h)(n) = n^{h^{-1}} \ .$$
Le groupe G est dit le *produit semidirect interne* de N et H.
Cet isomorphisme et l'identité du point précédent sont importants et pratiques puisqu'ils permettent d'ignorer la différence entre les produits semidirects internes et externes. En fait, ce qui est important, c'est de connaître la nature de l'action du sous-groupe d'automorphismes du sous-groupe distingué sur celui-ci.
6. Montrer que le groupe dans la preuve du théorème 1.2 est isomorphe au produit semidirect externe
$$(K,+) \rtimes_\phi (K^\times,.)$$
où pour tout $t \in K^\times$
$$\begin{array}{rccc} \phi(t) & : & (K,+) & \longrightarrow & (K,+) \\ & & u & \longmapsto & tu \end{array}$$
est un élément de $\mathrm{Aut}((K,+))$.

Exercice 1.4 C'est un exercice d'entraînement sur diverses propriétés des commutateurs.

1. Vérifier les égalités suivantes :
(i) $[x,yz] = [x,z][x,y]^z$,
(ii) $[xy,z] = [x,z]^y[y,z]$,
(iii) $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$,
(iv) $[x,y^n] = [x,y]\dots[x,y]^{y^{n-1}}$ $(n \in \mathbb{N}^*)$,
(v) $[x^n,y] = [x,y]^{x^{n-1}}\dots[x,y]$ $(n \in \mathbb{N}^*)$,
avec $x,y,z \in G$, G étant un groupe quelconque.
2. Soient G un groupe quelconque, H un sous-groupe abélien et $x \in N_G(H)$. Montrer que les applications
$$h \longmapsto [x,h]$$
et
$$h \longmapsto [h,x]$$
sont des endomorphismes de H.
3. Montrer que si G est un groupe, H et K deux sous-groupes de G alors K (resp. H) normalise $[H,K] = \langle [h,k] \mid h \in H,\ k \in K \rangle$. Montrer ensuite que $[H,K]K$ est le plus petit sous-groupe distingué contenant K, en d'autres termes, que c'est un sous-groupe distingué de G et qu'il est contenu dans tout sous-groupe distingué de G contenant K.

Exercice 1.5 (Les groupes nilpotents et les séries centrales *descendantes*)
Dans cet exercice nous étudierons les groupes nilpotents en utilisant les séries centrales descendantes :

$$\gamma_0(G) = G;$$
$$\text{pour tout } k \in \mathbb{N}, \quad \gamma_{k+1}(G) = [G, \gamma_k(G)] \ .$$

1. Montrer que si G est un groupe nilpotent de classe n alors $\gamma_i(G) \leq Z_{n-i}(G)$.
2. Montrer qu'un groupe G est nilpotent de classe n si et seulement si $\gamma_n(G) = 1$, et que pour tout $k < n$, $\gamma_k(G) \neq 1$.
3. Déterminer $\gamma_k(U(n, K))$ pour tout $k \in \mathbb{N}$ dans le groupe $U(n, K)$.

Exercice 1.6 (Propriétés structurelles des groupes nilpotents)
Montrer les énoncés suivants à propos d'un groupe G nilpotent :

1. Si H est un sous-groupe propre, alors $N_G(H) > H$.
2. Tout sous-groupe maximal de G est distingué dans G.
3. Pour tout nombre premier p, si G a un p-sous-groupe P qui est maximal par rapport à cette propriété, alors P est le seul p-sous-groupe maximal de G. Il découle du *lemme de Zorn* qu'il existe un tel sous-groupe maximal.
4. Si $N \lhd G$ et $N \neq \{1\}$, alors $N \cap Z(G) \neq \{1\}$.

Exercice 1.7 (De la nilpotence à la résolubilité)
...il y a un si long chemin qu'il y a même un livre qui s'intitule "Between nilpotent and solvable".

1. Montrer que tout groupe nilpotent est résoluble.
2. Montrer à l'aide d'un exemple que l'énoncé réciproque de celui de (a) est faux. Quel est le plus petit contrexemple ?
3. Soient G un groupe et N un sous-groupe distingué de G. Montrer que G est résoluble si et seulement si G/N et N sont résolubles. Montrer à l'aide d'un exemple que dans l'énoncé précédent on ne peut pas remplacer "résoluble" par "nilpotent".
4. Montrer qu'un groupe G est nilpotent si et seulement si il existe un sous-groupe $Z \leq Z(G)$ tel que G/Z soit nilpotent.

Exercice 1.8 (Between nilpotent and solvable)
Soit H un p-groupe infini et abélien. Pour concrétiser, vous pouvez supposer que H est $\mathbb{Z}_{p^\infty}$, ou $\oplus_{i\in I}(\mathbb{Z}/p\mathbb{Z}, +)$ avec I un ensemble d'indices. Mais tout ce dont nous avons besoin dans le cadre de cet exercice est qu'il soit un p-groupe, infini et abélien. Une fois H fixé, nous définissons un deuxième groupe en utilisant H comme ensemble d'indices : $N = \prod_{x\in H}(\mathbb{Z}/p\mathbb{Z}, +)$. Le groupe H opère sur le groupe N en "permutant les coordonnées", en d'autres termes si $x \in H$ et $f \in N$, alors à la paire (x, f) est associée l'élément $xf \in N$ tel que

$$xf(y) = f(xy) \text{ pour tout } y \in N \ .$$

1. Montrer que pour tout $x \in H$ l'application ϕ qui associe à chaque $f \in N$, $xf \in N$ défini comme ci-dessus est un homomorphisme injectif de H vers $\mathrm{Aut}(N)$. Il en découle que $G = N \rtimes_\phi H$ est un produit semidirect.
2. Vérifier que G est p-groupe.
3. Montrer que G est résoluble. Quelle est sa classe de résolubilité.
4. Montrer que G n'est pas nilpotent.

Exercice 1.9 (Détails de la preuve du théorème 1.2)
Montrer que les sous-ensembles XZ et YZ dans la preuve du théorème 1.1, quand munis de la multiplication usuelle des matrices, forment des sous-groupes. Montrer que $XZ = C_{U(3,K)}(x(1))$ et que $YZ = C_{U(3,K)}(y(1))$.

Montrer que si $x_1 \in XZ$ et $x_1' \in XZ$ tels que $[x_1, y(1)] = z_1$ et $[x_1', y(1)] = z_1$, alors $x_1^{-1}x_1' \in Z$, en d'autres termes, x_1 et x_1' sont dans la même classe de Z.

Montrer que $(Z; +, \bullet, z(0), z(1))$ et $(K; +, ., 0, 1)$ sont deux corps isomorphes.

Exercice 1.10 Le théorème 1.2 a utilisé le sous-groupe U pour "définir" une copie isomorphe au corps K. Définir un corps en utilisant le sous-groupe T comme ensemble sous-jacent.

Exercice 1.11 Fournir les détails manquants de la preuve du théorème 1.3.

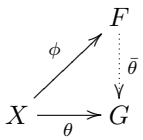
Chapitre 2

Groupes : combinatoire

Dans le premier chapitre nous avons abordé certains aspects algébriques des groupes en vue de la problématique de la théorie des modèles. Ce chapitre a pour objectif de mettre en relief des aspects combinatoires des groupes. Nous introduirons (réviserons ?) la notion de groupe libre dont nous étuiderons certaines propriétés de base. Nous tâcherons de ne pas oublier de faire des liens avec la théorie des modèles.

2.1 Groupes libres : propriétés de base.

Définition 2.1.1 *Soient F un groupe, X un ensemble non vide et ϕ une application de X vers F. Le groupe F est dit* libre *sur X si toute application θ de X vers un groupe G s'étend à un homomorphisme $\bar{\theta}$ et un seul tel que le diagramme suivant soit commutatif :*



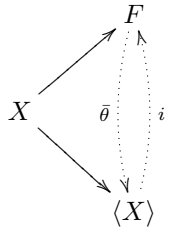
Lemme 2.1.2 *L'application ϕ dans la définition 2.1.1 est injective.*

Preuve. Soient $x_1, x_2 \in X$ tels que $\phi(x_1) = \phi(x_2)$. Si $x_1 \neq x_2$, alors il suffit de considérer un groupe G à au moins deux éléments g_1, g_2 et une application $\theta : X \longrightarrow G$ telle que $\theta(x_1) = g_1$ et $\theta(x_2) = g_2$. L'égalité $\theta = \bar{\theta} \circ \phi$ fournit une contradiction. □

Il s'ensuit de ce lemme que le groupe F de la définition 2.1.1 est libre sur $\phi(X)$ aussi. Par conséquent, un groupe libre est toujours libre sur une de ses parties. Une telle partie sera dite une *base* de F.

Lemme 2.1.3 *Soient F un groupe libre et $X \subset F$. Si F est libre sur X, alors $F = \langle X \rangle$.*

Preuve. Notons d'abord que $\langle X \rangle$ est aussi libre sur X. En effet, il suffit de restreindre l'application $\bar{\theta}$ de la définition 2.1.1 au sous-groupe $\langle X \rangle$. Par conséquent,



où l'application i est l'inclusion du groupe engendré par X tandis que $\bar{\theta}$ est l'application provenant de la définition 2.1.1. Par l'unicité des extensions dans la définition 2.1.1, la composition $i \circ \bar{\theta}$ est l'application identité de F. Par conséquent, si $f \in F$, alors $f = i \circ \bar{\theta}(f) = \bar{\theta}(f)$. □

Les bases d'un groupe libre des propriétés possédées par toute base d'objets universels dans leurs propres catégories :

Lemme 2.1.4 *Soient F_1 et F_2 deux groupes libres sur les bases X_1 et X_2 respectivement. Alors $F_1 \cong F_2$ si et seulement si $|X_1| = |X_2|$. En particulier, toutes les bases d'un groupe libre ont le même cardinal. Sur un ensemble X, à isomorphisme près, il n'existe qu'au plus un groupe libre.*

Preuve. La suffisance de la condition sur les cardinaux des bases est un exercice. Supposons maintenant que $F_1 \cong F_2$ et essayons de vérifier que $|X_1| = |X_2|$. Soit N_i ($i \in \{1, 2\}$) le sous-groupe de F_i engendré par les carrés des éléments de X_i. Alors $N_i \lhd F_i$ et le groupe quotient F_i/N_i est d'exposant 2 ; c'est un espace vectoriel sur le corps $\mathbb{F}_2$. L'isomorphisme entre F_1 et F_2 engendre un isomorphisme entre les quotients F_1/N_1 et F_2/N_2. Ce dernier isomorphisme est aussi un isomorphisme d'espaces vectoriels qui préserve la dimension. Or les dimensions de F_1/N_1 et de F_2/N_2 sont respectivement $|X_1|$ et $|X_2|$. □

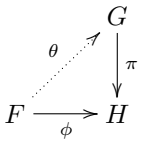
Le cardinal d'une base est donc un invariant d'un groupe libre, le terme utilisé sera *rang*.

La propriété d'extension qui caractérise les groupes libres permet de déduire des conclusions simples mais importantes. En voici quelques'unes :

Lemme 2.1.5 *Soient X et Y deux ensembles, F le groupe libre sur X et G un groupe engendré par Y. Toute surjection de X vers Y s'étend à un homomorphisme surjectif de F vers G. En particulier, tout groupe est l'image d'un groupe libre.*

Preuve. Exercice. □

Lemme 2.1.6 (Propriété projective des groupes libres) *Soient F un groupe libre, G et H deux autres groupes tels qu'il existe un homomorphisme de $\phi : F \longrightarrow H$ et un homomorphisme surjectif de $\pi : G \longrightarrow H$. Alors il existe un homomorphisme θ tel que le diagramme suivant commute :*



Preuve. C'est une autre application de la propriété d'extension définissant un groupe libre. Si X est une base de F, alors $\phi(x) \in \pi(G)$ pour tout $x \in X$,. Il existe alors un homomorphisme θ de F vers G qui étend la restriction de ϕ à la base X. Comme F est engendré par X, θ étend en fait l'homomorphisme ϕ, d'où la commutativité du diagramme. □

La propriété projective caractérise les groupes libres. Néanmoins, la vérification simple de cette conclusion utilise un théorème qui sera introduit dans la section 2.5.

2.2 Groupes libres : construction.

Existe-t-il un groupe libre sur chaque ensemble ? Dans le reste de cette section, nous détaillerons une réponse affirmative à cette question.

Soit X l'ensemble qui sera une base du groupe construit. Dans un premier temps, ce n'est qu'un ensemble de symboles. Nous introduisons deux autres ensembles de symboles :

$$X^{-1} = \{x^{-1} \mid x \in X\} \quad , \quad X^{\pm 1} = X \cup X^{-1} \ .$$

L'ensemble $X^{\pm 1}$ sera notre *alphabet*. Ses éléments seront parfois dits *lettres*. Un *mot* w est une suite $a_1 \dots a_n$ de lettres de $X^{\pm 1}$ avec $n \in \mathbb{N}$. Si $n = 0$, alors $w = 1$, le *mot vide*, qui représentera éventuellement l'élement neutre du groupe qui attend d'être construit.

Sur l'ensemble des mots écrits en utilisant l'alphabet $X^{\pm 1}$, noté $W(X)$, nous définissons une opération qui est celle de la *juxtaposition*. Si $a_1 \dots a_r$ et $b_1 \dots b_s$ sont deux mots alors leur juxtaposition est $a_1 \dots a_r b_1 \dots b_s$. En particulier, un mot non vide est la juxtaposition des membres de $X^{\pm 1}$. Voici des mots qui utilisent l'alphabet $\{a, b, a^{-1}, b^{-1}\}$:

$$a \ , \ b \ , \ ab \ , \ aa^{-1} \ , \ abaa \ .$$

Nous conviendrons que pour tout mot w, $w1 = 1w = w$ et définirons le *mot inverse* d'un mot $w = a_1 \dots a_r$, $w^{-1} = a_r^{-1} \dots a_1^{-1}$.

Deux mots w_1 et w_2 de $W(X)$ seront dits équivalents, noté $w_1 \sim w_2$, si l'un est obtenu de l'autre par une suite finie d'insertions ou de simplifications des suites de la forme xx^{-1} ou $x^{-1}x$ avec $x \in X^{\pm 1}$. Ces insertions ou simplifications sont dites des *transformations élémentaires*.

Lemme 2.2.1 *La relation $\sim$ est une relation d'équivalence sur $W(X)$.*

Preuve. Exercice. □

La classe d'équivalence d'un mot $x \in W(X)$ sera notée $[x]$. La totalité de ces classes sera notée $W(X)/\sim$.

Théorème 2.1 *1. La juxtaposition des mots induit une opération interne bien définie sur $W(X)$:*

$$\text{pour toute paire } (w_1, w_2) \in W(X)^2,\ [w_1][w_2] = [w_1 w_2] \ .$$

2. L'ensemble $W(X)/\sim$ muni de l'opération induite par la juxtaposition des mots est un groupe noté $F(X)$ dont l'élément neutre est la classe $[\,]$ du mot vide, et pour tout $w \in W(X)$, $[w^{-1}] = [w]^{-1}$.

3. Le groupe F est le groupe libre sur X.

Preuve. Les deux premiers points sont des exercices. Essayons de vérifier que F satisfait la propriété d'extension des groupes libres. L'application ϕ de la définition 2.1.1 sera celle qui associe à chaque $x \in X$, la classe $[x]$ dans F. Cette application est injective puisque pour $x_1,\ x_2 \in X$ distincts, $x_1 \not\sim x_2$. Soit G maintenant un groupe quelconque avec $\theta : X \longrightarrow G$ une application de X vers G. Pour tout mot $x_1^{n_1} \dots x_r^{n_r}$ avec $x_i \in X$ et $n_i \in \mathbb{Z}$, nous posons

$$\bar{\theta}([x_1]^{n_1} \dots [x_r]^{n_r}) = \theta(x_1)^{n_1} \dots \theta(x_r)^{n_r} \ .$$

En particulier pour tout $x \in X^{\pm 1}$, $\bar{\theta}([x][x]^{-1}) = \theta(x)\theta(x)^{-1} = 1$. Il en découle que $\bar{\theta}$ est bien définie.

Vérifions maintenant que $\bar{\theta}$ est un homomorphisme. Soient $[w_1]$, $[w_2] \in F$ avec $w_1 = x_1^{m_1} \dots x_r^{m_r}$, $w_2 = y_1^{n_1} \dots y_s^{n_s}$, les m_i, n_j dans $\mathbb{Z}$, et les x_i et y_j dans X. Alors,

$$\begin{aligned} \bar{\theta}([w_1][w_2]) &= \bar{\theta}([w_1 w_2]) \\ &= \theta(x_1^{m_1}) \dots \theta(x_r^{m_r})\theta(y_1^{n_1}) \dots \theta(y_s^{n_s}) \\ &= \bar{\theta}([w_1])\bar{\theta}([w_2]) \end{aligned}$$

Finalement, il reste à vérifier l'unicité de $\bar{\theta}$. Si θ' est une autre application telle que $\theta'\phi = \theta$, alors $\bar{\theta}$ et θ' associe les mêmes images aux éléments de $\langle \phi(X) \rangle$. Or, d'après le lemme 2.1.3, ce dernier sous-groupe est F tout entier. □

2.3 Mots réduits, formes normales

Dans cette section, nous continuerons d'utiliser la même notation que celle des précédentes. La construction de la section précédente utilise la combinatoire des mots dans un groupe libre et de leurs classes d'équivalence par rapport aux transformations élémentaires. C'est une question naturelle si ces classes ont des représentants canoniques. La réponse affirmative à cette question fait intervenir une notion importante : celle d'un *mot réduit*.

Avant de définir ce qu'est un mot réduit, nous introduisons une notion de *longueur de mot*. Pour un élément $w \in W(X)$ de la forme $w = x_1 \dots x_n$ avec $x_i \in X^{\pm 1}$, la longueur de w, notée $|w|$, est n. Notons que le mot vide est de longueur 0, et qu'avec cette notion de longueur deux mots équivalents mais distincts peuvent avoir différentes longueurs, en d'autres termes, cette notion de longueur, n'est pas uniquement définie pour les éléments de F. Aboutir à une notion bien définie équivaut en fait à trouver des représentants canoniques pour les classes d'équivalences par rapport à $\sim$.

Un mot de $W(X)$ est dit *réduit* s'il ne contient pas de suite de type xx^{-1} où $x \in X$. Comme chaque mot est de longueur finie, toute classe d'équivalence par rapport à $\sim$ a un représentant réduit.

Lemme 2.3.1 *Deux mots réduits sont équivalents si et seulement si ils sont égaux.*

Preuve. Soient u et v deux mots réduits et équivalents. Par l'absurde, supposons-les distincts. Alors, il existe une suite de transformations élémentaires

$$w_0 = u \quad \sim \quad w_1 \quad \sim \quad w_2 \quad \sim \quad \dots \quad \sim \quad w_n = v$$

telle que $n > 1$. Parmi ces suites, nous fixons une telle que n soit minimal. Alors, comme $n > 1$ et que u est réduite, $|u| < |w_1|$. Pour des raisons similaires, $|w_{n-1}| > |v|$. En particulier, il existe $i \in \{1, \dots, n-1\}$ tel que $|w_{i-1}| < |w_i|$ et $|w_{i+1}| < |w_i|$. Nous étudierons le plus petit i ayant cette propriété. Trois cas se présentent :

(i) Les transformations élémentaires de w_{i-1} à w_i et de w_i à w_{i+1} impliquent l'insertion et la simplification des mêmes lettres a et a^{-1} de $X^{\pm 1}$ au même endroit de w_i. Dans ce cas, $w_{i-1} = w_{i+1}$ et nous pouvons enlever de notre suite w_i et w_{i+1}, ce qui contredit le choix minimal de n.

(ii) Les transformations élémentaires de w_{i-1} à w_i et de w_i à w_{i+1} impliquent l'insertion et la simplification des mêmes lettres x et x^{-1} de $X^{\pm 1}$ aux endroits distincts mais avec intersection non vide. Alors, w_i possède une suite de la forme $xx^{-1}x$ ($x \in X^{\pm 1}$), et, suite à l'insertion et à la simplification, nous aboutissons encore une fois à la conclusion que $w_{i-1} = w_{i+1}$. C'est donc une contradiction.

(iii) Les transformations élémentaires de w_{i-1} à w_i et de w_i à w_{i+1} impliquent l'insertion et la simplification des suites xx^{-1} et yy^{-1} ($x,\ y \in X^{\pm 1}$) respectivement, à des endroits sans intersection. Or, comme u est réduit, l'insertion de yy^{-1} a eu lieu à une étape (w_{j-1},w_j) qui précède w_{i-1}. Comme i a été choisi minimal, quitte à permuter les w_j ($j < i-1$), nous pouvons supposer que yy^{-1} était inséré à l'étape (w_{i-2}, w_{i-1}). Alors, la suite des tranformations élémentaires

$$u \quad \sim \quad \dots \quad w_{i-2} \quad \sim \quad w_{i+1} \quad \sim \quad \dots \quad \sim \quad v$$

est plus courte que notre choix minimal du début. Cette dernière contradiction élimine le dernier cas. □

Dans la suite, afin de simplifier la notation, nous éviterons les crochets dans l'écriture des éléments de F. Il s'ensuit de cela que, quitte à fixer une base de F, tout élément $w \in F$ aura une écriture unique, dite *la forme normale* de w par rapport à X :

$$w = x_1^{n_1} \dots x_r^{n_r} \ ,$$

où tout $r \in \mathbb{N}$, $x_i \in X$, tout $n_i \in \mathbb{Z}^*$, et pour tout $i \in \{1, \dots, r-1\}$ $x_i \neq x_{i+1}$. Notre travail jusqu'à ce point montre que chaque élément peut s'écrire sous forme normale. En fait, dans un groupe G, l'existence pour tout élément d'une forme normale par rapport à un sous-ensemble X caractérise que G est libre :

Lemme 2.3.2 *Soient G un groupe et X une partie de G. Alors G est un groupe libre avec base X si et seulement s'il existe une forme normale par rapport à X et une seule pour tout élément $g \in G$.*

Preuve. Pour déduire la suffisance de la condition, il suffira d'utiliser la définition 2.1.1. □

Le lemme suivant se vérifie en utilisant les formes normales :

Lemme 2.3.3 *Soient X, Y deux ensembles, $\iota : X \longrightarrow Y$ une injection de X vers Y, et $F(X)$ $F(Y)$ les groupes libres sur X et Y respectivement. Alors, ι s'étend à un homomorphisme injectif et un seul de $F(X)$ vers $F(Y)$.*

Preuve. L'existence d'un homomorphisme de $F(X)$ vers $F(Y)$ est une conséquence de la propriété d'extension des groupes libres. L'injectivité découle de l'unicité de la forme normale représentant un élément d'un groupe libre. □

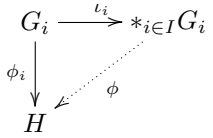
Ce lemme permet de voir un groupe libre comme un sous-groupe d'un autre quand il existe une injection d'une base de celui-ci vers une base du premier. Si X est une base pour un groupe libre et $X_0 \subset X$, alors l'inclusion induit le *plongement canonique* de $F(X_0)$ dans $F(X)$.

L'exercice 2.5 contient d'autres propriétés simples des groupes libres qui sont vérifiées en utilisant les formes normales.

2.4 Produits libres

Comme les groupes libres, les produits libres ont une définition "catégorique". En fait, un produit libre est un *coproduit* dans la catégorie des groupes.

Définition 2.4.1 *Soit $\{G_i \mid i \in I\}$ une famille de groupes. Un groupe $*_{i\in I}G_i$ est dit d'être le* produit libre *des G_i s'il existe des homomorphismes $\iota_i : G_i \longrightarrow G$ qui satisfont la propriété suivante : pour tout groupe H et toute famille d'homomorphismes $\{\phi_i \mid i \in I,\ \phi_i : G_i \longrightarrow H\}$, il existe un homomorphisme ϕ et un seul tel que tout diagramme*



commute.

Si I est une famille finie, parfois nous écrirons $G_1 * \ldots * G_k$ ou $*_{i=1}^{k}G_i$.

Pour motiver la définition, donnons un exemple de produit libre : si F est un groupe libre sur un ensemble X alors, $F \cong *_{i\in X}\mathbb{Z}$. Ceci se justifiera une fois que nous aurons donné la recette générale pour construire le produit libre d'une famille de groupes arbitraires (voir l'exerice 2.9).

Lemme 2.4.2 *Les homomorphismes ι_i dans la définition 2.4.1 sont injectifs.*

Preuve. Soient $g, g' \in G_i$ deux éléments distincts. Prenons pour H dans la définition 2.4.1 le groupe G_i, et pour ϕ_i l'application identité. Il en découle que $\iota(g) \neq \iota(g')$. □

Lemme 2.4.3 *A isomorphisme près, le produit libre d'une famille de groupes est unique.*

Preuve. Exercice. □

Lemme 2.4.4 *Le produit libre $*_{i\in I}G_i$ est engendré par les images $\iota_i(G_i)$.*

Preuve. Soit $H = \langle \iota_i(G_i) \mid i \in I \rangle$. Le groupe H est aussi un produit libre des G_i. En effet, il suffit de restreindre ϕ au sous-groupe H. Maintenant l'énoncé est démontré en appliquant le même raisonnement que celui du lemme 2.1.3. □

Comme dans le cas des groupes libres, il existe une question d'existence du produit libre d'une famille non vide de groupes. Le théorème suivant règle cette question de façon similaire à la section 2.2.

Théorème 2.2 *Soit $\{G_i \mid i \in I\}$ une famille non vide de groupes libres. Alors, le produit libre des G_i existe.*

Preuve. Soit $\mathcal{U}$ l'union disjointe des G_i. Un *mot* sur $\mathcal{U}$ est une suite finie

$$g_1 \dots g_r, \quad g_i \in G_i \ .$$

Le mot vide correspond au cas où $r = 0$.

Pour aboutir à une structure de groupe, dans un premier temps l'ensemble $\mathcal{W}(\mathcal{U})$ des mots sur $\mathcal{U}$ est muni de la juxtaposition qui suppose que $g1 = 1g = g$. L'inverse d'un mot non vide $g_1 \dots g_r$ est défini comme $g_r^{-1} \dots g_1^{-1}$, et $1^{-1} = 1$.

Nous définirons une relation d'équivalence sur $\mathcal{W}(\mathcal{U})$. Pour ce faire les opérations suivantes sur un mot sont introduites :

1. insertion de l'élément neutre d'un G_i ;
2. effacement de l'élément neutre d'un G_i ;
3. (contraction) remplacement de deux éléments consécutifs appartenant au même G_i par leur produit ;
4. (expansion) remplacement d'un élément d'un G_i par deux éléments consécutifs appartenant au même G_i dont il est le produit.

Nous dirons que deux mots g et h dans $\mathcal{W}(\mathcal{U})$ sont équivalents, noté $g \sim h$ si l'un est obtenu à partir de l'autre suite à un nombre fini des opérations introduites ci-dessus. C'est un exercice de vérifier que $\sim$ est une relation d'équivalence, et que la juxtaposition et l'inversion induisent respectivement une opération interne et une inversion bien définies sur l'ensemble $\mathcal{W}(\mathcal{U})/\sim$:

$$\text{pour tout } g,\ h \in \mathcal{U}, [g][h] = [gh] \quad , \quad [g]^{-1} = [g^{-1}] \ .$$

Nous obtenons donc une structure de groupe sur $\mathcal{W}(\mathcal{U})/\sim$ dont l'élément neutre est la classe de 1.

Nous procédons à vérifier que $\mathcal{W}(\mathcal{U})$, munie des opérations indiquées dans le paragraphe précédent, est le produit libre de $\{G_i \mid i \in I\}$. Pour chaque $i \in I$, ι_i est l'application qui associe à tout $g \in G_i$, sa classe $[g]$ dans $\mathcal{W}(\mathcal{U})/\sim$. C'est un homomorphisme.

Vérifions que la propriété d'extension d'homomorphismes est satisfaite. Pour ce faire, soit H un groupe et $\phi_i : G_i \longrightarrow H$ un homomorphisme pour chaque $i \in I$. L'application $\phi : \mathcal{W}(\mathcal{U}) \longrightarrow H$ recherchée est définie comme celle qui associe à tout $[g]$, l'élément $\phi_{i_1}(g_{i_1}) \dots \phi_{i_r}(g_{i_r})$ où $g_{i_1} \dots g_{i_r}$ est un représentant de la classe de $[g]$. L'application ϕ, quoique dépendante du choix de représentant, est définie sans ambiguité grâce aux opérations (1)-(4) ci-dessus. Par ailleurs, pour tout $i \in I$ et $g \in G_i$, $\phi(\iota_i(g)) = \phi([g]) = \phi_i(g)$. Cette vérification de la commutativité du diagramme de la définition 2.4.1 montre aussi qu'une autre extension ϕ' a la même définition sur chaque G_i que ϕ. L'unicité de ϕ en découle. Le groupe $\mathcal{W}(\mathcal{U})/\sim$ est le produit libre $*_{i\in I}G_i$. □

La construction du théorème 2.2 motive la question d'un représentant canonique d'une classe $[g] \in \mathcal{W}(\mathcal{U})/\sim$:

Définition 2.4.5 *Un mot $g \in \mathcal{W}(\mathcal{U})$ est dit* réduit *si aucun des symboles dans son écriture n'est l'élément neutre d'un G_i et si deux symboles distincts consécutifs dans son écriture appartiennent à deux G_i distincts.*

Afin de simplifier l'écriture, nous éviterons l'usage des crochets. En d'autres termes nous ne ferons pas de distinction entre les G_i formant un produit libre et leurs images $\iota_i(G_i)$ dans $*_{i\in I}G_i$. Ceci fournit comme dans le cas des groupes libres la notion de la *forme normale* d'un élément de $*_{i\in I}G_i$. En fait, pour tout élément de $*_{i\in I}G_i$ ce n'est que le mot réduit qui le présente.

