Groupes nilpotents sans torsion et complétés de Mal'cev

Esther Suisse

19 septembre 2007

Mémoire dirigé par Gwenaël Massuyeau

Université Louis Pasteur
UFR de Mathématiques et Informatique
Magistère de Mathématiques

2006/2007
Mémoire de Licence
Première Année

Remerciements

À mes amis, qui ont supporté mon travail et mes remarques incompréhensibles pendant de longs mois,

À mes parents, qui m'ont encouragée et qui m'ont donné les conditions nécessaires à un travail efficace,

À mon directeur de mémoire qui a gentiment et patiemment résolu toutes les impossibilités que j'ai soulevées au fur et à mesure de mes recherches,

je voudrais dire un grand $\mathcal{MERCI}$ *!*

Table des matières

Introduction

Ce mémoire a pour objet l'étude de quelques propriétés des groupes que l'on qualifie de *nilpotents*. Ces groupes constituent une généralisation des groupes abéliens : le commutateur de deux éléments a et b d'un groupe G, défini par $[a, b] = a^{-1}b^{-1}ab$, est toujours trivial dans un groupe commutatif. On dit d'un groupe G qu'il est nilpotent de classe 2 s'il vérifie la propriété moins forte que, pour tous éléments a, b et c du groupe, $[\,[a, b], c]$ est trivial. On observe de même des groupes nilpotents de classe n, où n est un entier naturel.

Nous nous intéresserons ici plus particulièrement aux groupes nilpotents de type fini, c'est-à-dire engendrés par un nombre fini d'éléments, ou sans torsion, ce qui se traduit par l'absence d'éléments périodiques dans le groupe.

Quelques rappels succincts me permettent, dans le premier chapitre, de rappeler quelques notions essentielles à l'étude des groupes dans leur ensemble, et à notre étude des groupes nilpotents en particulier. Ceux-ci sont complétés par une présentation rapide des différentes classes de groupes qui nous seront utiles, que l'on trouvera dans le chapitre deux. Nous y détaillerons les définitions des groupes abéliens, nilpotents, sans torsion et de type fini, mais également celles des termes *divisible* et *polycyclique*, qui auront un rôle important dans les considérations qui suivront.

L'objet du troisième chapitre touche, plus particulièrement, un type spécifique de clôture divisible, que l'on nomme *complété de Mal'cev*, du nom du mathématicien qui est à l'origine de sa construction. La clôture divisible d'un groupe nilpotent sans torsion est simplement une extension de ce groupe, elle-même nilpotente et dépourvue de torsion, dans laquelle sont assurées l'existence d'une solution à toute équation du type $x^n = g$, où g est un élément du groupe et n un entier naturel non nul, et l'unicité de cette solution. Afin de construire une telle clôture, nous nous intéresserons à un système de coordonnées d'un groupe nilpotent de type fini sans torsion, système auquel on donne le nom de *coordonnées de Mal'cev*. Celles-ci nous permettront d'édifier un complété de Mal'cev pour un groupe nilpotent de type fini sans torsion, et

par ce biais, de généraliser ce complété à tout groupe nilpotent sans torsion, auquel on n'impose plus d'être de type fini. Il est également intéressant de constater que cette clôture divisible est de plus unique à isomorphisme près.

Un exemple type de groupe nilpotent, qui est de plus sans torsion, est celui des matrices triangulaires supérieures d'ordre n à coefficients dans un corps K de caractéristique nulle, dont tous les éléments de la diagonale sont égaux à l'élément neutre multiplicatif de K, noté 1. Nous utilisons pour ce groupe la notation usuelle $UT_n(K)$. Nous constaterons au passage que le groupe $UT_n(\mathbb{Q})$ se trouve être divisible.

Le dernier chapitre de ce mémoire sera consacré à la recherche d'un plongement, pour un groupe G nilpotent de type fini, dans un groupe linéaire à coefficients entiers, $GL_n(\mathbb{Z})$, pour un entier naturel n dépendant de G. Nous préciserons en outre la démonstration pour obtenir un plongement de tout groupe nilpotent de type fini et sans torsion dans le groupe de matrices évoqué ci-dessus : $UT_n(\mathbb{Z})$.

La plupart des résultats que nous démontrerons et utiliserons sont dus à Anatoly Ivanovitch Mal'cev qui a réalisé une étude approfondie des groupes nilpotents. Quelques éléments de sa biographie sont consignés en annexe à la fin de ce mémoire.

Toutefois, c'est du livre de Mikhaïl Kargapolov et Iouri Merzliakov, *Éléments de la théorie des groupes* (voir la bibliographie en page 87), que je me suis largement inspirée pour établir la structure des preuves essentielles de ce mémoire. Plus particulièrement, ce sont les six premiers chapitres qui m'ont guidée dans mon travail, et surtout le chapitre six, intitulé précisément : *Groupes nilpotents*.

Chapitre 1

Quelques notions préalables sur les groupes

Commençons par rappeler quelques notations, termes et définitions usuels qui seront utilisés dans ce mémoire. Il est pour cela utile de revenir sur quelques propriétés bien connues des groupes.

1.1 Rappels sur les groupes et sur leurs homomorphismes

Commençons par quelques notations utiles :

- Un groupe G sera en général noté multiplicativement, c'est-à-dire que sa loi de composition interne est notée $\bullet$, et qu'elle sera omise en général. Ainsi, on écrira ab pour $a \bullet b$. Toutefois, il arrivera que nous dussions différencier deux lois de groupes. On écrit alors $(G, \bullet)$ pour préciser la notation utilisée pour la loi de G.
- L'élément neutre de G est en général noté e ou 1, éventuellement e_G si le contexte nécessite une différenciation entre les éléments neutres de deux groupes distincts. Un groupe restreint à son élément neutre est dit *trivial*.
- L'*ordre* d'un groupe G, c'est-à-dire son cardinal, est noté $|G|$.
- Si H est un sous-groupe de G, on notera : $H \leqslant G$. On dit qu'un sous-groupe H d'un groupe G est *propre* si $H \neq G$, et on utilisera alors éventuellement la notation $H < G$.
- Soit G un groupe quelconque. Si A est une partie de G, alors le *sous-groupe engendré* par les éléments de A, noté $\langle A \rangle$, ou $gr(A)$ selon le contexte, est l'intersection de tous les sous-groupes de G qui contiennent la partie A.

Soit $\mathcal{P}$ une propriété d'éléments du groupe G. Si $A = \{x \in G : x \text{ vérifie } \mathcal{P}\}$, alors on omet les accolades pour ne pas surcharger l'écriture :

$$\begin{aligned} \langle A \rangle &= \langle x \in G : x \text{ vérifie } \mathcal{P} \rangle \\ gr(A) &= gr(x \in G : x \text{ vérifie } \mathcal{P}). \end{aligned}$$

1.1.1 Propriétés préliminaires des groupes

Ici sont recensées quelques-unes des propriétés de groupes les plus connues, que nous utiliserons par la suite.

Produit de groupes

Si A et B sont deux sous-groupes d'un groupe G, leur *produit* $AB = \{ab \,|\, a \in A,\ b \in B\}$ est un groupe si, et seulement si $BA = AB$.

Démonstration — Supposons premièrement que AB est un sous-groupe. Alors, pour tout $x \in BA$, il existe $a \in A$ et $b \in B$ tels que $x = ba$; on a ainsi $x = (a^{-1}b^{-1})^{-1}$, c'est-à-dire $x \in AB$ car AB est un sous-groupe de G. D'où $BA \subseteq AB$. Soit maintenant $x \in AB$; AB étant un sous-groupe de G par hypothèse, il existe $a_1 \in A$, $b_1 \in B$ tels que $x = (a_1 b_1)^{-1}$, ce qui s'écrit exactement $x = b_1^{-1} a_1^{-1}$, où $a_1^{-1} \in A$ et $b_1^{-1} \in B$ car A et B sont des sous-groupes de G. On a ainsi montré que $x \in BA$, et donc que $AB \subseteq BA$. D'où l'égalité $AB = BA$. D'autre part, si l'on suppose cette même égalité, il est évident que le sous-ensemble AB de G est stable par passage à l'inverse, et pour $x = a_1 b_1 \in AB$ et $y = a_2 b_2 \in AB$, on a $xy = a_1 b_1 a_2 b_2$. Or on a par hypothèse : $b_1 a_2 \in BA = AB$, donc il existe $a \in A$ et $b \in B$ tels que $b_1 a_2 = ab$, et finalement $xy = a_1 abb_2$, avec $a_1 a \in A$ et $bb_2 \in B$, d'où $xy \in AB$, et AB est un sous-groupe de G. ⊠

Groupes cycliques

Rappelons qu'un groupe est généralement dit *cyclique* s'il est *monogène*, c'est-à-dire engendré par un seul élément, et fini. Dans ce mémoire, nous utiliserons le terme *cyclique* pour désigner à la fois ces groupes et les groupes monogènes, c'est-à-dire qu'un groupe cyclique ne sera pas nécessairement fini.
Une propriété bien connue de tels groupes est la suivante :

Propriété 1.1.1
Tout sous-groupe d'un groupe cyclique est lui-même cyclique.

Démonstration — Soit G un groupe cyclique, engendré par $a : G = \langle a \rangle$. Son sous-groupe $\{1\}$ est évidemment cyclique. Notons H un sous-groupe de G, non trivial. Soit m le plus petit entier naturel non nul tel que $a^m \in H$. On a alors évidemment $gr(a^m) \leqslant H$. Montrons qu'en fait ces deux sous-groupes de G se confondent. Choisissons un élément x de H. Comme $x \in G$, il existe un entier naturel n tel que $x = a^n$. Alors, en effectuant la division euclidienne dans $\mathbb{N}$ de n par m, on obtient : $n = mq + r$, où q, $r \in \mathbb{N}$, avec $0 \leqslant r < m$. Puisque a^n et $a^{-mq} = (a^{-m})^q$ sont des éléments du sous-groupe H, on a aussi $a^r = a^{n-mq} \in H$. La condition $r < m$ impose alors $r = 0$. D'où $x = a^{mq} \in gr(a^m)$, et $H = gr(a^m)$. ⊠

Classes suivant un sous-groupe, et indice d'un sous-groupe

Si H est un sous-groupe d'un groupe G, on définit, pour $g \in G$, l'ensemble $gH = \{gh \,|\, h \in H\}$, et on l'appelle *classe à gauche de g modulo H* (on dit aussi *suivant H*). On peut de même définir la classe à droite de g suivant H, notée Hg. H étant un sous-groupe, on a une correspondance bijective entre gH et Hg. Le nombre de classes à gauche ou à droite modulo H est donc le même : on appelle ce nombre *indice* de G par rapport à H, et on le note $|G : H|$.

Associons au sous-groupe H de G la relation d'équivalence suivante sur $G : \forall\, a, b \in G$,

$$\begin{aligned} a \sim b &\Leftrightarrow aH = bH \\ &\Leftrightarrow a^{-1}b \in H. \end{aligned}$$

Celle-ci permet de donner une nouvelle définition des classes à gauche modulo H comme les éléments de la partition de G que définit la relation $\sim$. Les classes à droite modulo H peuvent également être définies par une relation similaire : $a \sim b \Leftrightarrow ab^{-1} \in H$.

Lagrange a démontré le résultat suivant :

Théorème 1.1.2 (Lagrange)
Si H est un sous-groupe d'un groupe fini G, on a $|G| = |H| \cdot |G : H|$.

Ce théorème se généralise de la façon suivante :

Théorème 1.1.3
Soient A et B deux sous-groupes de G, tels que l'on ait $A \leqslant B \leqslant G$. Alors $|G : B|$ et $|B : A|$ sont finis si, et seulement si $|G : A|$ est fini.
Si $|G : A|$ est fini, on a de plus :

$$|G : A| = |G : B| \cdot |B : A|.$$

Démonstration — On travaille dans cette démonstration avec des classes à gauche, même si cela n'est pas systématiquement précisé. La démonstration est similaire avec les classes à droite.
Montrons pour commencer que $|G : B|$ et $|B : A|$ sont finis si $|G : A|$ est fini. Comme on a $A \leqslant B$, toute classe de G modulo A est contenue dans une classe de G modulo B. Il y a donc plus de classes modulo A que modulo B : $|G : B| \leqslant |G : A|$, donc le premier indice est fini lorsque le deuxième l'est. Pour montrer que $|B : A| \leqslant |G : A|$, on utilise le lemme suivant :

Lemme 1.1.4
Deux sous-groupes H_1 et H_2 d'un groupe G vérifient :

$$|H_1 : H_1 \cap H_2| \leqslant |G : H_2|.$$

Démonstration du lemme — Définissons les deux relations d'équivalence suivantes, associées respectivement aux classes à gauche de G modulo H_2 et à celles de H_1 modulo $H_1 \cap H_2$:

$$\begin{aligned} a \underset{1}{\sim} b &\Leftrightarrow a^{-1}b \in H_2 \quad \text{pour } a \text{ et } b \text{ dans } G \\ a \underset{2}{\sim} b &\Leftrightarrow a^{-1}b \in H_2 \cap H_1 \quad \text{pour } a \text{ et } b \text{ dans } H_1. \end{aligned}$$

On constate que $\underset{2}{\sim}$ est simplement la restriction de $\underset{1}{\sim}$ à H_1, ce qui nous donne $|H_1 : H_1 \cap H_2| \leqslant |G : H_2|$. □

Dans notre cas particulier, on a donc $|B : A| \leqslant |G : A|$.

Supposons maintenant $|B : A|$ et $|G : B|$ finis : notons $m = |G : B|$ et $n = |B : A|$. Soient $(\alpha_i A)_{i=1\ldots n}$ les classes à gauche de B modulo A, toutes distinctes, et $(\beta_j B)_{j=1\ldots m}$ les classes à gauche de G modulo B, elles aussi distinctes les unes des autres.
Montrons qu'alors $\beta_j \alpha_i A$ définit une classe à gauche de G modulo A, différente de toutes les autres $\beta_l \alpha_k A$, et qu'il n'y a pas d'autres classes que celles qui sont définies de la sorte.

- Si $l \neq j$, alors $\beta_j \alpha_i A \neq \beta_l \alpha_k A$; en effet, $\beta_j \alpha_i A \subset \beta_j B$ et $\beta_l \alpha_k A \subset \beta_l B$, où $\beta_j B$ et $\beta_l B$ sont disjointes.
- Si $\beta_j \alpha_i A = \beta_j \alpha_k A$, alors on a $(\beta_j \alpha_i)^{-1} \beta_j \alpha_k \in A$, c'est-à-dire $\alpha_i^{-1} \alpha_k \in A$, et $i = k$, par définition des α_i.
- Soit $g \in G$. Alors il existe j tel que $g \in \beta_j B$. g s'écrit alors $\beta_j b$, où $b \in B$. Comme les classes à gauche de B modulo A forment une partition de B, il existe i tel que $b \in \alpha_i A$, autrement dit, b s'écrit $\alpha_i a$, avec $a \in A$. On a donc écrit g sous la forme $g = \beta_j \alpha_i a$. Donc tout élément de G

appartient à l'une des classes décrites ci-dessus. Cela montre qu'il n'y en a pas d'autre ; G compte donc $m \cdot n$ classes à gauche modulo A.

Ainsi l'on a prouvé que, si $|B : A|$ et $|G : B|$ sont finis, alors

$$|G : A| = |G : B| \cdot |B : A| \ ;$$

on en déduit également qu'alors $|G : A|$ est lui-même fini. ⊠

1.1.2 Conjugaison et normalité

Définition 1.1.5
Un sous-groupe H est dit normal *ou* distingué *dans G si ses classes à gauche et à droite se confondent.*

Cela s'exprime de la manière suivante : $\forall x \in G,\ xH = Hx$, ce qui équivaut à $x^{-1}Hx = H$.

Définition 1.1.6
Pour a, b et x, éléments d'un groupe G, on dit que b est le conjugué *de a par x si $b = x^{-1}ax$. On note également : $b = a^x$.*

On a alors immédiatement :

Propriétés 1.1.7
Des éléments a, b, x et y de G vérifient

$$(ab)^x = a^x b^x \qquad \text{et} \qquad (a^x)^y = a^{xy}.$$

Plus généralement, on définit

$$\begin{aligned} A^x &:= \{a^x \mid a \in A\}, \\ \text{et } A^B &:= \{a^b \mid a \in A,\ b \in B\}. \end{aligned}$$

On obtient ainsi une définition équivalente à la définition **1.1.5** :

Définition 1.1.8
Un sous-groupe H d'un groupe G est normal *dans celui-ci si $H^G \subseteq H$. On note alors $H \trianglelefteq G$, et plus particulièrement $H \triangleleft G$ si $H \neq G$.*

1.1.3 Homomorphismes de groupes

J'utiliserai également dans ce mémoire la notion d'*homomorphisme de groupe*, difficilement dissociable de celle de *groupe*. Rappelons donc que :

Définition 1.1.9
Un homomorphisme ϕ *du groupe* $(A, \clubsuit)$ *vers le groupe* $(B, \diamondsuit)$ *est une application de* A *dans* B*, conservant la composition interne des éléments :*

$$\phi(a_1 \clubsuit a_2) = \phi(a_1) \diamondsuit \phi(a_2), \quad \text{pour } a_1, a_2 \in A.$$

Parmi ces homomorphismes, certains sont plus utilisés que d'autres. On leur a donc octroyé des noms particuliers :

Définition 1.1.10
Un endomorphisme *est un homomorphisme d'un groupe* A *dans lui-même.*
Un plongement *d'un groupe dans un autre est un homomorphisme de groupes injectif.*
Un isomorphisme *est un homomorphisme de groupes bijectif. Si* A *et* B *sont deux groupes, et s'il existe un isomorphisme entre* A *et* B*, on dit que* A *et* B *sont* isomorphes*, et on note* $A \simeq B$*.*
Un automorphisme *est à la fois un endomorphisme et un isomorphisme, c'est-à-dire qu'il envoie un groupe sur lui-même bijectivement.*

Étant donné un homomorphisme ϕ de G dans G', on note :

$$\mathrm{Ker}\,\phi := \{x \in G \,:\, \phi(x) = e_{G'}\} \text{ le } \textit{noyau} \text{ de } \phi,$$

$$\text{et } \mathrm{Im}\,\phi := \{y \in G' \,:\, \exists x \in G, \text{ tel que } y = \phi(x)\} \text{ son } \textit{image} \text{ dans } G'.$$

Il est évident alors que le noyau d'un homomorphisme de groupes est toujours un sous-groupe normal. Nous utiliserons aussi régulièrement le fait que le noyau d'un homomorphisme est trivial si et seulement si cet homomorphisme est injectif.

1.1.4 Groupes quotients

Je me servirai enfin de *groupes quotients* et des projections qui leur sont associées, ainsi que de quelques théorèmes sur ces groupes quotients.

Définition d'un groupe quotient

Soit G un groupe, et H un sous-groupe normal de G. On rappelle la relation d'équivalence déjà évoquée dans le cadre des classes de G suivant H, définie par

$$a \sim b \quad \Leftrightarrow \quad a^{-1}b \in H.$$

Celle-ci donne une partition de G, dont chacun des éléments est en fait une classe de G modulo H.

Définition 1.1.11
On appelle groupe quotient *de G par H, et on note G/H (ou $\frac{G}{H}$), l'ensemble des classes d'équivalence pour la relation ci-dessus.*

Il est évident que cet ensemble est un groupe.

Remarque 1.1.12 Il est inutile ici de préciser si les classes considérées le sont à gauche ou à droite, car H est normal dans G.

Remarque 1.1.13 On notera $\bar{a}$, ou tout simplement a, pour désigner la classe d'équivalence aH de a dans la relation d'équivalence ci-dessus : $\bar{a} \in G/H$, ou $a \in G/H$.

La construction de ce groupe quotient donne lieu à un homomorphisme canonique, aussi appelé *projection* π du groupe G vers le groupe G/H :

$$\begin{array}{rccc} \pi : & G & \longrightarrow & G/H \\ & a & \longmapsto & \bar{a}. \end{array}$$

Cet homomorphisme est surjectif par définition, et son noyau est le sous-groupe H. Il possède de plus une propriété utile, décrite dans le théorème qui suit. Définissons au préalable une notation qui simplifiera l'écriture de ce théorème : pour un groupe G, dont H est un sous-groupe, on désignera par $L(G, H)$ l'ensemble des sous-groupes de G dont H est lui-même un sous-groupe. Plus précisément,

$$L(G, H) := \{K \leqslant G \,:\, H \leqslant K\}\,;$$

$L(G, 1)$ désigne alors simplement l'ensemble des sous-groupes de G.

Théorème 1.1.14
Soit G un groupe, et H un sous-groupe distingué de G. Notons alors π l'homomorphisme canonique de G dans G/H. Alors l'application ψ définie de la manière suivante :

$$\begin{array}{rccc} \psi : & L(G,H) & \longrightarrow & L(G/H,1) \\ & K & \longmapsto & \pi(K) \end{array}$$

est en fait une bijection.

Démonstration — La démonstration est plus ou moins évidente. Soit

$$\begin{array}{rccc} \theta : & L(G/H,1) & \longrightarrow & L(G,H) \\ & I & \longmapsto & \pi^{-1}(I). \end{array}$$

Alors $\theta \circ \psi = Id$ et $\psi \circ \theta = Id$, d'où la bijectivité de ψ. ⊠

Théorème de factorisation

Énonçons à présent le théorème suivant, bien connu sous le nom de *théorème de factorisation des homomorphismes* :

Théorème 1.1.15 (Factorisation des homomorphismes)
Soit ϕ un homomorphisme de groupes, d'un groupe G vers un groupe G', dont le noyau est H, un sous-groupe de G. Alors on a $\phi(G) \simeq G/H$.

Plus précisément, l'homomorphisme ϕ revient à opérer d'abord l'homomorphisme canonique $\pi : G \longrightarrow G/H$, puis un isomorphisme $\tau : G/H \longrightarrow \phi(G)$. Autrement dit, on a $\phi = \tau \circ \pi$.