Théorème 2.3 *Soit $\{G_i \mid i \in I\}$ une famille de groupes. Tout élément du produit libre $*_{i\in I}G_i$ est représenté par un mot réduit et un seul.*

Preuve. Comme chaque mot est de taille finie, les opérations (2) et (3) se stabilisent au bout d'un nombre fini d'étapes. Le mot obtenu est réduit.

Afin de montrer l'unicité de la forme normale d'un élément, nous montrerons que pour tout $g \in *_{i\in I}G_i$, nous montrons d'abord que si $g_{i_1} \dots g_{i_n}$ est une formale normale de G et que $n > 0$, alors $g_{i_1} \dots g_{i_n} \neq 1$. Notons $\mathcal{W}_0$ l'ensemble de tous les mots réduits. Pour tout $i \in I$ et tout $g \in G_i$, nous définissons l'application $\bar{g}$ de $\mathcal{W}_0$ vers lui-même de la façon suivante :

$$\bar{g}(g_{i_1} \dots g_{i_n}) = \begin{cases} gg_{i_1} \dots g_{i_n} & \text{si} \quad g \notin G_{i_1} \\ (gg_{i_1})g_{i_2} \dots g_{i_n} & \text{si} \quad g \in G_{i_1} \\ g_{i_2} \dots g_{i_n} & \text{si} \quad g_{i_1} = g^{-1} \end{cases}$$

L'application $\bar{g}^{-1}$ définie de façon similaire est l'inverse de $\bar{g}$. Donc, $\bar{g} \in \mathrm{Sym}(\mathcal{W}_0)$, le groupe de permutations des mots réduits. Ces permutations induisent un homomorphisme

$$\begin{array}{ccc} *_{i\in I}G_i & \longrightarrow & \mathrm{Sym}(\mathcal{W}_0) \\ g & \longmapsto & \bar{g} = \bar{g}_{i_1} \circ \dots \circ \bar{g}_{i_n} \end{array}$$

où $g_{i_1} \dots g_{i_n}$ est un mot réduit représentant g. La permutation $\bar{g}$ envoie le mot vide à $g_{i_1} \dots g_{i_n}$. Ceci montre que si $g \neq 1$ si elle est représentée par un mot réduit non vide.

Du paragraphe précédent découle l'unicité de la forme normale (ou d'un mot réduit représentant un élément de $*_{i\in I}G_i$) par récurrence sur la longueur de deux mots réduits équivalents. C'est un exercice. □

Comme dans les groupes libres, l'existence d'une forme normale équivaut en fait à l'existence d'un produit libre :

Lemme 2.4.6 *Soit G un groupe engendré par une famille $\{G_i \mid i \in I\}$ de sous-groupes G_i. Alors $G = *_{i\in I}G_i$ si et seulement si tout élément de G a une écriture unique de la forme $g_{i_1} \dots g_{i_k}$ où chaque $g_{i_j} \in G_{i_j} \setminus \{1\}$ et $i_j \neq i_{j+1}$.*

Preuve. Pour déduire la suffisance de la condition, il suffit d'appliquer la définition du produit libre. □

2.5 Un peu de théorie des modèles

Dans cette section, nous démontrerons un résultat modeste qui néanmoins illustre la force des hypothèses de la théorie des modèles. Nous déduirons des propriétés simples des sous-groupes *élémentaires* (au sens de la théorie des modèles) d'un groupe libre de type fini.

Commençons par les notions de la théorie des modèles.

Définition 2.5.1 *Soient $\mathcal{L}$ un langage du premier ordre, $\mathcal{M}$ et $\mathcal{N}$ deux $\mathcal{L}$-structures telles que $\mathcal{M}$ soit une sous-structure de $\mathcal{N}$. La structure $\mathcal{M}$ est une* sous-structure élémentaire *de $\mathcal{N}$, ou $\mathcal{N}$ est une* extension élémentaire *de $\mathcal{M}$ si pour toute formule $\phi(x_1, \dots, x_k)$ de $\mathcal{L}$ et $\overline{m} = (m_1, \dots, m_k) \in M^k$, $\mathcal{M} \models \phi[\overline{m}]$ si et seulement si $\mathcal{N} \models \phi[\overline{m}]$. Dans ce cas, nous écrirons $\mathcal{M} \preceq \mathcal{N}$, la notation $\mathcal{M} \prec \mathcal{N}$ étant réservée pour le cas où $M \neq N$.*

De façon équivalente, par rapport au langage $\mathcal{L}(M)$ obtenu en ajoutant à $\mathcal{L}$ un symbole de constante pour nommer chaque élément de l'ensemble sous-jacent M de $\mathcal{M}$, les structures $(\mathcal{M}, m)_{m\in M}$ et $(\mathcal{N}, m)_{m\in M}$ sont élémentairement équivalentes. En particulier, si $\mathcal{M} \preceq \mathcal{N}$, alors $\mathcal{M} \equiv \mathcal{N}$.

S'il existe un plongement ϕ de $\mathcal{M}$ vers $\mathcal{N}$ tel que $\phi(\mathcal{M}) \preceq \mathcal{N}$, alors ϕ est dit un plongement élémentaire.

Les groupes libres fournissent une illustration claire des relations d'élémentarité, quoique à un prix élevé. En effet, le théorème suivant de Zlil Sela est non trivial :

Fait 2.5.2 [13] *Deux groupes libres de rangs finis au moins deux sont élémentairement équivalents. Plus généralement, soient $m, n \in \mathbb{N} \setminus \{0, 1\}$ tels que $m \leq n$. Alors le plongement canonique d'un groupe libre à m générateurs dans un groupe libre à n générateurs est élémentaire.*

Dans sa thèse de doctorat, Chloé Perin a obtenu l'inverse de ce résultat comme corollaire d'un théorème sur les groupes *hyperboliques* sans torsion :

Fait 2.5.3 [6] *Si F est un groupe libre de type fini et $H \preceq F$ (un sous-groupe élémentaire) alors il existe $K \leq F$ tel que $F = H * K$.*

Le résultat que nous démontrerons dans cette section, toujours de la thèse de Perin, est beaucoup plus simple... quitte à admettre certains théorèmes classiques sur les groupes et produits libres :

Théorème 2.4 [6] *Soient F un groupe libre de type fini et $H \preceq F$. Alors*

1. *le rang de H est inférieur ou égal à celui de F ;*
2. *H est un retract de F.*

Définition 2.5.4 *Soient G un groupe et H un sous-groupe de G. Le sous-groupe H est dit un* retract *de G s'il existe un homomorphisme surjectif π de G vers H tel que $\pi^2 = \pi$. De façon équivalente, π est l'identité sur H. L'homomorphisme π est dit une* rétraction.

Question non mathématique : Quel est un bon synonyme en français de "retract" ?

La preuve utilisera deux théorèmes classiques de la théorie combinatoire des groupes : le théorème de Nielsen-Schreier sur les sous-groupes des groupes libres et celui de Kuros sur les sous-groupes des produits libres. Ce sont deux résultats ayant un bon nombre de preuves distinctes et abordables. Néanmoins les preuves connues par l'auteur de ces lignes sont toutes trop longues pour être abordées ici.

Fait 2.5.5 (Nielsen-Schreier) [5, 12] *Tout sous-groupe d'un groupe libre est libre.*

Fait 2.5.6 (Kuros) [5, 12] *Soient $\{G_i \mid i \in I\}$ une famille de groupes et H un sous-groupe de leur produit libre $*_{i\in I} G_i$. Alors H est de la forme $H_0 * (*_{i\in I}(H \cap G_i^{x_i}))$ où H_0 est un groupe libre tandis que les x_i décrivent des représentants des (H, G_i)-classes doubles.*

Notons que chacun de ces deux énoncés peut être rendus plus précis et riches en information. En particulier, les relations entre les rangs d'un groupe libre et de ses sous-groupes peuvent être assez compliqués. Nous nous contentons de ce qui est nécessaire pour cette section.

Preuve du théorème 2.4. Soient F et H comme dans l'énoncé du théorème. Montrons le point (1). Par hypothèse, le rang de F est n avec n un nombre naturel au moins 2. Soient $X = \{x_1, \ldots, x_n\}$ une base de F, et Y une base de H dont nous supposons par l'absurde que le cardinal soit au moins $n+1$. Fixons arbitrairement $n+1$ membres distincts de Y : $h_1, \ldots, h_{n+1}$. Chacun de ces éléments s'écrit en fonction des $x_1, \ldots, x_n$, que nous pouvons même supposer de façon unique bien que ce ne soit pas nécessaire ici : $h_j = w_j(x_1, \ldots, x_n)$ $(1 \leq j \leq n+1)$.

Considérons l'énoncé suivant dans le langage des groupes augmenté par un symbole de constante pour chaque élément de H :

$$(*) \quad \exists x_1 \ldots x_n \bigwedge_{k=1}^{n+1} h_k = w_k(x_1, \ldots, x_n) \ .$$

Cet énoncé est vrai dans la structure $(F, h)_{h\in H}$. Comme $H \preceq F$, il existe $y_1, \ldots, y_n \in H$ tels que

$$(H, h)_{h\in H} \models \bigwedge_{k=1}^{n+1} h_k = w_k(y_1, \ldots, y_n)$$

Posons $H_0 = \langle h_1, \ldots, h_{n+1}\rangle$ et $H_1 = \langle y_1, \ldots, y_n\rangle$. Alors,

$$H_0 \leq H_1 \leq H \ .$$

D'après le fait 2.5.5, H est un groupe libre. Par conséquent, il en est de même pour H_0 et H_1. Comme l'ensemble $\{h_1, \ldots, h_{n+1}\}$ appartient à une base de H, $H = H_0 * H_0'$. D'après le fait 2.5.6, H_1 est un produit libre dont un facteur est $H_1 \cap H_0 = H_0$. Or, H_1 est de rang n tandis que son facteur libre H_0 est de rang $n+1$, une contradiction.

Il reste à démontrer le deuxième point pour lequel la finitude du rang de H est suffisante. En effet, il suffira de savoir qu'il existe $y_1, \ldots, y_n \in H$ tels que tout générateur de H s'écrive comme des mots en ces n éléments, et pour ce faire, un énoncé du premier ordre (donc de taille finie) comme (*) est suffisant. Soit n_H le rang de H. L'application qui associe à chaque x_i de X $y_i \in Y$ s'étend à un homomorphisme surjectif de F vers H. On obtient alors les égalités suivantes pour tout $k \in \{1, \ldots, n_H\}$:

$$f(h_k) = f(w_k(x_1, \ldots, x_n)) = w_k(y_1, \ldots, y_n) = h_k \ .$$

Le point (2) est vérifié. □

Dans cette section, nous avons étudié une question de la théorie des modèles des groupes libres. Elle est bien différente des deux premiers résultats du premier chapitre, plus proche des discussion autour de la simplicité bornée et donc du théorème 1.3 en raison de ses liens avec le passage aux extensions ou restrictions élémentaires. Néanmoins, la "définissabilité" joue un rôle important. Faisons un autre lien avec le premier chapitre en mentionnant un problème ouvert sur les groupes libres :

Question de recherche : Peut-on définir un corps dans un groupe libre ?

2.6 Exemples de produits libres

Jusqu'à maintenant, nous nous sommes contentés des recettes de construction générales pour les groupes et produits libres. Or, c'est une autre question de "reconnaître" un groupe ou produit libre au sein d'un groupe donné sous une autre forme. C'est une question qui peut s'avérer difficile et qui par conséquent peut nécessiter d'élaborer de nouvelles techniques. L'une des plus simples de ces techniques est le lemme de pingpong :

Lemme 2.6.1 (Lemme de pingpong) [5] *Soit G un groupe opérant sur un ensemble Ω par permutations et engendré par deux sous-groupes G_1 et G_2. Si Ω_1 et Ω_2 sont deux parties disjointes et non vides de Ω tels que*

$$\textit{pour tout } \ g_1 \in G_1^{\times}, \quad g_1\Omega_1 \subset \Omega_2 \ ,$$

$$\textit{pour tout } \ g_2 \in G_2^{\times}, \quad g_2\Omega_2 \subset \Omega_1 \ .$$

et que $|G_1| > 2$, alors G est le produit libre de G_1 et G_2.

Notons que dans l'énoncé la notation $g_1\Omega_1$ est utilisée pour noter l'action du groupe sur l'ensemble Ω.

Preuve. Soient g_1, g_2 deux éléments non triviaux et distincts de G_1. Alors $g_1^{-1}g_2 \in G_1^{\times}$, et par conséquent, $g_1^{-1}g_2\Omega_1 \cap \Omega_1 = \emptyset$. De façon équivalente, $g_1\Omega_1 \cap g_2\Omega_1 = \emptyset$. Alors $g_1\Omega$ est un sous-ensemble propre de Ω_2. Le même type de raisonnement s'applique à G_2 et Ω_2 aussi.

Nous utiliserons la remarque du paragraphe précédent pour montrer que tout mot réduit du type $w = g_1 g_2 \dots g_{2n-1} g_{2n}$, avec $n \in \mathbb{N}^*$, tel que les éléments à indice impair soient dans G_1 tandis que les autres sont dans G_2, est différent de l'élément neutre. La même conclusion pour toutes les formes normales découle de ce cas particulier (voyez-vous pourquoi ?). Or d'après le premier paragraphe, $g_{2n}\Omega_2 \subsetneq \Omega_1$ et $g_{2n-1}g_{2n}\Omega_2 \subsetneq \Omega_2$. Alors par récurrence, $w\Omega_2$ est une partie propre de Ω_2. Une telle conclusion ne serait pas possible si w était l'élément neutre.

Comme nous avons déjà indiqué dans la preuve du théorème 2.3 (voir aussi l'exercice 2.6), la conclusion du paragraphe précédent suffit à conclure que $G = G_1 * G_2$. □

Une question naturelle est ce qui se passe si dans le lemme 2.6.1, quand les deux groupes sont d'ordre 2. Dans ce cas, il y a deux possibilités. En effet, si $G_1 = \{1, x\}$ et $G_2 = \{1, y\}$, alors soit xy est d'ordre infini et $G \cong \langle x \rangle * \langle y \rangle$ qui est le groupe diédral infini ; soit xy est d'ordre fini n, et G est le groupe diédral d'ordre $2n$, noté parfois D_n. Ce deuxième cas n'est bien sûr pas le produit libre des deux groupes (voir aussi l'exercice 2.11).

Avant de passer à des applications du lemme de pingpong, soulignons que dans la preuve du théorème 2.3, nous avons d'une certaine manière joué au pingpong dans le groupe libre.

Pour finir, nous utiliserons le lemme de pingpong pour etudier certains sous-groupes libres du groupe $\mathrm{GL}_2(\mathbb{C})$ de matrices 2×2 à entrées complexes de déterminants non nulles. Ce groupe agit sur la droite projective complexe $\mathbb{C} \cup \{\infty\}$ par les transformations de Möbius,

$$z \longmapsto \frac{az+b}{cz+d} \text{ avec } a,\ b,\ c,\ d \in \mathbb{C} \text{ et } ad - bc \neq 0 .$$

Ces dernières forment un groupe Γ quand muni de la composition des applications. En effet, il existe un homomorphisme de $\mathrm{GL}_2(\mathbb{C})$ vers Γ qui associe à chaque matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

la transformation $z \longmapsto \frac{az+b}{cz+d}$. Le noyau de cet homomorphisme est le centre de $\mathrm{GL}_2(\mathbb{C})$, formé par les matrices scalaires $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, avec $\lambda \in \mathbb{C}^*$. Nous fixons $u \in \mathbb{C}$ tel que $|u| \geq 2$ et définissons deux éléments de Γ :

$$\begin{array}{rccc} \alpha & : & \mathbb{C}\cup\{\infty\} & \longrightarrow & \mathbb{C}\cup\{\infty\} \\ & & z & \longmapsto & z+u \end{array} \qquad \begin{array}{rccc} \beta & : & \mathbb{C}\cup\{\infty\} & \longrightarrow & \mathbb{C}\cup\{\infty\} \\ & & z & \longmapsto & \frac{z}{uz+1} \end{array} .$$

Soient maintenant $\Omega_1 = \{z \in \mathbb{C} \mid |z| < 1\}$ et $\Omega_2 = \{z \in \mathbb{C} \mid |z| > 1\}$. Le choix de la norme du vecteur u montre que toute puissance de α envoie Ω_1 dans Ω_2. Ce constat et le fait que $\beta = \gamma\alpha\gamma$ où γ est l'application $z \longmapsto \frac{1}{z}$, montrent que β envoie Ω_2 dans Ω_1. Par conséquent, le lemme de pingpong permet de conclure que $\Gamma = \langle \alpha \rangle * \langle \beta \rangle$. Par ailleurs, comme α et β sont d'ordre infini, Γ est un groupe libre à deux générateurs.

Maintenant, étendons notre conclusion du paragraphe précédent à certains sous-groupes de $\mathrm{GL}_2(\mathbb{C})$. Soit Γ_1 le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les matrices

$$A = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \ , \ B = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} .$$

L'application qui associe α et β à A et B respectivement n'est que la restriction de l'homomorphisme susmentionné de $\mathrm{GL}_2(\mathbb{C})$ vers Γ. Elle s'étend en particulier au sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par α et β. L'existence et l'unicité des formes normales dans $\langle \alpha, \beta \rangle$ nécessite la même conclusion dans $\langle A, B \rangle$. Par conséquent, $\langle A, B \rangle = \langle A \rangle * \langle B \rangle$, de façon équivalente, $\langle A, B \rangle$ est un groupe libre à deux générateurs.

En utilisant des raisonnements similaires mais un peu plus compliqués, il est possible de montrer que

$$\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/Z(\mathrm{SL}_2(\mathbb{Z})) \cong \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} .$$

Exercices

Exercice 2.1 Fournir les détails manquants de la preuve du lemme 2.1.4.

Exercice 2.2 Fournir les détails manquants de la preuve du lemme 2.2.1 et et du théorème 2.1.

Exercice 2.3 Démontrer que la propriété projective des groupes libres les caractérise.

Exercice 2.4 Soient F un groupe libre et G un sous-groupe *caractéristique* de F. Montrer que si $G < F$ alors G ne contien aucun générateur de F.

Exercice 2.5 1. Montrer que les groupes libres sont sans torsion.

2. Montrer que pour tout groupe libre F, $Z(F) = \{1\}$ si et seulement si F est de rang strictement supérieur à 1.

Exercice 2.6 Dans la preuve du théorème 2.3, vérifier l'unicité de la forme normale.

Exercice 2.7 Démontrer le lemme 2.3.2.

Exercice 2.8 1. Montrer que les groupes suivants ne sont pas libres :
(a) tout groupe fini,
(b) $(\mathbb{Q}, +)$,
(c) $U(3, K)$ avec K un corps commutatif quelconque.

2. Montrer que pour tout groupe libre F, $F' < F$.

Exercice 2.9 Montrer que si F est le groupe libre sur l'ensemble X, alors $F \cong *_{x \in X} \mathbb{Z}$.

Exercice 2.10 Montrer que le produit libre $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ est isomorphe au produit semi-direct $(\mathbb{Z}, +) \rtimes \langle \alpha \rangle$ où α est l'automorphisme de $(\mathbb{Z}, +)$ décrit par la loi $k \mapsto -k$.

Exercice 2.11 Soit $\{G_i \mid i \in I\}$ une famille de groupes. Vérifier les propriétés suivantes du produit libre $*_{i \in I} G_i$.

1. Un élément dont la forme normale est de la forme $g_{i_1} \dots g_{i_k}$ avec $k \geq 2$ tel que $i_1 \neq i_k$ est d'ordre infini. En particulier, si $|I| \geq 2$, alors $*_{i \in I} G_i$ est d'ordre infini.
2. Tout élément d'ordre fini dans $*_{i \in I} G_i$ est conjugué à un élément dans un G_i.
3. Pour tout $i \in I$ et $g \in G_i \setminus \{1\}$, $C_{G_i}(g) \leq G_i$.

Exercice 2.12 Soient G_1 et G_2 deux groupes. Montrer que $G_1 * G_2 \cong G_2 * G_1$.

Chapitre 3

Théorie des modèles des groupes, compacité en action

Dans ce chapitre, nous étudierons des classes de groupes et certaines de leurs propriétés selon l'optique suivante : est-ce que ces propriétés sont préservées par passage aux groupes élémentairement équivalentes, existe-t-il des extensions élémentaires ayant des propriétés particulières qui ne sont pas nécessairement celles du groupe de départ ? Tout au long de notre discussion, cette optique générale nous permettra d'aborder des questions liées ainsi que d'introduire de nouvelles classes de groupes. Dans certaines des preuves, le théorème de compacité sera clé.

3.1 Chauffons les esprits

Commençons par la question la plus basique. Soit $\mathcal{L} = \{., \ ^{-1}, 1\}$ le langage des groupes, les symboles ayant leurs interprétations usuelles. En particulier, un groupe est une $\mathcal{L}$-structure. Est-ce qu'une $\mathcal{L}$-structure élémentairement équivalente à un groupe est un groupe ? Votre réponse doit être : "Evidemment." Si ce n'est pas le cas, il est temps de faire des révisions. Nous pouvons allonger la liste de questions évidentes : est-ce qu'un groupe élémentairement équivalent à un groupe abélien est abélien. Votre réponse ne doit pas être différente, ni dans la forme ni dans le fond.

Posons maintenant une question dans le même esprit que la deuxième mais dont la réponse est moins évidente. Est-ce qu'une $\mathcal{L}$-structure élémentairement équivalente à un groupe nilpotent est nilpotent ? Introduisons une notation :

$$\text{pour tout } n \in \mathbb{N} \quad [x_1, \ldots, x_{n+1}] = [[x_1, \ldots, x_n], x_{n+1}] \ .$$

Il est sous-entendu que $[x] = x$.

Lemme 3.1.1 *Si G est un groupe nilpotent, alors pour tout $k \in \mathbb{N}^*$*

$$\gamma_k(G) = \langle [x_1, \ldots, x_{k+1}] \mid x_1, \ldots, x_{k+1} \in G \rangle \ .$$

Preuve. Notons H_k le groupe $\langle [x_1, \ldots, x_{k+1}] \mid x_1, \ldots, x_{k+1} \in G \rangle$. Comme chaque x_i dans la définition de H_k est un élément arbitraire de G, $H_k \lhd G$. Par conséquent, G/H_k est un groupe et les groupes H_k forment une suite descendante.

Supposons d'abord G nilpotent. Nous procéderons par récurrence sur k. Pour $k = 0$, il n'y a rien à faire puisque $\gamma_0(G) = G$.

Par définition, tout commutateur de type $[x_1, \ldots, x_{k+1}]$ appartient à $\gamma_k(G)$. Ainsi, $H_k \leq \gamma_k(G)$. Le quotient G/H_k est un groupe nilpotent, et par récurrence pour tout $i \in \{1, \ldots, k-1\}$

$$\gamma_i(G/H_k) = \gamma_i(G)H_k/H_k = H_iH_k/H_k = H_i/H_k = \gamma_i(G)/H_k \ .$$

Par conséquent, $\gamma_{k-1}(G)/H_k = H_{k-1}/H_k \leq Z(G/H_k)$. Ainsi $\gamma_k(G) \leq H_k$. Notons que la première égalité ci-dessus nécessite un petit raisonnement par récurrence, c'est un exercice. □

Lemme 3.1.2 *Soit $n \in \mathbb{N}^*$. Un groupe G est nilpotent de classe exactement n si et seulement si $[x_1, \ldots, x_n, x_{n+1}] = 1$ pour tous $x_1, \ldots, x_{n+1} \in G$, et qu'il existe $x_1, \ldots, x_n \in G$ tels que $[x_1, \ldots, x_n] \neq 1$.*

Preuve. Si G est nilpotent de classe n, alors le lemme 3.1.1 permet de conclure. En effet, tout commutateur de type $[x_1, \ldots, x_{n+1}]$ est trivial, et d'après la caractérisation des γ_n dans le lemme 3.1.1, si tout commutateur de type $[x_1, \ldots, x_n] = 1$, alors $\gamma_{n-1}(G) = \{1\}$, ce qui contredit notre hypothèse sur la classe de nilpotence.

Quant à la suffisance de la condition, nous procéderons par récurrence sur n. Si $n = 1$, alors le groupe est non trivial et abélien. Nous pouvons donc supposer $n > 1$. Il découle de l'hypothèse que $Z(G) \neq \{1\}$. En effet, il suffit de fixer $x_1, \ldots, x_n \in G$ tels que $[x_1, \ldots, x_n] \neq 1$, puisqu'il en existe un d'après l'hypothèse, et ensuite varier x_{n+1}.

Le quotient $G/Z(G)$ satisfait l'hypothèse $[\overline{x_1}, \ldots, \overline{x_n}] = 1$ pour tout $\overline{x_1}, \ldots, \overline{x_n}$ extraits de $G/Z(G)$ parce que tout commutateur dans $G/Z(G)$ de la forme $[\overline{x_1}, \ldots, \overline{x_n}]$ est représenté par un commutateur $[x_1, \ldots, x_n]$ de G. La raison pour ceci est que le quotientement est par le centre de G. Par ailleurs, l'hypothèse sur l'existence d'au moins un commutateur non trivial de la forme $[x_1, \ldots, x_n]$ implique l'existence d'un commutateur de la forme $[\overline{x_1}, \ldots, \overline{x_{n-1}}]$ et non trivial. Ainsi, par récurrence $G/Z(G)$ est nilpotent exactement de classe $n-1$. Puisque $Z(G) \neq \{1\}$, la conclusion découle. □

Corollaire 3.1.3 *Soient $n \in \mathbb{N}$ et $\mathcal{L}$ le langage des groupes. Si G est un groupe nilpotent de classe exactement n, alors il en est de même pour tout groupe élémentairement équivalent à G en tant que $\mathcal{L}$-structure.*

L'étude de la résolubilité est laissée comme exercice. Nous procédons vers une question abordée au premier chapitre dont la réponse, faute de connaissance de compacité, était laissée à un état loin d'être satisfaisant.

3.2 Groupes simples, une application du théorème de compacité

Dans cette section, nous retournons à la discussion de la simplicité non bornée (le théorème 1.3. Dans la section suivante, nous étudierons un exemple de groupe de simplicité bornée, dans le contexte des groupes linéaires algébriques.

Théorème 3.1 *Soit $\mathcal{L}$ le langage des groupes. Soit G un groupe simple de simplicité non bornée. Alors G a une extension élémentaire de même cardinal qui n'est pas simple.*

Preuve. Ajoutons au langage $\mathcal{L}$ un symbole de constante c_g pour chaque élément g de G ainsi que deux autres symboles de constante qui nous serviront à décrire la violation de la condition du lemme 1.2.7. Nous noterons $\mathcal{L}^+ = \mathcal{L} \cup \{c_g \mid g \in G\} \cup \{d, e\}$.

Nous posons ensuite

$$T^+ = \mathrm{Th}((G,g)_{g\in G}) \cup \left\{ d \neq 1 \wedge e \neq 1 \wedge \quad \forall z_1 \ldots z_n \bigwedge_{(\epsilon_1,\ldots,\epsilon_n) \in \{-1,1\}^n} (d \neq (e^{\epsilon_1})^{z_1} \ldots (e^{\epsilon_n})^{z_n}) \;\middle|\; n \in \mathbb{N}^* \right\}.$$

Comme G est de simplicité non bornée, toute partie finie de T^+ a pour modèle $(G,g)_{g\in G}$. En effet, si T_0 est une partie finie de T^+, alors $T_0 \cap \mathrm{Th}((G,g)_{g\in G})$ est un ensemble fini d'énoncés vrais dans $(G,g)_{g\in G}$; quant au nombre fini d'énoncés dans T_0 de type

$$d \neq 1 \wedge e \neq 1 \wedge \quad \forall z_1 \ldots z_n \bigwedge_{(\epsilon_1,\ldots,\epsilon_n) \in \{-1,1\}^n} (d \neq (e^{\epsilon_1})^{z_1} \ldots (e^{\epsilon_n})^{z_n}),$$

l'hypothèse de simplicité non bornée équivaut à l'existence de deux éléments d^G et e^G dans G qui les satisferont tous. Alors, par compacité, T^+ a un modèle. Le langage $\mathcal{L}^+$ ayant le même cardinal que G, le théorème de Löwenheim-Skolem assure que T^+ a en fait un modèle $\mathcal{M}^+$ exactement de ce cardinal. Le réduit de ce modèle au langage $\mathcal{L}$ est l'extension élémentaire recherchée puisqu'il contient une paire d'éléments qui ne satisfont pas la condition du lemme 1.2.7 □

Corollaire 3.2.1 *Le groupe* $\mathrm{Alt}(\mathbb{N})$ *a une extension élémentaire dénombrable qui n'est pas simple.*

3.3 Simplicité bornée, un exemple

Dans cette section, nous donnerons un exemple de groupe infini de simplicité bornée. En d'autres termes, un groupe infini et simple tel que tout groupe qui lui est équivalent élémentairement soit simple. La simplicité devient donc une propriété de la théorie du premier ordre du groupe en question.

Le groupe simple que nous étudierons est $\mathrm{PSL}_2(K)$ où K est un corps algébriquement clos. C'est en fait $\mathrm{SL}_2(K)/Z(\mathrm{SL}_2(K))$, $\mathrm{SL}_2(K)$ étant le groupe des matrices deux par deux, de déterminant 1. Notre étude est un cas particulier de celle plus générale des groupes algébriques dont les groupes susmentionnés sont des exemples.

Nos méthodes peuvent paraître trop arbitraires. Elles le sont et elles ne le sont pas. Elles le sont parce qu'elles sont conséquences d'une théorie bien plus générale et uniforme qui ne dépend pas des propriétés particulières que nous utiliserons pour rendre la discussion plus élémentaire. Elles ne le sont pas parce que, effectivement, elles portent des traces concrètes que nous tâcherons d'indiquer de ces méthodes abstraites. Par ailleurs, notre exemple particulier souligne l'origine si simple de nos méthodes : l'élimination de Gauss des matrices.

Théorème 3.2 *Le groupe simple* $\mathrm{PSL}_2(K)$ *avec* K *algébriquement clos est de simplicité bornée.*

Preuve. Nous travaillerons majoritairement dans $\mathrm{SL}_2(K)$. A la fin, il ne restera que le passage au quotient. En raison de notre cadre de travail, qui équivaut à étudier des représentants concrets des éléments de $\mathrm{PSL}_2(K)$ (des classes de $Z(\mathrm{SL}_2(K))$, des éléments "imaginaires" pour ainsi dire), les calculs avec les matrices seront parfois à multiplication par $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ près. C'est tout à fait naturel puisque $\mathrm{SL}_2(K)$ n'est pas un groupe simple sauf le cas particulier où K est de caractéristique 2.

Un élément arbitraire de $\mathrm{SL}_2(K)$ est de la forme

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

avec $ad - bc = 1$. Appliquons la méthode de Gauss à la première colonne :

$$\text{si } a \neq 0 \text{ , alors } \quad \begin{pmatrix} 1 & 0 \\ -a^{-1}c & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & -ba^{-1}c + d \end{pmatrix} ;$$

$$\text{si } a = 0 \text{ , alors } \quad \begin{pmatrix} 1 & 0 \\ -b^{-1}d & 1 \end{pmatrix} \begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix} = \begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix} .$$

Si $a = 0$, de la deuxième égalité découle

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -b^{-1}d & 1 \end{pmatrix} \begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix} = \begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix} .$$

La conclusion générale est que tout élément de $\mathrm{SL}_2(K)$ est soit déjà une matrice triangulaire supérieurement, soit s'écrit comme produit d'une matrice *unipotente* (valeurs propres ± 1) inférieurement, de l'élément $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et d'une matrice triangulaire supérieurement. Cette description est un cas particulier de la *décomposition de Bruhat* qui consiste à écrire certains groupes

comme une union finie de doubles classes assez canoniques. Dans notre cas, les doubles classes sont B et BwB, où B est le groupe des matrices triangulaires supérieures et $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Nous pouvons préciser notre décomposition. En effet, $B = U \rtimes T$ avec U formé des matrices *unipotentes supérieures*, en d'autres termes, les matrices triangulaires supérieures de valeur propre 1 (non diagonalisable sauf l'élément neutre), et T le groupe des matrices diagonales. Dans le langage érudit ces dernières appartiennent à la famille des matrices *semisimples*, les matrices diagonalisables. Un simple calcul montre que la conjugaison par w normalise T et induit une action par inversion sur ses éléments. En conclusion

$$\mathrm{SL}_2(K) = UT \sqcup UwTU \ .$$

L'ordre de T et U n'est pas important dans l'écriture pour plusieurs raisons (lesquelles ?).

Faisons plusieurs remarques techniques sur la conjugaison des éléments dans $\mathrm{SL}_2(K)$. La première est générale. Comme nous travaillons sur un corps algébriquement clos, toute matrice de $\mathrm{SL}_2(K)$ se met sous sa forme de Jordan, ce qui implique que toute élément de $\mathrm{SL}_2(K)$ est conjugué à un élément de B. Ce qui n'est pas clair est si cette conjugaison se fait dans $\mathrm{SL}_2(K)$ puisqu'a priori la matrice de conjugaison est une matrice de déterminant non nul mais pas nécessairement 1. Or, comme un corps algébriquement clos contient en particulier les racines carrées de ses éléments, le groupe des matrices sur K de déterminant non nul a la factorisation suivante :

$$\mathrm{GL}_2(K) = Z(\mathrm{GL}_2(K))\mathrm{SL}_2(K) \ .$$

Par conséquent, la conjugaison se fait aussi par l'intermédiaire d'une matrice de déterminant 1. Un théoricien de groupes finis vous dirait que $\mathrm{SL}_2(K)$ "contrôle la fusion" de ses éléments.

Une deuxième remarque qui est conséquence de la première et du fait que nos matrices sont 2×2 est que tout élément est soit conjugué à une matrice unipotente supérieure, donc un élément de U, ou soit semisimple.

La troisième remarque concerne la conjugaison dans B. Le sous-groupe T agit sur U par conjugaison. Encore une fois, comme le corps K contient ses racines carrées, cette action, quand restreinte sur les éléments non neutres, est transitive. En effet, l'identité suivante est vraie en générale :

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} 1 & t^2u \\ 0 & 1 \end{pmatrix}$$

Qu'est-ce qu'on peut dire des éléments non centraux de $B \setminus U$? C'est notre quatrième remarque. Comme T est abélien, le sous-groupe dérivé B' est contenu dans U. Par ailleurs, $B' \neq \{1\}$. En fait, $B' = U$. Nous pouvons préciser cette dernière égalité davantage, quoique ce ne soit pas nécessaire dans le reste de la preuve : pour tout $x \in B \setminus U$ qui n'est pas central dans B (équivalemment dans $\mathrm{SL}_2(K)$), $[x, U] = \{[x, u] \mid u \in U\}$. Ayant parlé des commutateurs, insérons, faute de connaissance d'un meilleur endroit la remarque suivante : $Z(B) = Z(\mathrm{SL}_2(K))$. Notons aussi que ce n'est pas une propriété particulière à $\mathrm{SL}_2(K)$.

Nous pouvons passer à l'attaque. Soient x et y deux éléments de $\mathrm{SL}_2(K)$ non centraux. Supposons d'abord qu'ils soient dans B. Voici les cas qui se présentent :

Les éléments x et y sont tous les deux dans U : La troisième remarque ci-dessus montre qu'il existe un élément de T qui conjugue x à y. La condition de simplicité bornée est donc satisfaite.

$x \in U$ et y est dans un B-conjugué de T : Nous pouvons supposer que $y \in T$. Alors, y est de la forme $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$ avec $t \neq \pm 1$. La troisième remarque ci-dessus et le fait que w inverse T montrent qu'il existe $g_1, g_2 \in T$ tel que x^{g_1} et x^{wg_2} soient $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ -t^{-1} & 1 \end{pmatrix}$ respectivement. Nous pouvons, en utilisant la même méthode, conjuguer x aux matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ en utilisant g_3 et g_4. Un peu de calcul matriciel montre alors que

$$-y \ = \ x^{g_1} \ x^{wg_2} \ x^{g_1} \ x^{g_3} \ x^{wg_4} \ x^{g_3} \ .$$

Les éléments x et y sont tous les deux dans $B \setminus U$: Dans ce cas, les deux éléments sont diagonalisables. Comme $x \notin Z(\mathrm{SL}_2(K))$, il existe $u \in U$ tel que $[x,u] \in U^\times$. Or $[x,u] = x^{-1}x^u$, et à la paire $[x,u]$ et y, nous pouvons appliquer le cas précédent.

Ces trois cas épuisent la possibilité que x et y appartiennent à B. Or, dans le cas général, nous pouvons utiliser la première remarque ci-dessus, remplacer x et y par leurs conjugués dans B et ensuite appliquer la discussion précédente.

Toutes les possibilités étant épuisées, nous passons au quotient $\mathrm{PSL}_2(K)$. Les mêmes conclusions y passent aussi. La simplicité bornée est vérifiée. □

3.4 Eléments d'histoire de la théorie des modèles des groupes

Dans cette section nous démontrerons un théorème ancien de Maltsev (Malcev ?) sur les *groupes linéaires*. Un groupe G est dit linéaire s'il est isomorphe à un sous-groupe d'un $\mathrm{GL}_n(K)$ où K est un corps commutatif. Dans une telle situation, G est dit d'avoir une *représentation linéaire fidèle de dimension n*.

La linéarité d'un groupe et des membres d'une classe de groupes est une question récurrente en mathématiques. Parfois, la réponse est immédiatement négative : considérez la somme directe

$$\oplus_{p \text{ nombre premier}} U(2, K_p)$$

où p décrit l'ensemble de tous les nombres premiers et K est un corps infini de caractéristique p. Parfois, elle est immédiatement positive : un sous-groupe d'un $\mathrm{GL}_n(K)$. Parfois, une conclusion plus forte que la seule existence d'une représentation fidèle est recherchée, par exemple en théorie des modèles on préfère des représentations qui ont de fortes propriétés de définissabilité.

Les groupes linéaires ont en effet des propriétés assez particulières dont l'une les rend encore plus intéressants pour les théoriciens des modèles : la *condition de chaîne descendante sur les centralisateurs*. Dans un groupe linéaire G, il n'existe pas de chaîne infinie descendante de sous-groupes

$$H_0 > H_1 > H_2 > \dots$$

où chaque H_i est de la forme $C_G(X_i)$ avec $X_i \subset G$. C'est une propriété commune à beaucoup de groupes pour lesquels les outils de la théorie des modèles sont efficaces. La vérification de cette propriété dans les groupes linéaires est assez simple : on résoud des systèmes d'équations linéaires. Néanmoins, la propriété est relativement faible. Quoique préservée par le passage aux sous-groupes, elle ne l'est point quand il s'agit des quotients. Nous retournerons à ces points plus tard dans le cours. Avant d'aborder le théorème principal de cette section, soulignons qu'un groupe peut être linéaire de plusieurs façons, en d'autres termes, il peut avoir plusieurs représentations fidèles.

Théorème 3.3 *Soient $n \in \mathbb{N}^*$ et G un groupe. Si tout sous-groupe de type fini de G a une représentation linéaire fidèle de dimension n, alors il en est de même pour G.*

Nous travaillerons dans un langage qui permettra d'incorporer à la fois le corps de représentation et le groupe qui s'y représente :

$$\mathcal{L}_{REP} = \{C, G, +, ., -, {}^{-1}, 0, 1, \rho_{ij} \ (1 \leq i, j \leq n)\} \ .$$

Les symboles C et G sont des symboles de relation unaire décrivant les éléments d'un corps et d'un groupe éventuellement représenté dans un GL_n sur ce corps. Les symboles de fonctions $+, ., -, {}^{-1}, 0, 1$ proviennent du langage des corps. Les symboles ρ_{ij} sont des symboles de fonctions unaires telles que pour tout x dans G et y dans C, $\rho_{ij}(x) = y$ si et seulement si y est l'entrée (i,j) de la matrice qui représente x par rapport à la représentation considérée.

Voici quelques énoncés du premier ordre dans le langage $\mathcal{L}_{REP}$:

1. $\forall x((C(x) \vee G(x)) \wedge (\neg(G(x) \wedge C(x)))$;

2. $\forall xy(C(x) \wedge C(y) \wedge C(z) \rightarrow$ ("je suis un corps")) ;
3. $\forall xy((\rho_{ij}(x) = y \rightarrow (C(y) \wedge G(x))))$;
4. $\forall x(G(x) \rightarrow$ ("je suis de déterminant non nul")) ;
5. $\forall xy \exists z \Big(\ G(x) \ \wedge G(y) \rightarrow (\ G(z) \wedge \ \bigwedge_{1 \leq i,j \leq n} \rho_{ij}(z) = \sum_{k=1}^{n} \rho_{ik}(x).\rho_{kj}(y)) \Big)$;
6. $\exists x(\ G(x) \ \wedge \ \bigwedge_{i=1}^{n} \rho_{ii}(x) = 1 \ \wedge \ \bigwedge_{1 \leq i \neq j \leq n} \rho_{ij}(x) = 0 \ )$;
7. "tout élément de G a un inverse" .

L'associativité découlant des opérations de corps, ces énoncés expriment que le groupe G se représente fidèlement dans $\mathrm{GL}_n(K)$ par le biais de l'homomorphisme injectif ρ.

Ces énoncés forment un ensemble consistant puisque toute paire (K, G), de corps et de groupe respectivement, tel qu'il existe un homomorphisme injectif $\rho : G \longrightarrow \mathrm{GL}_n(K)$ en est un modèle. Nous noterons T l'ensemble de ces énoncés et de leurs conséquences. Clairement, un groupe G est linéaire de dimension n si et seulement s'il existe un corps K tel que $(K \sqcup G; K, G, ...) \models T$.

Notons $\mathcal{LIN}$ la classe des groupes qui ont une représentation linéaire fidèle de dimension n. La question qui nous intéresse est la suivante : existe-t-il, dans le langage $\mathcal{L}_{Corps} = \mathcal{L}_{REP} \setminus \{G\}$, un ensemble d'énoncés de la forme $\forall x_1 \dots x_k \phi(x_1, \dots, x_k)$ avec ϕ sans quantificateur, un *énoncé universel*, dont les modèles sont exactement les membres de $\mathcal{LIN}$? C'est ce qui est appelé parfois, une *axiomatisation universelle*. Si vous voulez voir pourquoi cette question est pertinente, il est bon moment de lire la preuve du théorème 3.3 avant d'aborder le lemme suivant.

Lemme 3.4.1 *La classe $\mathcal{LIN}$ admet une axiomatisation universelle dans le langage $\mathcal{L}_{Corps}$. Plus précisément, il existe une théorie T_1 dans le langage $\mathcal{L}_{Corps}$ formée par les conséquences d'énoncés universels, dont les modèles sont exactement les membres de $\mathcal{LIN}$.*

Preuve. Dans cette preuve par l'appellation " groupe linéaire" il est sous-entendu "un groupe ayant une représentation linéaire fidèle de dimension n". Nous considérons l'ensemble de tous les énoncés universels dans le langage $\mathcal{L}_{Corps}$ qui sont vrais dans tous les membres de $\mathcal{LIN}$. C'est bien sûr un ensemble consistant d'énoncés puisque tout groupe linéaire en est un modèle, quitte à ne pas oublier la représentation fixée. Notons T_1, la théorie formée par ses conséquences. Notons qu'a priori, il n'y a aucune raison pour que chaque modèle de T_1 soit un groupe linéaire.

Soit $\mathcal{M}$ un modèle de T_1 dont l'ensemble sous-jacent sera noté M. Nous démontrerons que l'ensemble suivant d'énoncés dans le langage $\mathcal{L}^+ = \mathcal{L}_{REP} \cup \{c_m \mid m \in M\}$ est consistant :

$$\{ \ \phi(c_{m_1}, \dots, c_{m_k}) \mid \phi \text{ est une } \mathcal{L}_{corps}\text{-formule sans quantificateur }, \ (m_1, \dots, m_k) \in M^k \ , \ \mathcal{M} \models \phi(m_1, \dots, m_k) \ \} \cup \{ \ G(c_m) \mid m \in M \ \} \ \cup \ T$$

Nous procédons par l'absurde. Alors, il découle du théorème de compacité qu'il existe une $\mathcal{L}_{Corps}$-formule $\phi(x_1, \dots, x_k)$, $(m_1, \dots, m_k) \in M^k$ et un énoncé de $\theta \in T$ tels que

$$\phi(c_{m_1}, \dots, c_{m_k}) \ \wedge \ \bigwedge_{1 \leq i \leq k} G(c_{m_i}) \ \wedge \ \theta$$

soit inconsistant. Ceci implique

$$\theta \ \vdash \ \bigwedge_{1 \leq i \leq k} G(c_{m_i}) \ \rightarrow \ \neg\phi(c_{m_1}, \dots, c_{m_k}) \ ,$$

soit encore,

$$T \ \vdash \ \bigwedge_{1 \leq i \leq k} G(c_{m_i}) \ \rightarrow \ \neg\phi(c_{m_1}, \dots, c_{m_k}) \ .$$

Par conséquent,

$$T \ \vdash \ \forall x_1 \dots x_k \left(\bigwedge_{1 \leq i \leq k} G(x_i) \ \rightarrow \ \neg\phi(x_1, \dots, x_k) \right) \ .$$

Ainsi, $\forall x_1 \dots x_k \neg\phi(x_1, \dots, x_k) \in T_1$. Ceci contredit que $\mathcal{M} \models \phi(m_1, \dots, m_k)$.

Soit $\mathcal{N}^+$ un modèle de l'ensemble ci-dessus. Son réduit au langage $\mathcal{L}_{REP}$ sera noté $\mathcal{N}$, et son ensemble de base N. Par construction, M est l'ensemble défini par G dans $\mathcal{N}$. En d'autres termes, M est un groupe linéaire. □

Preuve du théorème 3.3. Si G est un groupe qui n'a pas de représentation linéaire fidèle de degré n, alors d'après le lemme 3.4.1, il existe une formule sans quantificateur $\phi(x_1, \dots, x_k)$ dans le langage $\mathcal{L}_{Corps}$ telle que $G \models \exists x_1 \dots x_k \neg\phi(x_1, \dots, x_k)$. Soit alors $(g_1, \dots, g_k) \in G^k$ une réalisation dans G de cette formule. Alors, $\langle g_1, \dots, g_k\rangle \models \exists x_1 \dots x_k \neg\phi(x_1, \dots, x_k)$ aussi. Par conséquent, $\langle g_1, \dots, g_k\rangle$ n'est pas linéaire non plus. □

3.5 Groupes algébriques étudiés définissablement

Nous avons abordé ce chapitre dans l'objectif d'étudier des propriétés des groupes qui sont préservées par équivalence élémentaire. Dans un paysage plus général, cet objectif fait partie de l'étude des propriétés des groupes en utilisant les méthodes de la théorie des modèles. Dans cette section nous continuerons dans cette direction afin de comprendre certaines propriétés fondamentales des *groupes algébriques sur des corps algébriquement clos*. Nous démontrerons un théorème de structure sur les quotients de ces groupes en utilisant une notion bien connue en théorie des modèles : *élimination des imaginaires*. Ceci consiste à remplacer des relations d'équivalences définissables par des fonctions définissables, ce qui est au coeur de ce que nous appelons "quotientement".

Nous commençons par une révision plus solide des notions de définissabilité déjà rencontrées. D'abord, les ensembles définissables :

Définition 3.5.1 *Soient $\mathcal{L}$ un langage du premier ordre et $\mathcal{M}$ une $\mathcal{L}$-structure de base M. Une partie D de M^k est dit* définissable dans $\mathcal{M}$ *s'il existe une $\mathcal{L}$-formule ϕ à exactement k variables libres telle que*

$$\phi(\mathcal{M}) \;=\; \{\; m \in M^k \mid \mathcal{M} \models \phi[m] \;\}$$

soit exactement D. Un ensemble D est dit définissable avec paramètres *provenant d'une partie de M, s'il existe $A \subset M$, tel que l'ensemble D soit définissable dans la $\mathcal{L}(A)$-structure $(\mathcal{M}, a)_{a\in A}$ obtenue après avoir ajouté au langage $\mathcal{L}$ un symbole de constante pour chaque élément de A.*

Ensuite, les structures définissables :

Définition 3.5.2 *Soient $\mathcal{L}$ et $\mathcal{L}'$ deux langages du premier ordre, et $\mathcal{M}$ et $\mathcal{M}'$ deux structures par rapport à $\mathcal{L}$ et à $\mathcal{L}'$, de bases M et M' respectivement. La structure $\mathcal{M}'$ est dite définissable dans $\mathcal{M}$ si les conditions suivantes sont satisfaites :*

1. *il existe $n \in \mathbb{N}$ et une partie $D_{\mathcal{M}'} \subset M^n$ définissable dans $\mathcal{M}$;*
2. *pour tout $k \in \mathbb{N}$ et pour toute fonction k-aire de $\mathcal{M}$, il existe une partie définissable dans $\mathcal{M}$ de $D^{k+1}_{\mathcal{M}'}$;*
3. *pour tout $k \in \mathbb{N}$, pour toute relation k-aire de $\mathcal{M}'$, il existe une partie définissable dans $\mathcal{M}$ de $D^k_{\mathcal{M}'}$;*
4. *il existe un isomorphisme de $\mathcal{M}$ vers la structure $(D_{\mathcal{M}'}; \dots)$ ainsi construite.*

Dans la définition précédente, pour ne pas compliquer davantage une description déjà suffisamment compliquée, nous n'avons pas mentionné les constantes puisqu'elles peuvent être vues comme des fonctions.

Dans cette section nous noterons $\mathcal{L}_C$ le langage des corps, en d'autres termes le langage $\{+, -, ., \ ^{-1}, 0, 1\}$. Dans ce langage sont écrits les énoncés suivants :

1. Axiomes décrivant un corps
2. $1 \neq 0$

3. (A_n) $(n \in \mathbb{N}^*)$ $\forall y_0 \dots y_{n-1} \exists x (y_0 + y_1.x + \dots + y_{n-1}.x^{n-1} + x^n = 0)$

4_p $\underbrace{1 + \dots + 1}_{p \text{ fois}} = 0$ si la caractéristique est un nombre p premier

4_0 (C_n) $\underbrace{1 + \dots + 1}_{n \text{ fois}} \neq 0$ pour tout $n \in \mathbb{N}^*$ si la caractéristique est nulle

Cet ensemble d'énoncés, quitte à fixer la valeur de p, est consistant puisque tout corps algébriquement clos de caractéristique p en est un modèle. Nous noterons la théorie formée par toutes ses conséquences CAC_p. C'est en fait une théorie complète qui jouit de beaucoup d'autres propriétés qui en ont fait presque un paradigme en théorie des modèles. Certaines de ces propriétés, dont la suivante, seront étudiées dans le cours général de théorie des modèles :

Fait 3.5.3 *Dans le langage $\mathcal{L}_C$, la théorie CAC_p élimine les quantificateurs. En d'autres termes, pour toute $\mathcal{L}_C$-formule $\phi(x_1, \dots, x_k)$ $(k \in \mathbb{N}^*)$ à exactement k variables libres, il existe une $\mathcal{L}_C$-formule $\psi(x_1, \dots, x_k)$ à k variables libres telle que*

$$\mathrm{CAC}_p \vdash \forall x_1 \dots x_k (\phi(x_1, \dots, x_k) \leftrightarrow \psi(x_1, \dots, x_k)) \ .$$

Nous nous contenterons de ce qui nous est nécessaire dans cette section afin d'introduire une certaine notion de *groupe algébrique* sans trop de peine.

Définition 3.5.4 *Un groupe G est dit algébrique s'il existe un corps algébriquement clos $\mathcal{K}$, de base K, plus précisément un modèle de CAC_p pour p premier ou 0, $A \subset K$ (A éventuellement vide) tels que G soit définissable dans la $\mathcal{L}_C(A)$-structure $(\mathcal{K}, a)_{a \in A}$.*

Notons que la définition de G est valable dans toute extension élémentaire de $\mathcal{K}$, ce qui donne des extensions élémentaires de G.

Tout groupe de matrices que nous avons rencontré lors de notre périple est un groupe algébrique quitte à choisir le corps de base algébriquement clos... ou affaiblir la définition 3.5.4 en permettant d'autres classes de corps. Cette possibilité, tout à fait légitime, ne sera pas abordée ici.

Une classe de groupes étroitement liée aux groupes algébriques est la famille des $\mathrm{PSL}_2(K)$ dont nous avons étudié la simplicité bornée quand K est algébriquement clos. C'est le quotient d'un groupe algébrique par son centre, un sous-groupe définissable dans le langage des groupes, donc dans $\mathcal{L}_C$ et par conséquent algébrique. En raison de ce quotientement, il n'est pas clair si $\mathrm{PSL}_2(K)$ est algébrique. Dans cette section, nous essayerons de clarifier cette situation affirmativement en démontrant un théorème général sur les modèles de CAC_p, qui est connu dans le jargon de la théorie des modèles sous l'appellation de *l'élimination des imaginaires*. Des quotients imaginaires, nous passerons à des éléments réels, et ce définissablement.

Nous commençons avec une rapide étude de certaines propriétés de CAC_p.

Définition 3.5.5 *Soient $\mathcal{L}$ un langage et $\mathcal{M}$ une $\mathcal{L}$-structure infinie et d'univers M.*

1. *La structure $\mathcal{M}$ est dite* minimale *si pour toute $\mathcal{L}$-formule $\phi(x, y_1, \dots, y_k)$ à $k+1$ variables libres avec $k \in \mathbb{N}$ et $(m_1, \dots, m_k) \in M^k$ la partie*

$$\phi(\mathcal{M}; m_1, \dots, m_k) \ = \ \{m \in M \mid \mathcal{M} \models \phi(m; m_1, \dots, m_k)\}$$

   de M est soit finie soit cofinie (de complémentaire fini).

2. *La structure $\mathcal{M}$ est dite* fortement minimale *si toute extension élémentaire de $\mathcal{M}$ est minimale.*

3. *Une $\mathcal{L}$-théorie complète est dite* fortement minimale *si tous ses modèles sont minimaux, équivalemment si elle est la théorie complète du premier ordre d'une $\mathcal{L}$-structure fortement minimale.*

Lemme 3.5.6 *Soient $\mathcal{L}$ un langage du premier ordre et T une $\mathcal{L}$-théorie complète fortement minimale. Alors pour toute $\mathcal{L}$-formule $\phi(x, y_1, \ldots, y_k)$ à exactement $k+1$-variables libres ($k \in \mathbb{N}$), il existe $b_\phi \in \mathbb{N}$ tel que pour tout modèle $\mathcal{M}$ de T, de base M, et tout $(m_1, \ldots, m_k) \in M^k$, l'ensemble $\phi(\mathcal{M}; m_1, \ldots, m_k)$ ou l'ensemble $\neg\phi(\mathcal{M}; m_1, \ldots, m_k)$ contient au plus b_ϕ éléments.*

Preuve. Un bon exercice de compacité. □

Lemme 3.5.7 *La théorie CAC_p est fortement minimale.*

Preuve. C'est une conséquence de l'élimination des quantificateurs. Soient $\mathcal{K} \models \mathrm{CAC}_p$, de base K, $\phi(x, y_1, \ldots, y_m)$ une formule à $m+1$ variables libres ($m \in \mathbb{N}$) et $(a_1, \ldots, a_m) \in K^m$. D'après le fait 3.5.3, il existe une formule $\psi(x, y_1, \ldots, y_m)$ à $m+1$ variables libres et sans quantificateurs telle que

$$\mathrm{CAC}_p \vdash \forall x y_1 \ldots y_m (\phi(x, y_1, \ldots, y_m) \leftrightarrow \psi(x, y_1, \ldots, y_m)) \ .$$

En particulier,

$$\mathcal{K} \models \forall x (\phi(x, a_1, \ldots, a_m) \leftrightarrow \psi(x, a_1, \ldots, a_m)) \ .$$

Or, $\psi(x, y_1, \ldots, y_m)$ est sans quantificateurs. Si elle est en outre atomique, alors il s'agit d'une équation polynomiale du type

$$P(X, Y_1, \ldots, Y_m) = 0 \ .$$

Or, l'équation

$$P(X, a_1, \ldots, a_m) = 0$$

a un nombre fini de solutions, et cette conclusion amorce une récurrence sur la compléxité des formules dans le langage $\mathcal{L}_C$. Si ψ est de la forme $\neg\theta$ alors $\psi(K, a_1, \ldots, a_m)$ est fini si et seulement si $\theta(K, a_1, \ldots, a_m)$ est cofini, et la conclusion pour le cardinal de $\psi(K, a_1 \ldots, a_m)$ découle de l'hypothèse de récurrence sur le cardinal de $\theta(K, a_1, \ldots, a_m)$. Une discussion légèrement plus compliquée règle le sort du cas où ψ est de la forme $\theta_1 \wedge \theta_2$.

Par ailleurs, étant algébriquement clos, K est un corps infini. Le corps K étant un modèle arbitrairement choisi de CAC_p, on conclut que CAC_p est fortement minimale. □

Théorème 3.4 ([9, Section 16.d],[11]) *Soit $\mathcal{K} = (K, +, -, ., \ ^{-1}, 0, 1)$ un modèle de CAC_p. Pour tout $A \subset K$, pour toute relation d'équivalence $E(x_1, \ldots, x_m; y_1, \ldots, y_m)$ définissable dans la $\mathcal{L}_C(A)$-structure $(\mathcal{K}, a)_{a \in K}$, il existe $l \in \mathbb{N}^*$ et une fonction définissable dans $\mathcal{K}$*

$$f_E \ : \ K^m \ \rightarrow \ K^l$$

telle que pour tous $x, \ y \in K^m$, $E(x, y)$ si et seulement si $f_E(x) = f_E(y)$.