Démonstration du théorème — Montrons que l'homomorphisme τ introduit ci-dessus est bijectif. Rappelons qu'il est défini de la manière suivante :

$$\begin{array}{rccc} \tau : & G/H & \longrightarrow & \phi(G) \\ & \bar{x} & \longmapsto & \phi(x). \end{array}$$

Il est bien défini car H est précisément le noyau de ϕ : si $\bar{x} = \bar{y}$, alors $xy^{-1} \in H$, ce qui signifie que $\phi(xy^{-1}) = 1$ et, par propriété d'homomorphisme, $\phi(x) = \phi(y)$.
L'application τ est surjective par définition : si $y \in \phi(G)$, alors il existe $x \in G$ vérifiant $y = \phi(x)$. On a alors $y = \tau(\bar{x})$. De plus, le noyau de τ est restreint à l'élément neutre 1 :

$$\begin{array}{rcl} \tau(\bar{x}) = 1 & \Leftrightarrow & \phi(x) = 1 \\ & \Leftrightarrow & x \in H \\ & \Leftrightarrow & \bar{x} = \bar{1}. \end{array}$$

τ est donc un isomorphisme de G/H dans $\phi(G)$. ⊠

De ce théorème on peut déduire deux corollaires, dont voici le premier :

Corollaire 1.1.16
Si H et A sont deux sous-groupes distingués d'un groupe G, et si H est un sous-groupe de A, alors le quotient de G/H par A/H est isomorphe au quotient de G par A :

$$\frac{G/H}{A/H} \simeq G/A.$$

Démonstration — Considérons l'application suivante :

$$\begin{array}{rccc} \phi : & G/H & \longrightarrow & G/A \\ & xH & \longmapsto & xA. \end{array}$$

Cette application est bien définie : en effet, si $xH = yH$, on a $x^{-1}y \in H$. Comme $H \leqslant A$, $x^{-1}y \in A$ et $xA = yA$. De plus, ϕ est surjective par définition, et cette application est un homomorphisme de groupes :

$$\begin{aligned}\phi(xH \cdot yH) &= \phi((xy)H) \\ &= (xy)A \\ &= xA \cdot yA \quad \text{dans le groupe } G/A \\ &= \phi(xH)\phi(yH).\end{aligned}$$

Le noyau de cet homomorphisme de groupes est clairement A/H, qui est donc un sous-groupe normal de G/H. Le théorème de factorisation **1.1.15** donne alors l'isomorphisme voulu. ⊠

Un deuxième corollaire du théorème **1.1.15** traitant d'un quotient de produits de groupes est le suivant :

Corollaire 1.1.17
Si A est distingué dans B, un sous-groupe de G, et si H est distingué dans G, alors on a

$$\frac{BH}{AH} \simeq \frac{B}{A(B \cap H)}.$$

En particulier,

$$\frac{BH}{H} \simeq \frac{B}{B \cap H}.$$

Démonstration — Montrons pour commencer que les groupes ci-dessus ont du sens. Comme H est normal dans G, on a, pour $x \in AH$ s'écrivant $x = ah$, $a \in A$ et $h \in H$: $x = aha^{-1}a \in HA$, d'où $AH \subset HA$. On montre de même l'autre inclusion, et donc $AH = HA$ et AH est un sous-groupe de G (en utilisant ce qui a été démontré en **1.1.1** à propos des produits de groupes). Avec les mêmes arguments, on montre que BH est lui-aussi un sous-groupe de G. D'autre part, on a un lemme utile :

Lemme 1.1.18
Si $A \trianglelefteq B$ et $H \trianglelefteq G$, alors $AH \trianglelefteq BH$.

Démonstration du lemme — Avec des notations évidentes, on peut écrire :

$$(bh)^{-1}(ah')(bh) = h^{-1}b^{-1}abhh^{-1}b^{-1}h'bh.$$

Comme $A \trianglelefteq B$, on a $b^{-1}ab \in A$; en outre, $h(h^{-1}b^{-1}h'bh) \in H \trianglelefteq G$, donc $(bh)^{-1}(ah')(bh) \in HAH = AH$ car $H \subset AH$. □

On a donc $AH \trianglelefteq BH$. Par des calculs semblables, on prouve également que $A(B \cap H)$ est un sous-groupe normal de B.

Considérons l'homomorphisme canonique, noté π, de BH dans BH/AH. Son noyau est évidemment AH. La restriction à B de π, $\pi_{|B}$, a donc pour noyau le sous-groupe $B \cap AH$ de B. De plus, $\pi_{|B}$ reste surjective : en effet, tout élément de BH/AH s'écrit sous la forme $bhAH$, qui est aussi $bhHA$, ou plus simplement bHA, c'est-à-dire encore $bAH = \pi_{|B}(b)$.
Le théorème **1.1.15** donne alors :

$$\frac{BH}{AH} \simeq \frac{B}{B \cap AH},$$

et il ne reste plus qu'à prouver l'égalité $B \cap AH = A(B \cap H)$. Choisissons dans $B \cap AH$ un élément $x = ah$. Comme $x \in B$ et $a \in B$, on a également $h \in B$, d'où la première inclusion. La seconde est évidente, et on a effectivement l'égalité des deux ensembles, ainsi que le résultat annoncé par le théorème.⊠

1.2 Centre et sous-groupe dérivé

Approfondissons à présent quelques notions plus spécifiques que nous utiliserons fréquemment au cours de ce mémoire.

L'étude d'un groupe G quelconque étant moins aisée que celle d'un groupe abélien, il est intéressant d'établir entre eux une analogie permettant de préciser en quelque sorte le *degré de commutativité* de G.

1.2.1 Centre

La définition du *centre* est la suivante :

Définition 1.2.1
Soit G un groupe quelconque. On appelle centre *et on note $Z(G)$ le sous-ensemble de G formé par les éléments du groupe qui commutent avec tous les autres. Autrement dit,*

$$Z(G) := \{z \in G \,:\, \forall x \in G,\, xz = zx\}.$$

On voit immédiatement que le centre de G vérifie la propriété suivante :

Propriété 1.2.2
$Z(G)$ est un sous-groupe de G, normal dans G. Plus précisément, tout sous-groupe du centre est normal dans G.

En particulier, on observe que le centre d'un groupe abélien se confond avec le groupe lui-même, et que l'élément neutre d'un groupe est toujours contenu dans le centre du groupe.

Exemple 1.2.3 Soit K un corps commutatif. Introduisons le groupe $GL_n(K)$ des matrices carrées inversibles d'ordre n, appelé *groupe linéaire*. On peut montrer que son centre est réduit aux matrices scalaires, c'est-à-dire que

$$Z\left(GL_n(K)\right) = \{\lambda \mathrm{Id} \,|\, \lambda \in K\},$$

où Id représente l'élément neutre de $GL_n(K)$, aussi appelé *matrice identité*.

Exemple 1.2.4 Désignons par $UT_n(K)$ le sous-groupe de $GL_n(K)$ formé par les matrices triangulaires supérieures dont les éléments diagonaux valent tous 1 :

$$UT_n(K) := \begin{pmatrix} 1 & K & \cdots & K \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & K \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Précisons que toutes les matrices de ce groupe sont *unipotentes*, c'est-à-dire que 1 est leur seule valeur propre, ou de façon équivalente, que pour toute matrice $a \in UT_n(K)$ il existe un entier positif m tel que $(a - \mathrm{Id})^m = 0$.
Le sous-groupe de $UT_n(K)$ contenant les matrices unipotentes dont $(m-1)$ diagonales au-dessus de la diagonale principale sont nulles est noté $UT_n^m(K)$. Montrons que le centre de $UT_n^m(K)$ est alors formé par les matrices $(\mathrm{Id} + a) \in UT_n^m(K)$, où a est une matrice dont tous les éléments sont nuls, sauf éventuellement ceux de son bloc supérieur de droite d'ordre m. On note pour ce faire t_{ij} la matrice dite *d'opération élémentaire*, égale à la somme de la matrice identité et de la matrice e_{ij} dont tous les éléments sont nuls sauf celui de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne, qui vaut 1.

Une matrice a de $UT_n^m(K)$ appartient à son centre si et seulement si elle commute avec toutes les matrices d'opérations élémentaires contenues dans le groupe, c'est-à-dire avec toute matrice t_{ij} où $j - i \geqslant m$. Or, on a évidemment l'équivalence suivante :

$$at_{ij} = t_{ij}a \quad \Leftrightarrow \quad ae_{ij} = e_{ij}a.$$

Notons $r = ae_{ij}$ et $\rho = e_{ij}a$, ainsi que ε pour la matrice e_{ij}. Alors on a :

$$r_{kl} = \sum_{p=1}^{n} a_{kp}\varepsilon_{pl} = \begin{cases} 0 & \text{si } l \neq j \\ a_{ki} & \text{si } l = j, \end{cases}$$

et

$$\rho_{kl} = \sum_{p=1}^{n} \varepsilon_{kp} a_{pl} = \begin{cases} 0 & \text{si } k \neq i \\ a_{jl} & \text{si } k = i. \end{cases}$$

Alors l'égalité de r et ρ s'écrit élément par élément, et l'on obtient les contraintes suivantes :

$$\begin{aligned} a_{jl} &= 0 \quad \text{si } l \neq j \\ a_{ki} &= 0 \quad \text{si } k \neq i, \end{aligned}$$

et ce pour tous i et j vérifiant $j - i \geqslant m$, c'est-à-dire en fait pour tout $j \geqslant m+1$ et pour tout $i \leqslant n-m$. D'où le résultat : seul le bloc supérieur de droite d'ordre m d'une matrice du centre de $UT_n^m(K)$ peut différer de zéro, excepté sa diagonale évidemment.

En particulier :

$$Z\left(UT_n(K)\right) = UT_n^{n-1}(K).$$

1.2.2 Commutateurs et sous-groupe dérivé

Définitions du commutateur et du sous-groupe dérivé

Si, dans un groupe G, deux éléments a et b commutent, on a $ab = ba$. Cela équivaut à dire que $a^{-1}b^{-1}ab = 1$. Ceci nous amène à introduire les notions suivantes :

Définition 1.2.5
Le commutateur *de a et b, noté $[a, b]$, est défini par*

$$[a, b] := a^{-1}b^{-1}ab.$$

On définit également également par récurrence le commutateur $[a_1, a_2, ..., a_n] := [[a_1, a_2, ..., a_{n-1}], a_n]$. On dira d'un tel commutateur qu'il est de poids n.

Définition 1.2.6
On appelle sous-groupe dérivé *de G le sous-groupe engendré par les commutateurs de tous les éléments de G. Il est noté $[G, G]$. Pour deux sous-ensembles L et M de G, on note aussi*

$$[L, M] := gr([a, b] \,|\, a \in L, b \in M).$$

$[L, M]$ est un sous-groupe de G par définition, ce qui implique en particulier que $[L, M] = [M, L]$.

Propriétés du commutateur et du sous-groupe dérivé

Le commutateur que nous venons de définir est compatible avec la conjugaison ; en effet, la propriété suivante est immédiate :

Propriété 1.2.7
Pour a, b et x des éléments d'un groupe G, on a $[a,b]^x = [a^x, b^x]$.

De cette propriété l'on déduit immédiatement que, si L et M sont deux sous-groupes normaux dans un groupe G, alors $[L,M]$ est lui-même un sous-groupe normal dans G.
Les propriétés qui suivent sont certes plus subtiles que la précédente, mais elles sont toutefois très utiles :

Propriétés 1.2.8
Pour des éléments a, b et c d'un groupe G, on a :

$$\begin{aligned} [a,b]^{-1} &= [b,a] \ ; \\ [ab,c] &= [a,c]^b[b,c] \ ; \\ [a^{-1},b] &= [b,a]^{a^{-1}}. \end{aligned}$$

Démonstration —

$$[a,b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b,a].$$
$$[ab,c] = b^{-1}a^{-1}c^{-1}abc = b^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = [a,c]^b[b,c].$$
$$[a^{-1},b] = ab^{-1}a^{-1}b = a(b^{-1}a^{-1}ba)a^{-1} = [b,a]^{a^{-1}}.$$

⊠

En relation avec les quotients de groupes, le sous-groupe dérivé d'un groupe G quelconque a une propriété immédiate qu'il est toutefois utile de relever :

Propriété 1.2.9
Soit G un groupe quelconque, et H un sous-groupe de G contenant le commutant $[G,G]$ de G. Alors le groupe quotient G/H est abélien.

Démonstration — Montrons d'abord que G/H est effectivement un groupe, c'est-à-dire que H est normal dans G. Soient $x \in H$ et $y \in G$. Alors $x^y = x[x,y] \in H[G,G] = H$ par hypothèse.
Soient alors $\bar{x}$ et $\bar{y}$, éléments de G/H, classes respectives de x et de y dans le quotient de G par H. L'égalité évidente $xy = yx[x,y]$ donne, par passage au quotient : $\bar{x}\bar{y} = \bar{y}\bar{x}$. Le groupe quotient est donc commutatif. ⊠

1.3 Séries centrales

Une notion qui nous servira très souvent dans ce mémoire est celle de *série*. Cette partie a pour but de définir non seulement une *série* à proprement parler, mais également quelques types particuliers de séries qui nous seront utiles.

1.3.1 Séries normales

Définissons dans un premier temps ce qu'est une *série* :

Définition 1.3.1
Une série *est une suite, finie ou infinie, de sous-groupes emboîtés d'un groupe G, contenant les sous-groupes $\{1\}$ et/ou G.*
On écrit une série croissante *d'un groupe G de la manière suivante :*

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n \leqslant \cdots . \tag{1.1}$$

Une série décroissante *est de la forme suivante :*

$$G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n \geqslant \cdots . \tag{1.2}$$

Nous nous intéresserons le plus souvent, dans ce mémoire, à des séries finies : une série croissante est dite *finie* si, pour n assez grand, $G_n = G$, tandis qu'une série décroissante est *finie* si $G_{n+1} = \{1\}$ lorsque n est grand. De telles séries s'écrivent donc respectivement

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_{n-1} \leqslant G_n = G \tag{1.3}$$

$$\text{et} \quad G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n \geqslant G_{n+1} = 1, \tag{1.4}$$

et contiennent à la fois le sous-groupe trivial $\{1\}$ et le groupe G lui-même.

Définition 1.3.2
Dans les séries finies ci-dessus, l'entier n est appelé la longueur *de la série.*

Définition 1.3.3
Une série normale *est une série de la forme de (1.1) ou de (1.2), dans laquelle on demande que, pour tout i, G_i soit normal dans G.*
La série croissante (1.1) est dite sous-normale *si la condition suivante, moins forte que la normalité, est vérifiée : pour tout $i \geqslant 0$, G_i est normal dans G_{i+1}. Le même adjectif* sous-normal *est appliqué à une série décroissante de la forme de (1.2) si pour tout $i \geqslant 2$, G_i est normal dans G_{i-1}.*

Une série normale est donc toujours sous-normale, et toute série d'un groupe abélien est normale.

Donnons des noms aux éléments de telles séries, afin de pouvoir les manipuler plus facilement :

Définition 1.3.4
On appelle termes *des séries (1.1) et (1.2) les sous-groupes G_i. Un* facteur *de la première série est un quotient de la forme G_{i+1}/G_i, $i \in \{0, \ldots, n-1\}$, et un* facteur *de la deuxième série est un quotient du type G_i/G_{i+1}, $i \in \{1, \ldots, n\}$.*

Ceci nous permet de préciser le vocabulaire :

Définition 1.3.5
Les termes d'une série sous-normale d'un groupe G, qui ne sont pas nécessairement normaux dans G, sont dits sous-normaux *dans G. Autrement dit, un groupe H est dit* sous-normal *dans G s'il existe une série sous-normale de G dont H soit un terme.*

Citons à présent trois exemples de séries.

Exemple 1.3.6 La série qui suit est une série croissante, finie et normale du fait de la commutativité du groupe $\mathbb{Z}$:

$$1 \leqslant 4\mathbb{Z} \leqslant 2\mathbb{Z} \leqslant \mathbb{Z}.$$

Ses termes sont les groupes $\{1\}$, $4\mathbb{Z}$, $2\mathbb{Z}$ et $\mathbb{Z}$; son premier facteur, $4\mathbb{Z}$, est isomorphe à $\mathbb{Z}$, tandis que le deuxième est isomorphe au dernier : $\mathbb{Z}/2\mathbb{Z}$.

Exemple 1.3.7 La série suivante, semblable à celle qui précède, est quant à elle infinie et décroissante :

$$\mathbb{Z} \geqslant 2\mathbb{Z} \geqslant 4\mathbb{Z} \geqslant \cdots \geqslant 2^n\mathbb{Z} \geqslant \cdots .$$

Exemple 1.3.8 Le groupe $T_n(K)$ des matrices triangulaires supérieures à coefficients dans un corps K possède une série normale finie :

$$T_n(K) \geqslant UT_n^1(K) \geqslant UT_n^2(K) \geqslant \cdots \geqslant UT_n^{n-1}(K) \geqslant 1.$$

Induction de séries normales

Il est temps maintenant de donner les deux théorèmes suivants qui donnent une série normale (resp. sous-normale) du sous-groupe ou du groupe quotient d'un groupe dont on connaît une série normale (resp. sous-normale).

Théorème 1.3.9
Soit G un groupe possédant une série normale (resp. sous-normale) croissante

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n \leqslant \cdots . \tag{1.5}$$

Alors, si H est un sous-groupe de G, l'intersection de cette série avec H donne une série normale (resp. sous-normale) croissante de H :

$$1 = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_n \leqslant \cdots , \text{ où } H_i = G_i \cap H. \tag{1.6}$$

Dans cette série, le facteur H_{i+1}/H_i est de plus isomorphe à un sous-groupe du groupe quotient G_{i+1}/G_i.
Le résultat est analogue pour une série normale (resp. sous-normale) décroissante du type

$$G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n \geqslant \cdots . \tag{1.7}$$

Démonstration — Si la série (1.5) de G est normale, on a, pour tout x dans H : $H_i^x \leqslant G_i$, par normalité de G_i dans G, et $H_i^x \leqslant H$, donc H_i est normal dans H.
Si la série (1.5) de G est sous-normale, on a, pour tout élément x de H_{i+1} : $H_i^x \leqslant G_i$ comme précédemment, et $H_i^x \leqslant H$ puisque $H_{i+1} \leqslant H$; donc H_i est normal dans H_{i+1}, et la série (1.6) est sous-normale.
De plus, d'après le deuxième corollaire du théorème de factorisation **1.1.15**, on a

$$H_{i+1}/H_i = \frac{H_{i+1}}{H_{i+1} \cap G_i} \simeq \frac{G_i H_{i+1}}{G_i} \leqslant G_{i+1}/G_i.$$

D'où le résultat attendu pour une série croissante. Un raisonnement similaire prouve le résultat concernant les séries décroissantes. ⊠

Le deuxième théorème annoncé traite du cas d'un groupe quotient :

Théorème 1.3.10
Soit G un groupe possédant une série normale (resp. sous-normale) croissante

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n \leqslant \cdots . \tag{1.8}$$

Alors, si H est un sous-groupe normal de G, la projection $G \longrightarrow G/H$ de la série ci-dessus donne une série normale (resp. sous-normale) croissante du groupe quotient G/H :

$$1 = \bar{G}_0 \leqslant \bar{G}_1 \leqslant \cdots \leqslant \bar{G}_n \leqslant \cdots , \text{ où } \bar{G}_i = G_i/(G_i \cap H). \tag{1.9}$$

Dans cette série, le facteur $\bar{G}_{i+1}/\bar{G}_i$ est en outre une image homomorphe de G_{i+1}/G_i.
Le résultat est analogue pour une série normale (resp. sous-normale) décroissante.

Démonstration — Nous montrerons uniquement le résultat pour les séries croissantes, puisque le raisonnement sur les séries décroissantes est similaire. Rappelons tout d'abord que, d'après le corollaire **1.1.17** du théorème de factorisation **1.1.15**, $\bar{G}_i = G_i/(G_i \cap H) \simeq G_iH/H$. Supposons la série (1.8) de G normale. Alors le lemme **1.1.18** donne, puisque $G_i \trianglelefteq G$ et $H \trianglelefteq G$, la normalité de G_iH dans G. Le quotient G_iH/H est alors normal dans G/H, ce qui donne la normalité de la série (1.9) des $\bar{G}_i$.
Dans le cas où la série (1.8) de G est sous-normale, le même lemme **1.1.18** donne, puisque $G_i \trianglelefteq G_{i+1}$ et $H \trianglelefteq G$, la normalité de G_iH dans $G_{i+1}H$. Cela implique la normalité de $\bar{G}_i$ dans $\bar{G}_{i+1}$, et donc la sous-normalité de la série (1.9).
En outre, en utilisant cette fois-ci le corollaire **1.1.16**, on obtient :

$$\bar{G}_{i+1}/\bar{G}_i = \frac{G_{i+1}H/H}{G_iH/H} \simeq \frac{G_{i+1}H}{G_iH} \simeq \frac{G_{i+1}}{G_i(G_{i+1} \cap H)}.$$

Définissons alors l'homomorphisme suivant :

$$\begin{array}{rccc} \phi: & G_{i+1}/G_i & \longrightarrow & \dfrac{G_{i+1}}{G_i(G_{i+1} \cap H)} \\ & aG_i & \longmapsto & aG_i(G_{i+1} \cap H). \end{array}$$

Cet homomorphisme est bien défini, surjectif par définition. Notons K son noyau. Alors le théorème de factorisation **1.1.15** donne l'isomorphisme suivant :

$$\frac{G_{i+1}}{G_i(G_{i+1} \cap H)} \simeq \frac{G_{i+1}/G_i}{K},$$

et le théorème est démontré. ⊠

1.3.2 Séries centrales

Introduisons à présent le concept de série *centrale* :

Définition 1.3.11
Soit G un groupe. Une série normale

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n \leqslant \cdots \tag{1.10}$$

est dite centrale *si l'une des deux conditions équivalentes suivantes est satisfaite :*

1. $G_{i+1}/G_i \leqslant Z(G/G_i)$ *pour tout* $i \geqslant 0$;
2. $[G_{i+1}, G] \leqslant G_i$ *pour tout* $i \geqslant 0$.

Pour une série décroissante

$$G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n \geqslant \cdots , \tag{1.11}$$

ces deux conditions s'écrivent de la manière suivante :

$$\begin{array}{lrcll} 1. & G_i/G_{i+1} & \leqslant & Z(G/G_{i+1}) & \textit{pour tout } i \geqslant 1\,; \\ 2. & [G_i, G] & \leqslant & G_{i+1} & \textit{pour tout } i \geqslant 1. \end{array}$$

Remarque 1.3.12 En fait, la deuxième condition ci-dessus implique en soi la normalité de la série : prenons le cas d'une série croissante. Si $x \in G$ et $g \in G_i$, pour $i \geqslant 1$, alors on a $x^{-1}gx = gg^{-1}x^{-1}gx = g[g, x]$ où, par hypothèse, $[g, x]$ appartient à $G_{i-1} \leqslant G_i$. D'où la normalité de G_i dans G.

Avant de nous intéresser à deux types de séries centrales particulières, donnons encore le théorème suivant, valable pour toute série centrale, et dont la démonstration est évidente :

Théorème 1.3.13
Toute subdivision d'une série centrale est encore une série centrale.

Définissons, comme préalable à la démonstration, ce qu'est une *subdivision* d'une série.