Lemme 3.5.8 ([4]) *Soient $\mathcal{K} = (K, +, -, ., \ ^{-1}, 0, 1)$ un modèle de CAC_p, A une partie éventuellement vide de K et ϕ une $\mathcal{L}_C(A)$-formule à exactement n variables libres ($n \in \mathbb{N}^*$). Il existe alors une $\mathcal{L}_C(A)$-formule ϕ^* à n variables libres et qui définit une partie non vide à k éléments de ϕ.*

Preuve. Le raisonnement est par récurrence sur n. Si $n = 1$, alors d'après les lemmes 3.5.6 et 3.5.7, il existe $b_\phi \in \mathbb{N}$ tel que soit ϕ soit $\neg\phi$ définisse un ensemble à au plus b_ϕ éléments. Alors, $\phi^*(x)$ est la formule suivante :

$$(\ \exists^{\leq b_\phi} x \phi(x) \ \wedge \ \phi(x) \ ) \ \vee \ (\ \exists^{> b_\phi} x \phi(x) \ \wedge \ (\ \neg\phi(x^2) \ \vee \ \neg\phi(x^3) \ \vee \ x = 1 \ )) \ .$$

Supposons maintenant $n > 1$. La formule $\exists x_n \phi(x_1, \ldots, x_{n-1}, x_n)$ définit la projection sur les $n-1$ premières coordonnées. Par récurrence, il existe une formule $(\exists x_n \phi(x_1, \ldots, x_{n-1}, x_n))^*$ qui définit une partie finie de cette projection : $\{a_1, \ldots, a_s\} \subset K^{n-1}$. D'après l'analyse du cas $n = 1$, pour chaque a_i, la formule

$$(\ \exists^{\leq b_\phi} x_n \phi(a_i, x_n) \ \wedge \ \phi(a_i, x_n) \ ) \ \vee \ (\ \exists^{> b_\phi} x_n \phi(a_i, x_n) \ \wedge \ (\ \neg\phi(a_i, x_n^2) \ \vee \ \neg\phi(a_i, x_n^3) \ \vee \ x_n = 1 \ ))$$

définit une partie à au plus b_ϕ éléments de $\phi(a_i, x_n)$, disons $\{c_{i1}, \ldots, c_{ib_\phi}\}$ $(1 \leq i \leq s)$. Nous avons donc trouvé notre ensemble, en l'occurrence

$$\bigcup_{i=1}^{s} \{(a_i, c_{i1}), \ldots, (a_i, c_{ib_\phi})\} \ .$$

La formule à n variables qui le définit est

$$(\exists x_n \phi(x_1, \ldots, x_{n-1}, x_n))^* \wedge$$

$$(\ \exists^{\leq b_\phi} x_n \phi(x_1, \ldots, x_{n-1}, x_n) \ \wedge \ \phi(x_1, \ldots, x_{n-1}, x_n) \ ) \ \vee \ (\ \exists^{> b_\phi} x_n \phi(x_1, \ldots, x_{n-1}, x_n)$$
$$\wedge \ (\ \neg\phi(x_1, \ldots, x_{n-1}, x_n^2) \ \vee \ \neg\phi(x_1, \ldots, x_{n-1}, x_n^3) \ \vee \ x_n = 1 \ ))$$

□

Lemme 3.5.9 ([4],[2, Article de A. Pillay]) *Soit $\mathcal{K} = (K, +, -, ., \ ^{-1}, 0, 1)$ un modèle de CAC_p. Soient $k, n \in \mathbb{N}^*$. Il existe $l \in \mathbb{N}^*$ et une fonction injective des parties à k éléments de K^n vers K^l telle que la loi de définition de la fonction soit $\mathcal{L}_C$-définissable.*

Preuve. Il suffit d'associer à $\{a_1, \ldots, a_k\} \subset K^n$ les cofficients du polynôme

$$P(Z, X_1 \ldots, X_n) = \prod_{i=1}^{k} (Z - a_{i1}X_1 - \ldots - a_{in}X_n) = \sum_{i_0 + i_1 + \ldots + i_n = k} c_{i_0, i_1, \ldots, i_k} Z^{i_0} X_1^{i_1} \ldots X_n^{i_n} \ .$$

L'injectivité découle du fait que $K[Z, X_1, \ldots, X_n]$ est un anneau factoriel. Alors, l est le nombre de coefficients. □

Preuve du théorème 3.4. Soit E une relation d'équivalence définie sur $K^m \times K^m$ dans le langage $\mathcal{L}_C(A)$. Chaque classe d'équivalence est de la forme $\{y \in K^m \mid E(a; y)\}$, avec $a \in K^m$. Les constructions dans les lemmes précédents fournissent des bornes uniformes sur l, indépendantes des classes d'équivalences fixées. Par construction, le l-uplet du lemme 3.5.9 reste invariant précisément sur une même classe d'équivalence. Ainsi, nous avons défini une fonction définissable de K^m vers K^l qui associe à chaque $x \in K^m$ le l-uplet qui est déterminé par et qui détermine sa classe d'équivalence. Nous avons éliminé les imaginaires. □

Corollaire 3.5.10 *Soient G un groupe algébrique et H un sous-groupe algébrique distingué de G. Alors le groupe quotient G/H est un groupe algébrique.*

Preuve. Par hypothèse, G et H sont $\mathcal{L}_C(A)$-définissables dans un corps K algébriquement clos avec $A \subset K$ éventuellement vide. Alors, le passage au quotient G/H correspond à une relation d'équivalence $\mathcal{L}_C(A)$-définissable. D'après le théoréme 3.4, il existe une fonction surjective $\mathcal{L}_C(A)$-définissable de G vers une partie définissable $D_{G/H}$ d'une puissance cartésienne de K qui est constante exactement sur chaque classe d'équivalence, et injective sur G/H. Il suffit de transporter $\mathcal{L}_C(A)$-définissablement la structure de groupe du quotient G/H à l'ensemble $D_{G/H}$. □

Exercices

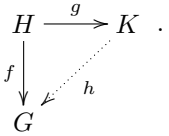
Exercice 3.1 Est-ce que la résolubilité et sa classe sont préservées par équivalence élémentaire.

Exercice 3.2 (Une preuve du théorème 3.3 en utilisant les ultraproduits) Nous essayerons d'obtenir un résultat un peu plus général. Soit $\mathcal{P}$ une propriété des groupes préservée par le passage aux sous-groupes et par les ultraproduits.

1. Nous vérifierons d'abord qu'un groupe G a la propriété $\mathcal{P}$ si et seulement si chaque sous-groupe de type fini a la propriété $\mathcal{P}$.
   (a) Soient I l'ensemble des parties finies de G et, pour tout $g \in G$, $I_g = \{ E \in I \mid g \in E \}$. Montrer que pour toute partie finie $\{g_1, \ldots, g_k\}$ de G, $I_{g_1} \cap \ldots \cap I_{g_k} \neq \emptyset$. En déduire qu'il existe un ultrafiltre $\mathcal{F}$ sur l'ensemble I contenant $\{ I_g \mid g \in G \}$.
   (b) Posons maintenant $\tilde{G} = \prod_{E \in I} \langle E \rangle / \mathcal{F}$. Montrer que l'application suivante est un homomorphisme injectif :
   $$\begin{array}{rcccl} f & : & G & \longrightarrow & \tilde{G} \\ & & g & \longmapsto & [(g_E)_{E \in I}] \quad \text{où} \quad g_E = \begin{cases} g & \text{si } g \in \langle E \rangle \\ 1 & \text{sinon.} \end{cases} \end{array}$$
   (c) Conclure.
2. Vérifier qu'un ultraproduit d'une famille de groupes linéaires de dimension n est un groupe linéaire de dimension n.
3. Conclure.

Exercice 3.3 La dernière phrase de la preuve du corollaire 3.5.10 est un peu rapidement dite. La détailler.

Exercice 3.4 (Groupes divisibles et abéliens) Un groupe D est dit *divisible* si pour tout $g \in D$ et $n \in \mathbb{N}^*$, il existe $h \in D$ tel que $h^n = g$. Quand D est abélien, il est possible de déterminer sa structure à isomorphisme près. C'est l'objectif de cet exercice. Comme c'est un résultat classique qu'on rencontre souvent dans les ouvrages, nous procéderons rapidement. Dans le reste de l'exercice D notera un groupe divisible et abélien. Pour éviter les trivialités, nous supposerons que D soit non trivial, en d'autres termes $D \neq \{1\}$.

1. Montrer que D est infini.
2. Montrer que toute image homomorphe de D est divisible aussi. En déduire que D n'a pas de sous-groupe propre d'indice fini. Notez que ces deux propriétés ne nécessitent pas la commutativité du groupe D.
3. Montrer que si $D = \oplus_{i \in I} D_i$, alors chaque D_i est divisible. Montrer qu'une somme directe des groupes divisibles est divisible.
4. Montrer qu'un groupe abélien G est divisible si et seulement s'il a la propriété suivante d'*injectivité* :
   pour tous groupes H et K, tout homomorphisme injectif g de H vers K et tout homomorphisme f de H vers G, il existe un homomorphisme H de K vers G tel que le diagramme suivant commute
   

   (*La nécessité de cette propriété utilise le lemme de Zorn pour vérifier l'existence de l'extension h.*)
5. Déduire du point précédent que si D est un sous-groupe d'un groupe quelconque abélien A, alors il existe un sous-groupe B de A tel que $A = D \oplus B$.

6. Montrer que si D n'a pas d'élément d'ordre fini, alors $D \cong \oplus_{i\in I}(\mathbb{Q}_i, +)$, avec I un certain ensemble d'indices.
7. Pour un nombre premier p fixé, notons $\mathbb{Z}_{p^\infty}$ le sous-groupe suivant de $(\mathbb{C}^*, .)$:

$$\{\ x \in \mathbb{C}^* \mid \text{il existe } n \in \mathbb{N}^* \text{ tel que } x^{p^n} = 1\ \}\ .$$

   Montrer que si D n'a que des éléments d'ordre fini alors

$$D \cong \oplus_{p\in\mathcal{P}} \left(\oplus_{I_p} \mathbb{Z}_{p^\infty}\right)$$

   où $\mathcal{P}$ est l'ensemble de tous les nombres premiers et chaque I_p est un ensemble d'indices de cardinal arbitraire, éventuellement vide.
8. En utilisant l'injectivité des groupes divisibles et abéliens, déduire de ce qui précède que

$$D \cong (\oplus_{i\in I}(\mathbb{Q}_i, +)) \oplus \left(\oplus_{p\in\mathcal{P}} \left(\oplus_{I_p} \mathbb{Z}_{p^\infty}\right)\right)\ .$$

Exercice 3.5 Soit $\mathcal{L}$ le langage des groupes.

1. Ecrire les énoncés dans $\mathcal{L}$ qui expriment que la $\mathcal{L}$-structure en question est un groupe non trivial, abélien, divisible et sans torsion (sans élément d'ordre fini autre que l'élément neutre).
2. Montrer en utilisant la méthode du va-et-vient que la théorie T formée par les conséquences des énoncés du premier point élimine les quantificateurs et qu'elle est complète.
3. Montrer que la théorie T est *non dénombrablement catégorique* ; en d'autres termes, deux modèles de T de même cardinal non dénombrable sont isomorphes (*Tout modèle de T est un $\mathbb{Q}$-espace vectoriel*).
4. Montrer en utilisant l'élimination des quantificateurs que T est fortement minimale.

Exercice 3.6 Montrer que, dans le langage des groupes, un groupe G minimal (au sens de la définition 3.5.5) est abélien. Vérifier que les deux cas suivants sont les seuls possibles pour sa structure algébrique :

1. il existe un nombre premier p tel que pour tout $g \in G$, $g^p = 1$;
2. G est divisible.

Exercice 3.7 Soit $\mathcal{L}$ le langage des groupes. Soit p un nombre premier fixé.

1. Ecrire les énoncés dans $\mathcal{L}$ qui expriment que la $\mathcal{L}$-structure en question est un groupe infini abélien dont chaque élément non neutre est d'ordre p.
2. Montrer en utilisant la méthode du va-et-vient que la théorie T formée par les conséquences des énoncés du premier point élimine les quantificateurs et qu'elle est complète.
3. Montrer que la théorie T est κ-*catégorique* pour tout cardinal infini κ ; en d'autres termes, deux modèles de T de même cardinal sont isomorphes. (*Tout modèle de T peut être vu comme un $\mathbb{F}_p$-espace vectoriel de dimension infinie.*)
4. Montrer que la théorie T est fortement minimale (*Vous pouvez étudier le sous-groupe engendré par les paramètres d'une formule du premier ordre à une seule variable*).

Chapitre 4

Groupes en théorie des modèles

Dans ce chapitre nous aborderons l'étude des classes de groupes définies par des propriétés de la théorie des modèles. Notre objectif principal sera une introduction à l'étude des *groupes stables*. La notion de stabilité est l'une des composantes fondamentales de la théorie des modèles. La quête et l'étude des groupes stables a été source de travaux mathématiques d'autant plus riches que d'un côté des questions de la théorie des modèles ont été résolues en utilisant la présence de ces groupes au sein de certaines structures, d'un autre côté des liens inattendus avec diverses branches de la théorie des groupes ont été noués.

Nous introduirons certaines de nos nouvelles notions d'abord en utilisant les propriétés combinatoires des formules du premier ordre. Celles-ci fournissent des caractérisations de diverses propriétés de façon assez élémentaire. Cette approche, efficace au début surtout pour comprendre certaines propriétés algébriques de nos objets d'étude, s'avérera insuffisant. Alors, nous ferons le nécessaire, comme dans les chapitres précédents.

4.1 Propriétés combinatoires des formules du premier ordre

Intuitivement, en théorie des modèles, ce qui est stable est ce dont les propriétés de définissabilité sont maîtrisables. Plus dans une structure on limite le "nombre" de parties définissables, plus proche elle est d'être stable. Un bon exemple est fourni par les théories fortement minimales. Alors, pour arriver à une stabilité, il faut minimiser les "coupures" définissables, en particulier éviter les relations d'ordre qui en sont les sources principales. Nous commençons donc, comme c'est d'ailleurs assez fréquent en théorie des modèles, par des notions négatives.

Définition 4.1.1 *Soient $\mathcal{L}$ un langage du premier ordre et T une théorie complète dans ce langage.*

1. *Soient $k \in \mathbb{N}^*$, $\phi(x,y)$ une $\mathcal{L}$-formule à $k+k$ variables libres, $\mathcal{M}$ un modèle de T de base M, et A un ensemble de k-uples extraits de M, indexés par un ensemble totalement ordonné I. La formule $\phi(x,y)$ est dite d'*ordonner *A si la relation suivante est un ordre total (relation réflexive, antisymétrique et transitive) sur A : pour tous $a, a' \in A$,*

$$a \leq a' \text{ si et seulement si } \mathcal{M} \models \phi(a,a') \ .$$

2. *Soient $k,l \in \mathbb{N}^*$. Une $\mathcal{L}$-formule $\phi(x,y)$ à $k+l$ variables libres a la* propriété de l'ordre *s'il existe un modèle $\mathcal{M}$ de T de base M et deux ensembles $\{a_m | m \in \mathbb{N}\} \subset M^k$ et $\{b_n | n \in \mathbb{N}\} \subset M^l$ tels que*

$$\mathcal{M} \models \phi(a_m, b_n) \text{ si } m \leq n \text{ et } \mathcal{M} \models \neg\phi(a_m, b_n) \text{ si } m > n \ .$$

3. *Soient $k,l \in \mathbb{N}^*$, $\phi(x,y)$ une $\mathcal{L}$-formule à $k+l$ variables libres, $\mathcal{M}$ un modèle de T de base M, et A une partie $\mathcal{L}$-définissable de M^l. On définit la relation $<$ sur A comme suit : pour*

tous $b, b' \in A$,

$$b < b' \text{ si et seulement si } \mathcal{M} \models \forall x \exists y (\ (\phi(x,b) \to \phi(x,b')) \ \wedge \ (\neg\phi(y,b) \wedge \phi(y,b'))\ ) \ .$$

La relation $<$ *est une relation d'ordre strict* (*antiréflexive, asymétrique, transitive*) *partielle. La formule* ϕ *a la* propriété de l'ordre strict *s'il existe* A *et* $\mathcal{M}$ *comme ci-dessus, et une partie infinie de* A *sur laquelle* $<$ *induit un ordre total* (*une chaîne*).

4. *Soient* $k, l \in \mathbb{N}^*$, $\phi(x,y)$ *une* $\mathcal{L}$*-formule à* $k+l$ *variables libres. La formule* ϕ *est dite d'avoir la* propriété d'indépendance *si pour tout* $n \in \mathbb{N}$, *l'énoncé suivant est une conséquence de* T :

$$\exists x_0 \dots x_i \dots x_{n-1} \exists y_0 \dots y_w \dots y_{2^n-1} \bigwedge_{w \in 2^n} \left(\bigwedge_{i \in w} \phi(x_i, y_w) \ \wedge \ \bigwedge_{i \notin w} \neg\phi(x_i, y_w) \ . \right)$$

Nous dirons qu'une théorie complète T *a l'une de ces propriétés si une formule l'a par rapport à* T, *et qu'une structure* $\mathcal{M}$ *a l'une de ces propriétés si* $Th(\mathcal{M})$ *l'a. Evidemment, tout ceci suppose la présence d'un langage du premier ordre fixé.*

Lemme 4.1.2 *Nous utiliserons la notation de la définition 4.1.1.*

1. *Il existe une* $\mathcal{L}$*-formule qui a la propriété de l'ordre si et seulement s'il en existe une qui ordonne un ensemble infini.*
2. *Une* $\mathcal{L}$*-formule* $\phi(x,y)$ *ordonne un ensemble infini de* M *si et seulement si* T *a un modèle dans lequel* ϕ *ordonne des ensembles finis arbitrairement larges.*
3. *Si* $\phi(x,y)$ *est une* $\mathcal{L}$*-formule qui a la propriété d'indépendance, alors pour tout cardinal* κ *il existe un modèle* $\mathcal{N}$ *de* T, *des parties* $\{a_i | i \in \kappa\}$ *et* $\{b_w | w \in 2^\kappa\}$ *de* M^k *et* M^l *respectivement telles ques* $\mathcal{N} \models \phi(a_i, b_w)$ *si et seulement si* $i \in w$.
4. *Une* $\mathcal{L}$*-formule* $\phi(x,y)$ *a la propriété de l'ordre strict si et seulement s'il existe un modèle* $\mathcal{M}$ *de* T *et une partie définissable de* M^k *sur lequel la relation d'ordre partielle* $<$ *induit des chaînes de longueurs arbitrairement larges.*
5. *Si une* $\mathcal{L}$*-formule a la propriété de l'ordre strict ou celle d'indépendance, alors il existe une* $\mathcal{L}$*-formule qui ordonne un ensemble infini.*

Preuve. Nous travaillerons dans un modèle $\mathcal{M}$ de la théorie complète T dont la base sera notée M.

1. Si $\phi(x,y)$ a la propriété de l'ordre, alors $\psi(x,y;x',y')$ définie par $\phi(x,y')$ ordonne l'ensemble $\{(a_i,b_i) | i \in \mathbb{N}\}$. Si $\phi(x,y)$ ordonne un ensemble infini A, il suffit d'extraire une partie infinie de A de même type d'ordre que $\mathbb{N}$ muni de son ordre usuel pour satisfaire la condition du point (2) de la définition 4.1.1.

2., 3., 4. Compacité. Détaillons le point (4), les autres points nécessitant le même style de raisonnement. La nécessité de la condition est immédiate. Nous utiliserons la lettre A comme le nom d'une $\mathcal{L}$-formule du premier ordre qui définit un ensemble dans M^l.

C'est une pratique assez fréquente en théorie des modèles de ne pas faire de distinction entre l'appellation pour un ensemble défini par une formule du premier ordre et celle pour la formule elle-même, ou enconre de penser à tous les ensembles définis par cette même formule dans tous les modèles de la théorie en question. Comme c'est une habitude qui confond parfois, nous avons pris soin de préciser que A est une formule. Ceci dit, l'ensemble sur lequel nous vérifierons l'existence des chaînes infinies sera défini par la même formule A mais sur un modèle éventuellement distinct de $\mathcal{M}$.

Supposons maintenant que pour tout $n \in \mathbb{N}^*$, il existe $\{b_1, \dots, b_n\} \subset M^l$ tels que

$$\mathcal{M} \models \bigwedge_{i=1}^{n} A(b_i) \quad \text{et} \quad b_1 < \dots < b_n \ .$$

Soit alors $\mathcal{L}^+ = \mathcal{L} \cup \{c_m | m \in M\} \cup \{b_{ij} | i \in \mathbb{N} \;\; 1 \leq j \leq k\}$. On définit

$$T^+ = \mathrm{Th}((\mathcal{M}, m)_{m \in M}) \cup \{ \; A(b_{i1}, \ldots, b_{ik}) \mid i \in \mathbb{N} \; \} \cup$$

$$\{ \; \forall x \exists y (\; (\phi(x, b_i) \rightarrow \phi(x, b_{i+1})) \;\wedge\; (\neg\phi(y, b_i) \wedge \phi(y, b_{i+1})) \;) \mid i \in \mathbb{N} \; \} \; .$$

Il découle de l'hypothèse sur les chaînes arbitrairement longues et de la compacité que cet ensemble est consistant. Par conséquent, dans une extension élémentaire de $\mathcal{M}$, l'ordre $<$ induit une chaîne infinie sur la partie définie par A. Notons que par construction nous avons obtenu une chaîne infinie croissante. En changeant la construction, nous pouvons obtenir toute sorte de chaîne de toute longueur infinie.

5. Soit $\phi(x, y)$ une formule qui a la propriété de l'ordre strict. Alors il existe une partie infinie de M^l, disons $\{b_i | i \in I\}$, telle que les formules $\{\phi(x, b_i) | i \in I\}$ définissent une chaîne infinie et stricte. Quitte à éliminer les répétitions en prenant un seul paramètre pour chaque élément de la chaîne, nous voyons que la formule

$$\forall x \exists y (\; (\phi(x, z) \rightarrow \phi(x, z')) \;\wedge\; (\neg\phi(y, z) \wedge \phi(y, z')) \;) \;\vee\; z = z'$$

ordonne l'ensemble $\{b_i | i \in I\}$.

Si $\phi(x, y)$ a la propriété d'indépendance, alors d'après le point (3), cette propriété est valable pour deux ensembles infinis $\{a_i | i \in \mathbb{N}\}$, $\{b_w | w \in 2^{\mathbb{N}}\}$ dans M^k et M^l respectivement. L'ordre suivant ordonne $\{(a_i, b_i) | i \in \mathbb{N}\}$:

$$(a_i, b_i) \leq (a_j, b_j) \;\text{ si et seulement si } \mathcal{M} \models \phi(a_i, b_j) \vee (a_i, b_i) = (a_j, b_j) \;\; .$$

□

Nous avons accumulé suffisamment d'arsenal pour introduire la notion de *théorie stable*.

Définition 4.1.3 *Soient $\mathcal{L}$ un langage du premier ordre et T une théorie complète dans ce langage. La théorie T sera dite* stable *si aucune formule n'a la propriété de l'ordre par rapport à T. Une $\mathcal{L}$-structure $\mathcal{M}$ est dite stable si* $\mathrm{Th}(\mathcal{M})$ *est stable.*

En fait, c'est une caractérisation. Les raisons principales pour lesquelles nous avons abordé le sujet de manière indirecte sont la simplicité de cette caractérisation et la force de ses conséquences dans des groupes. Néanmoins, le moment viendra où il faudra utiliser la définition officielle et d'autres caractérisations qui sont par ailleurs nombreuses.

Il convient de souligner un aspect fondamental de la définition 4.1.3. La stabilité est la propriété d'une théorie complète. La stabilité d'une structure est définie plutôt pour éviter de répéter l'expression longue "une structure dont la théorie du premier ordre est stable". En particulier, une formule qui cause l'instabilité d'une théorie complète peut ne pas ordonner un ensemble infini extrait d'un modèle particulier de cette théorie. Par contre, comme l'indique le lemme 4.1.2 (2), une telle formule ordonne dans tout modèle des parties finies arbitrairement larges. Illustrons ceci par un exemple simple : soit $\mathcal{L} = \{\preceq\}$ le langage d'une binaire. La $\mathcal{L}$-structure $\mathcal{N} = (\mathbb{N} \times \mathbb{N}; \leq)$ où $<$ ordonne les segments horizontaux en dessus de la droite $x = y$ est un ordre partiel défini par

$$(m, n) \preceq (m', n') \text{ si et seulement si } \begin{cases} n < n' \text{ ou } (n = n' \text{ et } m \leq m') & \text{quand } m \leq n \text{ et } m' \leq n' \\ m = m' \text{ et } n = n' & \text{quand } m > n \text{ ou } m' > n' \end{cases}$$

La formule $x \preceq y$ cause l'instabilité de $\mathrm{Th}(\mathcal{N})$ mais n'ordonne aucune partie infinie de $\mathbb{N} \times \mathbb{N}$.

Voici un lemme très utile qui découle rapidement des définitions 4.1.3 et 3.5.2 :

Lemme 4.1.4 *Soient $\mathcal{M}$ et $\mathcal{M}'$, des $\mathcal{L}$- et $\mathcal{L}'$-structures respectivement. Si $\mathcal{M}$ est stable et que $\mathcal{M}'$ est définissable dans $\mathcal{M}$, alors $\mathcal{M}'$ est aussi stable.*

Preuve. Exercice. □

Ce lemme offre un cadre plus général pour l'étude des groupes en théorie des modèles : un groupe est dit stable s'il est *définissable dans une structure stable*. Il devient possible d'élargir l'étude d'un groupe au cas où la structure ambiante peut induire une structure définissable supplémentaire que la seule structure de groupe ne pourrait fournir. Dans le contexte stable, au moins en ce qui concerne les paramètres, cet "enrichissement" structurel est maîtrisé grâce à un fait bien connu qui illustre une propriété fondamentale des ensembles définissables dans une structure stable :

Fait 4.1.5 ([9, Section 12.e] Théorème de séparation des paramètres) *Soient $\mathcal{L}$ un langage du premier ordre, $\mathcal{M}$ une $\mathcal{L}$-structure stable avec M pour base, $\phi(x)$ une $\mathcal{L}$-formule à une variable libre exactement. Si $\psi(x, y_1, \ldots, y_l)$ est une $\mathcal{L}$-formule $(b_1, \ldots, b_l) \in M^l$, alors il existe une $\mathcal{L}$-formule $\theta(x, y_1, \ldots, y_m)$, $(a_1, \ldots, a_m) \in M^m$ dont chaque coordonnée satisfait $\phi(x)$ telle que $\mathcal{M} \models \forall x((\phi(x) \wedge \psi(x, b_1, \ldots, b_l)) \leftrightarrow \theta(x, a_1, \ldots, a_m))$.*

Ce théorème vérifie une propriété fondamentale des théories stables qui est à l'origine d'une notion fréquemment rencontrée dans les généralisations de la stabilité : celle d'un ensemble *stablement plongé*. Comme nous préférons le plus possible démontrer tout nouveau résultat et que nous ne démontrerons pas le fait 4.1.5 dans l'immédiat, nous tâcherons d'éviter de l'utiliser.

Nous venons de parler des paramètres. Insérons un lemme utile dont la preuve simple est un exercice.

Lemme 4.1.6 *Nous utilisons la même notation que celle de la définition 4.1.1. Si une formule avec paramètres provenant d'un modèle de T a l'une des propriétés définies dans les points (1)-(4) de la définition 4.1.1, alors il existe une $\mathcal{L}$-formule qui a la même propriété.*

Nous n'avons donné aucun exemple jusqu'à maintenant. Nous voulons décaler leur étude pour voir immédiatement les effets de l'absence des notions de la définition 4.1.1 au sein des groupes. Néanmoins, nous fournissons une liste avec des indications sur la nature stable ou instable des groupes en question. Des exemples sont plus difficiles à trouver et vérifier que les contrexemples.

1. Nous venons de dire que des exemples sont plus difficiles à trouver. Il aurait fallu préciser qu'il s'agissait des exemples infinis. En effet, quelque soit le choix de langage du premier ordre, toute structure finie est stable.
2. Soit $\mathcal{L}$ le langage d'une relation binaire. Alors la structure $(\mathbb{N}, |)$ où $|$ est la relation de divisibilité a la propriété d'indépendance. L'ensemble $\{a_i | i \in \mathbb{N}\}$ des nombres premiers et celui de leurs produits sans carrés $\{\prod_{i \leq j \leq k} a_{i_j} | \{i_1, \ldots, i_k\} \subset \mathbb{N}\}$ satisfont la condition de la propriété d'indépendance.
   La relation de divisibilité induit aussi la propriété de l'ordre strict. En effet il suffit de considérer une suite strictement croissante de nombres naturels $(n_i)_{i \in \mathbb{N}}$ telle que $n_i | n_{i+1}$, et les formules $x | n_i$.
3. Soit $\mathcal{L} = \{+, -, ., \ ^{-1}, 0, 1\}$ le langage des corps. Le groupe additif du corps des réels en tant que structure définie dans ce corps qui en hérite la structure induite est un groupe qui a la propriété de l'ordre strict mais pas celle d'indépendance. La première propriété, négative quoique positivement énoncée, est immédiate. La deuxième, plutôt positive mais négativement énoncée, nécessite plus de travail.
4. Un exemple dans le même esprit que le point précédent mais plus simple est $\mathcal{Q} = (\mathbb{Q}, <)$, un ordre dense linéaire sans extrémités dans le langage d'une relation binaire. La théorie $\mathrm{Th}(\mathcal{Q})$ a la propriété de l'ordre strict mais pas celle d'indépendance. Afin d'avoir une idée intuitive sur ce point, c'est un bon exercice d'étudier les types à paramètres dans $\mathbb{Q}$.
5. Le groupe symétrique sur $\mathbb{N}$, en d'autres le groupes de toutes les permutations des nombres naturels, et le groupe alterné sur $\mathbb{N}$ ont la propriété d'indépendance et celle de l'ordre strict. En effet, les deux conclusions s'obtiennent en considérant la formule de commutation : $xy = yx$. Pour vérifier la propriété d'indépendance pour le groupe symétrique on peut par exemple considérer les ensembles de permutations suivantes :

   pour tout $n \in \mathbb{N}^*$, $\{ (0\, i) \mid i \in \{1, \ldots, n\}\}$ et $\{ (i_1 \ \ldots \ i_k) \mid \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ et $i_1 < \ldots < i_k \}$

Quant à la propriété de l'ordre strict, il suffit de considérer les centralisateurs des permutations de la forme $(0\ 1\ \ldots k)$ avec $k \in \mathbb{N}^*$. La vérification des détails et celle des mêmes propriétés dans $\mathrm{Alt}(\mathbb{N})$ est un exercice.

6. Nous avons déjà mentionné qu'une théorie fortement minimale est stable. C'est vrai, on s'y attend, mais l'effort investi pour vérifier cette conclusion est suffisant pour faire mieux.

   Les corps algébriquement clos sont fortement minimaux en tant que modèles des CAC_p. Ils sont donc stables. Alors, le lemme 4.1.4 montre immédiatement que les groupes algébriques sont stables. Un vivier d'exemples de groupes stables qui sont par ailleurs stables de façon assez forte.

7. Le groupe $(\mathbb{Z}, +)$ est stable. Il faudra une certaine étude pour y arriver. En fait, dans le langage des groupes, tout groupe abélien est une structure stable avec éventuellement divers degrés de stabilité. Notons que, dans un langage approprié, tous les modules sont des structures stables.

Assez pour les exemples pour le moment... passons aux faits.

Lemme 4.1.7 *Soit $\mathcal{L}$ le langage des groupes, ou un langage avec un seul symbole de fonction binaire. Les $\mathcal{L}$-structures suivantes sont des groupes :*

1. *un semigroupe stable qui est simplifiable à gauche et à droite ;*
2. *un semigroupe stable simplifiable à gauche et qui possède un élément neutre à droite.*

Preuve. Notons $\mathcal{M}$ notre structure, et M sa base. Soit $a \in M$. Alors pour $m, n \in \mathbb{N}^*$ tels que $m < n$ la formule $\exists z(xz = y)$ est satisfaite par (a^m, a^n) en remplaçant z par a^{n-m}. Comme $\mathrm{Th}(\mathcal{M})$ est stable, cette formule ne peut pas ordonner $\{a^m | m \in \mathbb{N}^*\}$. Par conséquent, il existe $m, n \in \mathbb{N}^*$, avec $m < n$, et $b \in M$ tels que $a^n b = a^m$. Posons $e = a^{n-m}b$. Alors $a^m e = a^m$. Soit maintenant $c \in M$ un élément arbitraire. En appliquant la simplifiabilité à gauche à $a^m ec = a^m c$, nous concluons que $ec = c$. Alors e est neutre à gauche. Soit en reprenant le même raisonnement avec $b'a^n = a^m$ et la simplifiabilité à droite, soit par l'hypothèse du deuxième point, il existe un neutre à droite. Il existe donc un neutre et un seul.

Quant à l'inverse d'un élément a, quitte à reprendre la notation du paragraphe précédent, $a^{n-m-1}b$ est un inverse à droite de a. C'est suffisant (pourquoi ?) pour conclure que M est en effet un groupe. □

Corollaire 4.1.8
1. *Une partie définissable d'un groupe stable stable par rapport au produit en est un sous-groupe.*
2. *Un anneau intègre stable est un corps.*

Le lemme suivant est une autre conclusion simple et pratique qui illustre les conséquences fortes de la stabilité.

Lemme 4.1.9 *Soit G un groupe stable agissant définissablement comme groupe de permutations d'un ensemble E. Plus précisément, supposons qu'il existe une structure stable $\mathcal{M} = (G, E, \ldots)$ où G est un groupe, E un ensemble sur lequel opère G de façon à ce que la fonction $G \times E \to E$ qui définit cette action soit définissable dans $\mathcal{M}$. Si A est une partie définissable de E et $g \in A$, alors $gA \subset A$ si et seulement si $gA = A$.*

Preuve. Si $gA \subsetneq A$, alors la formule $\exists x \phi(yx)$, avec $\phi(u)$ une formule qui définit A, ordonne l'ensemble $\{g^n | n \in \mathbb{N}\}$. □

4.2 Conditions de chaîne dans les groupes

Dans cette section nous abordons l'étude des groupes stables proprement dite. La notion suivante sera omniprésente.

Définition 4.2.1 (Familles uniformément définissables d'ensembles) *Soient $\mathcal{L}$ un langage du premier ordre, $\mathcal{M}$ une $\mathcal{L}$-structure de base M, et $\phi(x,y)$ une $\mathcal{L}$-formule à $k+l$ variables. Une famille des parties de M^k est dite* uniformément définissable *si ses membres sont définis par des formules de la forme $\phi(x,a)$ où a provient d'un ensemble de paramètres fixé au préalable.*

Dans l'étude des groupes stables, les *conditions de chaîne* sur des familles de sous-groupes (uniformément) définissables sont primordiales. Elles imposent des conditions de finitude qui font des groupes stables des structures assez particulières. Une analogie peut-être un peu trop soulignée mais non sans intérêt serait la suivante : comparez ces conditions de chaîne et celles de finitude qui en résultent à la condition d'être un groupe fini. Remarquablement, les groupes qui nous intéresseront seront infinis.

Qu'est-ce qu'une condition de chaîne ? Dans notre contexte, elle aura la forme suivante : il n'existe pas de suite *infinie* et *strictement* descendante de sous-groupes

$$H_0 > H_1 > \dots$$

ayant une certaine propriété. Renforcée d'hypothèses de la théorie des modèles, une telle condition de chaîne implique fréquemment une "borne uniforme" sur la longueur de ces chaînes.

Lemme 4.2.2 *Soit G un groupe qui n'a pas la propriété de l'ordre strict. Si $\mathcal{H} = \{H_i | i \in I\}$ est une famille uniformément définissable de sous-groupes, alors toute chaîne descendante*

$$H_{i_0} > H_{i_1} > \dots$$

formée par les membres de $\mathcal{H}$ est d'une taille finie qui est bornée indépendamment des paramètres utilisés pour définir les groupes H_i.

Preuve. C'est une conséquence du lemme 4.1.2 (4). □

Lemme 4.2.3 *Soit G un groupe sans propriété d'indépendance. Alors à toute formule $\phi(x,y)$ à $1+k$ variables est associé un naturel n tel que l'intersection d'une famille arbitraire et finie $\{\phi(x,a_1),\dots,\phi(x,a_m)\}$ de sous-groupes soit l'intersection d'au plus n d'entre eux.*

Preuve. Supposons que G soit un contrexemple à l'énoncé. Alors pour tout $n \in \mathbb{N}$, il existe des sous-groupes $\phi(x,b_1),\dots,\phi(x,b_n)$ de G tels qu'aucun des $\phi(x,b_i)$ ne contienne l'intersection des autres. Donc pour chaque $1 \leq i \leq n$ il existe h_i tel que $G \models \neg\phi(h_i,b_i) \wedge \bigwedge_{j\neq i} \phi(h_i,b_j)$.

Pour tout $I \subseteq \{1,\dots,n\}$, on définit $h_I = \prod_{k\in I} h_k$. Bien qu'il y ait plusieurs possibilités de produit en changeant l'ordre des h_k, ceci n'est pas un problème puisque nous pouvons prendre les k en ordre croissant. Il découle de cette construction que $\mathcal{M} \models \neg\phi(h_I,b_i)$ si et seulement si $i \in I$. Comme n est arbitrairement large, le lemme 4.1.2 (3) permet de conclure que nous avons contredit que G n'a pas la propriété d'indépendance. □

L'hypothèse de stabilité entraîne une conséquence plus forte.

Corollaire 4.2.4 (Baldwin-Saxl) *Soit G un groupe stable. Alors à chaque formule $\phi(x,y)$ à $1+k$ variables libres est associé un nombre naturel n tel que l'intersection d'une famille* arbitraire *$\{\phi(x,b_i) : i \in I\}$ de sous-groupes de G soit celle de n d'entre eux. En particulier, les intersections des sous-groupes $\phi(x,b)$ de G forment une famille uniformément définissable.*

Preuve. Le lemme 4.2.3 montre qu'il existe $n \in \mathbb{N}$ tel que les intersections finies des $\phi(x,b_i)$ soient celle d'au plus m d'entre eux et que par conséquent, ces intersections forment une famille uniformément définissable de sous-groupes de la forme $H_{i_1} \cap \dots \cap H_{i_m}$. Alors le lemme 4.2.2

s'applique à cette famille $\{\bigcap_{j=1}^{m} H_{i_j} | i \in I\}$ d'intersections finies et borne uniformément par un naturel n la taille de toute chaîne descendante.

Soit $K_1 > \ldots > K_n$ une chaîne non redondante telle que $K_i = \bigcap_{j=1}^{m} H_{i_j}$. Posons par ailleurs, $H = \cap_{i \in I} H_i$. Alors $H \leq K$. Il est par ailleurs impossible que $H < K$. En effet, une inclusion stricte serait causée par un certain H_i que nous pourrions utiliser pour former une nouvelle intersection K_{n+1} et donc une chaîne $K_1 \ldots > K_n > K_{n+1}$: c'est une contradiction. Ainsi, les tailles des intersections des H_i sont bornées par mn. □

Corollaire 4.2.5 *Dans un groupe stable G, les centralisateurs $\{C_G(X) : X \subseteq G\}$ forment une famille uniformément définissable : il existe un nombre naturel n tel que dans tout $X \subseteq G$ il existe $\{x_1, \ldots, x_k\}$ $(k \leq n)$ tels que $C_G(X) = \cap_{i=1}^{k} C_G(x_i)$. En particulier, tous les centralisateurs sont définissables. Ce nombre n borne aussi les longueurs de toutes les chaînes de centralisateurs.*

4.3 Notions de composante connexe ; conséquences algébriques

Les notions de "composante connexe" qui seront développées dans cette section ont une double importance. D'un côté elles ont des analogues dans des classes bien connues de groupes, d'un autre côté elles font partie intégrante de l'étude plus générale des *génériques* dans les groupes stables. En effet, les groupes stables satisfont non seulement des conditions de définissabilité particulières mais jouissent d'une "distribution uniforme et équivariante" des quantités de définissabilité, telle une notion de mesure qui leur donne une certaine géométrie.

Lemme 4.3.1 *Soient G un groupe arbitraire et H un sous-groupe d'indice fini dans G définissable par une formule éventuellement avec paramètres. Alors, le fait que $|G : H| = n$ s'exprime par un énoncé du premier ordre dans le langage des groupes augmenté éventuellement par les paramètres utilisés dans la formule qui définit H.*

Preuve. Exercice. □

Lemme 4.3.2 *Soient G un groupe stable et $\phi(x; y_1, \ldots, y_k)$ une formule à $1 + k$ variables libres dans le langage des groupes. L'intersection de tous les sous-groupes d'indice fini défini par une formule du type $\phi(x; g_1, \ldots, g_k)$ avec $(g_1, \ldots, g_k) \in G^k$ est l'intersection d'un nombre fini d'entre eux. En particulier, il est d'indice fini dans G.*

Cette intersection, notée $G^\circ(\phi)$ et dite la composante ϕ-connexe *de G, est définissable sans paramètres. En particulier, la formule qui la définit, définit la composante ϕ-connexe de toute extension élémentaire de G.*

Preuve. Fixons une formule $\phi(x; y_1, \ldots, y_k)$. D'après le Corollaire 4.2.4, il existe $n_\phi \in \mathbb{N}^*$ tel que toute intersection de sous-groupes définis par des formules $\phi(x; g_1, \ldots, g_k)$ avec $(g_1, \ldots, g_k) \in G^k$ soit l'intersection d'au plus n_ϕ d'entre eux. Il s'agit donc d'une autre famille uniformément définissable de sous-groupes.

D'après le lemme 4.2.2, la borne n_ϕ borne aussi la longueur des chaînes descendantes formées par ces intersections, en particulier celles formées par les sous-groupes d'indice fini dans G. Il en découle aussi que ces indices sont bornés et que la borne est l'indice dans G de l'intersection de tous les sous-groupes d'indice fini définis par une formule $\phi(x; g_1, \ldots, g_k)$ avec $(g_1, \ldots, g_k) \in G^k$. Si cet indice est noté K_ϕ, alors la formule suivante sans paramètres définit $G^\circ(\phi)$, quitte à abbrévier les y_i par y :

$$\forall y \exists x_1 \ldots x_{K_\phi} \forall z \left(\phi(x; y) \wedge \text{ "}\phi(x; y) \text{ est un sous-groupe" } \wedge \left(\bigwedge_{1 \leq i < j \leq K_\phi} \neg\phi(x_i^{-1} x_j; y) \wedge \bigvee_{1 \leq i \leq K_\phi} \phi(z^{-1} x_i; y) \right) \right)$$

□

Cette notion de "composante connexe locale" est réminiscente de celle en théorie des groupes algébriques. Dans des groupes stables avec des conditions plus fortes de chaînes, elle devient de plus en plus globale, et ressemble de plus en plus à la notion analogue dans les groupes algébriques. En effet, si la condition de chaîne descendante concernait tous les sous-groupes définissables de tous les modèles de $\mathrm{Th}(G)$, alors G aurait une *composante connexe* : l'intersection de tous les sous-groupes définissables d'indice fini. Cette composante connexe serait définissable sans paramètres.

Un groupe stable G qui est égale à $G^\circ(\phi)$ pour un certain ϕ est dit *ϕ-connexe*. Il est important de noter que la composante ϕ-connexe d'un groupe stable n'est pas nécessairement ϕ-connexe quand nous considérons celle-ci comme un groupe stable définissable dans une structure stable plus large. Donnons un exemple simple en admettant pour le moment que $\mathrm{Th}(\mathbb{Z}, +, -, 0)$ est stable. Fixons $n \in \mathbb{N} \setminus \{0, 1\}$ et notons $\phi(x)$ la formule $\exists y(ny = x)$. La formule $\phi(x)$ définit dans $\mathbb{Z}$ les multiples de n. Défini sans paramètres, ce sous-groupe est la composante ϕ-connexe de $\mathbb{Z}$. En particulier $\mathbb{Z}$ n'est pas ϕ-connexe. Or, $n\mathbb{Z}$ est isomorphe à $\mathbb{Z}$, ainsi il n'est pas formé par ses éléments qui sont multiples de n.

Le phénomène du paragraphe précédent est lié à la présence des quantificateurs dans la définition des multiples de n dans $\mathbb{Z}$, ce qui est inévitable sans changer de langage. Le lemme suivant explique ce qu'il en est avec des sous-groupes définis par les instances d'une formule sans quantificateur :

Lemme 4.3.3 *Soient G un groupe stable et $\phi(x; y)$ une formule à $1 + k$ variables sans quantificateurs. Alors, $G^\circ(\phi)$, la composante ϕ-connexe de G, est ϕ-connexe.*

Preuve. La composante ϕ-connexe $G^\circ(\phi)$ est définie par une conjonction finie de la forme $\wedge_{i=1}^{m} \phi(x; g_m)$, une intersection que nous pouvons supposer non redondante. Etant définissable dans G, c'est une sous-structure stable de G. En particulier, $(G^\circ(\phi))^\circ(\phi)$ existe et est une intersection de la forme $\wedge_{i=1}^{m'} \phi(x; h_m)$ avec $\{h_1, \ldots, h_{m'}\} \subset G^\circ(\phi)^k$. Si $(G^\circ(\phi))^\circ(\phi) < G^\circ(\phi)$, alors il existe $h \in G^\circ(\phi)$ tel que $G^\circ(\phi) \models \neg(G^\circ(\phi))^\circ(\phi)(h)$, soit encore, $G^\circ(\phi) \models \neg\wedge_{i=1}^{m'} \phi(h; h_{m'})$. Il existe ainsi $l \in \{1, \ldots, m'\}$ tel que $G^\circ(\phi) \models \neg\phi(h; h_l)$. Comme la formule $\neg\phi(x; y)$ est sans quantificateur, il s'ensuit que $G \models \neg\phi(h; h_l)$. Or, $G \models \wedge_{i=1}^{m} \phi(h; g_m)$ puisque h appartient à $G^\circ(\phi)$. Par conséquent, $\bigwedge_{i=1}^{m} \phi(x; g_m) \wedge \phi(x; h_l) < \bigwedge_{i=1}^{m} \phi(x; g_m)$, ce qui contredit la minimalité de $G^\circ(\phi)$. □

Une formule du premier ordre sans quantificateurs qui se dégage rapidement par son importance en théorie des groupes est celle du centralisateur : $xy = yx$. On parle alors de la composante *centralisateur-connexe* d'un groupe stable ou encore des *groupes centralisateur-connexes*. Dans un groupe stable centralisateur-connexe, le centralisateur de tout élément non central est d'indice infini.

Nous finissons cette section en démontrant certaines de leurs propriétés les plus simples dont les preuves portent les traces de raisonnements plus élaborés.

Lemme 4.3.4 *Dans un groupe G stable, toute partie finie et normalisée par G est centralisée par la composante centralisateur-connexe de G.*

Preuve. Si x appartient à une telle partie N de G, alors $x^G = \{g^{-1}xg | g \in G\} \subset N$. Par conséquent, $C_G(x)$ est d'indice fini dans G. □

Lemme 4.3.5 *Un groupe G stable qui a un nombre fini de commutateurs est* virtuellement central *ou* central par fini *; en d'autres termes, $|G : Z(G)| < \infty$.*

Preuve. Pour tout $g \in G$, $\{[g, x] | x \in G\}$ est de cardinal fini. Par conséquent g^G est fini. Alors, le lemme 4.3.4 s'applique à tout élément de G. □

Lemme 4.3.6 *Si G est un groupe stable centralisateur-connexe de centre fini, alors $Z(G) = Z_2(G)$.*

Preuve. Si $g \in Z_2(G)$, alors $\{[g, x] | x \in G\} \leq Z(G)$ et est fini. □

4.4 Stabilité et types

Cette section est consacrée à l'étude des propriétés des types d'une théorie stable. Comme nous l'avons indiqué, la définition 4.1.3 est en fait une caractérisation. Notre travail ci-dessous nous permettra d'obtenir son équivalence à la définition de la stabilité en fonction des types ainsi qu'à d'autres caractérisations de cette notion. C'est un travail relativement long au long duquel nous développerons des méthodes pour décider de la stabilité de certaines théories et des outils afin d'aboutir à une étude systématique des groupes stables.

Nous supposerons nos langages dénombrables. Par ailleurs, pour diminuer la taille de nos litanies introductrices à maints énoncés, nous supposerons que, sauf mention contraire, le langage du premier ordre sous-jacent est appelé $\mathcal{L}$ et une théorie du premier ordre est une $\mathcal{L}$-théorie.

Définition 4.4.1 *Soit T une $\mathcal{L}$-théorie complète, et κ un cardinal infini. La théorie T est dite κ-stable si pour tout modèle $\mathcal{M}$ de T de base M et toute partie A de M de cardinal au plus κ le cardinal de l'ensemble $S_1(A)$ est au plus κ. Une $\mathcal{L}$-structure $\mathcal{M}$ est dite κ-stable si* $\mathrm{Th}(\mathcal{M})$ *est κ-stable.*

C'est une définition qui n'est pas très motivante a priori. Néanmoins, il est bien visible qu'elle impose une certaine structure à ce qui est définissable dans les modèles d'une théorie complète. Nous verrons rapidement certaines de ses implications fortes qui nous permettront de vérifier certaines assertions faites dans la section 4.1. Mais avant d'aller plus loin débarassons-nous d'une classe de structures dont les propriétés de stabilité sont trop immédiates pour être utiles. La théorie d'une structure finie dans un langage du premier ordre est κ-stable pour tout κ. Nous supposerons que nos théories complètes n'ont pas de modèles finis.

Une composante majeure de nos objectifs principaux est de vérifier qu'une théorie est stable au sens de la définition 4.1.3 si et seulement si elle est κ-stable pour un cardinal infini κ. La vérification d'une certaine partie de cette équivalence est presque immédiate. C'est ce que nous ferons dans l'immédiat. Le lemme suivant élargira notre marge de manoeuvre :

Lemme 4.4.2 *Une théorie complète T est κ-stable si et seulement si pour tout $n \in \mathbb{N}$, pour tout ensemble A de paramètres extraits d'un modèle arbitraire de T, $|S_n(A)| \leq \kappa$.*

Preuve. La suffisance de la condition sur tous les types est claire. La preuve de sa nécessité se fait par récurrence sur n. Le cas $n = 0$ est clair, et le cas $n = 1$ est l'hypothèse. Considérons $S_{n+1}(A)$ où A est un ensemble de cardinal au plus κ. Soit p un élément de cet ensemble. Par définition d'un type, p contient un n-type aussi, par exemple ses formules dont les variables libres sont parmi $x_1, \ldots, x_n$. Soit $(\alpha_1, \ldots, \alpha_n)$ une réalisation de cette restriction. Alors $\{\phi(\alpha_1, \ldots, \alpha_n, x_{n+1}) | \phi(x_1, \ldots, x_{n+1}) \in p\}$ est un type dans $S_1(A \cup \{\alpha_1, \ldots, \alpha_n\})$. Le cardinal de $A \cup \{\alpha_1, \ldots, \alpha_n\}$ n'étant pas supérieur à κ, par hypothèse, il existe au plus κ 1-types sur $A \cup \{\alpha_1, \ldots, \alpha_n\}$. Par récurrence, p n'a qu'au plus κ restrictions de n variables. Par conséquent, il existe au plus κ $(n+1)$-types sur A. □

Lemme 4.4.3 *Pour tout cardinal infini κ, il existe une chaîne de cardinal κ^+ (le plus petit cardinal strictement suérieur à κ) ayant une sous-chaîne dense de cardinal κ.*

Preuve. Soient κ un cardinal infini et λ le plus petit cardinal tel que $\kappa^\lambda > \kappa$. Un tel cardinal λ existe et est en fait inférieur ou égal à κ puisque $\kappa^\kappa = 2^\kappa > \kappa$.

L'ensemble κ^λ des fonctions de λ vers κ muni de l'ordre *lexicographique* qui consiste à dire que

$$f < g \quad \text{si} \quad f(\alpha) < g(\alpha) \text{ au premier rang } \alpha < \lambda \text{ où } f(\alpha) \neq g(\alpha),$$

forment une chaîne de cardinal au moins κ^+. L'ensemble des fonctions éventuellement 0 est une sous-chaîne dense de cardinal κ. Il suffit donc de restreindre κ^λ à une sous-chaîne de cardinal κ^+ contenant les fonctions éventuellement 0. Les détails sont laissés comme exercice ou devoir de lecture ([9], le théorème 8.10). □

Corollaire 4.4.4 *Si une théorie complète T est κ-stable pour un certain cardinal infini κ, alors T est une théorie stable.*

Preuve. Supposons qu'il existe une formule $\phi(x, y)$ à $k+k$ variables libres ($k \in \mathbb{N}^*$) qui ordonne un ensemble infini de M^k, M étant la base M d'un modèle $\mathcal{M}$ de T. Nous montrerons que T n'est κ-stable pour aucun κ. En raisonnnant par compacité et en utilisant le lemme 4.4.3 (fournir les détails), nous pouvons montrer que $\mathcal{M}$ a une extension élémentaire, que nous continuerons d'appeler $\mathcal{M}$, telle que ϕ ordonne dans M^k une partie infinie indexée par une chaîne de cardinal κ^+ avec une sous-chaîne de cardinal κ. Notons C^+ et C ces parties de cardinaux κ^+ et κ respectivement. Pour $\alpha, \beta \in C^+ \setminus C$, si $\alpha \neq \beta$, alors $\mathrm{tp}(\alpha/C) \neq \mathrm{tp}(\beta/C)$ puisqu'il existe $c \in C$ tel que

$$\mathcal{M} \models (\phi(\alpha, c) \wedge \phi(c, \beta)) \vee (\phi(\beta, c) \wedge \phi(c, \alpha)) \quad .$$

Ainsi $|S_k(C)| > \kappa$. Le lemme 4.4.2 permet de conclure. □

Ce corollaire est très utile pour vérifier la stabilité de certaines théories. C'est ce que nous ferons immédiatement.

Lemme 4.4.5 *Une théorie fortement minimale est $\aleph_0$-stable, en particulier stable.*

Preuve. Soit T la théorie en question. Nous compterons les 1-types de T sur un ensemble dénombrable de paramètres. Il suffit en fait de faire le comptage sur la base M d'un modèle dénombrable $\mathcal{M}$ de T (pourquoi ?). Deux possibilités se présentent pour tout type p dans $S_1(M)$. Soit p contient une formule définissant un ensemble fini dans lequel cas il est déjà réalisé dans $\mathcal{M}$, soit p ne contient que des formules qui définissent des ensembles infinis, donc cofinis par hypothèse. Or, il n'existe qu'un seul type dans $S_1(M)$ qui a cette propriété. En effet, s'il y avait deux types "cofinis", disons p_1 et p_2, alors il existerait une formule θ qui les séparerait. Mais cette formule ne peut définir ni un ensemble fini ni un ensemble cofini, une contradiction. Puisque M est dénombrable, il découle que $S_1(M)$ est un ensemble dénombrable aussi. □

Corollaire 4.4.6 *Dans le langage $\mathcal{L}_C$ des corps, la théorie CAC_p est $\aleph_0$-stable, donc en particulier stable.*

Ce dernier corollaire peut être démontré plus directement en n'utilisant que les propriétés des polynômes. Pouvez-vous voir comment ?

La proposition suivante permet de tirer d'autres conclusions de stabilité à partir de celle des corps algébriquement clos. Elle sera utile dans d'autres contextes aussi.

Proposition 4.4.7 *Soient $\mathcal{M}$ et $\mathcal{M}'$, des $\mathcal{L}$- et $\mathcal{L}'$-structures respectivement. Si $\mathcal{M}$ est κ-stable pour un cardinal infini κ et que $\mathcal{M}'$ est définissable dans $\mathcal{M}$, alors $\mathcal{M}'$ est aussi κ-stable.*

La preuve est intuitivement claire puisqu'on s'attend à ce que la "traduction" de tout ensemble de paramètres permettant de définir beaucoup de types par rapport à $\mathrm{Th}(\mathcal{M}')$ ait le même effet sur $\mathrm{Th}(\mathcal{M})$. Le problème technique à régler est une question d'ordre général : pour toute extension élémentaire $\mathcal{N}'$ de $\mathcal{M}'$, en existe-t-il une, disons $\mathcal{N}$, de $\mathcal{M}$ dans laquelle $\mathcal{N}'$ est définie de la même façon que $\mathcal{M}'$ dans $\mathcal{M}$? Le lemme suivant répond à cette question.

Lemme 4.4.8 *Soient $\mathcal{M}$ et $\mathcal{M}'$, des $\mathcal{L}$- et $\mathcal{L}'$-structures respectivement telles que $\mathcal{M}'$ soit définissable dans $\mathcal{M}$ au sens de la définition 3.5.2, dont nous utiliserons la notation. Si $\mathcal{N}'$ est une extension élémentaire de $\mathcal{M}'$, alors $\mathcal{M}$ a une extension élémentaire $\mathcal{N}$ dans laquelle $\mathcal{N}'$ est définie en utilisant les mêmes formules qui définissent $\mathcal{M}'$ dans $\mathcal{M}$.*

Preuve. La preuve est par compacité. Nous augmentons d'abord le langage $\mathcal{L}$ à $\mathcal{L}^+$ en y ajoutant un symbole de constante c_a pour nommer chaque $a \in M$, la base de $\mathcal{M}$, et aussi des symboles $c_{b,j}$ $(1 \leq j \leq n)$ pour chaque $b \in N'$, la base de $\mathcal{N}'$. Nous posons ensuite

$$T^+ = \mathrm{Th}((\mathcal{M}, m)_{a \in M}) \cup \{\ D(c_{b_{11}}, \ldots, c_{b_{1n}}; \ldots; c_{b_{k1}} \ldots c_{b_{kn}}) \wedge$$

$$\phi(c_{b_{11}},\dots,c_{b_{1n}};\dots;c_{b_{k1}}\dots c_{b_{kn}}) \mid \mathcal{N}' \models \phi'(b_1,\dots,b_k) \}$$

où la formule D définit $\mathcal{M}'$ dans $\mathcal{M}$ et la formule ϕ est la traduction dans $\mathcal{L}$ de la $\mathcal{L}'$-formule ϕ', celle-ci décrivant toutes les $\mathcal{L}'$-formules. Une partie finie de T^+ est satisfaite dans $\mathcal{M}$ puisque $\mathcal{N}'$ est une extension élémentaire de $\mathcal{M}'$. En effet, si $\phi(c_{b_{11}},\dots,c_{b_{1n}};\dots;c_{b_{k1}}\dots c_{b_{kn}})$ traduit une satisfaction $\mathcal{N}' \models \phi'(b_1,\dots,b_k)$ alors, comme $\mathcal{M}' \preceq \mathcal{N}'$, il existe $(a_1,\dots,a_k) \in M'^k$ tel que $\mathcal{M}' \models \phi'(a_1,\dots,a_k)$. La définition de $\mathcal{M}'$ dans $\mathcal{M}$ implique alors que

$$\mathcal{M} \models D(a_{11},\dots,a_{1n};\dots;a_{k1},\dots,a_{kn}) \ \wedge \ \phi(a_{11},\dots,a_{1n};\dots;a_{k1},\dots,a_{kn}) \ .$$

Par conséquent, nous pouvons interpréter $c_{b_{ij}}$ $(1 \leq i \leq k,\ 1 \leq j \leq n)$ par les a_{ij} respectifs.

Par compacité, T^+ est consistant. Ainsi, après réduction au langage $\mathcal{L}$, nous concluons l'existence d'une extension élémentaire de $\mathcal{M}$ dans laquelle est définie $\mathcal{N}'$ en utilisant la même définition que celle de $\mathcal{M}'$ dans $\mathcal{M}$. □

Preuve de la proposition 4.4.7. Nous utiliserons la notation du lemme 4.4.8. Si $\mathrm{Th}(\mathcal{M}')$ n'est pas une théorie κ-stable, alors il existe un ensemble de paramètres A de cardinal au plus κ, contenu dans une extension élémentaire de $\mathcal{M}'$ tel que $|S_1(A)| > \kappa$. Le lemme 4.4.8 nous permet de supposer que cette extension élémentaire est $\mathcal{M}'$. L'ensemble A correspond alors à une partie A' de cardinal κ de M^n. Or deux types se distinguent par l'appartenance d'une formule au premier et de la négation de celle-ci au deuxième, ainsi $|S_n(A')| > \kappa$. D'après le lemme 4.4.2, $\mathrm{Th}(\mathcal{M})$ n'est pas κ-stable non plus. □

Il convient de remarquer un point important qui peut échapper à la première rencontre avec la question de définition d'une structure dans une autre. La proposition 4.4.7 montre que la structure $\mathcal{M}'$ est stable même avec une structure supplémentaire qui lui est imposée par la structure ambiante $\mathcal{M}$. C'est d'ailleurs ce sens plus général que nous accorderons à la notion de structure, en particulier groupe (κ-)stable : celui d'une structure (resp. un groupe) définissable dans une structure (κ-)stable munie de la structure éventuellement supplémentaire provenant de la structure ambiante.