Définition 1.3.14
Soit, dans un groupe G quelconque, la série suivante :

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n \leqslant \cdots . \tag{1.12}$$

Une subdivision *de cette série est elle-même une série de la forme*

$$1 = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_m \leqslant \cdots , \tag{1.13}$$

telle que pour tout entier i positif, il existe j dans $\mathbb{N}$, tel que $G_i = H_j$.
En d'autres termes, la subdivision *comprend les mêmes termes que la série d'origine, auxquels on a éventuellement ajouté des intermédiaires.*
On définit de la même manière ce qu'est une subdivision *pour une série décroissante.*

Voici à présent la preuve du théorème ci-dessus :

Démonstration du théorème **1.3.13** — Considérons le cas d'une série croissante. Soit G un groupe quelconque dont une série centrale croissante est de la forme de (1.12). Cette série vérifie, par définition :

$$\forall\, i \geqslant 0, \quad [G_{i+1}, G] \leqslant G_i.$$

Montrons que l'ajout d'un terme intermédiaire à cette série n'influe pas sur sa centralité. Supposons que l'on ait ajouté à (1.12) le terme H, tel que $G_i \leqslant H \leqslant G_{i+1}$, pour un certain i. Alors on a $[H, G] \leqslant [G_{i+1}, G] \leqslant G_i$, et $[G_{i+1}, G] \leqslant G_i \leqslant H$. La subdivision obtenue reste donc centrale. Ainsi, en procédant par récurrence sur le nombre de termes ajoutés à la série d'origine, on montre le théorème. ⊠

Séries centrales particulières

Des deux conditions équivalentes citées dans la définition **1.3.11** ci-dessus, on tire deux méthodes de construction de séries centrales. Définissons en effet une série croissante par :

$$\zeta_0 G = 1, \quad \zeta_{i+1} G / \zeta_i G = Z(G/\zeta_i G), \quad i = 0, 1, 2, ... \tag{1.14}$$

et une série décroissante par

$$\gamma_1 G = G, \quad \gamma_{j+1} G = [\gamma_j G, G], \quad j = 1, 2, ... \,. \tag{1.15}$$

Définition 1.3.15
On appelle les groupes $\zeta_i G$ hypercentres *de* G. *La série qu'ils forment est la* série centrale supérieure *de* G, *que l'on abrégera* SCS. *Ils sont notés* Z_i *lorsque le contexte ne présente pas d'ambiguïté.*
Les groupes $\gamma_i G$ *définissent quant à eux la* série centrale inférieure *de* G, *pour laquelle on utilisera l'abbréviation* SCI, *et sont notés* Γ_i *lorsque cela est possible.*

Remarquons que la définition de la série centrale supérieure revient à affirmer ce qui suit :

Remarque 1.3.16 Soit i un entier naturel. Alors un élément a de $\mathcal{G}$ commute avec tous les éléments de $\mathcal{G}$ modulo $\mathcal{G}_i$ si et seulement si a est un élément de $\mathcal{G}_{i+1}$. Autrement dit,

$$[a, \mathcal{G}] \leqslant \mathcal{G}_i \quad \Leftrightarrow \quad a \in \mathcal{G}_{i+1}.$$

Donnons à présent un exemple de telles séries :

Exemple 1.3.17 La série

$$UT_n(\mathbb{Z}) = UT_n^1(\mathbb{Z}) \geqslant UT_n^2(\mathbb{Z}) \geqslant \cdots \geqslant UT_n^n(\mathbb{Z}) = 1$$

vérifie

$$\begin{aligned} [UT_n^i(\mathbb{Z}), UT_n(\mathbb{Z})] &= UT_n^{i+1}(\mathbb{Z}) \\ \text{et} \quad UT_n^i(\mathbb{Z})/UT_n^{i+1}(\mathbb{Z}) &= Z\big(UT_n(\mathbb{Z})/UT_n^{i+1}(\mathbb{Z})\big). \end{aligned}$$

Ces relations peuvent être démontrées sur les matrices d'opérations élémentaires $t_{ij}(1)$ et $t_{ij}(-1)$, génératrices du groupe $UT_n^i(\mathbb{Z})$ lorsque $j - i \geqslant m$. La preuve de la deuxième relation s'appuie entre autres sur l'exemple **1.2.4**. Cette série est donc à la fois la série centrale inférieure et la série centrale supérieure du groupe $UT_n(\mathbb{Z})$.

Cet exemple n'exprime toutefois pas une généralité : les séries centrales inférieure et supérieure ne sont en général pas confondues, comme le prouve l'exemple **2.2.6**.

Remarque 1.3.18 Ces séries particulières vérifient entre autres les propriétés suivantes :
- s'il existe i tel que $\Gamma_i = \Gamma_{i+1}$, alors $\Gamma_k = \Gamma_i$ pour tout $k \geqslant i$;
- s'il existe i tel que $Z_i = Z_{i+1}$, alors $Z_k = Z_i$ pour tout $k \geqslant i$.

Relation entre les séries centrales d'un groupe G

Soit dans un groupe G une série centrale croissante, écrite comme suit :

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n \leqslant \cdots . \tag{1.16}$$

On peut alors établir une relation entre cette série centrale et la série centrale supérieure de G. Celle-ci est décrite dans le théorème qui suit.

Théorème 1.3.19
La série centrale supérieure de G étant notée

$$1 = Z_0 \leqslant Z_1 \leqslant \cdots \leqslant Z_n \leqslant \cdots , \tag{1.17}$$

on a, pour tout i de 0 à n, $G_i \leqslant Z_i$.

Démonstration — Montrons le théorème par récurrence sur i. On a évidemment $Z_0 = G_0$, et, par définition d'une série centrale supérieure, $G_1 = G_1/1 \leqslant Z(G/1) = Z(G) = Z_1$. Le théorème est donc montré pour $i = 0, 1$. Supposons maintenant que $G_i \leqslant Z_i$, pour $i \in \{0, 1, ..., n, ...\}$, et montrons que cette propriété est aussi vraie au rang $i + 1$.
Soit $p_i : G \longrightarrow G/G_i$ et $\pi_i : G \longrightarrow G/Z_i$ les projections canoniques. Par définition d'une série centrale,

$$G_{i+1} \leqslant p_i^{-1}(Z(G/G_i)),$$

et par définition de la série centrale supérieure :

$$Z_{i+1} = \pi_i^{-1}(Z(G/Z_i)).$$

Or, puisque $G_i \leqslant Z_i$ par hypothèse de récurrence, on a

$$p_i^{-1}(Z(G/G_i)) \leqslant \pi_i^{-1}(Z(G/Z_i)),$$

d'où $G_{i+1} \leqslant Z_{i+1}$. ⊠

Notons à présent

$$\mathcal{G} = \mathcal{G}_1 \geqslant \mathcal{G}_1 \geqslant \cdots \geqslant \mathcal{G}_n \geqslant \cdots \tag{1.18}$$

une série centrale décroissante quelconque du groupe G. On peut établir entre cette série et la SCI de G une relation similaire à celle qui est décrite dans le théorème précédent :

Théorème 1.3.20
La série centrale inférieure de G étant notée

$$G = \Gamma_1 \geqslant \Gamma_2 \geqslant \cdots \geqslant \Gamma_n \geqslant \cdots, \tag{1.19}$$

on a, pour tout j supérieur à 1 : $\Gamma_j \leqslant \mathcal{G}_j$.

Démonstration — Ce théorème est, à l'instar du précédent, démontré par récurrence. On a, pour commencer, $\Gamma_1 = G = \mathcal{G}_1$. Si l'on suppose maintenant que, pour $j \in \{1, 2, ..\}$, l'on ait $\Gamma_j \leqslant \mathcal{G}_j$. Alors on écrit $\Gamma_{j+1} = [\Gamma_j, G] \leqslant [\mathcal{G}_j, G] \leqslant \mathcal{G}_{j+1}$, car il est évident que $[A, C] \leqslant [B, C]$ si $A \leqslant B$, et le résultat est démontré. ⊠

Ces résultats seront réutilisés dans le paragraphe **2.2.2**, où il sera question plus particulièrement de séries centrales dans un groupe nilpotent.

Chapitre 2

Quelques classes importantes de groupes

Après ces généralités sur les groupes, intéressons-nous à quelques classes particulières de groupes. Une *classe* de groupes rassemble tous les groupes vérifiant une propriété $\mathcal{P}$ donnée. Par exemple, notons $\mathcal{P}$ la propriété *être abélien*. Celle-ci définit la classe des groupes abéliens.

Nous nous intéresserons dans ce chapitre aux classes de groupes nilpotents, de type fini, divisibles et polycycliques, sans oublier la classe déjà évoquée des groupes abéliens.

2.1 Groupes abéliens

Les groupes abéliens sont les groupes les plus faciles à étudier. Ils possèdent également nombre de propriétés remarquables, dont nous n'évoquerons ici que celles qui nous seront utiles.

2.1.1 Définition et notation

Rappelons pour débuter ce qui caractérise un groupe abélien.

Définition 2.1.1
Un groupe G est dit abélien, *ou* commutatif, *si ses éléments commutent deux à deux, c'est-à-dire si, pour tous éléments x et y de G, on a $xy = yx$.*

Des exemples de tels groupes sont évidents : il s'agit des groupes usuels $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ ou encore $(\mathbb{R}, +)$. Les groupes $(\mathbb{Q}^*, \cdot)$ et $(\mathbb{R}^*, \cdot)$ en sont deux exemples multiplicatifs.

En général, pour distinguer un groupe abélien d'un groupe quelconque, on lui associe une notation additive, à l'image de celle de $\mathbb{Z}$: on écrira $x + y$ de préférence à xy, et nx plutôt que x^n, ou n est un entier relatif.

2.1.2 Théorème de décomposition des groupes abéliens de type fini

L'étude des groupes abéliens est grandement facilitée par ce théorème de décomposition. Il permet en fait de classifier tous les groupes commutatifs de type fini, c'est-à-dire engendrés par un nombre fini d'éléments. Ce théorème nécessite quelques éclaircissements :

Définition 2.1.2
On dit qu'un groupe abélien G est libre *s'il existe un entier naturel non nul r, et un isomorphisme de groupes*

$$\varphi : \mathbb{Z}^r \longrightarrow G.$$

L'entier r est uniquement défini et appelé rang *de G, mais nous ne chercherons pas ici à en donner la preuve.*

Les démonstrations des lemmes qui suivent nécessiteraient l'introduction de notions supplémentaires, et ne constituent pas l'objet de ce mémoire. C'est pourquoi j'ai choisi de les énoncer sans toutefois donner leurs démonstrations. On pourra se référer pour plus de détails au cours d'algèbre commutative de licence : les résultats qui suivent y sont énoncés pour des modules sur un anneau principal. Or $\mathbb{Z}$ est un anneau principal, et la correspondance est biunivoque entre les $\mathbb{Z}$-modules et les groupes abéliens. Nous nous intéressons donc ici en particulier aux résultats concernant les groupes abéliens.

Lemme 2.1.3
Tout groupe abélien de type fini est isomorphe au produit d'un groupe abélien libre de rang fini par un groupe abélien fini. De plus, dans cette décomposition, le rang de la partie libre est uniquement déterminé, ainsi que la classe d'isomorphisme de la partie finie.

Lemme 2.1.4
Tout groupe abélien fini G est isomorphe à un produit de groupes cycliques. De plus, il existe un unique entier s, et des entiers $d_1, \ldots, d_s$ choisis de sorte que d_i divise d_{i+1}, tels que

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}.$$

De ces deux lemmes nous déduisons sans peine le théorème suivant :

Théorème 2.1.5 (Décomposition des groupes abéliens de type fini) *Tout groupe abélien de type fini G est isomorphe à une décomposition de la forme suivante :*

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z},$$

où pour chaque i de 1 à s, d_i divise d_{i+1}.

Ce fait est évident pour le groupe abélien de référence $\mathbb{Z}$ que nous avons déjà évoqué plus haut. Donnons pour clore cette partie un exemple un peu moins trivial :

Exemple Soit G le groupe $\mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/150\mathbb{Z}$. En décomposant tout d'abord ce groupe à l'aide du théorème chinois, on obtient :

$$G \simeq \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

En regroupant les termes des manière réfléchie, on obtient

$$G \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/900\mathbb{Z},$$

où sans conteste 6 divise 30, qui lui-même divise 900.

2.2 Groupes nilpotents

La classe de groupes qui nous intéresse dans ce mémoire est celle des *groupes nilpotents*.

2.2.1 Définition d'un groupe nilpotent

Commençons par en donner une définition :

Définition 2.2.1
Un groupe G est dit nilpotent *s'il admet une série centrale finie. Le nombre minimal de facteurs d'une telle série est appelé la* classe de nilpotence *de G.*

Donnons immédiatement un exemple simple :

Exemple 2.2.2 Tout groupe abélien G non trivial est nilpotent de classe 1, puisque $[G, G] = 1$.

Un autre exemple de groupe nilpotent, moins immédiat, a déjà été évoqué dans nos exemples précédents :

Exemple 2.2.3 Le groupe $UT_n(K)$ des matrices triangulaires supérieures à coefficients dans un corps K, dont les éléments de la diagonale sont égaux à 1, est nilpotent. En effet, la série

$$UT_n(K) = UT_n^1(K) \geqslant UT_n^2(K) \geqslant \cdots \geqslant UT_n^n(K) = 1$$

est une série centrale finie, composée de $(n-1)$ facteurs. La classe de nilpotence du groupe $UT_n(K)$ est donc inférieure ou égale à $(n-1)$. Puisque cette série est en fait la série centrale inférieure du groupe $UT_n(K)$, la classe de nilpotence de ce groupe est exactement $(n-1)$.

Remarquons en outre que, si $n > 2$, ce groupe de matrices n'appartient pas à la classe des groupes abéliens décrite précédemment.

Par ailleurs, il est clair que dans un groupe G quelconque, si l'un des hypercentres se confond avec le groupe G lui-même, ou si un terme de la SCI est trivial, alors G est nilpotent.

2.2.2 Relations entre les séries centrales d'un groupe nilpotent

Soit G un groupe nilpotent de classe s, et

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_{n-1} \leqslant G_n = G \tag{2.1}$$

une série centrale finie de G, avec par définition de la nilpotence : $n \geqslant s$. Les relations établies dans le paragraphe **1.3.2** entre une série centrale quelconque de G et sa SCI ou sa SCS sont schématisées, dans le cas de la série (2.1), sur le diagramme ci-dessous :

$$\begin{array}{ccccccccccccc}
1 & = & Z_0 & \leqslant & Z_1 & \leqslant & \cdots & \leqslant & Z_{n-1} & \leqslant & Z_n & \leqslant & \cdots \\
 & & \diagup\!\!\diagup & & \diagup\!\!\diagup & & & & \diagup\!\!\diagup & & \diagup\!\!\diagup & & \\
1 & = & G_0 & \leqslant & G_1 & \leqslant & \cdots & \leqslant & G_{n-1} & \leqslant & G_n & = & G \\
 & & \diagup\!\!\diagup & & \diagup\!\!\diagup & & & & \diagup\!\!\diagup & & \diagup\!\!\diagup & & \\
\cdots & \leqslant & \Gamma_{n+1} & \leqslant & \Gamma_n & \leqslant & \cdots & \leqslant & \Gamma_2 & \leqslant & \Gamma_1 & = & G.
\end{array}$$

Celui-ci explique l'origine des adjectifs *supérieur* et *inférieur* utilisés pour qualifier les séries centrales particulières que nous avons présentées. Il permet de plus de faire la remarque suivante :

Remarque 2.2.4 Des relations $Z_n \geqslant G_n = G$ et $\Gamma_{n+1} \leqslant G_0 = 1$ découle le fait que la SCI et la SCS de G sont finies et que leurs longueurs sont inférieures ou égales à n.

Cela nous amène à la propriété suivante :

Propriété 2.2.5
G est nilpotent de classe s
- *si et seulement si la longueur de sa* SCS *est s*
- *si et seulement si la longueur de sa* SCI *est s.*

Démonstration — Si G est nilpotent de classe s, il admet une série centrale de longueur s. En écrivant le schéma précédent pour cette série particulière, on en déduit que les longueurs des séries centrales inférieure et supérieure sont inférieures ou égales à s. D'autre part, l'hypothèse que G est nilpotent de classe s implique que les longueurs de ces séries en particulier sont supérieures ou égales à s. D'où la nécessité des conditions.

Leur suffisance vient du fait que, si la SCI ou la SCS est de longueur s, alors G est nilpotent de classe au plus s. En outre, cela impose, d'après la remarque précédente, que toute série centrale de G ait une longueur supérieure ou égale à s. G est donc nilpotent de classe s, et la propriété est démontrée. ⊠

Exemple 2.2.6 Le groupe $G = UT_3(\mathbb{Z}) \times \mathbb{Z}$ constitue un exemple de groupe pour lequel les séries centrales particulières que nous venons de présenter ne coïncident pas. En effet, on a clairement $\gamma_2 G = [G, G] \simeq UT_3^2(\mathbb{Z})$. Alors on a $\gamma_3 G = 1$. La série centrale inférieure comportant 3 termes, il en va de même pour la série centrale supérieure. Or, le premier hypercentre de G, $\zeta_1 G = Z(G) = UT_3^2(\mathbb{Z}) \times \mathbb{Z}$, n'est pas égal au sous-groupe dérivé de G. Les deux séries distinctes ainsi construites sont récapitulées ci-dessous :

$$\begin{array}{ccccc} 1 & \leqslant & UT_3^2(\mathbb{Z}) \times \mathbb{Z} & \leqslant & G \\ \| & & \vee\!\!/ & & \| \\ 1 & \leqslant & UT_3^2(\mathbb{Z}) & \leqslant & G. \end{array}$$

La définition même d'un groupe nilpotent suggère une méthode de démonstration naturelle pour les propriétés de tels groupes : la récurrence sur la classe de nilpotence. Nous aurons l'occasion dans ce mémoire de vérifier effectivement sa pertinence.

2.3 Groupes sans torsion

Les groupes que l'on qualifie de *sans torsion* forment une nouvelle classe de groupes à laquelle nous nous intéressons dans cette partie.

2.3.1 Définition et exemples

Commençons par préciser la signification du terme *torsion* :

Définition 2.3.1
On dit d'un groupe G qu'il est sans torsion *si aucun de ses éléments non triviaux n'est d'ordre fini, et qu'il est* de torsion *si tous ses éléments sont d'ordre fini. On dit aussi dans ce dernier cas que le groupe G est* périodique.

Un groupe est ainsi qualifié de *périodique* lorsque tous ses éléments sont d'ordres finis. On donne alors la définition complémentaire suivante :

Définition 2.3.2
*L'*exposant *d'un groupe de torsion désigne le plus petit commun multiple des ordres de ses éléments.*

Illustrons ces notions sur les quelques exemples qui suivent :

Exemple 2.3.3 Considérons, pour un entier naturel m donné, le groupe additif $\mathbb{Z}/m\mathbb{Z}$. Dire qu'un élément a est d'ordre fini revient donc à produire un entier n non nul vérifiant $na = 0$ dans le groupe $\mathbb{Z}/m\mathbb{Z}$ considéré. Or, tout élément a de ce groupe vérifie la relation $ma = 0$, et est donc d'ordre fini. $\mathbb{Z}/m\mathbb{Z}$ est donc périodique, et son exposant vaut m, qui est l'ordre de 1 dans le groupe.

Exemple 2.3.4 Un exemple de groupe sans torsion est le groupe des entiers relatifs $\mathbb{Z}$, qui est habituellement noté additivement. En effet, supposons que $na = 0$ où $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Ceci implique immédiatement que $a = 0$. $\mathbb{Z}$ est donc à la fois sans torsion et abélien.

Reprenons ensuite notre exemple favori :

Exemple 2.3.5 Le groupe $UT_n(K)$ est sans torsion pour tout corps K de caractéristique nulle. Pour le démontrer, intéressons-nous au lemme suivant :

Lemme 2.3.6
Si $a \in UT_n^m(K)$ est d'ordre fini, alors $a \in UT_n^{m+1}(K)$.

Démonstration — Soient x et y dans $UT_n(K)$, dont on note respectivement $x_1, \ldots, x_{n-m}$ et $y_1, \ldots, y_{n-m}$ les éléments de la $m^{\text{ème}}$ diagonale supérieure.

Alors on a

$$xy = \begin{pmatrix} 1 & 0 & \dots & 0 & x_1+y_1 & & \times \\ & \ddots & \ddots & & \ddots & \ddots & \\ & & \ddots & \ddots & & \ddots & x_{n-m}+y_{n-m} \\ & & & \ddots & \ddots & & 0 \\ & & 0 & & \ddots & \ddots & \vdots \\ & & & & & \ddots & 0 \\ & & & & & & 1 \end{pmatrix}.$$

Numérotons comme précédemment $a_1, \dots, a_{n-m}$ les éléments de la $m^{\text{ème}}$ diagonale supérieure de $a \in UT_n^m(K)$. Alors on a pour tout entier naturel r :

$$a^r = \begin{pmatrix} 1 & 0 & \dots & 0 & ra_1 & & \times \\ & \ddots & \ddots & & \ddots & \ddots & \\ & & \ddots & \ddots & & \ddots & ra_{n-m} \\ & & & \ddots & \ddots & & 0 \\ & & 0 & & \ddots & \ddots & \vdots \\ & & & & & \ddots & 0 \\ & & & & & & 1 \end{pmatrix}.$$

Supposons a d'ordre fini r, on a alors $a^r = \mathrm{Id}$, et en particulier $a_1 = \cdots = a_{n-m} = 0$. Donc $a \in UT_n^{m+1}(K)$. ⊠

Soit a d'ordre fini dans $UT_n(K)$. On obtient avec le lemme précédent qu'alors $a \in UT_n^n(K) = \{\mathrm{Id}\}$. D'où finalement $a = \mathrm{Id}$.

Ceci donne l'absence de torsion du groupe en question qui, d'après les résultats précédents, est également nilpotent, mais non abélien si $n > 2$.

Exemple 2.3.7 Donnons enfin un dernier exemple pour mettre en évidence le fait qu'un groupe sans torsion n'est pas nécessairement nilpotent : en effet, le groupe libre à deux générateurs x et y, noté $\mathbf{F}(x, y)$, est par définition dépourvu de toute relation entre ses générateurs. Cela implique qu'il est à la fois sans torsion et non nilpotent.

2.3.2 Sous-groupe d'un groupe sans torsion

Ce paragraphe a pour but de souligner le fait immédiat que, si un groupe G est sans torsion, alors tout sous-groupe de G est sans torsion.

Cela n'est pas nécessairement vrai pour un quotient du groupe G par un sous-groupe normal H.

Les premiers exemples du paragraphe qui précède nous fournissent une bonne illustration de cette dernière affirmation : le groupe $\mathbb{Z}$ est sans torsion, mais ses quotients de la forme $\mathbb{Z}/m\mathbb{Z}$ sont de torsion.

2.4 Groupes de type fini

Évoquons ensuite la classe des groupes dits *de type fini*.

Définition 2.4.1
On dit d'un groupe G quelconque qu'il est de type fini *s'il est engendré par un ensemble fini.*

On peut également exprimer cela à l'aide de la propriété suivante :

Propriété 2.4.2
Un groupe G est de type fini *si et seulement s'il existe un entier naturel n et un homomorphisme surjectif de groupes du groupe libre à n générateurs $\mathbf{F}(x_1, \ldots, x_n)$ sur le groupe G.*

Les éléments d'un groupe G de type fini s'expriment en fait sous forme de produits finis en les éléments générateurs de G et en leurs inverses. En particulier, un groupe fini est de type fini.

Exemple 2.4.3 Un premier exemple de groupe de type fini est celui, en notation additive, de $\mathbb{Z}$, engendré par 1. On écrit : $\mathbb{Z} = \langle 1 \rangle$.
On a également $\mathbb{Z}/n\mathbb{Z} = \langle 1 \mathrm{mod}.n \rangle$. Tout groupe monogène est en fait de type fini (engendré par un seul élément), qu'il soit ou non sans torsion.

Exemple 2.4.4 Le *groupe symétrique* $\mathfrak{S}_n$ est quant à lui engendré par ses transpositions (ij), et même par les transpositions de la forme $(1j)$, $j = 2, 3, ..., n$, puisque $(ij) = (1i)(1j)(1i)$. Les différents cycles à trois éléments de $\mathfrak{S}_n$ engendrent le *groupe alterné* $\mathfrak{A}_n$. $\mathfrak{S}_n$ et $\mathfrak{A}_n$ sont donc tous deux de type fini.