Corollaire 4.4.9 *Un groupe algébrique est une $\mathcal{L}_C$-structure $\aleph_0$-stable. Par conséquent, c'est aussi une $\mathcal{L}_G$-structure $\aleph_0$-stable où $\mathcal{L}_G$ est le langage des groupes.*

Preuve. La première conclusion découle du corollaire 4.4.6 et de la proposition 4.4.7. La deuxième est une conséquence de la première, de la proposition 4.4.7 et du fait que la structure de groupe d'un groupe algébrique est définissable dans la structure de corps. □

Après ce retour à notre univers principal, celui des groupes, nous amorçons le dernier volet du périple général. Nous montrerons l'équivalence entre la stabilité et la κ-stabilité pour un κ convenable (Théorème 4.1). Le raisonnement donne une idée plus fine de la combinatoire, déjà rencontrée, de la stabilité en théorie des modèles et permet d'introduire certaines notions fondamentales que nous utiliserons plus tard.

Définition 4.4.10 *Soient T une théorie complète, $\mathcal{M}$ un modèle de T de base M, $A \subset B \subset M$ et $k, l \in \mathbb{N}$. Un type $p \in S_k(B)$ est dit* A-définissable *si pour toute $\mathcal{L}$-formule $\phi(x,y)$ à $k+l$ variables libres, il existe une $\mathcal{L}(A)$-formule $\psi(y)$ telle que pour $b \in B^l$, $\phi(x,b) \in p$ si et seulement si $\mathcal{M} \models \psi(b)$. Le type sera dit définissable si $A = B$.*

Fréquemment la notation $d_p\phi(y)$, ou une légère variante de celle-ci, est utilisée pour noter une formule de définition.

Dans un premier temps, nous donnons deux exemples de définissabilité de types, le premier général, le deuxième appartenant à un contexte instable afin de souligner que la notion n'est pas contrainte par des hypothèses de stabilité.

1. Soient T une théorie complète arbitraire, $\mathcal{M}$ un modèle de T de base M et $A \subset M$. Si $p \in S_k(A)$ est un type isolé pour un certain $k \in \mathbb{N}$, alors p est définissable. En effet,

supposons que la formule $\psi(x,a)$ avec $a \in A^l$ isole p. Alors, pour toute $\mathcal{L}$-formule $\phi(x,y)$ et tout uple b de paramètres extraits de A, $\phi(x,b)$ appartient à p si et seulement si

$$\mathcal{M} \models \forall x(\psi(x,a) \longrightarrow \phi(x,b)) \ .$$

Il en découle que $d_p\phi(y)$ est la formule $\forall x(\psi(x,a) \longrightarrow \phi(x,y))$. Notez que p est en fait a-définissable.

2. Considérons maintenant la structure $\mathcal{Q} = (\mathbb{Q}, <)$, les rationnels munis de leur ordre usuel. La théorie complète en question est celle des chaînes denses sans extrémités. Nous étudierons deux 1-types à paramètres dans $\mathbb{Q}$, qui est la base d'un modèle. Le premier sera définissable, le deuxième non.

   Fixons $q \in \mathbb{Q}$ et considérons le type q^+ contenant les formules suivantes :

$$\{\ x < r \mid r \in \mathbb{Q} \text{ et } q < r\ \} \ \cup\ \{\ r < x \mid r \in \text{ et } r \leq x\} \ .$$

   C'est un type non réalisé dans $\mathcal{Q}$.

   Avant de discuter de la définissabilité de q^+, faisons une remarque sur la détermination de q^+. Les formules ci-dessus ne sont en fait pas seulement contenues dans q^+, elles le déterminent ; il n'existe pas d'autre 1-type dans $S_1(\mathbb{Q})$ qui contient ces formules. En effet, comme la théorie des chaînes denses sans extrémités, donc $\mathrm{Th}(\mathcal{Q})$, élimine les quantificateurs, toute formule à paramètres dans $\mathbb{Q}$ et à une variable est équivalente à une combinaison booléenne des formules de la forme $x < r$ et $r < x$ avec $r \in \mathbb{Q}$. Donc toute paire d'éléments dans une extension élémentaire $\mathcal{Q}$ satisfaisant les formules ci-dessus ont même type. Il est de coutume de dire que le type d'un élément est déterminé par son *type sans quantificateur*, en d'autres termes la restriction de son type aux formules sans quantificateurs de celui-ci. C'est une autre façon de dire que la théorie en question élimine les quantificateurs.

   Toujours grâce à l'élimination des quantificateurs, afin de vérifier la définissabilité de q^+ il suffit de trouver des formules de définition pour les formules $x < y$, $y < x$ et $x = y$ dans lesquelles la variable y sera remplacée par des paramètres. La liste suivante fait la tâche :

$$d_{q^+}(\ x < y\ ) \ =\ q < y \quad ; \quad d_{q^+}(\ y < x\ ) \ =\ y < q \vee y = q \quad ; \quad d_{q^+}(\ x = y\ ) \ =\ y \neq y \ .$$

   Maintenant fixons un élément α dans une extension élémentaire de $\mathcal{Q}$, qui n'est pas dans $\mathbb{Q}$ et qui décrit une *coupure* dans $\mathbb{Q}$. En d'autres termes, α est minoré et majoré par des rationnels, et l'ensemble de ses minorants (resp. majorants) ne possède pas de borne supérieure (resp. inférieure). Nous pouvons choisir un nombre réel irrationnel pour représenter α. Décrivons le type $\mathrm{tp}(\alpha/\mathbb{Q})$:

$$\{\ x < q \mid q \in \mathbb{Q} \text{ et } \alpha < q\ \} \ \cup\ \{\ q < x \mid q \in \text{ et } q \leq \alpha\} \ .$$

   L'élimination des quantificateurs implique que ces formules déterminent $\mathrm{tp}(\alpha/\mathbb{Q})$. Contrairement à q^+, $\mathrm{tp}(\alpha/\mathbb{Q})$ n'est pas définissable. En effet, s'il l'était, la formule $x < y$ aurait une définition $d_\alpha(x < y)$ à paramètres $q_1, \ldots, q_l$ dans $\mathbb{Q}$ que nous pouvons supposer en ordre strictement croissant. Par élimination des quantificateurs, $d_\alpha(x < y)$ est une combinaison booléenne des formules du type $y < q_i$ et $q_j < y$.

   Maintenant montrons que les données du paragraphe précédent aboutissent à une contradiction. Soit q un rationnel supérieur à α. Par conséquent, $x < q \in \mathrm{tp}(\alpha/\mathbb{Q})$, équivalemment $\mathcal{Q} \models d_{\mathrm{tp}(\alpha/\mathbb{Q})}(x < y)(q)$. Si $q_i < \alpha$ pour tout $i \in \{1, \ldots, l\}$, alors $d_{\mathrm{tp}(\alpha/\mathbb{Q})}(x < y)$ est de la forme

$$\bigwedge_{i=1}^{l} q_i < y \ .$$

   Or, il existe $s \in \mathbb{Q}$ tel que $q_l < s < \alpha$, et par conséquent $\mathcal{Q} \models d_{\mathrm{tp}(\alpha/\mathbb{Q})}(x < y)(s)$ bien que $x < s$ n'appartienne pas à $\mathrm{tp}(\alpha/\mathbb{Q})$. Ainsi, il existe $i \in \{1, \ldots, l\}$ tel que $\alpha < q_i$. Dans ce

cas, choisissons $s_1, s_2 \in \mathbb{Q}$ tels que $\alpha < s_1 < q_i < s_2$. Alors, $x < s_1$ et $x < s_2$ appartiennent à $\mathrm{tp}(\alpha/\mathbb{Q})$, mais

$$\mathcal{Q} \models \neg(d_{\mathrm{tp}(\alpha/\mathbb{Q})}(x < y)(s_1) \wedge d_{\mathrm{tp}(\alpha/\mathbb{Q})}(x < y)(s_2)) \ .$$

Cette contradiction finit la vérification de la non définissabilité de $\mathrm{tp}(\alpha/\mathbb{Q})$.

Nous avons déjà souligné que la notion de κ-stabilité signifie la maîtrise de la structure définissable dans les modèles d'une théorie complète. La définissabilité d'un type offre un autre aspect, équivalent à la stabilité comme le montrera le théorème 4.1, du même phénomène. Non seulement elle signifie la définissabilité de l'appartenance à un type mais, vérifiant ceci explicitement au niveau des paramètres (les formules de définition doivent être satisfaites par les paramètres de la formule concernée), elle met en relief une forte symétrie entre une formule du premier ordre et ses paramètres, ou plus concrètement entre les éléments satisfaisant cette formule (appartenant à l'ensemble défini par celle-ci) et les mêmes paramètres. Cette symétrie est liée aux notions de symétrie qui seront introduites à la fin de cette section.

Lemme 4.4.11 *Soient $\phi(x, y)$ une $\mathcal{L}$-formule à $k+l$ variables libres, $\mathcal{M}$ et $\mathcal{N}$ deux $\mathcal{L}$-structures de base M et N respectivement. Si $\mathcal{M} \preceq \mathcal{N}$ et $c \in N^k$, alors toute formule $\phi(x, a)$ du $\mathrm{tp}(c/M)$ est satisfaite par un élément de M^k.*

Preuve. Comme $\mathcal{N} \models \phi(c, a)$ et que $\mathcal{M} \preceq \mathcal{N}$, il existe un élément $c' \in M^k$ tel que $\mathcal{M} \models \phi(c', a)$. □

Lemme 4.4.12 *Une $k + l$-formule $\phi(x, y)$ n'a pas la propriéte de l'ordre si et seulement si $\neg\phi(x, y)$ ne l'a pas.*

Preuve. La négation d'une formule n'en est pas moins une formule que celle dont elle est la négation. □

Le lemme suivant est la clé technique pour le théorème 4.1. Nous suivons la preuve donnée dans [7]. Il y a d'autres manières d'aboutir aux mêmes conclusions de façon plus confortable et conceptuelle mais il faut développer d'autres notions, ce qui reste bien en dehors de nos objectifs. Par ailleurs, la méthode de preuve ci-dessous explicite clairement la formule de définition ainsi que sa construction dans un modèle fixé.

Notons aussi que la preuve aboutit même sans l'hypothèse de stabilité de T. Il suffit que la formule en question n'ait pas la propriété de l'ordre. La même construction est possible à partir de cette hypothèse locale et du lemme 4.4.12 qui implique l'absence de la propriéte de l'ordre pour la négation.

Lemme 4.4.13 *Soient T une théorie complète stable et $\mathcal{M}$ un modèle de T de base M. Pour tout $k \in \mathbb{N}$, tout k-type de $S_k(M)$ est définissable.*

Preuve. La preuve consiste à construire pour chaque formule $\mathcal{L}$-formule $\phi(x, y)$ à $k+l$ variables, qui n'a pas la propriété de l'ordre, une définition en suivant une recette inductive. Pour commencer, nous fixons la notation de départ. Soit c une réalisation de p. En général, c est un k-uple extrait de la base d'une extension élémentaire $\mathbb{C}$ de $\mathcal{M}$. Comme cette extension élémentaire n'intervient que pour des satisfactions dans les raisonnements suivants, afin de ne pas alourdir la notation et pour d'autres raisons aussi, nous éviterons d'utiliser la lettre $\mathbb{C}$; en particulier, nous noterons $\models \phi...$ toute satisfaction dans $\mathbb{C}$.

Soit donc $\phi(x, y)$ une $k + l$-formule arbitraire. D'après les lemmes 4.1.2 (1) et (2), et 4.4.12 il existe une borne d'alternance $N \in \mathbb{N}$ tel qu'il n'existe pas

de suites $(a_i)_{i\leq N}$ et $(b_i)_{i\leq N}$ extraites de M^k et M^l telles que $\mathcal{M} \models \phi(a_i, b_j)$ si et seulement si $i < j$,

de suites $(a_i)_{i\leq N}$ et $(b_i)_{i\leq N}$ extraites de M^k et M^l telles que $\mathcal{M} \models \neg\phi(a_i, b_j)$ si et seulement si $i < j$.

Remarquons que c'est le seul point où la stabilité de T, voire celle "d'une formule", intervient.

Nous construirons deux suites de parties finies M^l qui seront notées A_i et B_i ($i \in \mathbb{N}$) respectivement. Cette construction se fera en parallèle avec la construction d'une suite de réalisations dans $\mathcal{M}$ des instances de la formule $\phi(x, y)$ ou de sa négation, notées c_i ($i \in \mathbb{N}$). Pour chaque $n \in \mathbb{N}$ nous utiliserons deux ensembles K_n et L_n de parties de $\{0, \ldots, n-1\}$.

Nous commençons à définir K_n, L_n et c_n pour à partir de $n = 0$. Pour tout $a \in M^l$, l'un des deux cas suivants se présente :

$$\models \neg\phi(c, a) \quad , \quad \models \phi(c, a) \ .$$

Nous choisissons arbitrairement $a_0^\emptyset \in M^l$, $b_0^\emptyset \in M^l$ témoins respectifs de ces deux possibilités qui se présentent, en d'autres termes

$$\models \neg\phi(c, a_0^\emptyset) \quad , \quad \models \phi(c, b_0^\emptyset) \ .$$

Nous posons ensuite $A_0 = \{a_0^\emptyset\}$ et $B_0 = \{b_0^\emptyset\}$ pourvu qu'un tel l-uple existe. Sinon, l'ensemble correspondant est vide. Quoi qu'il en soit, l'un des deux ensembles sera non vide. Suivant lequel est non vide, nous posons $K_0 = \{\emptyset\}$ ou $L_0 = \{\emptyset\}$. Il reste à trouver un c_0. D'après le lemme 4.4.11, il existe $c_0 \in M^k$ tel que

$$\mathcal{M} \models \neg\phi(c_0, a_0^\emptyset) \wedge \phi(c_0, b_0^\emptyset) \ ,$$

ou l'une des deux moitiés correspondant à A_0 et B_0 si l'autre est vide.

A l'étape inductive, nous reprenons la même approche avec les ensembles K_{n+1} et L_{n+1} définis de la manière suivante :

$$K_{n+1} = \{W \subset \{0, \ldots, n\} \mid \text{ il existe } a \in M^l \text{ tel que } \mathcal{M} \models \phi(c_i, a) \text{ pour tout } i \in W \text{ mais que } \models \neg\phi(c, a)\} \ ;$$

$$L_{n+1} = \{W \subset \{0, \ldots, n\} \mid \text{ il existe } b \in M^l \text{ tel que } \mathcal{M} \models \neg\phi(c_i, b) \text{ pour tout } i \in W \text{ mais que } \models \phi(c, b)\} \ .$$

Ensuite, on pose

$$A_{n+1} = A_n \cup \{ \ a_{n+1}^W \mid a_{n+1}^W \text{ témoigne un événement } W \text{ de } K_{n+1} \ \} \ ;$$

$$B_{n+1} = B_n \cup \{ \ b_{n+1}^W \mid b_{n+1}^W \text{ témoigne un événement } W \text{ de } L_{n+1} \ \} \ .$$

D'après le lemme 4.4.11, il existe $c_{n+1} \in M^l$ tel que

$$\mathcal{M} \models \bigwedge_{W \subset \{0,\ldots,n\}} \bigwedge_{a_i^W \in A_{n+1}} \bigwedge_{b_i^W \in B_{n+1}} \neg\phi(c_{n+1}, a_i^W) \wedge \phi(c_{n+1}, b_i^W)$$

Avant de procéder vers l'étape finale, notons que ce choix pour la construction des c_i entraîne la conclusion suivante :

$$(\dagger) \quad \text{pour tout } y \in \bigcup_n A_n \cup B_n \ , \ \mathcal{M} \models \phi(c_i, y) \text{ si et seulement si } \models \phi(c, y) \ .$$

Maintenant, nous montrerons que si $i_0 < i_1 < \ldots < i_n \in \mathbb{N}$ et qu'il existe $a \in M^l$ tels que

$$(*) \qquad \models \phi(c_{i_0}, a) \wedge \ldots \wedge \phi(c_{i_n}, a) \wedge \neg\phi(c, a) \ ,$$

alors il existe $d_0, \ldots, d_n \in M^l$ tels que pour tous j, k entre 0 et n,

$$\models \phi(c_{i_j}, d_k) \text{ si et seulement si } j < k \ .$$

L'hypothèse (*) énonce que $\models \neg\phi(c, a)$ pour un certain $a \in M^l$. Par conséquent, l'ensemble K_{i_0-1} ne peut être vide puisqu'il contient $\emptyset$. Alors, nous posons $d_0 = a_{i_0}^W$ où $W \in K_{i_0}$. Ce choix entraîne $\models \neg\phi(c_{i_0}, d_0)$ d'après la conclusion (†).

Pour passer de d_k à d_{k+1} $(0 \leq k < n)$, nous procédons par récurrence. L'hypothèse (*) implique que $\{i_0, \ldots, i_k\} \in K_{i_k+1}$. Il suffit alors de choisir un $a^W_{i_k}$ arbitrairement quitte à assurer que $W \in K_{i_k+1}$ et de poser $d_{k+1} = a^W_{i_k+1}$. Il découle de (†) que ce choix entraîne $\models \phi(c_{i_j}, d_{k+1})$ pour tout $j \in \{0, \ldots, k\}$ et $\models \neg\phi(c_{i_{k+1}}, d_{k+1})$. La construction est terminée.

De manière analogue à ce que nous venons de faire, une suite $\{e_0, \ldots, e_n\} \subset M^l$ est construite s'il existe $i_0 < i_1 < \ldots < i_n \in \mathbb{N}$ et $b \in M$ tels que

$$\models \neg\phi(c_{i_0}, b) \wedge \ldots \wedge \neg\phi(c_{i_n}, b) \wedge \phi(c, b) \ ,$$

cette fois-ci la condition à satisfaire étant la suivante :

$$\text{pour tous } j, k \text{ entre 0 et } n \ , \ \models \neg\phi(c_{i_j}, e_k) \text{ si et seulement si } j < k \ .$$

Nous sommes arrivés à l'étape finale, celle qui nous fournira une définition de $\phi(x, y)$ par rapport à $p(x)$ grâce à la borne d'alternance N imposée par l'hypothèse de stabilité. Soit $\phi(x, a)$ une instance de $\phi(x, y)$ avec $a \in M^l$. Il existe une partie W de taille $N + 1$ dans $\{0, \ldots, 2N\}$ tel que $\mathcal{M} \models \bigwedge_{i \in W} \phi(c_i, a)$ ou bien $\mathcal{M} \models \bigwedge_{i \in W} \neg\phi(c_i, a)$. Alors, les constructions ci-dessus des suites de d_i ou de e_i montrent que $\models \phi(c, a)$ ou $\models \neg\phi(c, a)$ respectivement puisque sinon la borne d'alternance serait dépassée. Dans le premier cas, $\phi(x, a) \in p$ tandis que dans le deuxième cas $\neg\phi(x, a) \in p$. Il en découle que la formule $d_p\phi(y)$ est la suivante :

$$\bigvee_{W \subset \{0,\ldots,2N\} \ , \ |W| = N+1} \left(\bigwedge_{i \in W} \phi(c_i, y) \right)$$

□

Théorème 4.1 *Soit T une théorie complète. Alors les énoncés suivants sont équivalents :*

1. *la théorie T est κ-stable pour tout cardinal κ tel que $\kappa = \kappa^{\aleph_0}$;*
2. *aucune formule de la théorie T n'a la propriété de l'ordre.*
3. *pour tout modèle $\mathcal{M} \models T$ de base M, pour tout $k \in \mathbb{N}$, tout k-type de $S_k(M)$ est définissable.*

Preuve. Il reste peu à faire. L'implication ((1) ⇒ (2)) est vérifiée dans le corollaire 4.4.4. L'implication ((2) ⇒ (3)) est le lemme 4.4.13. Pour boucler tout, il suffira donc vérifier ((3) ⇒ (1)). Ceci n'est qu'un comptage. A partir d'un langage de base de cardinal $\aleph_0$, ce qui est notre hypothèse générale sur $\mathcal{L}$, et d'un ensemble de paramètres de taille κ, on ne peut obtenir que $\kappa^{\aleph_0}$ formules du premier ordre, donc autant de formules de définitions pour les types à paramètres dans l'ensemble fixé. □

Nous finissons cette section avec une rapide étude des *héritiers* et *cohéritiers*. Ce sont des extensions très particulières des types sur des modèles qui forment aussi le cas particulier principal d'une notion fondamentale, celle d'*extension non déviante*.

Définition 4.4.14 *Soient T une théorie complète, $\mathcal{M}$ un modèle de T de base M et A un ensemble de paramètres.*

1. *Une $\mathcal{L}(A)$-formule à $k+l$ variables $\phi(x, y)$ est dite* représentée *dans un type $p \in S_k(A)$ s'il existe $a \in A^l$ tel que $\phi(x, a) \in p$.*
2. *Si $M \subset A$, alors un type $p \in S_K(A)$ est dit* finiment satisfaisable *dans M si pour toute $k + l$-formule $\phi(x, a) \in p$, il existe $b \in M^k$ qui satisfait $\phi(x, a)$, en d'autres termes pour toute extension élémentaire $\mathbb{C}$ de $\mathcal{M}$ contenant A, $\mathbb{C} \models \phi(b, a)$.*

Définition 4.4.15 *Soient T une théorie complète, $\mathcal{M}$ un modèle de T de base M, A un ensemble de paramètres dans une extension élémentaire de $\mathcal{M}$ qui contient M et $p \in S_k(M)$ pour un certain $k \in \mathbb{N}$.*

1. *Une extension q de p à $S_k(A)$ est dite un* héritier *si toute $\mathcal{L}(M)$-formule représentée dans q est représentée dans p.*
2. *Une extension q à $S_k(A)$ est dite un* cohéritier *de p si q est finiment satisfaisable dans M.*

L'héritier d'un type sur un ensemble de paramètres contenant un modèle est un exemple d'extension très particulière. Elle préserve le même "degré d'indépendance" du type qu'il étend. En effet, aucune nouvelle formule n'est représentée dans l'extension, aucune contrainte supplémentaire n'est imposée. Comme le lemme 4.4.16 montre la notion de cohéritier est duale à celle d'héritier.

Les deux notions existent sans dépendre de la stabilité. Nous donnons trois exemples, un trivial, un instable et un stable.

1. Toute extension d'un type réalisé en est un héritier et un cohéritier.
2. L'exemple instable concerne les chaînes denses sans extrémités. Soit donc $\mathcal{Q}$ un modèle de base Q. Bien sûr, nous pouvons poser $Q = \mathbb{Q}$, les rationnels, afin de concrétiser ce dont nous parlons, mais c'est inutile. Fixons $q \in Q$ et utilisons de nouveau la notation q^+ pour le type déterminé par les formules

$$\{\ x < r \mid r \in Q \text{ et } q < r\ \} \cup \{\ r < x \mid r \in Q \text{ et } r \leq x\} .$$

   Nous déterminerons les héritiers et les cohéritiers de q^+ dans une extension élémentaire $\tilde{\mathcal{Q}}$ $\mathcal{Q}$. Rappelons que $q^+ \in S_1(Q)$ est le type déterminé par

$$\{\ x < r \mid r \in \tilde{Q} \text{ et } q < r\ \} \cup \{\ r < x \mid r \in \tilde{Q} \text{ et } r \leq x\} .$$

   Soit $\tilde{q^+}$ un héritier de q^+ sur $\tilde{\mathcal{Q}}$. Cette existence est le sujet du lemme 4.4.17. Si $\alpha \in \tilde{Q}$ tel que $q < \alpha$ et $\alpha < r$ pour tout $r \in Q$ tel que $q < r$. En d'autres termes, α est une réalisation de q^+ dans $\tilde{\mathcal{Q}}$. La formule $\alpha < x$ n'appartient pas à $\tilde{q^+}$ parce que sinon, $q < \alpha \wedge \alpha < x$ appartiendrait à $\tilde{q^+}$ aussi, et il en découlerait, comme q^+ est supposé être un héritier de q^+, qu'il existe $\alpha' \in Q$ tel que $q < \alpha' \wedge \alpha' < x$. Or, ce n'est pas le cas. Donc, une réalisation de $\tilde{q^+}$ minore toutes les réalisations de q^+ dans $\tilde{Q}$. En plus, elle est certainement strictement supérieure à q puisque sinon $\tilde{q^+}$ représenterait $x = y$, ce qui n'est pas le cas pour q^+. Tout cela montre que $\tilde{q^+}$ qui est un héritier arbiraire de q^+ décrit la même coupure que q^+ dans $\tilde{\mathcal{Q}}$. En particulier, c'est le seul héritier.

   Maintenant, nous montrerons que q^+ n'a qu'un seul cohéritier sur $\tilde{\mathcal{Q}}$. Soit de nouveau α une réalisation de q^+ dans $\tilde{Q}$. La formule $x < \alpha$ n'appartient pas à un cohéritier de q^+ car sinon, $q < x \wedge x < \alpha$ aussi appartiendrait à ce cohéritier, et par satisfaisabilité finie il existerait $a \in Q$ tel que $\tilde{\mathcal{Q}} \models q < a \wedge a < \alpha$, ce qui contredit que α réalise q^+. Donc le cohéritier est unique et majore toutes les réalisations de q^+ dans $\tilde{\mathcal{Q}}$.

   La conclusion finale est que q^+ a un héritier et un seul, et un cohéritier et un seul bien que ces deux extensions ne soient pas égales. Le même raisonnement appliqué à un type "irrationel" montre que celui-ci a exactement deux héritiers qui sont aussi cohéritiers : les extensions qui majore et minore les réalisations de q^+ dans le modèle considéré.

   Pour une description complète des types des chaînes denses sans extrémités, les chapitres 11 et 12 de [9] sont une excellente référence.
3. L'exemple stable concerne CAC_p. Soit donc $k \models \mathrm{CAC}_p$. Un élément α dans une extension élémentaire de k est transcendant sur k si et seulement si son type sur k n'est pas réalisé dans k. En effet, si α est un élément tel que $\mathrm{tp}(\alpha/k)$ ne soit pas réalisé dans k, alors $\mathrm{tp}(\alpha/\bar{k})$ ne contient pas d'équation de la forme $P[X] = 0$ où P est un polynôme d'une seule variable et à coefficients dans k parce que les racines d'un tel polynôme sont toutes dans k. Inversement, si $\alpha \in \bar{k}$, alors α est la racine d'un polynôme à coefficients dans k. Si K est une extension élémentaire de k, alors le seul héritier et en fait cohéritier de $\mathrm{tp}(\alpha/k)$ est le type d'un élément transcendant sur K.

Lemme 4.4.16 *Soient T une théorie complète, $\mathcal{M}$ un modèle de T de base M, a et b deux uples non nécessairement de même arité extraits d'une extension élémentaire de $\mathcal{M}$. Alors* $\mathrm{tp}(a/M \cup b)$ *est un héritier de* $\mathrm{tp}(a/M)$ *si et seulement si* $\mathrm{tp}(b/M \cup a)$ *est un cohéritier de* $\mathrm{tp}(b/M)$.

Preuve. Exercice. □

Lemme 4.4.17 *Soient T une théorie complète, $\mathcal{M} \preceq \mathcal{N}$ deux modèles de T de bases M et N respectivement et A un ensemble de paramètres tels que $M \subset A \subset N$.*

1. *Soient $p \in S_k(M)$ et π est un ensemble consistant de formules (un* type incomplet*) à paramètres dans A qui étend p. Si toute formule de π est représentée dans p, alors il existe $q \in S_k(A)$ qui contient π et qui est un héritier de p.*
2. *Si π est un ensemble consistant de formules à paramètres dans A dont chaque membre est finiment satisfaisable dans M, alors il existe $q \in S_k(A)$ qui contient π et qui est un cohéritier de sa restriction à M.*

Preuve. Entraînement en compacité. □

Corollaire 4.4.18 *Soient T une théorie complète, $\mathcal{M}$ un modèle de T et A un ensemble de paramètres contenant M.*

1. *Tout type $p \in S_k(M)$ s'étend à un héritier dans $S_k(A)$.*
2. *Tout type $p \in S_k(M)$ s'étend à un cohéritier dans $S_k(A)$.*

Lemme 4.4.19 *Soient T une théorie complète et $\mathcal{M}$ un modèle de T. Un type de $S_k(M)$ est définissable si et seulement s'il n'a qu'un seul héritier sur chaque ensemble de paramètres étendant M.*

Preuve. Commençons avec un type définissable p dans $S_k(M)$. Pour toute $\mathcal{L}$-formule $\phi(x, y)$ représentée dans p, il existe une formule de définition $d_p\phi(y)$ à paramètres dans M. Soient A est un ensemble de paramètres contenant M et q un héritier de p sur A. Alors, il n'est pas possible que la formule $\neg(\forall y(d_p\phi(y) \leftrightarrow \phi(x, y)))$ soit représentée dans q. L'unicité de l'héritier en découle.

L'autre direction de l'équivalence utilise un théorème classique de la théorie des modèles : le théorème de définissabilité de Beth. Pour éviter un trop large détour, nous n'incluons pas sa preuve. Pour inciter nos lecteurs à feuilleter les sources, nous n'incluons pas son énoncé. Nous nous contenterons de donner la préparation qui mène au point où le théorème de Beth intervient et boucle assez rapidement le raisonnement. Cette préparation a sa propre valeur.