Exemple 2.4.5 Donnons enfin un exemple matriciel : soit K un corps, et $GL_n(K)$ l'ensemble des matrices carrées d'ordre n, inversibles, à coefficients dans K.
On note $t_{ij}(\alpha) = \mathrm{Id} + \alpha e_{ij}$, pour $i \neq j$ et $\alpha \in K$, et $d(\beta) = \mathrm{Id} + (\beta - 1)e_{nn}$, où $\beta \in K \backslash \{0\}$. e_{ij} représente ici la matrice dont tous les éléments sont nuls, excepté l'élément de la $i^{ème}$ ligne et $j^{ème}$ colonne, qui vaut 1, et Id

est l'élément neutre du groupe, communément appelé *matrice identité*. Les matrices t_{ij} sont des matrices d'*opérations élémentaires* : multiplier à gauche par une telle matrice revient à ajouter une ligne, multipliée par un scalaire α, à une autre ligne. Multiplier à droite par une matrice d'opération élémentaire revient à effectuer une transformation similaire sur les colonnes.
Soit a une matrice de $GL_n(K)$. La première ligne étant non nulle, on peut effectuer une opération élémentaire afin que le coefficient a_{12} soit non nul. On peut alors, en ajoutant à la première colonne la deuxième, multipliée par le scalaire $\frac{1-a_{11}}{a_{12}}$, ce qui ramène l'élément a_{11} à 1. On annule alors facilement tous les autres éléments de la première ligne, ainsi que ceux de la première colonne. On répète ce même processus sur le bloc inférieur de droite, d'ordre $n-1$, pour arriver finalement à une matrice du type $d(\beta)$. On a donc montré que

$$a = t_1 t_2 \dots t_r d(\beta) t_{r+1} \dots t_s,$$

où les t_i sont des matrices d'opérations élémentaires ; cela montre que

$$GL_n(K) = \langle t_{ij}(\alpha), d(\beta) \mid \alpha, \beta \in K, i \neq j \rangle.$$

On peut de même montrer, pour le groupe $T_n(K)$, défini en **1.3.8** à la page 23, que

$$T_n(K) = \langle t_{ij}(\alpha), \mathrm{diag}(\beta_1, \dots, \beta_n) \mid \alpha, \beta_k \in K, i < j \rangle,$$

et que

$$UT_n^m(K) = \langle t_{ij}(\alpha) \mid \alpha \in K, j - i \geqslant m \rangle.$$

Les groupes $GL_n(K)$, $T_n(K)$ et $UT_n^m(K)$ sont donc de type fini si le corps K est lui-même fini.

Précisons enfin que tout quotient d'un groupe de type fini est encore de type fini : en effet, le quotient est engendré par les classes des éléments générateurs du groupe de départ.

2.5 Groupes divisibles

2.5.1 Définitions

Nous aborderons dans cette seconde partie la notion de *groupe divisible*. Pour un groupe abélien, noté de façon additive, dire qu'il est *divisible* revient à dire que, pour tout élément g du groupe, et pour tout entier naturel n, il existe, dans le groupe, au moins une solution x de l'équation $nx = g$.

Dans un groupe G quelconque, en notation multiplicative, la définition est la suivante :

Définition 2.5.1
Le groupe G est divisible *si, pour tout élément g de G, et pour tout entier naturel n non nul, il existe une solution $x \in G$ de l'équation*

$$x^n = g.$$

Définition 2.5.2
La solution x de l'équation ci-dessus est appelée une racine *de g. On précise parfois que x est une* racine $n^{\text{ième}}$ *de g.*

Donnons quelques exemples de tels groupes.

Exemple 2.5.3 Des exemples simples de groupes divisibles sont les groupes additifs $\mathbb{Q}$ et $\mathbb{R}$. Le groupe multiplicatif $(\mathbb{R}_+^*, \cdot)$ est également divisible.

Exemple 2.5.4 Le groupe $UT_n(\mathbb{Q})$ est divisible. On définit, pour tout $a \in UT_n(\mathbb{Q})$ et pour tout $\mu \in \mathbb{Q}$:

$$p(a,\mu) = \sum_{i=0}^{n-1} \binom{\mu}{i} (a - \mathrm{Id})^i \quad \in UT_n(\mathbb{Q}), \tag{2.2}$$

où

$$\binom{\mu}{i} = \frac{\mu(\mu-1)...(\mu-i+1)}{i!} \quad \text{pour } i \text{ non nul, et} \quad \binom{\mu}{0} = 1.$$

Si $\mu \in \mathbb{N}$, on a $p(a,\mu) = a^\mu$ car la formule du binôme de Newton donne dans ce cas l'égalité suivante :

$$a^\mu = ((a - \mathrm{Id}) + \mathrm{Id})^\mu = \sum_{i=0}^{n-1} \binom{\mu}{i} (a - \mathrm{Id})^i. \tag{2.3}$$

D'autre part, la série

$$a^\mu = e^{\mu \ln((a-\mathrm{Id})+\mathrm{Id})} \tag{2.4}$$

converge pour tout $\mu \in \mathbb{Q}$: le développement en série du logarithme népérien comporte un nombre fini de termes puisque a est unipotente, et le développement en série de l'exponentielle converge toujours.

Notons $\alpha_k(\mu)$ les coefficients de la série (2.4). Étant donné le nombre fini de termes du développement du logarithme, on peut montrer que ces coefficients sont polynomiaux en μ. Or, sur $\mathbb{N}$, on a l'égalité

$$\alpha_k(\mu) = \binom{\mu}{k}$$

d'après la relation (2.3). Les deux membres de cette équation, polynomiaux en μ, coïncident sur l'ensemble infini $\mathbb{N}$. Ils sont donc égaux en tant que polynômes, ce qui nous donne en particulier :

$$p(a, \mu) = a^{\mu} \quad \forall\, \mu \in \mathbb{Q}.$$

Cette définition est accompagnée par les relations habituelles suivantes :

$$a^{\mu+\nu} = a^{\mu} a^{\nu}, \quad a^{\mu\nu} = (a^{\mu})^{\nu}$$

pour μ et ν rationnels. En particulier, $\frac{1}{m} \in \mathbb{Q}$, et $a^{\frac{1}{m}}$ est une racine $m^{\text{ième}}$ de a et $UT_n(\mathbb{Q})$ est divisible.

En fait, pour tout corps K de caractéristique nulle, $UT_n(K)$ est divisible.

Intéressons-nous à présent à la propriété d'unicité de la racine dans un groupe nilpotent sans torsion, ainsi qu'à quelques conséquences de ce fait.

2.5.2 Extraction univoque de la racine dans un groupe nilpotent sans torsion

Le premier paragraphe de cette partie a pour but de démontrer la proposition **2.5.5** qui nous servira dans la preuve d'unicité de la racine, au paragraphe suivant.

Classe de nilpotence du sous-groupe $\langle a, [G, G] \rangle$

Soient G un groupe nilpotent de classe $s \geqslant 2$, et a un élément de ce groupe. Nous cherchons à montrer le lemme suivant :

Proposition 2.5.5
Le sous-groupe $\langle [G, G], a \rangle$, engendré par le sous-groupe dérivé et un élément a de G, est nilpotent de classe strictement inférieure à la classe s de nilpotence de G.

Afin de démontrer cette proposition, nous commençons par le lemme suivant :

Lemme 2.5.6
Soit une série centrale d'un groupe quelconque G, notée

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n \leqslant \cdots, \tag{2.5}$$

et H un sous-groupe de G. Alors la série des termes $H_i = G_i \cap H$,

$$1 = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_n \leqslant \cdots \tag{2.6}$$

est également une série centrale.

Démonstration — La définition d'une série centrale donne $[G_{i+1}, G] \leqslant G_i$. Soient alors $a \in H \cap G_{i+1}$ et $b \in H$. On a clairement $[a, b] \in G_i$. D'autre part, H étant un sous-groupe, $[a, b]$ est également un élément de H. D'où

$$[H_{i+1}, H] \leqslant H_i,$$

et la série (2.6) des H_i est centrale. ⊠

Il va de soi que le même résultat reste valable pour une série centrale décroissante.

D'autre part, on utilisera le lemme suivant :

Lemme 2.5.7
Le quotient d'un groupe G par son centre ne peut pas être monogène et différent de $\{1\}$.

Démonstration — Supposons que $G/Z(G) = \langle a \rangle$. Soit $x \in G$. Il s'écrit $x = a^n y$, où n est un entier relatif, et y appartient au centre de G. Montrons que $a \in G$ commute avec x :

$$\begin{array}{rcll} ax & = & aa^n y & \\ & = & a^n ay & \\ & = & a^n ya & \text{car } y \in Z(G) \\ ax & = & xa. & \end{array}$$

On a montré ainsi que $a \in Z(G)$. Sa classe dans $G/Z(G)$ est donc celle de 1, et $G/Z(G) = \{1\}$. ⊠

Nous pouvons maintenant proposer une démonstration de la proposition qui fait l'objet de ce paragraphe :

Démonstration de la proposition **2.5.5** — Notons pour commencer :

$$H = \langle [G, G], a \rangle.$$

Les séries centrales inférieure et supérieure de G sont notées de la façon usuelle (cf. 1.10 et 1.11), et comportent toutes deux s facteurs exactement. D'après les théorèmes **1.3.19** et **1.3.20**, on a $\gamma_2 G \leqslant \zeta_{s-1} G$, c'est-à-dire $[G, G] \leqslant \zeta_{s-1} G$. Comme, par définition de H, $[G, G] \leqslant H$, on obtient : $[G, G] \leqslant H \cap \zeta_{s-1} G$.
Notons alors $H_i = H \cap \zeta_i G$. D'après le lemme précédent, la série (2.6) des H_i est centrale, à l'instar de la série supérieure de G dont elle est déduite. Le théorème **1.3.19** appliqué au groupe H nous permet d'en déduire que $H_i \leqslant \zeta_i H$, pour tout i de 0 à n, et en particulier pour $i = s - 1$. On en tire que $H \cap \zeta_{s-1} G \leqslant \zeta_{s-1} H$, et donc que $[G, G] \leqslant \zeta_{s-1} H$.

Par définition de H, le groupe $H/\zeta_{s-1}H$ est alors monogène. Or ce groupe est isomorphe au groupe

$$K = \frac{H/\zeta_{s-2}H}{\zeta_{s-1}H/\zeta_{s-2}H},$$

où $\zeta_{s-1}H/\zeta_{s-2}H = Z(H/\zeta_{s-2}H)$. Le groupe K est donc le quotient d'un groupe par son centre, et monogène, ce qui implique qu'il est trivial (lemme **2.5.7**). On a ainsi montré que $H/\zeta_{s-1}H$ est trivial, c'est-à-dire que $\zeta_{s-1}H = H$, ce qui prouve bien que la classe de nilpotence de H est strictement inférieure à celle de G. ⊠

Unicité de la racine dans un groupe nilpotent sans torsion

Forts de la proposition précédente, nous pouvons maintenant montrer le théorème suivant :

Théorème 2.5.8
Soit G un groupe nilpotent sans torsion. Dans ce groupe, l'extraction de la racine est une opération univoque, c'est-à-dire que l'égalité $a^n = b^n$ pour $n \neq 0$ implique que $a = b$.

Remarque 2.5.9 On se contente, dans ce théorème, d'affirmer l'unicité de la racine. Le problème de son existence n'est pas traité ici, ce qui signifie que la racine peut très bien ne pas être définie partout dans $G \ldots$ Ce problème est traité au Chapitre **3**.

Démonstration — Nous utilisons ici une récurrence sur la classe de nilpotence du groupe G.
Si celui-ci est abélien, c'est-à-dire de classe 1, le théorème est évident :

$$\begin{aligned} a^n = b^n &\Leftrightarrow a^n b^{-n} = 1 \\ &\Leftrightarrow (ab^{-1})^n = 1, \end{aligned}$$

ce qui implique que $a = b$ puisque G est sans torsion.
Soit à présent un groupe G nilpotent sans torsion, non abélien, de classe de nilpotence s, et deux de ses éléments, a et b, vérifiant $a^n = b^n$. On considère son sous-groupe $H = \langle a, [G, G]\rangle$, dont la classe de nilpotence est strictement inférieure à s d'après la proposition **2.5.5**. Par hypothèse de récurrence, le théorème est vérifié par H. Or $a \in H$ et $a^b = a[a, b] \in H$. Étant donné que

$$(a^b)^n = (a^n)^b = (b^n)^b = b^n = a^n,$$

le théorème appliqué à H donne $a^b = a$, ce qui signifie que a et b commutent. On a alors, dans G :

$$\begin{array}{rcl} a^n = b^n & \Leftrightarrow & (ab^{-1})^n = 1 \\ & \Leftrightarrow & a = b \end{array}$$

car G est sans torsion. Ceci termine la preuve du théorème. ⊠

L'unicité de la racine dans un groupe nilpotent sans torsion donne immédiatement une propriété des éléments d'un tel groupe. Celle-ci est exprimée ci-après :

Propriété 2.5.10
Si x et y sont deux éléments d'un groupe nilpotent sans torsion, et m et n deux entiers naturels non nuls, alors

$$x^m y^n = y^n x^m \Leftrightarrow xy = yx.$$

La démonstration est immédiate :

Démonstration — On a

$$\begin{array}{rcrcl} x^m y^n = y^n x^m & \Leftrightarrow & y^{-n} x^m y^n & = & x^m \\ & \Leftrightarrow & (x^{(y^n)})^m & = & x^m \\ & \Leftrightarrow & x^{(y^n)} & = & x \quad \text{par unicité de la racine.} \end{array}$$

En réitérant les mêmes étapes à l'aide de la conjugaison par x^{-1} cette fois et non plus par y^n, on arrive à la conclusion : $xy = yx$. ⊠

En particulier, si x^n est central, il en va de même pour x lui-même.

Conséquence sur la série centrale supérieure d'un groupe nilpotent sans torsion

Le théorème **2.5.8** permet également d'affirmer la proposition suivante :

Proposition 2.5.11
Dans un groupe nilpotent sans torsion, tous les facteurs de la série centrale supérieure sont, eux aussi, sans torsion.

Démonstration — Soit G un groupe nilpotent sans torsion, et

$$1 = Z_0 \leqslant Z_1 \leqslant \cdots \leqslant Z_n = G \tag{2.7}$$

sa série centrale supérieure, où n est la classe de nilpotence de G.

Montrons au préalable le lemme suivant :

Lemme 2.5.12
Si H est un groupe nilpotent sans torsion, alors $H/Z(H)$ est également sans torsion.

Démonstration du lemme — Soient $\bar{a} \in H/Z(H)$ et $r \in \mathbb{N}^*$. Supposons que $\bar{a}^r = 1$. On a alors $\overline{a^r} = 1$, c'est-à-dire que a^r appartient au centre de H. Alors, d'après la propriété **2.5.10**, $a \in Z(H)$ et donc $\bar{a} = 1$, d'où l'on déduit le résultat. □
Montrons alors par récurrence sur i que G/Z_i est sans torsion pour i de 0 à n : supposons que G/Z_i soit sans torsion. Alors on a, avec le corollaire **1.1.16** du théorème de factorisation :

$$\frac{G}{Z_{i+1}} \simeq \frac{G/Z_i}{Z_{i+1}/Z_i}.$$

Or, le deuxième membre de cette relation est, par définition de la série centrale supérieure, égal à

$$\frac{G/Z_i}{Z(G/Z_i)},$$

qui est sans torsion d'après le lemme qui précède.

G étant par hypothèse sans torsion, la récurrence est fondée et G/Z_i est sans torsion pour tout i de 0 à n. Enfin, pour $i = 1, \ldots, n$, Z_{i+1}/Z_i est sans torsion comme sous-groupe de G/Z_i. ⊠

2.6 Groupes polycycliques

Introduisons à présent la notion de *groupe polycyclique*, qui nous sera utile pour présenter les complétés de Mal'cev dans le chapitre suivant.

2.6.1 Définition d'un groupe polycyclique

Le caractère polycyclique d'un groupe lui est conféré par ses séries. C'est pourquoi nous commençons par la définition suivante :

Définition 2.6.1
Une série sous-normale finie est dite polycyclique *si tous ses facteurs sont cycliques, qu'ils soient finis ou non.*

On peut donner une dénomination commune aux groupes possédant de telles séries :

Définition 2.6.2
Tout groupe possédant une série polycyclique est dit lui-même polycyclique.

Exemple 2.6.3 Le groupe alterné $\mathfrak{A}_4$ possède une série polycyclique :

$$1 \leqslant \{1, (12)(34)\} \leqslant \{1, (12)(34), (13)(24), (14)(23)\} \leqslant \mathfrak{A}_4. \qquad (2.8)$$

En effet, son premier facteur, $\{1, (12)(34)\} = \langle (12)(34) \rangle$, est cyclique.

Son deuxième facteur est engendré par $\overline{(13)(24)}$ et $\overline{(14)(23)}$, où la barre supérieure désigne en fait la classe, dans le quotient considéré, de l'élément. Or, l'égalité $(13)(24)(12)(34) = (14)(23)$ montre que les deux générateurs du facteur considéré sont égaux, donc qu'il est cyclique.

Le fait que le troisième facteur soit monogène est moins évident. En fait, le groupe $\mathfrak{A}_4$ est engendré par les cycles de longueur 3, au nombre de huit. Or, on a pour i, j et k distincts dans $\{1, 2, 3, 4\}$, les égalités suivantes :

$$\begin{aligned} (ijk)(ij)(kl) &= (ikl) \\ (ijk)(ik)(jl) &= (jlk) \\ (ijk)(il)(jk) &= (ikl). \end{aligned}$$

Celles-ci donnent les égalités de classes suivantes dans le troisième facteur :

$$\begin{aligned} \overline{(123)} = \overline{(134)} = \overline{(142)} = \overline{(243)} \\ \overline{(234)} = \overline{(124)} = \overline{(132)} = \overline{(143)}. \end{aligned}$$

Il n'y a donc que deux classes non triviales dans ce facteur, vérifiant de plus :

$$(123)^2 = (132) \qquad \text{et} \qquad (123)^3 = 1,$$

ce qui donne la cyclicité du dernier facteur de $\mathfrak{A}_4$.

Montrons encore que cette série est sous-normale : Par conjugaison dans $\mathfrak{S}_4$, la décomposition en cycles disjoints d'une permutation conserve sa structure, c'est-à-dire en particulier qu'un produit de deux cycles à supports disjoints reste, après conjugaison, un produit de deux cycles à supports disjoints. Les longueurs des cycles restent elles aussi inchangées. Il en découle que le troisième terme de la série (2.8) est normal dans $\mathfrak{A}_4$.

D'autre part, on remarque que la permutation $(12)(34)$ commute à la fois avec $(13)(24)$ et avec $(14)(23)$, ce qui donne la normalité de $\{1, (12)(34)\}$ dans $\{1, (12)(34), (13)(24), (14)(23)\}$.

La série (2.8) est donc effectivement polycyclique.

Exemple 2.6.4 Un deuxième exemple découle du théorème de décomposition des groupes abéliens de type fini (**2.1.5**). En effet, tout groupe décomposé sous la forme

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$$

admet une série polycyclique, centrale par commutativité du groupe :

$$1 \leqslant \mathbb{Z} \leqslant \cdots \leqslant \mathbb{Z}^r \leqslant (\mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z}) \leqslant \cdots \leqslant G.$$

Donnons encore une propriété vérifiée par la classe des groupes polycycliques :

Propriété 2.6.5
Tout sous-groupe d'un groupe polycyclique reste polycyclique.
Tout quotient d'un groupe polycyclique reste polycyclique.

Démonstration — Ce résultat découle immédiatement des théorèmes **1.3.9** et **1.3.10**, ainsi que, pour la première partie de l'assertion, de la propriété **1.1.1** selon laquelle tout sous-groupe d'un groupe cyclique est lui-même cyclique. La preuve de la deuxième partie du théorème nécessite quant à elle la remarque suivante : l'image homomorphe d'un groupe cyclique G est elle-même cyclique, engendrée par l'image de tout générateur du groupe G de départ. ⊠

Remarque 2.6.6 Tout groupe G polycyclique est de type fini. Cela découle directement de la définition : soit

$$1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n = G \tag{2.9}$$

une série polycyclique du groupe G. Choisissons alors une famille $\mathcal{F} = \{g_1, \ldots, g_n\}$ d'éléments de G telle que pour tout i de 1 à n, la classe de g_i engendre le facteur G_i/G_{i-1}. Alors le groupe G est engendré par la famille $\mathcal{F}$.

La propriété et la remarque qui précèdent donnent lieu au corollaire suivant :

Corollaire 2.6.7
Tout sous-groupe d'un groupe polycyclique est de type fini.

2.6.2 Cas d'un groupe nilpotent polycyclique

Nous montrons à présent que, pour un groupe nilpotent, être de type fini revient à être polycyclique. Pour cela, nous utiliserons le lemme suivant :

Lemme 2.6.8
Soit G un groupe quelconque. Si G est engendré par un ensemble M, alors $\gamma_i G$ est engendré par $\gamma_{i+1}G$, et par des commutateurs de poids i en éléments de M.

Démonstration — Montrons ce lemme par récurrence sur i : il est évident pour $i = 1$. Supposons qu'il soit vérifié pour i. Par définition, $\gamma_{i+1}G$ est engendré par les éléments $[x, y]$, où $x \in \gamma_i G$ et $y \in G$. Par hypothèse de récurrence, x s'exprime comme un produit de commutateurs de poids i en des éléments $x_j,\ j = 1, ..., m$, de M et d'un élément de $\gamma_{i+1}G$, noté z :

$$x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} z,$$

où pour tout j de 1 à m, ε_j vaut soit 1, soit (-1). En outre, y s'exprime comme un produit d'éléments ou d'inverses d'éléments de M.
Les relations sur les commutateurs, montrées dans la propriété **1.2.8**, permettent alors d'affirmer que $[x, y]$ est un produit d'éléments ou d'inverses d'éléments de la forme $[x_j, a]^g = [x_j, a][x_j, a, g]$, où $a \in M$ et $g \in G$, et $[z, a]^g$. Puisque $[x_j, a, g]$ et $[z, a]$ sont des éléments de $\gamma_{i+2}G$, nous avons démontré le lemme. ⊠

On dira qu'un groupe *possède presque* une propriété donnée s'il contient un sous-groupe normal d'indice fini qui possède la propriété en question.

Nous pouvons maintenant donner le théorème qui nous intéresse :

Théorème 2.6.9
Tout groupe nilpotent de type fini G admet une série centrale polycyclique et est presque sans torsion.
Si G est sans torsion, alors les facteurs de cette série sont des groupes cycliques infinis.

Démonstration — La démonstration se fait en deux étapes :

1. Supposons G de type fini et nilpotent. Chaque facteur de sa série centrale inférieure est un groupe abélien de type fini : en effet,

   $$[\gamma_{i-1}G, \gamma_{i-1}G] \leqslant [\gamma_{i-1}G, G],$$

   ce qui implique que $\gamma_{i-1}G/[\gamma_{i-1}G, G]$ est abélien ; il est de type fini du fait du lemme précédent. Le théorème de décomposition des groupes abéliens de type fini (**2.1.5**) montre alors que chacun des facteurs de la série centrale inférieure de G admet une série dont les facteurs sont cycliques. Étant donné que toute subdivision d'une série centrale reste une série centrale (théorème **1.3.13**), on a montré que G admet une série centrale dont les facteurs sont cycliques.
   Montrons à présent, par récurrence sur le nombre de termes de cette série centrale polycyclique, que G est presque sans torsion. Notons $(\mathcal{S})$ cette série, et n sa longueur. Supposons avoir montré que, si un groupe possède une série centrale polycyclique de longueur $(n-1)$, alors il

est presque sans torsion. Soit H le terme le plus grand (au sens de l'inclusion) de $(\mathcal{S})$, distinct de G, et soit a un générateur de G/H. Par hypothèse de récurrence, H est presque sans torsion, puisqu'il possède une série centrale polycyclique à n termes.
Alors, il existe m tel que $H^m = \langle h^m \,|\, h \in H\rangle$ soit sans torsion : en effet, H étant presque sans torsion, il existe un sous-groupe normal H' de H, d'indice fini dans H, qui soit sans torsion. Considérons alors le groupe $K = H/H'$. Il est fini, donc de torsion. Cela signifie qu'il existe un entier m tel que $K^m = 1$ (le cardinal de K par exemple). C'est-à-dire qu'en fait $H^m/H' = 1$, puisque $\overline{h}^m = \overline{h^m}$. Pour tout élément h de H, on a donc $h^m \in H'$, et donc aussi $H^m \leqslant H'$. H' étant sans torsion, on a montré ainsi que H^m est également sans torsion.
Montrons à présent le lemme suivant :

Lemme 2.6.10
Tout groupe nilpotent de type fini et périodique est fini.

Démonstration du lemme — Soit K un groupe nilpotent périodique de type fini. Étant nilpotent et de type fini, on vient de montrer que K est polycyclique, c'est-à-dire qu'il admet une série dont les facteurs sont tous monogènes. La périodicité de K impose de plus à tous ces facteurs d'être finis. Une récurrence simple sur le nombre de facteurs de la série en question implique que K est fini. En effet, si K' est fini, et que K/K' est fini, alors le théorème de Lagrange (**1.1.2**) donne le résultat suivant : $|K| = |K'| \cdot |K/K'|$. □

Or, H/H^m est nilpotent du fait de la nilpotence de G. Il est périodique puisque chacun de ses éléments vaut 1 à la puissance m. Enfin, H étant de type fini d'après la remarque **2.6.6**, on a également H/H^m de type fini. D'où avec le lemme précédent : $|H : H^m| < \infty$.
À présent, deux cas se distinguent : si $|G : H|$ est fini, alors H^m est le sous-groupe recherché, d'indice fini dans G et sans torsion. Sinon, le quotient $G/H = \langle a\rangle$ est infini, donc sans torsion. De plus, on a, d'après le deuxième corollaire du théorème **1.1.15** de factorisation :

$$|G : \langle a\rangle H^m| = |H : H \cap \langle a\rangle H^m| \leqslant |H : H^m| < \infty.$$

Le fait que $\langle a\rangle H^m$ soit sans torsion est une conséquence du lemme suivant :

Lemme 2.6.11
Soient L un groupe et K un sous-groupe normal de L. Supposons que K et L/K soient sans torsion. Alors L est sans torsion.

Démonstration du lemme — Tout élément x de L s'écrit $x = \alpha\beta$, où $\beta \in K$ et $\bar{\alpha} = \bar{x}$ dans L/K. Alors :

$$\begin{aligned}(\alpha\beta)^n &= \alpha\beta \dots \alpha\beta \\ &= \alpha^2\beta[\beta,\alpha]\dots\alpha\beta.\end{aligned}$$

Or $[\beta,\alpha] = \beta \cdot \beta^\alpha \in K \trianglelefteq L$. On arrive ainsi à $1 = (\alpha\beta)^n = \alpha^n k$, avec $k \in K$. Cela entraîne directement l'égalité suivante : $\bar{\alpha}^n = 1$ dans L/K. Comme L/K est sans torsion, cela revient à affirmer que $n = 0$ ou que $\alpha = 1$. Dans le premier cas, on a montré que L est sans torsion. Dans le deuxième cas, $x \in K$ et n'est donc pas d'ordre fini puisque K est sans torsion.
On arrive finalement à la conclusion que L est sans torsion. □

En appliquant ce lemme avec $L = \langle a\rangle H^m$ et $K = H^m$, on a montré que $\langle a\rangle H^m$ est sans torsion.

Introduisons à présent le groupe suivant :

$$\mathcal{H} = \bigcap_{g\in G} (\langle a\rangle H^m)^g.$$

Soient $h \in \mathcal{H}$ et $g \in G$. Fixons un élément x de G, et vérifions que $h^g \in (\langle a\rangle H^m)^x$. Comme $h \in \mathcal{H}$, on a en particulier $h \in (\langle a\rangle H^m)^{xg^{-1}}$. Cela entraîne immédiatement le résultat voulu. Comme cela est vrai pour tout x de G, on a également $h^g \in \mathcal{H}$ pour tout élément g de G, ce qui signifie que $\mathcal{H}$ est normal dans G.
$\mathcal{H}$ étant en outre d'indice fini et sans torsion, nous avons finalement prouvé que G est presque sans torsion.

2. Supposons que G soit un groupe nilpotent, de type fini, et sans torsion. Nous venons de voir qu'alors G est polycyclique. Nous avons montré que les facteurs de sa série centrale inférieure sont également polycycliques ; en utilisant la propriété **2.6.5**, on obtient le caractère polycyclique des facteurs de la série centrale supérieure de G. Celle-ci peut donc être subdivisée en une nouvelle série centrale, notée $(\mathcal{S}')$, dont les facteurs sont cycliques. D'après la proposition **2.5.11**, les facteurs de la série centrale supérieure de G sont aussi sans torsion. Ceci impose que les facteurs de $(\mathcal{S}')$ soient infinis.

Le théorème se trouve ainsi démontré. ⊠

On a ainsi montré qu'un groupe G nilpotent de type fini est polycyclique. Avec la remarque **2.6.6** de la page 47, on a donc prouvé le théorème suivant :

Théorème 2.6.12
Soit G un groupe nilpotent. Alors G est de type fini si et seulement si G est polycyclique.

Ce résultat, associé à la propriété **2.6.5**, donne lieu au corollaire qui suit :

Corollaire 2.6.13
Tout sous-groupe d'un groupe nilpotent de type fini est de type fini.

En particulier, tout sous-groupe d'un groupe abélien de type fini est lui-même de type fini.

Les résultats que nous venons de prouver serviront de base à la construction des coordonnées de Mal'cev dans le chapitre suivant.

Chapitre 3

Complété de Mal'cev d'un groupe nilpotent sans torsion

Ce chapitre a pour but d'approfondir un type de complété bien particulier, celui dit de *Mal'cev*.

3.1 Coordonnées de Mal'cev dans un groupe nilpotent de type fini sans torsion

3.1.1 Définition des coordonnées

Quelques définitions préalables

Commençons par définir ce que nous appelons *famille de coordonnées* :

Définition 3.1.1
La famille $\{f_i\}_{i=1\ldots s}$ *de fonctions* $f_i : G \longrightarrow \mathbb{Z}$, *où* G *est un groupe, est une* famille de coordonnées *si l'application* $x \longmapsto (f_1(x), \ldots, f_s(x))$ *est une injection de* G *dans* $\mathbb{Z}^s$.

Poursuivons avec les définitions des termes *polynomial* et *linéaire* dans le contexte des groupes :

Définition 3.1.2
Soit $G \subseteq \mathbb{Z}^s$ *; une application* $\varphi : G \longrightarrow \mathbb{Z}^r$, *pour* $r \leqslant s$, *est dite* polynomiale *s'il existe des polynômes* f_1, $f_2, \ldots, f_r$ *de* s *variables à coefficients dans* $\mathbb{Q}$ *tels que* $\varphi(x) = (f_1(x), \ldots, f_r(x))$ *pour* $x \in G$.

Définition 3.1.3
En reprenant les notations de la définition précédente, si les polynômes $f_1, \ldots, f_r$ *sont de degré* 1, *on dit que* φ *est une application* linéaire.

Construction des coordonnées de Mal'cev

Nous avons démontré dans le chapitre précédent qu'un groupe nilpotent de type fini sans torsion admet une série centrale polycyclique dont tous les facteurs sont isomorphes à $\mathbb{Z}$. Soit G un tel groupe. Écrivons cette série de la manière suivante :

$$G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_{s+1} = 1. \tag{3.1}$$

Les facteurs de cette série étant monogènes, on peut choisir des éléments $a_1, \ldots, a_s$ de G tels que, pour tout i de 1 à s, on ait $G_i = \langle G_{i+1}, a_i \rangle$.
Chaque élément x de G s'écrit alors de façon unique sous la forme suivante :

$$x = a_1^{t_1(x)} a_2^{t_2(x)} \ldots a_s^{t_s(x)},$$

où $t_i(x) \in \mathbb{Z}$ pour i allant de 1 à s.
En effet, soit $x \in G$. Dans le quotient G/G_2, la classe de x notée $\bar{x}$ est une puissance de celle de a_1. Donc il existe $g_2 \in G_2$, tel que, dans G, $x = a_1^{t_1(x)} g_2$. En supposant, par récurrence, que g_2 se laisse mettre sous la forme unique : $g_2 = a_2^{t_2(g_2)} \ldots a_s^{t_s(g_2)}$, on obtient, de façon unique puisque $\langle a_1 \rangle$ est sans torsion :

$$x = a_1^{t_1(x)} a_2^{t_2(g_2)} \ldots a_s^{t_s(g_2)}.$$

En posant alors pour tout i de 2 à s : $t_i(x) = t_i(g_2)$, on a le résultat attendu. $(t_1, \ldots, t_s)$ forme donc un système de coordonnées de G dans $\mathbb{Z}^s$.

Définition 3.1.4
Le système ordonné $(a_1, \ldots, a_s)$ est appelé base de Mal'cev *du groupe G, tandis que $t_1(x), t_2(x), \ldots, t_s(x)$ sont les* coordonnées de Mal'cev *de x dans cette base. On notera $t(x)$ pour abréger l'écriture de la famille $(t_1(x), \ldots, t_s(x))$.*

Nous savons maintenant exprimer un élément de G dans la base de Mal'cev. Mais qu'en est-il des coordonnées d'un produit d'éléments de G ? Nous traitons de cela dans la partie qui suit.

3.1.2 Expression polynomiale des coordonnées d'un produit et d'une puissance

L'objectif de ce paragraphe est de montrer la propriété suivante :

Propriété 3.1.5
Les coordonnées de Mal'cev d'un produit et de l'élévation à une puissance d'éléments d'un groupe G nilpotent de type fini sans torsion s'exprime de façon polynomiale en les coordonnées de Mal'cev des éléments de départ.

Plus exactement, si x, y sont des éléments de G, m un entier relatif et i vérifie $1 \leqslant i \leqslant s$, alors on a :

1. $$t_i(xy) = P(t(x), t(y)) + t_i(x) + t_i(y),$$
   où $P(t(x), t(y))$ est en fait un polynôme sur $\mathbb{Q}$ en les coordonnées de Mal'cev de x et y précédentes : $\{t_\alpha(x), t_\alpha(y) \mid \alpha < i\}$.
2. $$t_i(x^m) = Q(m, t(x)) + mt_i(x),$$
   où $Q(m, t(x))$ est en fait un polynôme sur $\mathbb{Q}$ en m et en les coordonnées de Mal'cev de x précédentes : $\{t_\alpha(x) \mid \alpha < i\}$.

Démonstration — Rappelons que les coordonnées de Mal'cev sont définies sur la base d'une série centrale polycyclique. Nous noterons Γ_i les termes successifs de la SCI de G, et G_i les termes de la série centrale polycyclique de G à facteurs isomorphes à $\mathbb{Z}$ par rapport à laquelle les coordonnées de Mal'cev sont calculées.

Remarquons en premier lieu que, la série

$$G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_s \geqslant G_{s+1} = 1$$

étant centrale, chaque sous-groupe G_i est normal dans G. Dans le quotient G/G_{i+1}, les coordonnées de $\bar{x}$, $\bar{y}$ et $\overline{xy}$ sont les i premières coordonnées de x, y et xy respectivement. On a ainsi $t_i(xy) = t_i(\bar{x}\bar{y})$. La $i^{\text{ème}}$ coordonnée du produit xy ne peut donc dépendre que des i premières coordonnées de x et de y : $\{t_\alpha(x), t_\alpha(y) | \alpha \leqslant i\}$.

La centralité de la série donne en outre, puisque $G_i/G_{i+1} \leqslant Z(G/G_{i+1})$, que a_i en particulier commute avec tous les éléments de G/G_{i+1}. Ceci nous permet alors d'écrire dans ce groupe quotient :

$$\begin{aligned} xy &= a_1^{t_1(x)} \dots a_i^{t_i(x)} a_1^{t_1(y)} \dots a_i^{t_i(y)} \\ &= a_1^{t_1(x)} \dots a_{i-1}^{t_{i-1}(x)} a_1^{t_1(y)} \dots a_{i-1}^{t_{i-1}(x)} a_i^{t_i(x)+t_i(y)}. \end{aligned}$$

De cela découle que

$$\begin{aligned} t_i(xy) &= t_i(x) + t_i(y) + f(t(x), t(y)) \\ \text{et } t_i(x^m) &= mt_i(x) + g(m, t(x)), \end{aligned}$$

où f est une fonction des $2(i-1)$ coordonnées $\{t_\alpha(x), t_\alpha(y) \mid \alpha < i\}$, et g est une fonction des i variables $\{m\} \cup \{t_\alpha(x) \mid \alpha < i\}$.

Il nous reste à démontrer que la dépendance de f et g en les coordonnées de x et y est polynomiale. Nous démontrerons cette propriété simultanément pour les deux assertions, par récurrence sur la longueur de la base de Mal'cev de G. Il est évident que si celle-ci vaut 1, alors $t_1(xy) = t_1(x) + t_1(y)$ et $t_1(x^m) = mt_1(x)$. Les polynômes P et Q sont alors nuls.

Supposons le théorème vérifié pour toute base de longueur strictement inférieure à s. Soit G un groupe possédant une base de Mal'cev $(a_1, \ldots, a_s)$ de longueur s. Notons pour simplifier : $\zeta_i = t_i(x)$ et $\eta_i = t_i(y)$, pour i allant de 1 à s. On a :

$$\begin{aligned} xy &= a_1^{\zeta_1} a_2^{\zeta_2} \ldots a_s^{\zeta_s} a_1^{\eta_1} a_2^{\eta_2} \ldots a_s^{\eta_s} \\ &= a_1^{\zeta_1+\eta_1} (a_1^{-\eta_1} a_2^{\zeta_2} a_1^{\eta_1}) \ldots (a_1^{-\eta_1} a_s^{\zeta_s} a_1^{\eta_1}) a_2^{\eta_2} \ldots a_s^{\eta_s} \\ xy &= a_1^{\zeta_1+\eta_1} (a_1^{-\eta_1} a_2^{-1} a_1^{\eta_1})^{-\zeta_2} \ldots (a_1^{-\eta_1} a_s^{-1} a_1^{\eta_1})^{-\zeta_s} a_2^{\eta_2} \ldots a_s^{\eta_s}. \end{aligned} \tag{3.2}$$

Or

$$\begin{aligned} a_1^{-\eta_1} a_i^{-1} a_1^{\eta_1} &= a_1^{-\eta_1} (a_i^{-1} a_1^{\eta_1} a_i) a_i^{-1} \\ &= a_1^{-\eta_1} (a_i^{-1} a_1 a_i)^{\eta_1} a_i^{-1} \end{aligned}$$

et $a_i^{-1} a_1 a_i = a_1 [a_1, a_i]$. Or le commutateur $[a_1, a_i]$ appartient à G_{i+1}, ce qui signifie qu'il s'écrit sur les coordonnées de Mal'cev de ce groupe :

$$[a_1, a_i] = a_{i+1}^{\phi_{i,i+1}} \ldots a_s^{\phi_{i,s}}.$$

Alors on a

$$a_i^{-1} a_1 a_i = a_1 a_{i+1}^{\phi_{i,i+1}} \ldots a_s^{\phi_{i,s}},$$

d'où par hypothèse de récurrence appliquée au groupe $\langle a_1, a_{i+1}, \ldots, a_s \rangle$, dont la base de Mal'cev a une longueur strictement inférieure à s pour $i \geqslant 2$:

$$(a_i^{-1} a_1 a_i)^{\eta_1} = a_1^{\eta_1} a_{i+1}^{\varphi_{i,i+1}} \ldots a_s^{\varphi_{i,s}},$$

avec les fonctions $\varphi_{i,j}$ polynomiales en η_1.
Alors

$$\begin{aligned} a_1^{-\eta_1} a_i^{-1} a_1^{\eta_1} &= a_{i+1}^{\varphi_{i,i+1}} \ldots a_s^{\varphi_{i,s}} a_i^{-1} \\ &= a_i^{-1} a_{i+1}^{\psi_{i,i+1}} \ldots a_s^{\psi_{i,s}} \end{aligned}$$

où les fontions $\psi_{i,j}$ sont elles aussi polynomiales en η_1. En utilisant l'hypothèse de récurrence sur G_i pour élever cette expression à la puissance $(-\zeta_i)$, on obtient

$$(a_1^{-\eta_1} a_i^{-1} a_1^{\eta_1})^{-\zeta_i} = a_i^{\zeta_i} a_{i+1}^{\rho_{i,i+1}} \ldots a_s^{\rho_{i,s}},$$

où les fonctions $\rho_{i,j}$ sont polynomiales en η_1 et en ζ_i. En injectant ce résultat dans l'expression (3.2), on obtient :

$$xy = a_1^{\zeta_1+\eta_1} \left(\Pi_{i=2}^n a_i^{\zeta_i} a_{i+1}^{\rho_{i,i+1}} \ldots a_s^{\rho_{i,s}} \right) a_2^{\eta_2} \ldots a_s^{\eta_s},$$

produit de $a_1^{\zeta_1+\eta_1}$ avec un produit d'éléments de G_2. En appliquant l'hypothèse de récurrence à ce dernier groupe, on peut écrire finalement :

$$xy = a_1^{\zeta_1+\eta_1} a_2^{\tau_2} \dots a_s^{\tau_s}$$

où pour tout $i \geqslant 2$, τ_i est polynomial en les coordonnées $\{\zeta_1, \dots, \zeta_s, \eta_1, \dots, \eta_s\}$ de x et y.

La combinaison de ce résultat avec ce que nous avons déjà affirmé plus haut nous donne la première assertion du théorème que nous nous efforçons de démontrer.

Afin d'en démontrer la deuxième partie, écrivons $x^n = x^{n-1}x$.
Par hypothèse de récurrence, les coordonnées de x^{n-1} sont polynomiales en celles de x et en $(n-1)$, c'est-à-dire en n. La première partie du théorème, que nous venons de démontrer, nous donne alors la polynomialité des coordonnées du produit $x^{n-1} \cdot x$ en les coordonnées de x^{n-1} et en celles de x, c'est-à-dire finalement en n et en les coordonnées de x. Comme dans la partie précédente, c'est en alliant ce résultat à ce que nous avons remarqué au début de la démonstration que nous obtenons la formule *2* du théorème. ⊠

3.2 Exemple de clôture divisible dans un groupe divisible

Nous cherchons maintenant à étudier la clôture divisible d'un sous-groupe dans un groupe divisible. Commençons par définir ce qu'est une clôture divisible.

3.2.1 Définition d'une clôture divisible

C'est la notion d'existence de la racine, dont on sait déjà qu'elle est unique dans un groupe nilpotent sans torsion, qui amène le concept de groupe *divisible*. Rappelons qu'un tel groupe est défini par la propriété suivante :

$$\forall\, g \in G,\ \forall\, n \in \mathbb{N},\ \exists\, x \in G \text{ tel que } x^n = g \quad \text{(définition } \mathbf{2.5.1}\text{)}.$$

Dans un groupe quelconque G, il peut également être nécessaire de s'assurer de cette existence, tout en conservant les propriétés du groupe G. C'est pourquoi on introduit ici la notion de *clôture divisible* dans une classe de groupes donnée, définie ci-dessous.

Définition 3.2.1
Soit G un groupe de classe $\mathcal{P}$. Une clôture divisible de G *dans la classe $\mathcal{P}$ est définie comme un couple (H, i) vérifiant les axiomes suivants :*

1. *H est de classe $\mathcal{P}$ et divisible,*
2. *$i : G \longrightarrow H$ est un plongement de groupes,*
3. *pour tout élément h de H, il existe un entier $n > 0$ tel que h^n appartienne à $i(G)$.*

Exemple 3.2.2 En premier lieu, évoquons l'exemple évident de $\mathbb{Q}$ qui constitue une clôture divisible du groupe $\mathbb{Z}$ dans la classe des groupes abéliens. L'isomorphisme en jeu est assimilé à l'identité.

Exemple 3.2.3 D'autre part, le groupe divisible $UT_n(\mathbb{Q})$ est une clôture divisible du groupe $UT_n(\mathbb{Z})$ dans la classe des groupes nilpotents sans torsion, avec encore une fois l'identité comme isomorphisme associé, ce qui nous donne l'axiome 2 de la définition **3.2.1**.
L'axiome 1 découle de ce qui a été présenté dans l'exemple **2.5.4**.
Vérifions donc le troisième axiome : soit $a \in UT_n(\mathbb{Q})$. Alors, pour tout entier naturel m on a, comme dans l'exemple **2.5.4**,

$$a^m = \sum_{i=0}^{n-1} \binom{m}{i} (a - \mathrm{Id})^i = \mathrm{Id} + \sum_{i=1}^{n-1} \binom{m}{i} (a - \mathrm{Id})^i \; ;$$

le coefficient binomial est exprimé de la manière suivante :

$$\binom{m}{i} = \frac{m(m-1)\dots(m-i+1)}{i!}.$$

Notons N le plus petit commun multiple des dénominateurs de tous les éléments des matrices $\{(a - \mathrm{Id})^i\}_{i=1,\dots,n-1}$. Si l'on choisit maintenant $m = (n-1)!N$, le coefficient binomial

$$\binom{m}{i} = \frac{(n-1)!}{i!} N(m-1)\dots(m-i+1)$$

est multiple de N pour tout i de 1 à $(n-1)$.
La puissance a^m de a est donc un élément de $UT_n(\mathbb{Z})$ comme somme d'éléments de $UT_n(\mathbb{Z})$, ce qui prouve que l'axiome 3 de la définition **3.2.1** est vérifié.

3.2.2 Construction de la clôture divisible

Dans ce numéro, nous construisons une clôture divisible dans un groupe divisible, à l'aide du théorème suivant :

Théorème 3.2.4
Soit G un groupe divisible, nilpotent et sans torsion. Soit H un sous-groupe de G. Notons $\sqrt{H}$ l'ensemble de tous les éléments de G dont H contient une puissance :

$$\sqrt{H} = \{g \in G \,:\, \exists\, m \in \mathbb{N} \text{ tel que } g^m \in H\}.$$

Cet ensemble est un sous-groupe de G, il forme une clôture divisible de H et est appelé radical *de H dans G.*

Démonstration — Montrons en premier lieu que $\sqrt{H}$ est un sous-groupe de G. $\sqrt{H}$ est clairement stable par passage à l'inverse ; montrons qu'il est également stable par produit. Soient x et y des éléments de $\sqrt{H}$. Posons $A = \langle x, y\rangle$, $B = A \cap H$ et pour tout i, $A_i = \gamma_i A$ est le $i^{\text{ème}}$ terme de la SCI de A.