Notre objectif est de vérifier la définissabilité d'un type $p \in S_k(M)$ sur lequel la seule hypothèse est qu'il ait un héritier et un seul sur chaque ensemble de paramètres contenant M. Nous commençons par introduire des témoins de cette hypthèse. Pour chaque $\mathcal{L}$-formule $\phi(x, y)$ à $k + l$ variables, nous introduisons un symbole de relation l-aire $d_p\phi$ et posons :

$$\mathcal{L}^+ \;=\; \mathcal{L} \;\cup\; \{\; d_p\phi(y) \mid \phi(x, y) \text{ est une } \mathcal{L}\text{-formule} \;\} \;.$$

Nous notons $\mathcal{M}^+$ l'expansion de $\mathcal{M}$ à $\mathcal{L}^+$, telle que pour toute $\mathcal{L}$-formule $\phi(x, y)$ à $k+l$ variables,

$$\mathcal{M} \;\models d_p\phi(m) \text{ si et seulement si } \;\phi(x, m) \in p \;.$$

Tout modèle $\mathcal{N}^+$ de $\mathrm{Th}((\mathcal{M}^+, m)_{m\in M})$ dans le langage $\mathcal{L}^+(M)$ est une extension élémentaire de $\mathcal{M}^+$, et le réduit $\mathcal{N}$ de $\mathcal{N}^+$ au langage $\mathcal{L}$ est une extension élémentaire de $\mathcal{M}$. Sur une telle extension élémentaire $\mathcal{N}$, nous considérons la famille suivante de $\mathcal{L}(N)$-formules

$$\{\; \phi(x, b) \mid \phi(x, y) \text{ est une } \mathcal{L}\text{-formule} \;,\; b \in N^l \;(l \in \mathbb{N}),\; \mathcal{N}^+ \models d_p\phi(b) \;\} \;.$$

Cette famille est consistante puisque

$$\mathcal{M} \;\models\; \forall y_1 \dots y_n(\bigwedge_{i=1}^{n} d_p\phi_i(y_i) \;\leftrightarrow\; d_p(\bigwedge_{i=1}^{n} \phi_i)(y_1, \dots, y_n) \;) \;.$$

Un type q qui contient cette famille est un héritier de p. Par hypothèse, q est unique. Il en découle que la structure $(\mathcal{N}, m)_{m\in M}$ a au plus une expansion à un modèle de $\mathrm{Th}((\mathcal{M}^+, m)_{m\in M})$. A ce point, le théorème de Beth permet de conclure que nous pouvons remplacer tous les symboles de relations $d_p\phi$ par des formules dans le langage $\mathcal{L}(M)$. Ainsi p est définissable. □

Lemme 4.4.20 *Soient T une théorie complète et stable, $\mathcal{M}$ et $\mathbb{C}$ deux modèles de T, de bases M et C respectivement, tels que $\mathcal{M} \preceq \mathbb{C}$. Pour $a \in C^k$ et $b \in C^l$, si $\mathrm{tp}(b/M \cup a)$ est héritier (resp. cohéritier) de $\mathrm{tp}(b/M)$, alors $\mathrm{tp}(b/M \cup a)$ est cohéritier (resp. héritier) de $\mathrm{tp}(b/M)$.*

Preuve. Nous procédons par l'absurde. Supposons donc qu'il existe une $\mathcal{L}(M)$-formule $\phi(x,y)$ à $k+l$ variables telle que $\phi(a,y) \in \mathrm{tp}(b/M \cup a)$ et que $\phi(a,y)$ ne soit pas finiment satisfaisable dans M. En d'autres termes,

$$\models \neg\phi(a,m) \ \text{ pour tout } \ m \in M^l \ .$$

(De manière analogue à la preuve du lemme 4.4.13, $\models ...$ veut dire $\mathbb{C} \models ...$, $\mathbb{C}$ étant une extension élémentaire où tout ce qui n'est pas dans $\mathcal{M}$ trouve sa place.)

Nous construirons une suite de $(a_i, b_i) \in M^{k+l}$ $(i \in \mathbb{N})$ qui monteront que $\phi(x,y)$ a la propriété de l'ordre. Plus précisément, la construction donnera à son étape n, les conditions suivantes :

$$\models \phi(a,b) \wedge \bigwedge_{0\leq i\leq n} \neg\phi(a,b_i) \wedge \bigwedge_{0\leq i\leq n} \phi(a_i,b) \wedge \bigwedge \text{“ propriété de l'ordre sur } \{(a_i,b_i)|0 \leq i \leq n\}\text{”} \ .$$

Pour trouver a_0, nous utilisons l'hypothèse d'héritage pour $\mathrm{tp}(b/M \cup a)$. Il existe $a_0 \in M^k$ tel que $\phi(a_0,y) \in \mathrm{tp}(b/M)$. D'après le lemme 4.4.11, il existe $b_0 \in M^l$ tel que

$$\mathcal{M} \models \phi(a_0,b_0) \ .$$

Comme $\mathrm{tp}(b/M \cup a)$ est supposé ne pas être cohéritier de sa restriction à M, nous avons les données suivantes :

$$\models \phi(a,b) \ \wedge \ \neg\phi(a,b_0) \ \wedge \ \phi(a_0,b) \ \wedge \ (a_0,b_0) \ ,$$

qui est exactement l'étape 0 des conditions de construction.

Le passage de l'étape n à l'étape $n+1$ suit exactement la même méthode. Par héritage, il existe $a_{n+1} \in M^k$ tel que

$$\models \phi(a_{n+1},b) \wedge \bigwedge_{0\leq i\leq n} \neg\phi(a_{n+1},b_i) \wedge \bigwedge_{0\leq i\leq n} \phi(a_i,b) \wedge \bigwedge \text{“ propriété de l'ordre sur } \{(a_i,b_i)|0 \leq i \leq n\}\text{”} \ .$$

Alors le lemme 4.4.11 fournit $b_{n+1} \in M^l$ tel que

$$\models \phi(a_{n+1},b) \wedge \bigwedge_{0\leq i\leq n} \neg\phi(a_{n+1},b_i) \wedge \bigwedge_{0\leq i\leq n} \phi(a_i,b_{n+1}) \wedge \bigwedge \text{“ propriété de l'ordre sur } \{(a_i,b_i)|0 \leq i \leq n\}\text{”} \ .$$

Finalement, le non cohéritage assure que

$$\models \neg\phi(a,b_{n+1}) \ .$$

La construction est terminée et la propriéte de l'ordre s'ensuit ainsi que la contradiction à l'hypothèse de stabilité. □

Théorème 4.2 *Soient T une théorie complète et stable, $\mathcal{M}$ un modèle de T, A un ensemble de paramètres contenant M et $p \in S_k(M)$. Alors le seul héritier de p dans $S_k(A)$ est aussi son seul cohéritier.*

Preuve. Notons d'abord que l'unicité de l'héritier découle du lemme 4.4.19 et du théorème 4.1. Appelons q cet unique héritier. Soient maintenant b un k-uple réalisant q et a un l-uple extrait de A. Alors, $\mathrm{tp}(b/M \cup a)$ est héritier de $\mathrm{tp}(b/M)$. D'après le lemme 4.4.20, $\mathrm{tp}(b/M \cup a)$ est cohéritier de $\mathrm{tp}(b/M)$. Le lemme 4.4.16 implique alors que $\mathrm{tp}(a/M \cup b)$ est héritier de $\mathrm{tp}(a/M)$. Une nouvelle application du lemme 4.4.20 montre cette fois-ci que $\mathrm{tp}(a/M \cup b)$ est cohéritier de $\mathrm{tp}(a/M)$. Le lemme 4.4.16 boucle les implications en nous permettant de retrouver que $\mathrm{tp}(b/M \cup a)$ est héritier de $\mathrm{tp}(b/M)$.

Finalement, comme a était arbitrairement extrait de A, nous concluons que q hérite de p si et seulement s'il cohérite de p. L'unicité déjà connue de l'héritier implique alors celle du cohéritier. □

Corollaire 4.4.21 (Symétrie de la déviation : cas particulier des (co)héritiers) *Soient T une théorie complète et stable, $\mathcal{M}$ et $\mathbb{C}$ deux modèles de T, de bases M et C respectivement, tels que $\mathcal{M} \preceq \mathbb{C}$. L'héritage est une relation symétrique : si $a \in C^k$ et $b \in C^l$, alors* $\mathrm{tp}(a/M \cup b)$ *est (co)héritier de* $\mathrm{tp}(a/M)$ *si et seulement si* $\mathrm{tp}(b/M \cup a)$ *est (co)héritier de* $\mathrm{tp}(b/M)$.

Remarquablement, dans une théorie stable, la symétrie de la déviation peut être définie pour un type arbitraire qui n'est pas nécessairement à paramètres dans un ensemble contenant la base d'un modéle. Nous nous contenterons de donner les traits généraux de ce développement sans détailler les preuves qui sont par ailleurs réminiscentes du développement précedent, mais bien sûr plus subtiles. Certaines propriétés de la déviation seront introduites au fur et à mesure dans le contexte des groupes.

Tout ce qui suit suppose la présence d'une théorie T complète et stable. La notion d'héritier met en relief la représentation d'une formule dans une extension d'un type. Une nouvelle formule représentée dans une extension d'un type correspond à une perte d'indépendance, phénomène naturel en mathématiques qui est mesuré dans le contexte d'une théorie stable et des types à paramètres dans des ensembles contenant un modèle, par le non héritage. L'extension aux types sur des ensembles de paramètres se fait en passant par des extensions aux modèles. L'utilisation simple mais cruciale du lemme 4.4.11 justifie ce détour.

Maintenant nous décrirons la feuille de route pour introduire la notion générale de *déviation*. Nous travaillerons sur ensemble arbitraire A de pamaètres et fixerons $p \in S_k(A)$. Pour tout modèle $\mathcal{M}$ de base M contenant A, il existe par compacité des extensions de p à M. Nous pouvons alors comparer ces extensions sur un modèle en comparant les formules qu'elles représentent.

Plus précisément, pour tout type $p \in S_k(A)$, on introduit sa *classe*, qui est l'ensemble de $\mathcal{L}$-formules qu'elle représente

$$\mathrm{cl}_A(p) \;=\; \{\; \phi(x,y) \mid \text{ il existe } a \in A^l \text{ tel que } \phi(x,a) \in p \;\}\;.$$

Cette notion, restreinte aux types sur des modèles, permet de les comparer en comparant leurs classes :

$$\text{pour deux modèles } \mathcal{M} \text{ et } \mathcal{M}',\ p \in S_k(M),\ q \in S_k(M'),\ p \geq q \text{ si } \mathrm{cl}_M(p) \subset \mathrm{cl}_{M'}(q)\;.$$

Intuitivement, dans cet ordre connu sous l'appellation *ordre fondamental*, un type sur un modèle est de plus grande classe s'il a moins de contraintes, donc plus d'indépendance. En particulier, il est plus loin d'être réalisé qu'un type de classe inférieure.

Le *théorème de la borne*, dont la preuve est réminiscente de celle de l'existence d'un cohéritier, montre que si $p \in S_k(A)$ parmi ses extensions à un modèle fixé $\mathcal{M}$ il en existe un qui est de classe maximale parmi ces extensions. Elle est donc l'extension la plus proche de p. Comme l'ordre fondamental est défini sur des modèles de T et qu'elle ne fait intervenir que des $\mathcal{L}$-formules, ces *bornes* de p ne dépendent pas du choix de modèle. La conclusion plus difficile à vérifier est l'*unicité de la borne* qui se fait en utilisant un raisonnement de symétrie.

Une fois qu'on peut parler de *la* borne d'un type, il est possible d'introduire la notion générale de déviation. Soient donc $A \subset B$ deux ensembles de paramètres, et $p \in S_k(A)$, $q \in S_k(B)$ tels que q étende p. Le type q est dit une extension *non déviante* de p si la borne de q est égale à celle de la borne de p. En particulier, un héritier, de façon équivalente un cohéritier, est une extension non déviante.

Le corollaire 4.4.21 de symétrie reste vrai quand le modèle $\mathcal{M}$ est remplacé par un ensemble arbitraire de paramètres. Un type sur un ensemble de paramètres A a une extension non déviante à un type sur tout ensemble de paramètres contenant A. Cette extension n'est pas nécessairement unique, en effet pour un ensemble $B \supset A$ fixé il peut y en avoir une infinité mais tout cela est "bien maîtrisé".

4.5 Génériques

Un ensemble, type, plus globalement "point" *générique* est un objet "large" par rapport à ses semblables. Ce fait d'être large s'exprime de diverses façons en théorie des modèles :

posséder la plus haute dimension ; être une extension nondéviante, un héritier, un cohéritier de ses restrictions à tous les ensembles de paramètres de plus petite taille ; être en nombre borné ou couvrir l'univers en nombre fini de translatés. Sous des hypothèses bien établies, dans des conditions plus précises ces ces conditions s'avèrent fort liées. Pour les objectifs de ce cours, [10] est la meilleure référence. [14] et [7] sont très utiles pour des progrès plus récents et des élaborations techniques aussi bien que des détails qui peuvent manquer dans le style conceptuel de [10]. Finalement, pour les génériques dans les groupes dont la théorie du premier ordre est simple, [15] est la référence.

Avant d'aborder le sujet concrètement, il convient de fixer certaines données générales. Notre langage sera noté $\mathcal{L}$ et incluera, sauf mention contraire, celui des groupes. Il peut être plus large, en d'autres termes les groupes en vue peuvent porter de la structure définissable supplémentaire qui n'est pas nécessairement définissable à partir du langage des groupes. En particulier, un groupe G est stable s'il est définissable dans une structure stable, ce qui implique que $\mathrm{Th}(G)$ est stable dans le langage des groupes aussi. Nous utiliserons la même lettre pour un groupe en tant que structure et pour sa base.

Il convient de préciser une pratique assez récurrente dans ce qui suit. Sauf mention contraire, les paramètres proviendront d'un modèle, plus précisément de la partie "groupe" d'un modèle de la $\mathcal{L}$-théorie complète dans les modèles de laquelle sont définissables les groupes que nous étudierons. Nous utiliserons l'appellation "modèle" pour nous référer à cette partie groupe de la structure stable en question. Notons aussi qu'un groupe est définissable dans une structure éventuellement avec des paramètres provenant de cette structure. Nous supposerons que ces paramètres appartiennent au langage $\mathcal{L}$ de base.

Dans l'esprit de la section précédente, nous écrirons parfois $\models \phi...$ quand l'extension élémentaire où la satisfaction a lieu n'est pas importante. Cette extension certainement existe et l'on peut supposer, par amalgamation, qu'elle contienne toutes les réalisations qui nous inéressent. Pourquoi le taire, il s'agit de ce "modèle monstre" dans lequel aiment travailler les théoriciens des modèles.

Occasionnellement, pour alléger l'écriture nous remplacerons les formules du premier ordre par une écriture ensembliste du type "$x \in X$". Il ne faut bien sûr pas oublier qu'un ensemble définissable est une entité qui a tendance à croître suite aux passages à des extensions élémentaires. Ce qui reste intact est la formule du premier ordre qui le définit.

Définition 4.5.1 *Soient G un groupe stable et X une partie définissable de G éventuellement avec des paramètres provenant de G.*

1. *La partie X est dite* générique *s'il existe $\{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_n\} \subset G$ tels que $G \subset \bigcup_{i=1}^{n} a_i X b_i$.*
2. *La partie X* générique à droite *s'il existe $\{a_1, \ldots, a_n\} \subset G$ tels que $G \subset \bigcup_{i=1}^{n} X a_i$.*
3. *La partie X* générique à gauche *s'il existe $\{a_1, \ldots, a_n\} \subset G$ tels que $G \subset \bigcup_{i=1}^{n} a_i X$.*
4. *Un type dans $S_1(G)$ est dit* générique *si toutes les formules qu'il contient sont génériques. Plus généralement, si A est un ensemble arbitraire de paramètres, alors un type p dans $S_1(A)$ est dit générique si A est contenu dans un modèle G tel qu'il existe $q \in S_1(G)$, un type générique qui étend p, en d'autres termes $p \subset q$.*

Faisons quelques remarques élémentaires :

1. Un ensemble définissable qui contient un ensemble générique (resp. générique à droite ou à gauche) est un ensemble générique (resp. générique à droite ou à gauche)
2. Les premiers objectifs seront de vérifier l'existence des génériques et l'équivalence de la généricité à celle à droite et celle à gauche. Notons que celle à droite ou à gauche implique, en utilisant l'élément neutre, la généricité.
3. Il est de coutume d'appeler *point générique* une réalisation d'un type générique. Cette réalisation n'est pas dans l'ensemble qui fournit les paramètres puisqu'un singleton n'a aucune chance d'être générique dans un groupe infini. Si a est un point générique, alors a^{-1} l'est aussi.

Après les remarques, donnons quelques exemples pour motiver la définition 4.5.1 et donner un avant-goût de la "largeur" que représente un ensemble générique.

1. La formule $x = x$ définit un ensemble générique, et l'ensemble vide $x \neq x$ n'est pas générique. Plus généralement, un ensemble fini, qui est définissable avec paramètres pourvu que ceux-ci soient disponibles, n'est pas générique puisque nous étudions des groupes infinis. Un ensemble cofini est générique.
2. Un sous-groupe définissable d'indice fini est générique. Il faut bien remarquer que toute classe, à gauche ou à droite, d'un tel sous-groupe, une fois que des représentants de ces classes sont présents dans l'ensemble de paramètres, est aussi un générique. En particulier, à la fois un ensemble définissable et son complémentaire peuvent être génériques.
3. Un sous-groupe définissable d'indice infini n'est pas générique.
4. Donnons un exemple plus concret en utilisant le lemme 4.5.2. Considérons le groupe résoluble
$$G = \left\{ \begin{pmatrix} t & u \\ 0 & t^{-1} \end{pmatrix} \ : \ t \in K^\times, \ u \in K \right\}$$
sur un corps algébriquement clos K. Plus précisément, K est un modèle de CAC_p pour un certain p premier ou 0. Le sous-groupe
$$U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \ : \ \ u \in K \right\}$$
est définissable à partir du langage des groupes aussi bien que de celui des corps, éventuellement avec paramètres (vérifiez ceci, à la rigueur vous pouvez simplifier la question en remplaçant U par $UZ(G)$). Le sous-groupe U, d'indice infini dans G, n'est pas un ensemble générique. Alors, le lemme 4.5.2 montre que son complémentaire est générique. En utilisant un peu d'algèbre linéaire, vous pouvez montrer que ce complémentaire est l'union des conjugués du *tore*
$$T = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \ : \ t \in K^\times \right\} .$$
En d'autres termes, l'ensemble définissable $\bigcup_{g \in G} T^g$ est un ensemble générique.
Ce n'est pas une coïncidence. Dans les groupes algébriques linéaires, les conjugués des centralisateurs des *tores maximaux*, en d'autres termes des sous-groupes diagonalisables maximaux, ont tendance à être génériques.
5. Considérons, dans le langage des corps, un modèle K de CAC_p. Nous savons que c'est une structure fortement minimale. Par conséquent, toute formule à une seule variable libre définit dans chaque modèle un ensemble fini ou cofini. Cette propriété est héritée par les groupes additifs et multiplicatifs quand on les traite de réduits avec la structure suppémentaire provenant de l'expansion qu'est le corps K. Par conséquent les seuls ensembles génériques sont cofinis, et $S_1(K)$ n'a qu'un seul type générique, qui est réalisé par un élément si et seulement si cet élément est transcendant sur K. En particulier, la déviation est exactement la perte d'indépendance algébrique au sens de la théorie des corps.
6. Pour finir ce cours, nous étudierons un résultat récent d'Anand Pillay sur les génériques dans les groupes libres non abéliens.

Voici un lemme dont l'énoncé et la preuve reflètent l'esprit de beaucoup de résultats de symétrie que vous avez rencontrés dans le contexte des structures stables.

Lemme 4.5.2 *Soient G un groupe stable et X une partie définissable de G. Alors, X est générique à droite ou $\neg X$ est générique à gauche. En particulier, X ou $\neg X$ est générique.*

Preuve. Nous procédons par l'absurde. Soit donc X un contrexemple. Nous construirons deux suites d'éléments $(a_i)_{i \in \mathbb{N}}$ et $(b_i)_{i \in \mathbb{N}}$ dans G telles que $a_i b_j \in X$ si et seulement si $i < j$ dans

l'ordre usuel des nombres naturels. Quand $i = 0$, il suffit d'utiliser l'hypothèse contradictoire puisque pour tout a_0, il existe b_0 tel que $b_0 \notin a_0^{-1}X$. Supposons maintenant $(a_i)_{i\leq n}$ et $(b_i)_{i\leq n}$ déterminées pour un certain $n \in \mathbb{N}$. Il existe alors $b_{n+1} \notin \bigcup_{i=0}^{n} a_i^{-1}\neg X$. Ensuite, il existe $a_{n+1} \notin \bigcup_{i=0}^{n+1} Xb_i^{-1}$. La construction est terminée et la propriété de l'ordre contredit la stabilité. □

Lemme 4.5.3 *Soient X et Y deux parties définissables dont l'union est générique. Alors l'une d'entre eux est générique.*

Preuve. D'après l'hypothèse

$$\models \exists x_1 y_1 \dots x_n y_n \forall z \left(\bigvee_{i=1}^{n} (x_i z y_i \in X \vee x_i z y_i \in Y) \right) .$$

De manière équivalente,

$$\models \exists x_1 y_1 \dots x_n y_n \forall z \left(\bigvee_{i=1}^{n} x_i z y_i \in X \ \vee \ \bigvee_{i=1}^{n} x_i z y_i \in Y \right) .$$

D'après le lemme 4.5.2 et la première remarque aprés la définition 4.5.1 l'une des deux unions est générique. □

Corollaire 4.5.4 *L'ensemble $S_1(G)$ contient un type générique.*

Preuve. Le lemme 4.5.2 assure l'existence d'un ensemble générique. Fixons-en un, disons X, et considérons les familles de formules génériques contenant X telles que dans toute famille l'intersection d'un nombre fini de membres reste générique.

La famille $\{X\}$ est un exemple d'une telle famille et une application du lemme de Zorn permet de conclure qu'il existe une famille maximale. Soit p_0 une telle famille maximale. La famille p_0 est stable par intersections finies par construction. Il découle du lemme 4.5.3 et de la maximalité de p_0 que pour tout ensemble définissable Y tel que $\neg Y$ ne soit pas générique $Y \in p_0$. Alors, pour aboutir à un type générique, il suffit de compléter p_0 à un ensemble maximal consistant de formules. □

Lemme 4.5.5 *Si $\phi(x, y)$ est une $\mathcal{L}$-formule à $1+l$ variables dont certaines instances définissent des parties génériques d'un groupe stable, alors le nombre de translatés nécessaires est borné de façon indépendante du choix de valeurs pour le l-uple de paramètres y.*

Preuve. Soit p un type générique. Alors, $\phi(x, g)$ définit un ensemble générique si et seulement s'il existe un translaté de cet ensemble qui appartient à p. Plus précisément,

$$\exists tz \ \phi(txz, g) \in p .$$

Par définissabilité des types, ceci équivaut à la satisfaction

$$\models \exists tz \ d_p\phi(t, z, g) .$$

Par l'absurde, nous supposerons que pour tout $n \in \mathbb{N}$ il existe g_n tel que au moins n translatés de l'ensemble $\phi(x, g_n)$ soient nécessaires pour couvrir le groupe tout entier. Un raisonnement de compacité permet d'aboutir à une contradiction. Introduisons au langage $\mathcal{L}(G)$ un l-uple de symboles de constantes $(c_1, \dots, c_l)$ pour les paramètres et un symbole de constante d. L'ensemble d'énoncés

$$\{ \ \exists uv \ d_p\phi(u, v, c) \ , \ \neg\exists \ x_1 \dots x_n y_1 \dots y_n \bigvee_{i=1}^{n} \phi(x_i d y_i, c) \mid n \in \mathbb{N}^* \ \}$$

est consistant. C'est une contradiction puisque $\phi(x, c)$ appartient à un type générique. □

Corollaire 4.5.6 *L'héritier d'un type générique est un type générique.*

Preuve. Nous utilisons la notation du lemme 4.5.5. Un type est générique si et seulement s'il ne représente pas la formule $\phi(x,y) \wedge \neg\exists tz\ d_p\phi(t,z,y)$. Cette propriété est héritée par un héritier. □

En fait, nous pouvons faire mieux.

Lemme 4.5.7 *Soit p un type générique. Alors p est une extension non déviante de sa restriction à $\emptyset$.*

Preuve. Soit A l'ensemble de paramètres de p. Nous utiliserons le rang D et le théorème 8.17 du cours général. Comme la structure ambiante est stable, donc simple, la propriété d'extension de l'indépendance et le théorème 8.17 du cours général montrent qu' il suffit de vérifier que $D(p,\phi,k)$ est maximal pour toute $\mathcal{L}$-formule $\phi(x,y)$ à $1+l$ variables et pour tout $k \in \mathbb{N}$.

Soient alors g une réalisation de p et h une réalisation d'un type q qui satisfait la propriété de maximalité que nous voulons vérifier pour p. En utilisant la propriété d'extension de l'indépendance, nous pouvons supposer g et h indépendantes sur A. Alors, le théorème 8.17 du cours montre que pour toute ϕ et tout k comme ci-dessus

$$D(h/A,\phi,k) = D(h/A \cup g,\phi,k) = D(gh/A \cup h,\phi,k) \leq D(gh/A,\phi,k)\ .$$

Notons que la deuxième égalité se vérifie par récurrence. Le choix maximal de q et le théorème 8.17 du cours montrent que gh et h sont indépendants sur A aussi. Le même type de raisonnement montre l'indépendance de gh^{-1} et h. Le théorème 8.17 montre alors

$$\begin{aligned} D(h/A,\phi,k) &= D(h/A \cup gh^{-1},\phi,k) \\ &= D((gh^{-1})h/A \cup gh^{-1},\phi,k) \\ &= D(g/A \cup gh^{-1},\phi,k) \\ &\leq D((g/A,\phi,k)\ . \end{aligned}$$

La maximalité est vérifiée. □

Ce lemme important montre que la notion de générique décrit des ensembles définissables larges. En effet, l'absence de déviation est la préservation d'un degré d'indépendance. Ceci est perdu quand de nouvelles formules du premier ordre sont représentées dans les extensions d'un type. De telles représentations qui apparaissent dans des extensions de types ont comme conséquence la diminution de la "taille" des formules contenues dans les types concernés puisqu'elles augmentent les possibilités de conjonctions de formules, en d'autres termes les contraintes.

Corollaire 4.5.8 *Si $p \in S_1(A)$ un type générique, alors toute extension non déviante de p est générique.*

Preuve. D'après la définition 8.8 du cours général la division pour une formule implique la déviation pour cette formule.

Dans notre cas, soient B un ensemble de paramètres contenant A, q une extension non déviante de p à B et G un modèle qui contient une extension générique r de p (la définition 4.5.1 (iv)). En utilisant la propriété d'extension de l'indépendance, nous concluons qu'il existe une extension élémentaire G' de G telle que $S_1(G')$ contienne une extension non déviante q' de q. Il découle alors de la transitivité de l'indépendance que q' est une extension non déviante de p et donc de sa restriction q_0 à G. Par conséquent q' ne divise pas sur G non plus.

Maintenant nous montrerons que q' est un cohéritier de sa restriction à G. En fait, c'est un raisonnement général qui n'est pas restreint au contexte des groupes stables. Soit par l'absurde une formule $\phi(x,b) \in q'$ qui n'est satisfait par aucun élément de G. Alors, pour aucun $g \in G$, $\phi(g,y)$ n'est dans $\mathrm{tp}(b/G)$. Si $(b_i)_{i\in\mathbb{N}}$ est une suite de Morley de $\mathrm{tp}(b/G)$, forcément $\{\phi(x,b_i)|i \in \mathbb{N}\}$ est inconsistante. Ceci contredit que q' ne divise pas sur G.

Comme notre structure ambiante est stable, le paragraphe précédent montre que q' hérite de sa restriction à G. Par ailleurs, d'après le lemme 4.5.7, le générique r est une extension non déviante de p aussi. Par conséquent, r et q_0 représentent les mêmes $\mathcal{L}$-formules. De façon similaire au corollaire 4.5.6, le type q_0 est générique aussi. Ainsi q' est générique, et forcément, q est générique. □

Le lemme 4.5.7 et le corollaire 4.5.8 caractérisent les types génériques comme ceux de rang de D maximal. Il est presque clair que notre façon d'arriver à cette équivalence n'est pas très efficace. Le corollaire 4.5.8 suit un chemin assez sinueux. Néanmoins, il permet de clarifier le lien entre la division, le rang D et diverses notions autour de la définissabilité (héritiers, cohéritiers, définissabilité des types) que nous avons introduites jusqu'à ce point. Ces notions, équivalentes dans le contexte des théories stables qui sont les théories les plus équilibrées de ce point de vue, deviennent individuellement importantes pour des raisons différentes quand il s'agit des généralisations de la stabilité, un domaine de recherche riche et actif.

Les corollaires suivants sont utiles dans des contextes algébriques aussi.

Corollaire 4.5.9 *Tout élément d'un groupe stable est le produit de deux réalisations d'un type générique.*

Preuve. Soit g un élément fixé. Comme un type générique ne dévie pas sur $\emptyset$, nous pouvons considérer un élément x tel que $\mathrm{tp}(x/\emptyset)$ soit générique. Ce type a une extension non déviante à l'ensemble $\{g\}$, qui est générique d'après le corollaire 4.5.8. Nous pouvons supposer que x est aussi une réalisation de cette extension. Alors, gx et x^{-1} sont génériques sur $\{g\}$. □

Ce corollaire a un corollaire immédiat et simple mais qui est lié à un vaste domaine de recherche : les *propriétés génériques* des groupes stables.

Corollaire 4.5.10 *Un groupe stable génériquement abélien est abélien. Plus précisément, si toutes les réalisations des types génériques sur un ensemble fixé commutent, alors le groupe stable ambiant est commutatif.*

Avant de faire quelques commentaires supplémentaires sur les *équations génériques*, vérifions certaines propriétés de base des génériques qui sont indispensables pour les manipuler.