Lemme 3.2.5
La série

$$A = BA_1 \geqslant BA_2 \geqslant \cdots \tag{3.3}$$

est sous-normale et ses facteurs sont tous abéliens.

Démonstration du lemme **3.2.5** — Les relations entre commutateurs (propriétés **1.2.8**) donnent l'inclusion suivante :

$$[BA_i, BA_i] \leqslant [B, B]^{A_i}[A_i, B]^{A_i}[A_i, A_i].$$

Puisque $[B, B]^{A_i} \leqslant [B, B]\,[[B, B], A_i] \leqslant BA_{i+1}$, et que l'on a clairement $[A_i, B]^{A_i}[A_i, A_i] \leqslant A_{i+1}$, cela implique que

$$[BA_i, BA_i] \leqslant BA_{i+1}. \tag{3.4}$$

De plus, nous pouvons écrire que

$$\begin{aligned} BA_i\, BA_{i+1}\, BA_i &\leqslant BA_{i+1}[BA_{i+1}, BA_i] \\ &\leqslant BA_{i+1}[BA_i, BA_i] \\ &\leqslant BA_{i+1}. \end{aligned}$$

Ceci implique directement la sous-normalité de la série, tandis que la relation précédente (3.4) montre que les groupes quotients BA_i/BA_{i+1} sont abéliens. On a ainsi démontré ce premier lemme. □

Montrons à présent le

Lemme 3.2.6
Tous les indices $|BA_i : BA_{i+1}|$ sont finis.

Démonstration du lemme **3.2.6** — Soit $m \in \mathbb{N}^*$ tel que x^m et y^m appartiennent à B. On montre par récurrence sur i que BA_i/BA_{i+1} est de type fini et d'exposant divisant m^i. Ceci impliquera finalement que les quotients BA_i/BA_{i+1}, étant abéliens, sont aussi finis.

Commençons par baser cette récurrence en montrant que BA_1/BA_2 est de type fini et d'exposant divisant m. Ce quotient s'écrit plus simplement A/BA_2, puisque $B \leqslant A_1 = A$. En tant que quotient d'un groupe de type fini, il est lui-même de type fini. On a montré dans le lemme précédent que ce facteur est abélien. Tout élément de A/BA_2 à la puissance m est alors un produit en les classes de x et y, élevées à la puissance m. Or, x^m et y^m sont des éléments de $B \leqslant BA_2$, donc A/BA_2 est d'exposant divisant m.

Supposons à présent que BA_{i-1}/BA_i soit fini et d'exposant divisant m^i. A étant nilpotent comme sous-groupe de G, de type fini par définition, tous ses sous-groupes sont également de type fini (corollaire **2.6.13**) : en particulier, BA_i est de type fini, donc BA_i/BA_{i+1} est aussi de type fini.

Il reste à montrer que le groupe BA_i/BA_{i+1} a un exposant qui divise m^i. Pour cela, on travaille modulo A_{i+1}, c'est-à-dire que l'on travaille sur les classes modulo ce groupe, tout en gardant la notation plus simple des éléments. Tout élément de A_{i+1} est alors égal à 1. On a ainsi :

$$\begin{aligned} [A_{i-1}, A, A] &= [[A_{i-1}, A], A] \\ &= [A_i, A] \\ &= A_{i+1} \\ &= 1 \mod A_{i+1}. \end{aligned}$$

D'autre part, l'application f définie par

$$\begin{array}{rccc} f : & A_{i-1} \times A & \longrightarrow & A_i \\ & (u, v) & \longmapsto & [u, v] \end{array}$$

est homomorphe en ses deux arguments, toujours modulo A_{i+1}. En effet, d'après les relations entre commutateurs **1.2.8**, on a :

$$f(uu', v) = [u, v]^{u'}[u', v],$$

où $[u, v]^{u'} = [u, v]\,[[u, v], u'] = [u, v] \mod A_{i+1}$. Donc

$$f(uu', v) = f(u, v)f(u', v) \mod A_{i+1}$$

et f est homomorphe en son premier argument. De même, puisque

$$[u, vv'] = [u, v'][u, v]^{v'},$$

et que A_i/A_{i+1} est commutatif, on a

$$f(u,vv') = f(u,v)f(u,v') \mod A_{i+1}.$$

Cela implique, au niveau des ensembles et non plus des éléments, que

$$A_i^{m_i} = [A_{i-1}, A]^{m_i} \leqslant [A_{i-1}^{m_{i-1}}, A^m]A_{i+1} ;$$

en effet, modulo A_{i+1}, si $u \in A_{i-1}$ et $v \in A$:

$$\begin{aligned} [u,v]^{m^i} &= \left([u,v]^{m^{i-1}}\right)^m \\ &= [u^{m^{i-1}}, v]^m \text{ par homomorphisme,} \\ &= [u^{m^{i-1}}, v^m] \in \left[A_{i-1}^{m^{i-1}}, A^m\right]. \end{aligned}$$

Montrons à présent l'isomorphisme suivant :

$$\frac{BA_{i-1}}{BA_i} \simeq \frac{A_{i-1}}{A_i(A_{i-1} \cap B)}.$$

Donnons pour commencer un sens au quotient $A_i/A_{i+1}(A_i \cap B)$: soient $a \in A_i$ et $b \in A_{i+1}(A_i \cap B)$, que l'on écrit sous la forme $b = b_1 b_2$ où $b_1 \in A_{i+1}$ et $b_2 \in A_i \cap B$. Alors $b^a = b_1^a b_2^a$, où $b_1^a \in A_{i+1}$ par normalité de la série centrale inférieure de A. On a d'autre part $b_2^a = b_2[b_2, a] \in (A_i \cap B)A_{i+1} = A_{i+1}(A_i \cap B)$. Le groupe $A_{i+1}(A_i \cap B)$ est donc normal dans A_i.

On peut donc définir l'homomorphisme de groupes qui suit :

$$\begin{array}{rccc} \pi : & \dfrac{A_i}{A_{i+1}(A_i \cap B)} & \longrightarrow & \dfrac{BA_i}{BA_{i+1}} \\ & \overline{a} & \longmapsto & \overline{a}. \end{array}$$

Cet homomorphisme associe à la classe d'un élément de A_i dans le premier quotient sa classe dans le second quotient. Il est bien défini car $A_{i+1}(A_i \cap B) \leqslant BA_{i+1}$. D'autre part, cet homomorphisme est surjectif : si ba est un élément de BA_i, alors sa classe est celle de a puisque $b \in B \leqslant BA_{i+1}$. Finalement, BA_i/BA_{i+1} est de type fini comme quotient du groupe de type fini $A_i/A_{i+1}(A_i \cap B)$, en utilisant le théorème **1.1.15**. On peut également montrer, et cela nous sera utile par la suite, que l'homomorphisme π est injectif : en effet, si la classe $\overline{\alpha}$ d'un élément α de A_i est dans le noyau de π, on a $\alpha \in BA_{i+1}$. Il s'écrit donc $\alpha = ba$, où $a \in A_{i+1}$ et $b = \alpha a^{-1} \in B \cap A_i$. La classe de α dans le quotient $A_i/A_{i+1}(A_i \cap B)$ est donc celle de 1 également. On a donc montré en fait l'isomorphisme des deux quotients considérés :

$$\frac{BA_{i-1}}{BA_i} \simeq \frac{A_{i-1}}{A_i(A_{i-1} \cap B)}.$$

La combinaison de celui-ci avec l'hypothèse de récurrence, qui affirme que

$$\left(\frac{BA_{i-1}}{BA_i}\right)^{m^{i-1}} \simeq 1,$$

nous donne la relation suivante :

$$\frac{A_{i-1}^{m^{i-1}}}{A_i(A_{i-1}\cap B)} \simeq 1,$$

ce qui se traduit par l'inclusion $A_{i-1}^{m^{i-1}} \leqslant A_i(A_{i-1}\cap B)$.

D'autre part, nous avons déjà vu que A/BA_2 est d'exposant divisant m. Cela implique que $A^m \leqslant BA_2$.
Les deux inclusions que nous venons de montrer nous permettent d'établir que

$$\left[A_{i-1}^{m^{i-1}}, A^m\right] \leqslant \left[A_i(A_{i-1}\cap B), BA_2\right].$$

Si l'on choisit des éléments $\alpha \in A_i$, $\beta \in A_{i-1}\cap B$, $\gamma \in B$ et $\delta \in A_2$, on a, à l'aide des relations sur les commutateurs données dans la propriété **1.2.8** :

$$[\alpha\beta, \gamma\delta] = [\alpha,\delta]^{\beta}[\alpha,\gamma]^{\delta\beta}[\beta,\delta][\beta,\gamma]^{\delta}.$$

Or, $[\alpha,\delta]$ et $[\alpha,\gamma]$ ainsi que leurs conjugués appartiennent clairement à A_{i+1}. De plus, $[\beta,\delta]$ appartient à $[A_{i-1}, A_2]$ dont on peut montrer par les mêmes relations sur les commutateurs qu'il est inclus dans A_{i+1}. Enfin, $[\beta,\gamma]$ est un élément à la fois de B et de A_i. Notons-le b. Alors $b^{\delta} = b[b,\delta]$, où le commutateur impliqué appartient à A_{i+1}. Finalement, on a ainsi montré que

$$\left[A_{i-1}^{m^{i-1}}, A^m\right] \leqslant BA_{i+1},$$

et donc que

$$A_i^{m^i} \leqslant BA_{i+1},$$

d'où il découle que l'exposant de BA_i/BA_{i+1} divise m^i. Le facteur en question est donc fini et la récurrence est prouvée, ainsi que le lemme. □

De ce lemme on déduit, avec le théorème de Lagrange **1.1.2**, que $|A : B| = |A : BA_2| \cdot |BA_2 : BA_3| \cdot \ldots \cdot |BA_s : B|$, où s est la classe de nilpotence de A, est lui aussi fini. Le nombre de classes dans A modulo $B = A\cap H$ est donc fini, ce qui implique que pour tout élément a de A, il existe un entier k tel que $a^k \in B$. En particulier, il existe k_0 tel que $(xy)^{k_0} \in A\cap H \leqslant H$. On a donc prouvé que $xy \in \sqrt{H}$, et ainsi que $\sqrt{H}$ est un groupe.

Montrons à présent qu'il constitue une clôture divisible de H. Pour cela, vérifions les trois axiomes de la définition **3.2.1**.

1. Le groupe $\sqrt{H}$ est nilpotent et sans torsion comme sous-groupe de G. Il appartient donc à la même classe que H. De plus, $\sqrt{H}$ est divisible. En effet, si h appartient à $\sqrt{H}$ et si n est un entier naturel, alors il existe k tel que $h^k \in H$. G étant divisible, il existe un élément g tel que $g^n = h$; il suffit alors de montrer que $g \in \sqrt{H}$. Cela est évident puisque $(g^n)^k \in H$. Le groupe $\sqrt{H}$ est effectivement divisible.
2. Le plongement de groupe est l'inclusion naturelle : $H \hookrightarrow \sqrt{H}$. En effet, il est évident que $H \leqslant \sqrt{H}$.
3. Le troisième axiome est vérifié par définition de $\sqrt{H}$, en précisant simplement que $id(H) = H$.

D'où la conclusion du théorème. ⊠

3.2.3 Relations entre les hypercentres de H et de $\sqrt{H}$

Il se trouve que les hypercentres d'un sous-groupe H et de son radical $\sqrt{H}$, telle qu'il est défini dans le théorème précédent, au sein d'un groupe G divisible, sont reliés de la façon suivante :

Théorème 3.2.7
Avec les notations du théorème **3.2.4**, *nous avons*

$$\zeta_i(\sqrt{H}) = \sqrt{\zeta_i H} \quad et \quad \zeta_i H = H \cap \sqrt{\zeta_i H}.$$

Démonstration — Pour simplifier, nous utiliserons la notation suivante : $H_i = \zeta_i H$. Raisonnons par récurrence sur i pour établir le théorème. Lorsque $i = 0$, les égalités sont triviales.
Supposons qu'elles soient vraies au rang i. Soit $x \in \zeta_{i+1}(\sqrt{H})$. Il existe un entier naturel m vérifiant $x^m \in H$. Cela implique évidemment que $[x^m, H] \leqslant H$. On a en outre $[x^m, H] \leqslant [x^m, \sqrt{H}] \leqslant \zeta_i(\sqrt{H})$. L'utilisation des deux parties de l'hypothèse de récurrence permet d'en déduire que

$$[x^m, H] \in H \cap \sqrt{H_i} = H_i.$$

C'est alors la remarque **1.3.16** qui implique que $x^m \in H_{i+1}$. Cela revient à dire que $x \in \sqrt{H_{i+1}}$, et donc que $\zeta_{i+1}(\sqrt{H}) \leqslant \sqrt{H_{i+1}}$.

La réciproque est vraie aussi : montrer que $\sqrt{H_{i+1}} \leqslant \zeta_{i+1}(\sqrt{H})$ revient à montrer, d'après le lemme qui précède, que $\sqrt{H_{i+1}}$ et $\sqrt{H}$ commutent modulo $\sqrt{H_i}$.
Soient $x \in \sqrt{H}$ et $y \in \sqrt{H_{i+1}}$. On peut trouver $m, n \in \mathbb{N}$ tels que $x^m \in H$ et $y^n \in H_{i+1}$. La série des H_i étant en particulier centrale, on a $[H, H_{i+1}] \leqslant H_i$. Cela signifie que x^m et y^n commutent modulo H_i, et donc modulo $\sqrt{H_i}$

puisque $H_i \leqslant \sqrt{H_i}$. On a donc $x^m y^n = y^n x^m$ dans $\sqrt{H}/\sqrt{H_i}$, groupe qui est sans torsion comme facteur de la série centrale supérieure d'un groupe sans torsion (proposition **2.5.11**). La propriété **2.5.10** implique qu'alors $xy = yx$ modulo $\sqrt{H_i}$, ce qui confirme l'inclusion $\sqrt{H_{i+1}} \leqslant \zeta_{i+1}(\sqrt{H})$, et donc l'égalité de ces deux ensembles.

Il reste à montrer que $H \cap \sqrt{H_{i+1}} = H_{i+1}$. Choisissons un élément x dans l'intersection $H \cap \sqrt{H_{i+1}}$. Il existe un entier m correspondant tel que $x^m \in H_{i+1}$. Alors x^m commute avec tous les éléments de H modulo H_i (remarque **1.3.16**) ce qui implique, comme ci-dessus, que x commute avec tout élément de H modulo H_i (proposition **2.5.11** et propriété **2.5.10**). Cela signifie, toujours avec le même lemme, que $x \in H_{i+1}$, d'où $H \cap \sqrt{H_{i+1}} \leqslant H_{i+1}$. L'autre inclusion étant évidente, on a prouvé la récurrence et, par là même, le théorème. ⊠

Le résultat central de ce paragraphe en découle immédiatement :

Corollaire 3.2.8
Les sous-groupes H et $\sqrt{H}$ de G ont même classe de nilpotence.

3.3 Existence et unicité de la clôture divisible

Jusqu'à présent, nous n'avons montré ni l'existence, ni l'unicité d'une clôture divisible d'un groupe G dans une classe de groupes quelconque. Notre objectif est ici de montrer à la fois son existence et son unicité, dans la classe particulière des groupes nilpotents sans torsion.

3.3.1 Unicité à isomorphisme près de la clôture divisible d'un groupe nilpotent sans torsion.

Intéressons-nous pour commencer à l'unicité d'une clôture divisible, dans le cadre des groupes nilpotents sans torsion. On n'impose pas ici que le groupe soit *de type fini*, hypothèse que l'on retrouvera dans le paragraphe suivant, au travers des coordonnées de Mal'cev.

Montrons donc le théorème suivant :

Théorème 3.3.1
Deux clôtures divisibles d'un groupe G dans la classe des groupes nilpotents sans torsion sont isomorphes.

Démonstration — Soient G_1 et G_2 des copies isomorphes de G, et soit $\varphi : G_1 \longrightarrow G_2$ un isomorphisme entre ces deux copies. Notons $\overline{G_1}$ et $\overline{G_2}$

deux clôtures divisibles, de G_1 et G_2 respectivement, dans la classe des groupes nilpotents et sans torsion. Le plongement associé est évidemment l'identité. Notons $P = \overline{G_1} \times \overline{G_2}$, divisible et sans torsion comme produit direct de groupes divisibles et sans torsion. Considérons son sous-groupe $D = \{(x, \varphi(x)) \,|\, x \in G_1\}$ et plus précisément son radical $\sqrt{D}$ dans P.

Appelons $\pi_i : P \longrightarrow \overline{G_i}$ la projection de P sur $\overline{G_i}$, $i = 1, 2$, et $\pi_{i|_{\sqrt{D}}}$ sa restriction à $\sqrt{D}$. Ces projections constituent de toute évidence des homomorphismes de groupes, puisqu'elles sont définies par $\pi_1(x, y) = x$ et $\pi_2(x, y) = y$. Montrons qu'elles sont injectives : choisissons un élément $x = (x_1, x_2)$ de $\sqrt{D}$ vérifiant $\pi_{1|_{\sqrt{D}}}(x) = 1_{\overline{G_1}}$. Cela implique directement que $x_1 = 1$. Montrons qu'alors on a aussi $x_2 = 1$. On peut choisir un entier m vérifiant $x^m = (x_1^m, x_2^m) \in D$. Or, cela signifie exactement que $x_2^m = \varphi(x_1^m) = \varphi(1) = 1$, ce qui implique que $x_2 = 1$, puisque $\overline{G_2}$ est sans torsion.
Choisissons x vérifiant $\pi_{2|_{\sqrt{D}}}(x) = 1_{\overline{G_2}}$. Cela équivaut à dire que $x_2 = 1$. Mais alors, comme précédemment, on peut trouver m tel que $x^m = (x_1^m, x_2^m) \in D$. En d'autres termes, on a alors $x_1^m = \varphi^{-1}(x_2^m) = 1$. $\overline{G_1}$ étant sans torsion, on peut alors affirmer que x_1 vaut 1.
On a finalement, dans les deux cas, $x = (1, 1) = 1_{\sqrt{D}}$, c'est-à-dire que $\pi_{1|_{\sqrt{D}}}$ et $\pi_{2|_{\sqrt{D}}}$ sont injectifs et constituent deux plongements, de $\sqrt{D}$ dans $\overline{G_1}$ et $\overline{G_2}$ respectivement.

Il découle alors des propriétés d'un morphisme de groupes que $\pi_1(\sqrt{D})$ est divisible. Comme évidemment $\pi_1(D) \leqslant \pi_1(\sqrt{D})$, on a aussi une première inclusion : $\sqrt{\pi_1(D)} \leqslant \pi_1(\sqrt{D})$. D'autre part, si $y \in \pi_1(\sqrt{D})$, alors il existe un unique $x \in \sqrt{D}$ vérifiant $y = \pi_1(x)$, et un entier m correspondant tel que $x^m \in D$. Par conséquent, $y^m = \pi_1(x)^m = \pi_1(x^m) \in \pi_1(D)$, d'où $y \in \sqrt{\pi_1(D)}$, et enfin l'égalité

$$\pi_1(\sqrt{D}) = \sqrt{\pi_1(D)}.$$

Étant donné que $\pi_1(D) = G_1$, on déduit de l'égalité précédente que

$$\overline{G_1} = \sqrt{\pi_1(D)} = \pi_1(\sqrt{D}).$$

Par un raisonnement symétrique, on arrive au résultat suivant :

$$\overline{G_2} = \sqrt{\pi_2(D)} = \pi_2(\sqrt{D}).$$

Les applications π_1 et π_2 se trouvent donc être, au final, deux isomorphismes.

L'isomorphisme recherché, de $\overline{G_1}$ sur $\overline{G_2}$, est donc donné par

$$\psi = \pi_{2|_{\sqrt{D}}} \circ \pi_{1|_{\sqrt{D}}}^{-1}.$$

Ceci conclut la démonstration : la clôture divisible d'un groupe G nilpotent sans torsion est unique à isomorphisme près. ⊠

Cette démonstration donne en fait un résultat plus fort :

Théorème 3.3.2
Soit G un groupe nilpotent sans torsion. Étant données deux clôtures divisibles $\overline{G_1}$ et $\overline{G_2}$ de ce groupe, alors tout automorphisme φ de G donne lieu à un isomorphisme entre $\overline{G_1}$ et $\overline{G_2}$ qui prolonge φ.

Il suffit, dans la démonstration précédente, de faire coïncider G_1 avec G et G_2 avec $\varphi(G)$. Le fait que ψ soit alors un prolongement de φ est immédiat.

3.3.2 Existence pour un groupe nilpotent de type fini sans torsion

Soit G un groupe nilpotent de classe s, de type fini, et sans torsion. Soit $a = (a_1, \ldots, a_n)$ une base de Mal'cev de G, et $t = (t_1, \ldots, t_n)$ les fonctions coordonnées de Mal'cev associées à cette base. On notera $x = a^{t(x)}$. De plus, on notera pour tout $\tau \in \mathbb{Z}^n$:

$$a^\tau := a_1^{\tau_1} \cdots a_n^{\tau_n}.$$

Le symbole $\mathbb{Q}$ désigne comme à l'ordinaire le corps des nombres rationnels. On a montré en **3.1.2** que les coordonnées de Mal'cev d'un produit et d'une puissance m d'éléments de G se trouvent être des polynômes en les coordonnées des éléments de départ et en m. Soient $\xi_1, \ldots, \xi_n$ des fonctions polynomiales à coefficients rationnels et à $2n$ variables telles que

$$x \cdot y = a_1^{\xi_1(t(x),t(y))} \ldots a_n^{\xi_n(t(x),t(y))}, \quad \forall\, x, y \in G.$$

De même, soient $\omega_1, \ldots, \omega_n$ des fonctions polynomiales à coefficients rationnels et à $(n+1)$ variables telles que

$$x^m = a_1^{\omega_1(m,t(x))} \ldots a_n^{\omega_n(m,t(x))}, \quad \forall\, x \in G, \forall\, m \in \mathbb{Z}.$$

L'existence de ces fonctions polynomiales est assurée par la propriété **3.1.5**. Ainsi, $\xi_i = \xi_i(t(x), t(y))$ est en fait un polynôme en les coordonnées de Mal'cev de ses deux arguments : $\xi_i = \xi_i\,(t_1(x), \ldots, t_n(x), t_1(y), \ldots, t_n(y))$, tandis que $\omega_i = \omega_i(m, t(x))$ s'écrit comme un polynôme en m et en les coordonnées de Mal'cev de x : $\omega_i = \omega_i\,(m, t_1(x), \ldots, t_n(x))$.