Corollaire 4.5.11 *Soient a et b deux réalisations indépendantes de deux types sur un ensemble A. Si $\mathrm{tp}(a/A)$ est générique, alors a et ab sont indépendants et génériques ; a et ba sont indépendants et génériques sur A.*

Preuve. D'après l'hypothèse du corollaire, $\mathrm{tp}(a/A \cup b)$ est une extension non déviante de $\mathrm{tp}(a/A)$. D'après le corollaire 4.5.8, $\mathrm{tp}(a/A \cup b)$ est un type générique. Il en découle que $\mathrm{tp}(ba/A \cup b)$ est un type générique. D'après le lemme 4.5.7, $\mathrm{tp}(ba/A \cup b)$ ne dévie pas sur A. Certainement $\mathrm{tp}(ba/A)$ est générique aussi. Même type de raisonnement est valable pour a et ab puisque nous travaillons avec des génériques bilatères. □

Des corollaires 4.5.10 et 4.5.11cela, on peut rapidement déduire le premier pas de la question d"'équations génériques" dans un groupe stable :

Corollaire 4.5.12 *Un groupe stable dont tout générique est d'ordre 2, est un groupe d'exposant 2. En particulier, il est abélien.*

Le cas de l'exposant 3 est aussi connu : le groupe est nilpotent d'exposant 3. Néanmoins, le raisonnement est plus long. La réponse est affirmative pour les groupes résolubles d'après les travaux de Khaled Jaber et Frank Wagner. La réponse en toute généralité n'est pas connue.

Corollaire 4.5.13 *Soient $p \in S_1(G)$ un type arbitraire et $\phi(x)$ une formule générique. Alors, il existe un élément $c \in G$ tel que $\phi(cx) \in p$. De manière analogue, il existe $c \in G$ tel que $\phi(xc) \in p$.*

Preuve. Soient a une réalisation de p et b une réalisation d'un type générique contenant ϕ. Nous pouvons choisir a et b de manière indépendante sur G. Alors, $b = (ba^{-1})a$ et ba^{-1} est générique sur $G \cup a$. Par symétrie de la déviation, $\mathrm{tp}(a/G \cup ba^{-1})$ ne dévie pas sur G. Par conséquent, $\mathrm{tp}(a/G \cup ba^{-1})$ hérite de sa restriction à G. Or, $\models \phi((ba^{-1})a)$, en d'autres termes, $\phi((ba^{-1})x) \in p$. Il existe donc $c \in G$ tel que $\phi(cx) \in p$.

Quant au dernier énoncé il suffit de refaire le raisonnement précédent en constatant que $b = a(a^{-1}b)$. □

Le corollaire suivant permettra d'éviter de ne plus faire mention des génériques à gauche ou à droite.

Corollaire 4.5.14 *Une formule du premier ordre qui est générique, l'est aussi à gauche et à droite.*

Preuve. La conclusion découle d'un raisonnement de compacité et du corollaire 4.5.13. Soit ϕ une formule générique qui refuse de l'être disons à gauche. Alors l'ensemble $\{\neg\phi(gx)|g \in G\}$ à paramètres dans G est consistant avec $\mathrm{Th}((G, g)_{g\in G})$. En effet, pour tout choix de $g_1, \ldots, g_k \in G$, $\neg(\phi(g_1x) \vee \ldots \vee \phi(g_kx))$ équivaut à $\neg\phi(g_1x) \wedge \ldots \neg \wedge \phi(g_kx)$.

Soit d une réalisation de cet ensemble dans une extension élémentaire de G. D'après le paragraphe précédent, $\phi(x)$ ne peut pas être translaté dans $\mathrm{tp}(d/G)$. Ceci contredit le corollaire 4.5.13. □

4.6 Action d'un groupe stable sur ses types, retour aux composantes connexes

Dans cette section, nous étudierons l'action d'un groupe stable sur ses 1-types. Ceci permettra de faire le lien avec les composantes connexes de la section 4.3. Un groupe stable agit sur ses types façon très naturelle :

$$\begin{array}{ccc} G \times S_1(G) & \longrightarrow & S_1(G) \\ (g, \mathrm{tp}(x/G)) & \longmapsto & \mathrm{tp}(gx/G)\ . \end{array}$$

Une question naturelle est de faire émerger une notion de définissabilité pour une telle action. L'approche à cette question naturelle est tout aussi naturelle : l'action sera dite définissable si et seulement si le *stabilisateur d'un type* est définissable. Clairement, la définissabilité d'un type jouera le rôle clé dans cette définition.

Fixons d'abord une $\mathcal{L}$-formule $\phi(x, y)$ à $1+1+k$ variables libres, et considérons la restriction d'un type $p \in S_1(G)$ aux instances de $\phi'(x, z, y)$ et de $\neg\phi'(x, z, y)$ représentées dans p. Alors, le stabilisateur de ce type partiel est définissable

$$\forall y(d_p\phi'(1, y) \longleftrightarrow d_p\phi'(z, y))\ .$$

La notation utilisée est un peu déroutante mais il faut bien prendre en compte l'action de groupe : $\phi'(x, z, y)$ est la formule $\phi(zx, y)$. Nous noterons ce stabilisateur $\mathrm{Stab}(p, \phi)$.

Le stabilisateur de p, pour lequel nous utiliserons la notation usuelle $\mathrm{Stab}(p)$ de la théorie des groupes, n'est pas nécessairement définissable. Il est ∞-*définissable* : c'est l'intersection d'une famille de formules qui forment un type partiel sur un ensemble de paramètres fixés,.

Le lien entre ces deux stabilisateurs est réminiscent de celui entre les ϕ-composantes connexes d'un groupe stable et sa *composante connexe* que nous noterons G° : c'est l'intersection de toutes les ϕ-composantes connexes. Comme celles-ci sont d'indices finis dans le groupe ambiant, leurs formules de définition forment un type partiel. Par ailleurs, ce type est de cardinal borné par celui du langage puisque les ϕ-composantes connexes sont définissables sans paramètres. La notion de composante connexe a donc un côté absolu qui est préservée quand on passe aux extensions élémentaires. Tout lien avec l'action sur les types éventuellement rendra cette action plus robuste. Voici le lien :

Lemme 4.6.1 *1. Pour un type arbitraire $p \in S_1(G)$, $\mathrm{Stab}(p) \leq G^\circ$.*

2. Si p est un type générique, alors pour toute formule ϕ, $\mathrm{Stab}(p, \phi)$ est d'indice fini dans le groupe ambiant et $G^\circ = \mathrm{Stab}(p)$.

Preuve. 1. Soient $\phi(x, y)$ une formule définissant un sous-groupe après avoir remplacé y par des paramètres provenant de G, et p un type dans $S_1(G)$. Alors p détermine une classe de $G^\circ(\phi)$ et une seule. En effet, pour tout $g \in G$, soit la formule qui définit $gG^\circ(\phi)$ appartient à p, soit c'est le cas contraire. Il en existe certainement une puisque les classes de $G^\circ(\phi)$ couvrent G. Par ailleurs, comme deux classes distinctes d'un sous-groupe sont disjointes, si $gG^\circ(\phi) \in p$ et $hg^\circ(\phi) \in p$, alors $gG^\circ(\phi) = hG^\circ(\phi)$.

Si maintenant $g \in \mathrm{Stab}(G)$, alors $gp = p$. Le paragraphe précédent nous montre qu'il existe $h \in G$ tel que $ghG^\circ(\phi) = hG^\circ(\phi)$, ce qui équivaut à $g \in G^\circ(\phi)^{h^{-1}} = G^\circ(\phi)$. Comme ϕ était arbitrairement choisi, $g \in G^\circ$.

2. Comme p est générique, pour toute formule ϕ, $\mathrm{Stab}(p, \phi)$ est d'indice fini. En effet, si $\mathrm{Stab}(p, \phi)$ est d'indice infini, alors, en utilisant la compacité, nous montrons que pour tout cardinal infini κ il existe une extension élémentaire du groupe ambiant dans laquelle $\mathrm{Stab}(p, \phi)$ est d'indice au moins κ. Par conséquent, le cardinal des translatés du ϕ-type de p n'a pas de borne. Chaque translaté correspond à un type générique différent. Or, les génériques sont en nombre borné.

Il découle du paragraphe précédent que $\mathrm{Stab}(p) \geq G^\circ$. L'autre inclusion ayant déjà été vérifiée, l'égalité s'ensuit. □

Lemme 4.6.2 *Soient G un groupe stable et $p \in S_1(G)$ un type générique. Pour tout $g \in G$, les formules $g\mathrm{Stab}(p, \phi)$ dont l'intersection éventuellement infinie définit gG°, est un type partiel qui se complète à un type générique et un seul : toute classe de G° "contient" un générique et un seul.*

Preuve. Soit $p \in S_1(G)$ un type générique. D'après le lemme 4.6.1, $G^\circ = \mathrm{Stab}(p)$.

Pour toute formule $\phi(x, y)$, nous avons vérifié dans la preuve du lemme 4.6.1 (i) que p détermine une classe et une seule de $G^\circ(\phi)$. L'intersection de toutes ces classes quand ϕ varie sur toutes les possibilités est réalisée dans une extension élémentaire $\tilde{G}$ de G. Cette réalisation appartient à la classe de G° qui correspond à p.

Si maintenant on considère une classe arbitraire de la composante connexe dans cette extension élémentaire, on peut translater la classe de p par un élément $\tilde{g}\tilde{G}$. Alors, l'héritier $\tilde{p}$ de p sur $\tilde{G}$, qui est générique, se translate à $\tilde{g}\tilde{p}$ qui est aussi générique. Ceci montre que chaque classe de la composante connexe dans toute extension élémentaire de G correspond à un générique.

Maintenant nous vérifierons l'unicité du générique trouvé dans une classe arbitraire de G°. Il suffira de faire cette vérification pour G° puisque la conclusion sera préservée par les translations. Soient a et b des réalisations indépendantes sur G de deux génériques dans G°. Nous montrerons qu'ils réalisent le même type générique. D'après le corollaire 4.5.11, a, b et ab sont indépendants et génériques sur G. Or, nous avons vérifié dans le lemme 4.6.1 (ii) que G° stabilise un type générique. Ainsi, a et b réalisent le même générique. □

Corollaire 4.6.3 *Un groupe stable suffisamment saturé agit sur ses type génériques transitivement.*

Preuve. Le lemme 4.6.2 montre que l'indice dans un groupe stable G, $|G : G^\circ|$ est borné par un cardinal. Alors l'hypothèse de saturation assure que chaque classe de G° est représentée dans G. Dans un tel groupe, l'action sur les types génériques équivaut à l'action sur les classes de G°. □

Corollaire 4.6.4 *Dans un groupe stable G, un type est générique si et seulement si son stabilisateur est G°.*

Preuve. La nécessité de la condition a déjà été vérifiée dans le lemme 4.6.1. Quant à sa suffisance, soit p un type stabilisé par G°. Soient a et b des réalisations indépendantes de p et du générique de G° respectivement. Alors $\mathrm{tp}(b/G \cup a)$ et par conséquent $\mathrm{tp}(ba/G \cup a)$ sont génériques. Ainsi $\mathrm{tp}(ba/G)$ est générique. Or, b stabilise $\mathrm{tp}(a/G)$. Donc, $\mathrm{tp}(a/G) = \mathrm{tp}(ba/G)$. □

4.7 Génériques dans les groupes libres non abéliens

Dans cette section nous démontrerons un théorème récent d'Anand Pillay qui caractérise les réalisations du type générique d'un groupe libre non abélien de type fini. Ce que nous venons de dire est déjà remarquable puisque d'un côté nous admettons la stabilité de la théorie concernée, d'un autre, nous nous permettons de parler "du" type générique. Cette dernière conclusion est plus simple à obtenir et elle constitue notre point de départ.

Commençons par un lemme important dû à Poizat qui ne nécessite pas l'hypothèse de stabilité :

Lemme 4.7.1 (Poizat) *Soit F un groupe libre non abélien. Si A est une partie définissable et générique dans F, alors pour toute base X de F, $X \setminus A$ est un ensemble fini.*

Preuve. Soit $X = \{x_i | i \in I\}$ une base de F. Soient $g_1, \ldots, g_n \in F$ tels que $F = Ag_1 \cup \ldots \cup Ag_n$. Alors, il existe $x_{i_1}, \ldots, x_{i_r} \in X$ qui sont utilisés dans les formes normales de $g_1, \ldots, g_n$ et des paramètres pour définir X. Soit $y \in X \setminus \{x_{i_1}, \ldots, x_{i_r}\}$. Alors $y \in Ag_i$ pour un certain $i \in \{1, \ldots, n\}$. Equivalemment, $yg_i^{-1} \in A$. Or $(X \setminus \{y\}) \cup \{yg_i^{-1}\}$ est aussi une base de F. Ainsi, la bijection qui fixe $(X \setminus \cup\{y\})$ et transforme yg_i^{-1} en y induit un automorphisme de F qui stabilise X. Par conséquent, $y \in A$. □

Le théorème suivant est l'un des résultats fondamentaux de Sela :

Fait 4.7.2 *Soit F_n le groupe libre non abélien à n générateurs. Alors* $\mathrm{Th}(F_n)$ *est stable.*

Grâce aux autres résultats fondamentaux de Sela évoqués dans le deuxième chapitre (le fait 2.5.2), la théorie du premier ordre de tous les groupes libres non commutatifs est stable. On obtient alors immédiatement le corollaire suivant du lemme 4.7.1 :

Corollaire 4.7.3 *Soit F un groupe libre non commutatif avec une base $X = \{x_i | i \in I\}$.*

1. *F a un seul type générique. En particulier, il est connexe.*
2. *Si p note le seul générique sur $\emptyset$ (le lemme 4.5.7), alors X est un ensemble indépendant de réalisations de X.*

Preuve. Le premier point découle immédiatement du lemme 4.7.1. Quant au deuxième, considérons pour un $i \in I$ fixé, le type $\mathrm{tp}(x_i/X \setminus \{x_i\})$. En utilisant les automorphismes, comme dans le lemme 4.7.1, nous voyons que toute formule à paramètres dans $X \setminus \{x_i\}$ qui définit un ensemble générique appartient à $\mathrm{tp}(x_i/X \setminus \{x_i\})$. Par conséquent, $\mathrm{tp}(x_i/X \setminus \{x_i\})$ est générique dans $S_1(X \setminus \{x_i\})$. Ainsi, il ne dévie pas sur $\emptyset$ d'après le lemme 4.5.7. □

Dans ce qui suit p sera utilisé pour noter le seul type générique sur $\emptyset$ du groupe libre non commutatif à n générateurs. Le théorème suivant de Pillay offre un inverse au deuxième point du corollaire 4.7.3

Théorème 4.3 [8] *Soit F_n le groupe libre à n générateurs ($n \geq 2$). Alors toute réalisation de p appartient à une base de F.*

Preuve. Posons $X = \{x_1, \ldots, x_n\}$, une base pour F_n qui se plonge dans $F_{n+1} = \langle X \cup \{x_{n+1}\}\rangle$ élémentairement d'après le fait 2.5.2. Soit y une réalisation de p dans F_n. Comme $F_n \preceq F_{n+1}$, y réalise p dans F_{n+1} aussi.

Comme $F_n = \langle x_1, \ldots, x_n\rangle$ et que x_{n+1} est indépendant de $\{x_1, \ldots, x_n\}$ sur $\emptyset$, x_{n+1} est indépendant de F_n sur $\emptyset$, en particulier de y sur $\emptyset$. Comme conséquence de cette indépendance,

le sous-groupe engendré par $\{x_{n+1}, y\}$ a le même type dans F_{n+1} que celui d'une base de F_2. En effet, il s'agit de deux éléments indépendants sur $\emptyset$ qui sont tous les deux génériques sur $\emptyset$. Alors, $\langle x_{n+1}, y\rangle$ est un groupe libre et une sous-structure élémentaire de F_{n+1}.

Comme $\langle x_{n+1}, y\rangle \preceq F_{n+1}$, le fait 2.5.3 montre que $\langle x_{n+1}, y\rangle$ est un facteur libre de F_{n+1}. Par conséquent, $\{x_{n+1}, y\}$ se complète en une base $\{x_{n+1}, y, z_1, \ldots, z_{n-1}\}$. L'homomorphisme surjectif ϕ défini comme l'identité sur F_n et qui associe l'élément neutre à x_{n+1} implique que $\{y, \phi(z_1), \ldots, \phi(z_{n-1})\}$ soit un ensemble de générateurs pour F_n. Ayant exactement au plus n éléments, c'est forcément une base d'après le lemme 2.1.4. Ainsi, y appartient à une base de F_n. □

Les théorèmes de Sela n'ont pas seulement vérifié l'équivalence élémentaire des groupes libres non commutatifs mais ont motivé une vaste quantité de travaux sur les groupes qui sont élémentairement équivalents aux groupes libres. Nous finissons en mentionnant un théorème récent qui montre les liens avec le cours de Julien Melleray :

Fait 4.7.4 [3] *Un groupe élémentairement équivalent à un groupe libre lui est mesure-équivalent.*

Exercices

Exercice 4.1 Montrer que si un groupe arbitraire G a un sous-groupe H d'indice fini, alors H a un sous-groupe H_1 d'indice fini qui est distingué dans G.

Exercice 4.2 Vérifier les points (2), (3), (4) du lemme 4.1.2.

Exercice 4.3 Vérifier le lemme 4.1.4.

Exercice 4.4 Etudier les diverses propriétés d'ordre et d'indépendance dans le groupe symétrique et le groupe alterné sur les nombres naturels.

Exercice 4.5 Démontrer les lemmes 4.1.4 et 4.1.6.

Exercice 4.6 Soit G un groupe stable avec exactement deux classes de conjugaison. En d'autres termes, pour tout $x \in G \setminus \{1\}$, $G = x^G \cup \{1\}$. Montrer que si G est stable, alors G est d'ordre 2. Vous pouvez suivre la stratégie suivante :

1. Vérifier que tout élément de G est conjugué à son inverse et en déduire que le centralisateur de tout élément non trivial est strictement contenu dans celui de son carré.
2. Conclure dans le cas où G contient un élément d'ordre 2.
3. Vérifier que si G n'a pas d'élément d'ordre 2, alors G est infini.
4. Montrer qu'il existe dans G un élément dont le centralisateur est strictement contenu dans celui d'un de ses conjugués.
5. En utilisant le point précédent construire une suite infinie et ascendante de centralisateurs.

Exercice 4.7 Montrer que dans un groupe stable centralisateur-connexe et nilpotent, tout sous-groupe distingué et infini contient une infinité d'éléments centraux.

Exercice 4.8 Soit G un groupe $\aleph_0$-stable.

1. Montrer que dans G il n'existe pas de chaîne infinie descendante de sous-groupes définissables avec éventuellement paramètres provenant de G. Vous pouvez procéder en suivant la stratégie suivante
   (a) Par l'absurde, supposer que
   $$H_0 > H_1 > H_2 > \dots$$
   est une chaîne infinie et descendante. Vérifier qu'il existe pour tout $i \in \mathbb{N}$, un élément $g_i \in H_i \setminus H_{i+1}$ tel que les
   $$H_{i+1} \prod_{j \in J} g_j \quad \text{(indices des } g_j \text{ en ordre décroissant)}$$
   où $J \subset \{0, \dots, i\}$ forment des classes de H_{i+1} deux à deux disjointes dans H_i.
   (b) Construire en utilisant le premier point un arbre binaire infini de formules du premier ordre décrivant des classes des H_i dont les branches sont des familles consistantes deux à deux distinctes.
   (c) Vérifier que les formules de l'arbre binaire du point précédent nécessitent un ensemble dénombrable de paramètres.
   (d) Conclure.
2. Montrer que G a un plus petit sous-groupe définissable d'indice fini et que ce sous-groupe peut être défini par une formule sans paramètres.
3. Appelons le sous-groupe du point précédent la *composante connexe* de G et notons-le G°. Montrer que $(G^\circ)^\circ = G^\circ$.

4. Montrer que le groupe $(\mathbb{Z}, +)$ n'est pas $\aleph_0$-stable. En déduire qu'aucun groupe libre n'est $\aleph_0$-stable.
5. Montrer que si G est un groupe commutatif, alors G a un sous-groupe définissable et divisible D et un sous-groupe définissable d'exposant borné U tel que $G = DU$.
6. Montrer qu'une partie quelconque X de G est contenue dans un plus petit sous-groupe définissable de G, l'*enveloppe définissable* de X, noté $d(X)$. Montrer que si X est un sous-groupe abélien, il en est de même pour $d(X)$.

Exercice 4.9 (Exposants génériques dans un groupe stable ; un théorème de Poizat) Soit G un groupe stable. L'objectif de cet exercice est de montrer que si

$$(*) \quad G \text{ est } \textit{génériquement d'exposant } 3,$$

alors il est d'exposant 3. Plus précisément, si tout x tel que $\mathrm{tp}(x/G)$ soit un type générique dans $S_1(G)$ satisfait l'équation $x^3 = 1$, alors tout $g \in G$ satisfait la même équation. Il en découle bien sûr que la même propriété est vraie dans tout modèle de $\mathrm{Th}(G)$. Ci-dessous, sauf mention contraire G sera un groupe stable satisfaisant (*).

1. Dans ce point G est un groupe stable arbitraire. Montrer que si $A \subset G$ est un ensemble de paramètres, que $\mathrm{tp}(x/A)$ est générique dans $S_1(A)$, alors x est générique sur toute partie $B \subset \langle A \rangle$. (*On peut soit aborder la question directement, soit la lier à la préservation de l'indépendance quand on passe à la clôture algébrique d'un ensemble.*)
2. Soient maintenant $g \in G$ et x générique sur $\{g\}$, en d'autres termes $\mathrm{tp}(x/\{g\})$ est générique (on peut toujours supposer que $\mathrm{tp}(x/G)$ est un type générique dans $S_1(G)$). Vérifier que gx^{-1} et xg sont génériques sur $\{g\}$.
3. Vérifier en utilisant le point précédent et l'hypothèse (*) que $gg^x = g^{x^2} = g^x g$.
4. Soit g^G la classe de conjugaison. Montrer qu'il existe $a_1, \ldots, a_k \in G$ tels que $C_G(g^G) = C_G(g^{a_1}, \ldots, g^{a_k})$.
5. Montrer que nous pouvons supposer x générique sur $\{g, a_1, \ldots, a_k\}$. En déduire que g^x et g^{a_i} commutent pour tout $i \in \{1, \ldots, k\}$.
6. Montrer que $g^G \subset C_G(g^G)$. En d'autres termes, deux éléments arbitraires de la classe de conjuguaison de g dans G commutent.
7. Déduire du point précédent que si $g, h \in G$ satisfont $g^3 = h^3 = 1$, alors $(gh)^3 = 1$ aussi.
8. Conclure que pour tout $g \in G$, $g^3 = 1$.

(*Nous aurions pu procéder en utilisant $S_1(G)$ ce qui éviterait de jongler avec les ensembles de paramètres. Néanmoins, c'est un bon entrînement. Par ailleurs, il existe des groupes stables où la structure des extensions élémentaires sont peu connues et il faut se débrouiller en utilisant des génériques sur de petits ensembles de paramètres. Les groupes libres non abéliens fournissent un exemple de cette situation.*

En utilisant des résultats sur les groupes satisfaisant la condition de chaîne descendante sur les centralisateurs il est possible de conclure que G est nilpotent.)

Exercice 4.10 (Enveloppe définissable d'un groupe nilpotent dans un groupe sans la propriété d'indépendance ; un théorème de Aldama)

Dans cet exercice nous essayerons de détailler un résultat récent de Ricardo de Aldama :

Soit G un groupe infini dont la théorie n'a pas la propriété d'indépendance. Si A est une partie de G telle que $[x_0, \ldots, x_n] = 1$ pour tout $x_0, \ldots, x_n \in A$ et que G est $|A|^+$-saturé, alors A est contenu dans un sous-groupe définissable (éventuellement avec paramètres) nilpotent de classe n de G.

Nous procéderons par une suite d'étapes parfois générales. Le langage $\mathcal{L}$ sera celui des groupes : $\{., \ ^{-1}, 1\}$.

1. Soient G un groupe arbitraire et $A \subset G$ tel que $[x_0, \ldots, x_n] = 1$ pour tout $x_0, \ldots, x_n \in A$. Montrer que le sous-groupe engendré par A ($\langle A \rangle$) est nilpotent de classe n.
2. Ce point est une variante du lemme 4.2.3. Soient G un groupe sans indépendance et $\phi(x, y)$ une $\mathcal{L}$-formule à $1+k$ variables libres. Alors, il n'existe pas de ensembles $\{g_i | i \in \mathbb{N}, g_i \in G\}$ et $\{h_i | i \in \mathbb{N}, h_i \in G^k\}$ tels que $G \models \phi(g_i, h_j)$ si et seulement si $i \neq j$.
3. C'est un point avec plusieurs étapes. L'objectif est de montrer l'énoncé suivant :

   Soient G un groupe infini sans indépendance qui est $|A|^+$-saturé où A est un sous-groupe de G non nécessairement définissable. Soient

   $\Phi = \{\phi(x) \mid A \subset \phi(G)\ ,\ \phi$ *est une* $\mathcal{L}(\mathcal{G})$*-formule.* $\}$ *et* $\Psi = \{\psi(x) \mid Z(A) \subset \psi(G)\ ,\ \psi$ *est une* $\mathcal{L}(\mathcal{G})$*-formule.* $\}$.

   Alors, $\Phi(x) \cup \Psi(y) \vdash xy = yx$; en d'autres termes, si x réalise Φ et y réalise Ψ, alors x et y commutent.
   (*Un mot sur la notation : pour toute $\mathcal{L}(G)$-formule ϕ à une variable libre, $\phi(G)$ est utilisé pour noter l'ensemble défini par ϕ. Accessoirement, notons aussi que Φ et Ψ sont des types partiels.*)

   La preuve est par l'absurde.
   (a) Montrer qu'il existe $\{(a_i, b_i) \in G^2 | i \in \mathbb{N}\}$ tel que pour tout $n \in \mathbb{N}$, a_n et b_n réalise les restrictions $\Phi|_{A \cup \{a_i, b_i | i<n\}}$ et $\Psi|_{A \cup \{a_i, b_i | i<n\}}$ respectivement, et que $a_i b_i \neq b_i a_i$ pour tout $i \in \mathbb{N}$.
   (b) Montrer, en utilisant la $\mathcal{L}$-formule $xy = yx$, que si $a \in A$, alors $a \in C_G(b_j)$ pour tout $j \in \mathbb{N}$.
   (c) Montrer, en utilisant la $\mathcal{L}$-formule $xy = yx$ que, si $b \in Z(A)$, alors $a_i \in C_G(b)$ pour tout $i \in \mathbb{N}$.
   (d) Déduire des deux points précédents que $a_i \in C_G(b_j)$ si et seulement si $i \neq j$. (*Vous pouvez raisonner en deux étapes utilisant Φ ou Ψ en suivant si $i > j$ ou $j > i$*).
   (e) Conclure.

   A partir de maintenant nous travaillerons dans un groupe G sans indépendance qui contient un ensemble A ayant la propriété de commutateurs de l'énoncé du théorème et qui est $|A|^+$-saturé. Soulignons que l'ensemble A n'est pas nécessairement définissable.

4. C'est un point avec plusieurs étapes. En utilisant la préparation faite jusqu'à ce point, nous démontrerons le théorème de de Aldama.
   (a) Vérifier que nous pouvons supposer que A soit un sous-groupe.
   (b) Soient Φ et Ψ les types partiels du point 3. Montrer qu'il existe deux $\mathcal{L}(G)$ formules $\phi(x)$ et $\psi(x)$ à une variable libre chacune appartenant Φ et Ψ respectivement telles que $\phi(x) \wedge \psi(y) \vdash xy = yx$.
   (c) Vérifier le théorème pour $n = 1$, en utilisant $Z(\ C_G((\phi \wedge \psi)(G))\ )$.

   On suppose le théorème vrai pour $n \geq 1$ et procède par récurrence sur la classe de nilpotence de A, notée n. Posons $H = Z(C_G(\psi(G)))$; en d'autres termes, $H = C_G(C_G(\psi(G))) \cap C_G(\psi(G))$.

   (d) Vérifier que $A \leq C_G(H)$ et que $Z(A) \leq H$.
   (e) Déduire du point précédent que le quotient AH/H est de classe de nilpotence au plus $n-1$. Vérifier aussi que $AH/H \leq C_G(H)/H$.
   (f) Montrer que la structure $C_G(H)/H$ est un groupe sans indépendance.
   (g) Conclure qu'il existe un sous-groupe E définissable nilpotent de classe n tel que $A \leq E \leq C_G(H)$.

Bibliographie

[1] R. de Aldama *Thèse de doctorat*. Institut Camille Jordan, 2009.

[2] E. Bouscaren (Ed.). *Model Theory and Algebraic Geometry*. LNM 1696. (Springer, 1999).

[3] M. Bridson, M. Tweedale, H. Wilton. *Limit groups, positive-genus towers and measure-equivalence. Ergodic Theory and Dynamical Systems* (2007), 27 :3 :703–712.

[4] J. Holly. *Definable operations on sets and elimination of imaginaries. Proc. Amer. Math. Soc.* **117** (1993), 1149–1157.

[5] R. C. Lyndon, P. E. Schupp. *Combinatorial Group Theory*. Classics in Mathematics. (Springer-Verlag, 1977).

[6] C. Perin. *Elementary embedings in torsion-free hyperbolic groups*. Thèse de doctorat (2008).

[7] A. Pillay. *Geometric Stability Theory*. Oxford Logic Guides 32. (Oxford University Press, 1996).

[8] A. Pillay. *On genericity and weight in the free group. Proc. Amer. Math. Soc.* **137** (2009),11,3911-3917.

[9] B. Poizat. *Cours de Théorie des Modèles*. Nur Al-Mantiq Wal-Ma'rifah, Villeurbanne, France, (1985).

[10] B. Poizat. *Groupes Stables*. Nur Al-Mantiq Wal-Ma'rifah, Villeurbanne, France, (1987).

[11] B. Poizat. *Une théorie de Galois imaginaire. J. Symbolic Logic* **48** (1983), 1151–1170.

[12] D. J. S. Robinson. *A Course in the Theory of Groups*. Graduate Text in Mathematics 80. (Springer-Verlag, 1996).

[13] Z. Sela. `http ://www.ma.huji.ac.il/~ zlil/`.

[14] F. Wagner. *Stable Groups*. LMS Lecture Note Series 240. (CUP, 1997).

[15] F. Wagner. *Simple Theories*. Mathematics and Its Applications 503. (Kluwer Academic, 2000).