Après ces quelques précisions, nous pouvons nous atteler à la construction de la clôture divisible de G. Définissons $\overline{G}$ comme l'ensemble des produits formels a^τ où les composantes $\tau_1, \ldots, \tau_n$ de τ sont des éléments de $\mathbb{Q}$. Sur cet ensemble, on définit la multiplication et l'élévation à une puissance arbitraire $m \in \mathbb{Q}$ à l'aide des polynômes $(\xi_i)_{i=1,\ldots,n}$ et $(\omega_i)_{i=1,\ldots,n}$. On pose ainsi

$$\begin{aligned} xy &= a_1^{\xi_1(t(x),t(y))} \cdots a_n^{\xi_n(t(x),t(y))} \quad \in \overline{G} \\ x^m &= a_1^{\omega_1(t(x),m)} \cdots a_n^{\omega_n(t(x),m)} \quad \in \overline{G}. \end{aligned}$$

L'ensemble $\mathbb{Q}$ étant un corps, les polynômes rationnels évalués en des nombres rationnels restent dans $\mathbb{Q}$. De plus, $G \hookrightarrow \overline{G}$ car $\mathbb{Z} \subset \mathbb{Q}$.
Avec cette définition de la multiplication, $\overline{G}$ se trouve muni d'une structure de groupe : les axiomes à vérifier s'expriment par des identités polynomiales satisfaites par $\xi_1, \ldots, \xi_n, \omega_1, \ldots, \omega_n$. Considérons par exemple l'associativité de la multiplication dans G : on a

$$\begin{aligned}(xy)z &= \left(a_1^{\xi_1(t(x),t(y))} \ldots a_n^{\xi_n(t(x),t(y))}\right) a_1^{t_1(z)} \ldots a_n^{t_n(z)} \\ &= a_1^{\xi_1(\xi(t(x),t(y)),t(z))} \ldots a_n^{\xi_n(\xi(t(x),t(y)),t(z))}\end{aligned}$$

et

$$x(yz) = a_1^{\xi_1(t(x),\xi(t(y),t(z)))} \ldots a_n^{\xi_n(t(x),\xi(t(y),t(z)))}.$$

Or, les polynômes $\xi_i(\xi(T,T'),T'')$ et $\xi_i(T,\xi(T',T''))$ sont égaux sur les entiers car, dans G, la multiplication est associative. T, T' et T'' désignent chacun n indéterminées, et ξ désigne $(\xi_1, \ldots, \xi_n)$. Ces polynômes ont une infinité de racines communes, ils sont donc égaux, d'où l'associativité de la multiplication de $\overline{G}$.

Définissons à présent $\overline{G_i}$ comme l'ensemble des élément a^τ de $\overline{G}$ vérifiant $t_1 = t_2 = \cdots = t_{i-1} = 0$. Alors

$$\overline{G} = \overline{G_1} > \overline{G_2} > \cdots > \overline{G_{n+1}} = 1 \tag{3.5}$$

est une série centrale de $\overline{G}$: en effet, si l'on choisit des éléments $g \in \overline{G}$ et $g_i \in \overline{G_i}$, les coordonnées de Mal'cev du commutateur $[g_i, g]$ sont polynomiales en les coordonnées de Mal'cev de g, de g_i et de leurs inverses :

$$t_j([g_i,g]) = P_j(t(g), t(g_i), t(g^{-1}), t(g_i^{-1})).$$

Or, pour $h \in G$ et $h_i \in G_i$, on a $[h_i, h] \in G_{i+1}$, c'est-à-dire que les i premières coordonnées de ce commutateur sont nulles. En d'autres termes, le polynôme P_j est nul, pour $j \leqslant i$, lorsque ses arguments sont entiers. On en conclut donc que ces polynômes P_j sont identiquement nuls. Le commutateur $[g_i, g]$ a donc ses i premières coordonnées nulles, et appartient à $\overline{G_{i+1}}$. On a ainsi montré que $[G, G_i] \leqslant G_{i+1}$, c'est-à-dire que la série est centrale. En outre, cette série (3.5) est telle que chacun de ses facteurs $\overline{G_{i-1}}/\overline{G_i}$ soit isomorphe au groupe additif sous-jacent à $\mathbb{Q}$.

Puisqu'il admet une série centrale finie, le groupe $\overline{G}$ est nilpotent. Il est également sans torsion : l'égalité $x^m = 1$ signifie que $\omega_i(m, t(x)) = 0$ pour tout i allant de 1 à n. Or, on sait de par la propriété **3.1.5** que $\omega_i(m, t(x)) = mt_i(x) + Q(x)$ où Q est un polynôme rationnel en les coordonnées de Mal'cev de x, de rang stictement inférieur à i. On en déduit donc que si $\omega_i(m, t(x)) = 0$

pour tout i de 1 à n, alors on a $m = 0$ ou $t_i(x) = 0$ pour tout i, de quoi découle qu'alors m est nul ou x est l'élément neutre. $\overline{G}$ est donc effectivement sans torsion.

Nous avons donc montré que $G \subset \overline{G}$. Il reste à prouver que le radical $\sqrt{G}$ de G dans $\overline{G}$ se confond avec $\overline{G}$. On sait que, pour tout i, $a_i^{p/q} \in \sqrt{G}$ car $\left(a_i^{p/q}\right)^q = a_i^p \in G$. Tout produit de tels éléments appartient alors à $\sqrt{G}$, d'où $\overline{G} \subset \sqrt{G}$.

Finalement, $\overline{G} = \sqrt{G}$ et $\overline{G}$ est nilpotent de même classe que G d'après le corollaire **3.2.8** de la partie précédente. $(\overline{G}, id)$ est donc une clôture divisible de G dans la classe des groupes nilpotents de classe s sans torsion.

3.3.3 Existence pour un groupe nilpotent sans torsion

Le groupe G considéré reste toujours nilpotent et sans torsion. Considérons l'ensemble $\mathcal{E}$ des symboles formels $\sqrt[m]{g}$, où g appartient au groupe G, et $m = 1, 2, \ldots$. On munit cet ensemble de la relation d'équivalence suivante :

$$\sqrt[m]{g} \sim \sqrt[n]{g_1} \quad \Leftrightarrow \quad g^n = g_1^m \quad \text{dans } G.$$

Notons $\overline{G}$ l'ensemble des classes d'équivalence de cette relation. On munit G d'une structure de groupe en multipliant $\sqrt[m]{g}$ et $\sqrt[n]{g_1}$, ou plus exactement leurs classes, de la même manière que ces éléments seraient multipliés dans la clôture divisible de $\langle g, g_1 \rangle$. Ce dernier groupe étant de type fini, on a déjà montré qu'il admet une clôture divisible unique à isomorphisme près. On peut donc en quelque sorte *transposer* sa loi dans $\overline{G}$, pour multiplier entre eux les éléments correspondants.

Muni de cette loi, $\overline{G}$ est un groupe. Montrons par exemple l'associativité de la loi : soient x, y et z dans $\overline{G}$. On a

$$\begin{aligned} x &= \sqrt[n_1]{x_1} \\ y &= \sqrt[n_2]{y_1} \\ z &= \sqrt[n_3]{z_1}. \end{aligned}$$

Le produit xy est effectué dans $\sqrt{\langle x_1, y_1 \rangle}$: il existe α_1 et m_1 tels que $xy = \sqrt[m_1]{\alpha_1}$. Le produit $(xy)z$ est quant à lui calculé dans le radical de $\langle \alpha_1, z_1 \rangle$: $(xy)z = \sqrt[m_2]{\alpha_2}$. De la même manière, on peut écrire $x(yz) = \sqrt[l_2]{\beta_2}$ dans $\sqrt{\langle x_1, \beta_1 \rangle}$.
Or, $\alpha_1 \in \langle x_1, y_1 \rangle$, donc $\langle \alpha_1, z_1 \rangle \leqslant \langle x_1, y_1, z_1 \rangle$. De même, $\langle x_1, \beta_1 \rangle \leqslant \langle x_1, y_1, z_1 \rangle$. Les radicaux suivent évidemment les mêmes inclusions. Or, dans le groupe divisible $\sqrt{\langle x_1, y_1, z_1 \rangle}$, $(xy)z = x(yz)$ par associativité de la loi de ce groupe.

La loi introduite sur $\overline{G}$ est donc elle aussi associative. L'existence dans $\overline{G}$ d'un inverse pour tout élément se montre de la même manière.

$\overline{G}$ est divisible par définition : supposons que $x \in \overline{G}$ et $m \in \mathbb{N}$. Alors il existe $g \in G$, $n \in \mathbb{N}$ tels que $x = \sqrt[n]{g}$, c'est-à-dire que $x^n \in G$. On note alors $y = \sqrt[mn]{g} \in \overline{G}$ (on travaille évidemment sur les classes d'équivalence, sans pour autant le noter explicitement, afin d'alléger la notation). Or, on a $y^{mn} = g = x^n$, ce qui implique en particulier, par définition de la relation d'équivalence, que $y^m = x$. Cela prouve que $\overline{G}$ est divisible.

À proprement parler, on ne peut pas dire que $G \leqslant \overline{G}$. Mais on a évidemment $G \subset \mathcal{E}$. On peut donc choisir comme plongement de G dans $\overline{G}$ la projection $\phi : G \subset \mathcal{E} \longrightarrow \overline{G}$, qui à tout élément associe sa classe d'équivalence dans $\overline{G}$.

De plus, il est relativement clair que le radical $\sqrt{G}$ de G dans $\overline{G}$ s'identifie à $\overline{G}$. Le corollaire **3.2.8** donne alors l'égalité des classes de nilpotence de G et de $\sqrt{G} = \overline{G}$. $(\overline{G}, \phi)$ est ainsi une clôture divisible de G dans la classe des groupes nilpotents de classe s, sans torsion.

Concluons ce chapitre avec son résultat principal :

Théorème 3.3.3
Dans la classe des groupes nilpotents de classe s et sans torsion, tout groupe admet une clôture divisible, unique à isomorphisme près.

C'est à cette clôture divisible que l'on donne le nom de **complété de Mal'cev**, du nom du mathématicien qui, le premier, en donna la méthode de construction.

Chapitre 4

Plongement des groupes nilpotents de type fini dans les groupes linéaires

4.1 Plongement d'un groupe nilpotent de type fini sans torsion dans $GL_n(\mathbb{Z})$

L'objectif premier de cette partie est de montrer l'existence, pour un groupe nilpotent G de type fini sans torsion donné, d'un plongement de G dans un groupe linéaire à coefficients entiers, $GL_n(\mathbb{Z})$. Nous montrerons également que ce plongement est polynomial, d'inverse linéaire, selon les définitions données en **3.1.1**.

4.1.1 Action de groupe

Définissons pour commencer ce qu'est une *action de groupe*.

Définition 4.1.1
Une action *du groupe G sur un ensemble $\mathcal{E}$ est un homomorphisme de groupes :*

$$\begin{array}{rccc} \widehat{\cdot}: & G & \longrightarrow & \mathfrak{S}(\mathcal{E}) \\ & g & \longmapsto & \widehat{g} \end{array}$$

où $\mathfrak{S}(\mathcal{E})$ est le groupe des bijections de $\mathcal{E}$.

Sans nous étendre sur les notions associées à celle-ci, rappelons tout de même la définition suivante :

Définition 4.1.2
*L'*orbite *de $x \in \mathcal{E}$ désigne l'ensemble $\{\widehat{g}(x) \,|\, g \in G\}$.*

Soit G nilpotent de type fini et sans torsion, et choisissons une base de Mal'cev $(a_1, \ldots, a_s)$ pour G. Afin de définir une action de ce groupe, reprenons la notation $\mathbb{Q}[T] = \mathbb{Q}[T_1, \ldots, T_s]$ pour désigner l'anneau des polynômes sur $\mathbb{Q}$ en s indéterminées. Notons $\mathrm{Aut}_{\mathcal{A}}(\mathbb{Q}[T])$ le groupe des automorphismes de l'anneau $\mathbb{Q}[T]$. Un *automorphisme d'anneaux* se distingue d'un automorphisme de groupes en ce qu'il est compatible, non seulement avec la loi du groupe sous-jacent, mais aussi avec la loi multiplicative propre à l'anneau.

Définissons le plongement suivant, qui en fait se résume à une action de groupe :

$$\begin{array}{rccc} \widehat{\cdot}\ : & G & \longrightarrow & \mathrm{Aut}_{\mathcal{A}}(\mathbb{Q}[T]) \\ & g & \longmapsto & \widehat{g}, \end{array}$$

où $\widehat{g} : \mathbb{Q}[T] \longrightarrow \mathbb{Q}[T]$ est l'homomorphisme d'anneaux défini en spécifiant $\widehat{g}(T_i)$ pour $i = 1, \ldots, s$:

$$\widehat{g}(T_i)(t_1(x), \ldots, t_s(x)) = t_i(xg), \quad \forall\, x \in G.$$

Ceci définit bien $\widehat{g}(T_i) \in \mathbb{Q}[T]$ car on a montré, avec la propriété **3.1.5**, que $t_i(xg) = t_i(x) + t_i(g) + P(t(x), t(g))$, où P est un polynôme en les coordonnées de Mal'cev de x et de g. En fait $\widehat{g}(T_i) = T_i + P(T, t(g)) + t_i(g) \in \mathbb{Q}[T]$.
Montrons que $\widehat{\cdot}$ définit un homomorphisme de groupes. On a, pour tout élément x de G :

$$\begin{aligned} \widehat{gh}(T_i)(t_1(x), \ldots, t_s(x)) &= t_i(x(gh)) \\ &= t_i((xg)h) \\ &= \widehat{h}(T_i)(t_1(xg), \ldots, t_s(xg)) \\ &= \widehat{h}(T_i)(\widehat{g}(T_1)(t(x)), \ldots, \widehat{g}(T_s)(t(x))) \\ &= \widehat{g} \circ \widehat{h}(T_i)(t_1(x), \ldots, t_s(x)), \end{aligned}$$

ce qui prouve que $\widehat{\cdot}$ est bien un homomorphisme et que pour tout $g \in G$, $\widehat{g} : \mathbb{Q}[T] \longrightarrow \mathbb{Q}[T]$ est bijective : $\widehat{g} \in \mathrm{Aut}_{\mathcal{A}}(\mathbb{Q}[T])$.
Enfin, $\widehat{\cdot}$ est injective : tout élément g de son noyau vérifie $\widehat{g} = id$, ce qui implique que pour tout i de 1 à s, $\widehat{g}(T_i)(t_1(x), \ldots, t_s(x)) = t_i(x)$, c'est-à-dire $t_i(xg) = t_i(x)$. On a alors $xg = x$, ce qui revient à dire que $g = e$.

4.1.2 Construction du plongement

Donnons à tout élément de $\mathbb{Q}[T]$ de la forme $M(T_1, \ldots, T_s) = T_1^{m_1} \cdots T_s^{m_s}$ le nom de *monôme* en $T_1, \ldots, T_s$.

Les notations de la partie précédente étant conservées, on peut écrire, d'après les résultats de la partie **3.1.2** :

$$\widehat{g}(T_i) = T_i + \sum_j c_{ij}(g) M_{i,j}(T_1, \ldots, T_s), \tag{4.1}$$

où les $c_{ij}(g)$ sont polynomiaux à coefficients dans $\mathbb{Q}$ en les coordonnées de Mal'cev de g, et les $M_{i,j}(T_1, \ldots, T_s)$ apparaissant avec des coefficients non nuls (en nombre fini) sont en fait des monômes en $T_1, \ldots, T_{i-1}$ seulement.

Soit H le sous-groupe (additif et abélien) de $\mathbb{Q}[T]$ engendré par l'orbite de $\{T_1, \ldots, T_s\}$ sous l'action de G, c'est-à-dire par les images des indéterminées $T_1, \ldots, T_s$ par tous les $\widehat{g},\ g \in G$. De la relation (4.1) on déduit que, pour un certain entier N positif, H est contenu dans le sous-groupe K engendré par les $(T_i)_{i=1,\ldots,s}$ et les fonctions $\frac{1}{N}M_{i,j}(T_1, \ldots, T_s)$; K est clairement de type fini, ce qui entraîne que H est également de type fini, en tant que sous-groupe d'un groupe abélien de type fini (théorème **2.6.13**).

Le théorème de décomposition des groupes abéliens de type fini (**2.1.5**), ajouté au fait que H est clairement sans torsion (comme sous-groupe de $\mathbb{Q}[T]$), donne la liberté de H dans la classe des groupes abéliens ou autrement dit comme $\mathbb{Z}$-module. Soit alors $\{h_1, \ldots, h_n\}$ une base de H. On peut alors écrire

$$\forall\, x \in G, \quad \widehat{x}(h_k) = \sum_l \psi_{kl}(x) h_l \quad \in H \subset \mathbb{Q}[T]. \tag{4.2}$$

La matrice $(\psi_{kl}(x))_{kl}$ est la matrice de la restriction de $\widehat{x}$ à H, relativement à la base $\{h_1, \ldots, h_n\}$. On peut ainsi définir l'homomorphisme $\psi : G \longrightarrow GL_n(\mathbb{Z})$ par $\psi(x) = (\psi_{kl}(x))_{kl}$, dont la multiplicativité découle immédiatement de celle de $\widehat{\cdot}$.
De plus, $\psi(x)$ est inversible, par propriété d'homomorphisme, et son inverse est $\psi(x^{-1})$.

La liberté de la base $\{h_1, \ldots, h_n\}$ choisie dans H et l'injectivité de $\widehat{\cdot}$ impliquent directement que l'homomorphisme ψ est injectif : il forme un plongement de G dans le groupe linéaire d'ordre n à coefficients entiers.

4.1.3 Polynomialité du plongement

Montrons à présent que le plongement ψ construit dans la partie précédente est polynomial, et que son inverse est linéaire. On conserve donc toutes les notations précédemment établies. On identifie ici le groupe G à $\mathbb{Z}^s$ à l'aide de ses coordonnées de Mal'cev, et $GL_n(\mathbb{Z})$ à une partie de $\mathbb{Z}^{n^2}$ de manière évidente.

Les indéterminées T_i, $i = 1, \ldots, s$ appartiennent à H : elles s'expriment linéairement en fonction des éléments de la base libre de ce sous-groupe. Donc, pour tout x appartenant à G, sa $i^{\text{ème}}$ coordonnée de Mal'cev $t_i(x)$

dépend linéairement de $h_1(t(x)), \ldots, h_n(t(x))$. D'autre part, on a :

$$\begin{aligned} \forall\, x \in G, \quad h_k(t_1(x), \ldots, t_s(x)) &= h_k(\widehat{x}(T_1)(0), \ldots, \widehat{x}(T_s)(0)) \\ &= h_k(\widehat{x}(T_1), \ldots, \widehat{x}(T_s))(0) \\ &= \widehat{x}(h_k)(0). \end{aligned}$$

Or, la relation fonctionnelle (4.2) nous donne l'égalité suivante :

$$\widehat{x}(h_k)(0) = \sum_l \psi_{kl}(x) h_l(0) \quad \in \mathbb{Q},$$

ce qui montre la linéarité des $h_k(t(x))$ en les entrées $\psi_{kl}(x)$, $l = 1, \ldots, n$. De ceci découle que les fonctions coordonnées $t_i(x)$ sont linéaires en les coefficients de la matrice $(\psi_{kl}(x))_{kl}$. Ainsi, l'inverse de ψ est linéaire.

Montrons enfin que ψ est polynomial, i.e. que les fonctions $\psi_{kl} : G \longrightarrow \mathbb{Q}$ sont en fait les restrictions à G de polynômes à coefficients dans $\mathbb{Q}$.
Soit $x \in G$. Comme h_k est une combinaison linéaire sur $\mathbb{Z}$ de certains $\widehat{g}(T_i)$, $g \in G$, on en déduit que $\widehat{x}(h_k)$ est une combinaison analogue en les $\widehat{xg}(T_i)$, où

$$\widehat{xg}(T_i) = T_i + \sum_j c_{ij}(xg) M_{i,j}(T_1, \ldots, T_s).$$

Par conséquent, il existe des polynômes P_{kj} à coefficients dans $\mathbb{Q}$ tels que

$$\widehat{x}(h_k) = \sum_j P_{kj}(t(x)) M_j(T_1, \ldots, T_s), \tag{4.3}$$

où l'on a renuméroté les monômes $M_{i,j}$ de telle sorte que l'on ait $M_{1,1} = M_1$, $M_{1,2} = M_2$, ... et que les $\{M_j\}_{j=1,2,\ldots}$ soient linéairement indépendants dans $\mathbb{Q}[T]$. En particulier,

$$h_k = \sum_j P_{kj}(0) M_j(T_1, \ldots, T_s). \tag{4.4}$$

Puisque $h_1, \ldots, h_n$ sont linéairement indépendants sur $\mathbb{Q}$, il en est de même pour les lignes de la matrice $(P_{kj}(0))_{kj}$.

En remplaçant, dans (4.2), $\widehat{x}(h_k)$ et h_l par leurs expressions données respectivement par (4.3) et (4.4), on obtient, grâce à l'indépendance linéaire des $M_j(T_1, \ldots, T_s)$, un système d'équations linéaires en les $\psi_{kl}(x)$:

$$P_{kj}(t(x)) = \sum_l \psi_{kl}(x) P_{lj}(0),$$

ce système étant inversible du fait de l'indépendance des lignes de la matrice $(P_{kj}(0))_{kj}$. Les fonctions $\psi_{kl}(x)$ sont donc linéaires en les $P_{kj}(t(x))$, et donc polynomiales en les coordonnées de Mal'cev de x, ce que l'on cherchait à démontrer.

On a ainsi montré le théorème suivant :

Théorème 4.1.3
Tout groupe nilpotent de type fini sans torsion se plonge dans un groupe linéaire à coefficients entiers, au moyen d'un plongement polynomial, dont l'inverse est linéaire.

4.2 Plongement dans $UT_n(\mathbb{Z})$ d'un groupe nilpotent de type fini sans torsion

Montrons à présent un résultat plus fin en poursuivant la preuve précédente :

Théorème 4.2.1
Soit G un groupe nilpotent de type fini sans torsion. Alors il existe un entier positif $n = n(G)$ et un plongement $\phi : G \longrightarrow UT_n(\mathbb{Z})$, tel que ϕ soit une application polynomiale sur G, et que son inverse ϕ^{-1} soit linéaire sur $\phi(G)$.

4.2.1 Matrices unipotentes

Commençons par montrer que les matrices qui constituent le groupe $\psi(G)$ sont toutes *unipotentes*, c'est-à-dire que, si $a \in \psi(G)$, alors il existe un entier naturel r tel que $(a - \mathrm{Id})^r = 0$. Autrement dit, la seule valeur propre de a est 1. Les notations utilisées sont évidemment celles qui ont été introduites et utilisées dans la partie précédente.

Considérons l'endomorphisme d'anneaux $(\widehat{g} - \widehat{e}) \in \mathrm{End}_{\mathcal{A}}(\mathbb{Q}[T])$. D'après la relation (4.1), il envoie chaque monôme $M(T_1, \ldots, T_s)$ soit sur 0, soit sur une combinaison linéaire de monômes strictement inférieurs au monôme de départ. La relation d'ordre prise en compte ici est la suivante :

$$T_1^{m_1} \cdots T_s^{m_s} \; < \; T_1^{n_1} \cdots T_s^{n_s}$$

si pour un certain k on a

$$\begin{array}{rcll} m_i & = & n_i & \text{pour } i > k, \\ \text{et } m_k & < & n_k. & \end{array}$$

En effet,

$$(\widehat{g} - \widehat{e})(T_i) = \sum_j c_{ij}(g) M_{i,j}(T_1, \ldots, T_s).$$

Donc tout monôme $M(T_1, \ldots, T_s)$ est annulé par $(\widehat{g} - \widehat{e})^m$, pour un m assez grand, qui dépend du monôme en question.

En se restreignant au sous-groupe H de $\mathbb{Q}[T]$, de type fini, on obtient ainsi la trivialité de $\left((\widehat{g} - \widehat{e})_{|_H}\right)^k$ pour k assez grand. La seule valeur propre de l'homomorphisme $\widehat{g}$ est donc 1 et les plongements $g \mapsto \widehat{g}$ et $g \mapsto (\psi_{kl}(g))_{kl}$ impliquent que la matrice $(\psi_{kl}(g))_{kl}$ a, elle aussi, 1 comme seule valeur propre. Elle est donc unipotente.

4.2.2 Plongement dans $UT_n(\mathbb{Q})$

Notons à présent $\mathcal{H}$ le sous-groupe $\psi(G)$ qui, comme nous venons de le prouver, est constitué uniquement de matrices unipotentes.

Considérons $GL_n(\mathbb{Q})$ comme le groupe des automorphismes d'un espace vectoriel V de dimension n sur le corps des rationnels, $\mathbb{Q}$. Soit

$$0 = V_0 \ < \ V_1 \ < \ \cdots \ < \ V_m = V \tag{4.5}$$

une série non subdivisible de V telle que V_i soit invariant par $\mathcal{H}$ pour tout $i = 0, \ldots, m$. Précisons qu'être invariant par $\mathcal{H}$ signifie que

$$h(V_i) \subset V_i, \quad \forall\, h \in \mathcal{H} \leqslant GL_n(\mathbb{Q}).$$

L'existence d'une telle série se démontre par récurrence : supposons avoir montré son existence pour tout espace vectoriel de dimension strictement inférieure à n. Deux cas se présentent alors pour l'espace vectoriel V de dimension n : s'il n'existe pas de sous-espace de V stable par $\mathcal{H}$, alors la série $0 < V$ est non subdivisible et constitue la série recherchée. D'autre part, s'il existe un sous-espace W invariant par $\mathcal{H}$, la dimension des espaces W et V/W est strictement inférieure à n. Par hypothèse de récurrence, ils possèdent chacun une série non subdivisible invariante par $\mathcal{H}$, séries desquelles on déduit la série recherchée.

Choisissons une base $\mathcal{B}$ adaptée à cette série, c'est-à-dire que pour chaque terme V_i on peut trouver un ensemble d'éléments de $\mathcal{B}$ formant une base de V_i. Relativement à cette base, tout automorphisme élément de $\mathcal{H}$ s'écrit sous la forme d'une matrice par blocs. En effet, tout automorphisme $h \in \mathcal{H}$ laisse stable chacun des termes V_i de la série ci-dessus. Les blocs sous la diagonale principale sont alors nuls, et le $i^{\text{ème}}$ bloc diagonal est associé à l'action de h sur V_i/V_{i-1}.

Montrons que l'action de $\mathcal{H}$ sur chacun des V_i/V_{i-1} est triviale, c'est-à-dire que tout automorphisme $h \in \mathcal{H}$ vérifie $h_{|_{V_i/V_{i-1}}} = id$. Notons U un facteur du type V_i/V_{i-1} et raisonnons par récurrence sur la classe de nilpotence de $\mathcal{H}$. Supposons que, pour tout groupe nilpotent K de classe inférieure à celle de $\mathcal{H}$, la série non subdivisible correspondante soit composée de facteurs de dimension 1, sur lesquels l'action de K est triviale. Cela est vrai en particulier pour le sous-groupe $[\mathcal{H}, \mathcal{H}]$ de $\mathcal{H}$: la série (4.5) ci-dessus se subdivise en une nouvelle série non subdivisible, dont tous les termes sont laissés invariants par $[\mathcal{H}, \mathcal{H}]$. Par hypothèse de récurrence, tous ses facteurs sont de dimension 1, et l'action de $[\mathcal{H}, \mathcal{H}]$ sur eux est triviale. Les automorphismes éléments de $[\mathcal{H}, \mathcal{H}]$ étant aussi dans $\mathcal{H}$, on a déjà montré que leur matrice est triangulaire supérieure par blocs. Cette nouvelle subdivision donne en plus que, dans une nouvelle base $\mathcal{B}'$, les blocs de la diagonale sont triangulaires supérieurs, et que les éléments de la diagonale sont tous égaux à un. Ceci implique qu'il existe un vecteur non nul u de U qui soit fixé par tout automorphisme élément de $[\mathcal{H}, \mathcal{H}]$.

Notons $\mathcal{U} = \text{Vect}(u \in U \ : \forall\, h \in [\mathcal{H}, \mathcal{H}],\ h(u) = u)$ le sous-espace vectoriel engendré par les vecteurs de U invariants par tout automorphisme de $[\mathcal{H}, \mathcal{H}]$. Ce sous-espace est invariant par $\mathcal{H}$. En effet, si $u \in \mathcal{U}$, $h \in \mathcal{H}$ et $h' \in [\mathcal{H}, \mathcal{H}]$, on a :

$$h'(h(u)) = h \circ h' \circ [h', h](u) = h(u)$$

car h' et $[h', h]$ appartiennent à $[\mathcal{H}, \mathcal{H}]$. Puisque U ne contient pas de sous-espace propre invariant par $\mathcal{H}$, on a $\mathcal{U} = U$, c'est-à-dire que $[\mathcal{H}, \mathcal{H}]$ a une action triviale sur U, ou encore que $\mathcal{H}_{|_U} = \{h_{|_U} \,|\, h \in \mathcal{H}\}$ est un groupe abélien.

Tous les automorphismes de $\mathcal{H}_{|_U}$ commutent, donc ils admettent un vecteur propre commun dans l'espace vectoriel défini sur l'extension de corps obtenue après avoir ajouté les valeurs propres des automorphismes, c'est-à-dire en fait sur $\mathbb{Q}$ puisque les valeurs propres des automorphismes de $\mathcal{H}$ sont toutes égales à 1. Ce vecteur propre commun engendre un sous-espace de dimension 1 qui est laissé stable par $\mathcal{H}$. Or, par définition de la série (4.5), U ne contient pas de sous-espace propre invariant par $\mathcal{H}$. On en déduit donc que U est de dimension 1. De plus, comme $\mathcal{H}$ est formé d'automorphismes unipotents, il est clair que la valeur propre associée au vecteur propre trouvé ne peut être différente de 1, d'où la trivialité de l'action de $\mathcal{H}$ sur U.

On a ainsi montré qu'il existe une matrice $a \in GL_n(\mathbb{Q})$ de changement de base telle que $\mathcal{H}^a \leqslant UT_n(\mathbb{Q})$. Ceci nous donne le plongement suivant

$$\begin{array}{rccc} \psi_1 : & \mathcal{H} & \hookrightarrow & UT_n(\mathbb{Q}) \\ & h & \mapsto & h^a \end{array}$$

de $\mathcal{H}$ dans $UT_n(\mathbb{Q})$. On en déduit finalement que l'isomorphisme $\psi_1 \circ \psi$ constitue un plongement du groupe G nilpotent de type fini sans torsion de départ dans le groupe des matrices triangulaires supérieures à coefficients dans $\mathbb{Q}$, dont la diagonale est unitaire.

Remarque 4.2.2 (Nouvelle démonstration de l'existence de la clôture divisible)
On a montré dans cette partie que tout groupe nilpotent de type fini sans torsion se plonge dans $UT_n(\mathbb{Q})$. Ceci nous permet d'établir une nouvelle démonstration de l'existence de la clôture divisible d'un tel groupe.

Démonstration — Soit G un groupe nilpotent de type fini sans torsion. Les considérations qui précèdent indiquent l'existence d'un entier naturel non nul n et d'un plongement ϕ de G dans $UT_n(\mathbb{Q})$. Notons $\mathcal{H}$ l'image de G par ϕ. $\mathcal{H}$ est un sous-groupe de $UT_n(\mathbb{Q})$, dont on a montré en **2.5** qu'il est divisible. Le théorème **3.2.4** donne alors l'existence d'une clôture divisible de $\mathcal{H}$, que l'on note $\sqrt{\mathcal{H}}$. Alors le couple $(\sqrt{\mathcal{H}}, \phi)$ constitue une fermeture divisible de G. ⊠

4.2.3 Plongement dans $UT_n(\mathbb{Z})$

Toujours en conservant les notations précédentes, nous donnons à présent la preuve de l'existence d'un plongement de G non seulement dans $UT_n(\mathbb{Q})$, mais également dans $UT_n(\mathbb{Z})$.

Le groupe $\mathcal{H}^a$ se trouve être l'image de G par l'isomorphisme $\psi_1 \circ \psi$. Il est donc de type fini comme G. Soit donc un ensemble fini $\mathcal{M}$ de matrices engendrant $\mathcal{H}^a$. Notons N un dénominateur commun de tous les éléments des matrices de $\mathcal{M}$. Appelons b la matrice diagonale dont les éléments sont $1, N, N^2, \ldots, N^{n-1}$. Alors il est évident, avec les calculs qui suivent, que $\mathcal{H}^{ab} \leqslant UT_n(\mathbb{Z})$:

$$\begin{pmatrix} 1 & h_{12} & h_{13} & \cdots & h_{1n} \\ 0 & 1 & h_{23} & \cdots & h_{2n} \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & h_{n-1,n} \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \cdot b = \begin{pmatrix} 1 & Nh_{12} & N^2h_{13} & \cdots & N^{n-1}h_{1n} \\ 0 & N & N^2h_{23} & \cdots & N^{n-1}h_{2n} \\ \vdots & \ddots & N^2 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & N^{n-1}h_{n-1,n} \\ 0 & \cdots & \cdots & 0 & N^{n-1} \end{pmatrix}$$

$$b^{-1} \cdot \begin{pmatrix} 1 & h_{12} & h_{13} & \cdots & h_{1n} \\ 0 & 1 & h_{23} & \cdots & h_{2n} \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & h_{n-1,n} \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \cdot b = \begin{pmatrix} 1 & Nh_{12} & N^2h_{13} & \cdots & N^{n-1}h_{1n} \\ 0 & 1 & Nh_{23} & \cdots & N^{n-2}h_{2n} \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & Nh_{n-1,n} \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

On a donc construit un plongement de G dans $UT_n(\mathbb{Z})$: si l'on note $\psi_2 : \mathcal{H}^a \longrightarrow UT_n(\mathbb{Z})$ défini par $\psi_2(h) = h^b$, alors le plongement en question s'écrit $\phi = \psi_2 \circ \psi_1 \circ \psi$, où ψ_1 et ψ ont été définis précédemment.

D'autre part, les changements de base ψ_1 et ψ_2 ne changent pas le caractère polynomial ou linéaire du plongement ψ ou de son inverse. ϕ est effectivement polynomial, d'inverse linéaire, ce qui achève la démonstration du théorème **4.2.1**.

Exemple de $\mathbf{F}_2/\gamma_3\mathbf{F}_2 \hookrightarrow UT_3(\mathbb{Z})$

Étudions à présent un exemple simple d'un tel plongement. Notons $\mathbf{F}_2$ le groupe librement engendré par deux générateurs, que l'on appelle a et b. On se reportera, pour plus de détails sur les groupes libres, au cinquième chapitre, et plus particulièrement au paragraphe 14 de l'ouvrage commun de Kargapolov et Merzliakov ([1]).

Considérons le quotient du groupe $\mathbf{F}_2$ par le troisième terme de sa SCI :

$$G = \mathbf{F}_2/\gamma_3\mathbf{F}_2.$$

Celui-ci est nilpotent de classe 2 : en effet, $\gamma_3 G = 1$. Le groupe G est donc nilpotent, de type fini comme quotient d'un groupe de type fini, et sans torsion du fait de l'absence de relations dans $\mathbf{F}_2$.

Intéressons-nous à présent à une base de Mal'cev de ce groupe. Tout élément de $\mathbf{F}_2$ s'écrit comme un produit en les générateurs a et b. Notons c le commutateur de a et b, et donnons le lemme suivant :

Lemme 4.2.3
Tout élément g du groupe G peut se mettre de façon unique sous la forme

$$g = a^\alpha b^\beta c^\gamma,$$

où α, β et γ sont des entiers relatifs.

Démonstration — Afin de montrer cette affirmation, considérons les éléments de $\mathbf{F}_2$ comme des *mots* en a, b et leurs inverses, c'est-à-dire comme une succession de ces symboles, et raisonnons sur la *longueur* de ces mots, autrement dit sur le nombre de symboles qu'ils contiennent.

Il est évident que tout mot de longueur 1 se met sous la forme indiquée ci-dessus. Supposons à présent que tout mot de longueur inférieure à l se mette sous cette forme. Soit alors un mot z de $\mathbf{F}_2$, de longueur l. Commençons par noter que, dans le groupe G, le commutateur c commute avec tout élément, par définition de G comme quotient par le troisième terme de la SCI. Écrivons le mot z sous la forme $z_1 x^\varepsilon$, où x vaut soit a, soit b, et ε vaut 1 ou -1. Par

hypothèse de récurrence, on écrit $z_1 = a^{\alpha_1} b^{\beta_1} c^{\gamma_1}$. Traitons le cas $x = a$, la situation alternative étant immédiate par commutativité de c. On a donc $z = a^{\alpha_1} b^{\beta_1} c^{\gamma_1} a^{\varepsilon}$. Comme c commute avec a^{ε}, il est évident que $z = a^{\alpha_1} b^{\beta_1} a^{\varepsilon} c^{\gamma_1}$.

Étant donné que l'on a toujours $xy = yx[x, y]$, on obtient, avec les relations sur les commutateurs, les quatre égalités qui suivent :

$$\begin{aligned} ba &= abc^{-1} \\ ba^{-1} &= a^{-1}bc \\ b^{-1}a &= ab^{-1}c \\ b^{-1}a^{-1} &= a^{-1}b^{-1}c^{-1}. \end{aligned}$$

Celles-ci nous permettent d'affirmer, avec une récurrence simple sur β_1 si celui-ci est positif, ou sur $-\beta_1$ sinon, qu'il existe γ_2, tel que $b^{\beta_1} a^{\varepsilon} = a^{\varepsilon} b^{\beta_1} c^{\gamma_2}$. De ceci on déduit qu'alors $z = a^{\alpha_1 + \varepsilon} b^{\beta_1} c^{\gamma_1 + \gamma_2}$, d'où le résultat attendu.

La famille $\{a, b, c\}$ est en fait une base de Mal'cev de $\mathbf{F}_2/\gamma_3\mathbf{F}_2$, associée à la série polycyclique suivante :

$$\mathbf{F}_2/\gamma_3\mathbf{F}_2 \geqslant \langle b, c\rangle \geqslant \langle c\rangle \geqslant 1.$$

Cette série est sous-normale : $\langle c\rangle$ est normal dans $\langle b, c\rangle$ car $c \in Z(G)$. De plus, $b^g = b[b, g]$ où $b \in \langle b, c\rangle$ et $[b, g] \in \langle b, c\rangle$. Donc $\langle b, c\rangle$ est normal dans G. De ceci découle en outre que que les entiers α, β et γ introduits ci-dessus sont uniquement déterminés par $x \in G$. ⊠

Avec des considérations de la même nature, montrons que

$$a^{\alpha_1} b^{\beta_1} c^{\gamma_1} a^{\alpha_2} b^{\beta_2} c^{\gamma_2} = a^{\alpha_1 + \alpha_2} b^{\beta_1 + \beta_2} c^{\gamma_1 + \gamma_2 + \alpha_2 \beta_1}. \tag{4.6}$$

On a évidemment

$$a^{\alpha_1} b^{\beta_1} c^{\gamma_1} a^{\alpha_2} b^{\beta_2} c^{\gamma_2} = a^{\alpha_1} b^{\beta_1} a^{\alpha_2} b^{\beta_2} c^{\gamma_1} c^{\gamma_2}. \tag{4.7}$$

Résumons les quatre relations évoquées ci-dessus en la suivante :

$$b^{\eta} a^{\varepsilon} = a^{\varepsilon} b^{\eta} c^{-\eta\varepsilon}, \quad \varepsilon, \eta \in \{-1, 1\}.$$

Si l'on note $b^{\beta_1} = (b^{\eta})^{|\beta_1|}$ et $a^{\alpha_2} = (a^{\varepsilon})^{|\alpha_2|}$, où η et ε valent 1 ou -1 en fonction du signe de α_1 et β_1, cette égalité nous permet d'affirmer que

$$(b^{\eta})^{|\beta_1|} \cdot (a^{\varepsilon})^{|\alpha_2|} = a^{\varepsilon} \cdot (b^{\eta})^{|\beta_1|} \cdot (a^{\varepsilon})^{|\alpha_2|-1} \cdot (c^{-\varepsilon\eta})^{|\beta_1|},$$

ceci par une récurrence rapide sur $|\beta_1|$. Avec une récurrence analogue sur $|\alpha_2|$, on arrive à

$$(b^{\eta})^{|\beta_1|} \cdot (a^{\varepsilon})^{|\alpha_2|} = (a^{\varepsilon})^{|\alpha_2|} \cdot (b^{\eta})^{|\beta_1|} \cdot (c^{-\varepsilon\eta})^{|\beta_1| \cdot |\alpha_2|},$$

ce qui s'écrit plus simplement :

$$b^{\beta_1}a^{\alpha_2} = a^{\alpha_2}b^{\beta_1}c^{-\beta_1\alpha_2}.$$

En injectant ce résultat dans (4.7), on obtient immédiatement le résultat cherché, énoncé en (4.6).

Or, on remarque que, dans $UT_3(\mathbb{Z})$, on a

$$\begin{pmatrix} 1 & \beta_1 & \gamma_1 \\ 0 & 1 & \alpha_1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \beta_2 & \gamma_2 \\ 0 & 1 & \alpha_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \beta_1+\beta_2 & \gamma_1+\gamma_2+\alpha_2\beta_1 \\ 0 & 1 & \alpha_1+\alpha_2 \\ 0 & 0 & 1 \end{pmatrix},$$

ce qui induit l'isomorphisme (et non seulement le plongement) suivant :

$$\begin{cases} \mathbf{F}_2/\gamma_3\mathbf{F}_2 & \longrightarrow & UT_3(\mathbb{Z}) \\ a^\alpha b^\beta c^\gamma & \longmapsto & \begin{pmatrix} 1 & \beta & \gamma \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix}. \end{cases}$$

4.3 Plongement d'un groupe nilpotent de type fini dans $GL_n(\mathbb{Z})$

Nous cherchons dans cette partie à lever l'hypothèse "sans torsion" que nous avons utilisée jusqu'à présent pour obtenir le plongement d'un groupe nilpotent de type fini dans un groupe linéaire.

Commençons par définir ce qu'est un *anneau de groupe* :

Définition 4.3.1
*L'*anneau du groupe *H sur l'anneau $\mathcal{R}$, noté $\mathcal{R}[H]$, est formé par l'ensemble des combinaisons formelles $r_1h_1 + \cdots + r_sh_s$, où pour tout i, r_i appartient à $\mathcal{R}$ et h_i est un élément de H :*

$$\mathcal{R}[H] := \{r_1h_1 + \cdots + r_sh_s \,|\, s \in \mathbb{N},\, r_i \in \mathcal{R},\, h_i \in H\}.$$

Les lois sur cet anneau sont définies de la manière suivante :

$$\begin{aligned} \sum_i r_ih_i + \sum_i s_ih_i &= \sum_i (r_i+s_i)h_i\,; \\ \sum_i r_ih_i \cdot \sum_j s_jf_j &= \sum_{i,j} r_is_j\, h_if_j. \end{aligned}$$

Définition 4.3.2
On définit également le groupe linéaire à coefficients dans un anneau $\mathcal{A}$ comme l'ensemble des matrices carrées et inversibles à coefficients dans cet anneau $\mathcal{A}$. Il est noté $GL_n(\mathcal{A})$.

Lemme 4.3.3
Soit a une matrice carrée $n \times n$ à coefficients dans un anneau $\mathcal{A}$. Alors $a \in GL_n(\mathcal{A})$ si et seulement si $\det(a) \in \mathcal{U}(\mathcal{A})$, groupe multiplicatif des unités (i.e. des éléments inversibles pour la multiplication) de $\mathcal{A}$.

Démonstration — Supposons qu'une matrice a appartienne à $GL_n(\mathcal{A})$. Alors on a $aa^{-1} = \mathrm{Id}$, ce qui implique par multiplicativité du déterminant que $\det(a) \cdot \det(a^{-1}) = 1$. Le déterminant de la matrice a est donc inversible et appartient de ce fait à $\mathcal{U}(\mathcal{A})$.
Réciproquement, si $\det(a) \in \mathcal{U}(\mathcal{A})$, alors la matrice définie par

$$(\det a)^{-1}\ {}^t\mathrm{com}(a)$$

convient comme inverse de a, et $a \in GL_n(\mathcal{A})$. ⊠

Rappelons que $\mathrm{com}(a)$ désigne la comatrice de la matrice a, tandis que la notation ${}^t a$ se rapporte à la transposée de la matrice a.

Ces définitions étant posées, intéressons-nous au lemme suivant :

Lemme 4.3.4 (Frobenius)
Tout groupe G possédant un sous-groupe H d'indice fini m dans G se plonge dans le groupe linéaire $GL_m(\mathbb{Z}[H])$, où $\mathbb{Z}[H]$ est l'anneau du groupe H sur l'anneau $\mathbb{Z}$.

Démonstration — Soit $\{x_1, \ldots, x_m\}$ un système fixé de représentants des classes de G modulo H. Afin de démontrer le résultat annoncé, introduisons l'action suivante du groupe G sur l'ensemble G/H de ses classes à gauches suivant H :

$$\begin{array}{rccc} \widehat{\cdot}: & G & \longrightarrow & \mathfrak{S}(G/H) \\ & g & \longmapsto & \widehat{g} = \begin{pmatrix} x_1 H & \cdots & x_m H \\ g x_1 H & \cdots & g x_m H \end{pmatrix}. \end{array}$$

La notation parenthésée est celle qui est commune aux permutations. En effet, $\widehat{g}$ appartient au groupe $\mathfrak{S}(G/H)$ des permutations des classes de G : si l'on suppose que $gx_iH = gx_jH$, on est amené d'après les axiomes du groupe G à la conclusion que $x_i = x_j$. Les classes $\{gx_iH\}_{i=1,\ldots,m}$ sont donc effectivement toutes distinctes.

Montrons que l'application $\widehat{\cdot}$ est un homomorphisme de groupes. On a

$$\begin{aligned}
\widehat{g_1} \circ \widehat{g_2} &= \widehat{g_1} \circ \begin{pmatrix} x_1H & \cdots & x_mH \\ g_2x_1H & \cdots & g_2x_mH \end{pmatrix} \\
&= \begin{pmatrix} x_1H & \cdots & x_mH \\ g_1g_2x_1H & \cdots & g_1g_2x_mH \end{pmatrix} \\
&= \widehat{g_1g_2}.
\end{aligned}$$

Cette action de groupe $\widehat{\cdot}$ associe à chaque élément g de G :
- une permutation des représentants $x_1, \ldots, x_m$ des classes de G modulo H, que l'on note π_g,
- des facteurs supplémentaires $\{h_i(g)\}_{i=1,\ldots,m}$ définis par la relation suivante :

$$gx_i = x_{\pi_g(i)}h_i(g).$$

Notons encore $Mat(\pi_g)$ la matrice constituée de zéros et de uns associée naturellement à la permutation π_g dans $\mathfrak{S}_m$, et $diag(\alpha_1, \ldots, \alpha_m)$ pour une matrice dont tous les éléments sont nuls exceptés ceux de la diagonale, qui valent dans l'ordre $\alpha_1, \ldots, \alpha_m$.

Alors l'application

$$\varphi : g \longmapsto Mat(\pi_g) \cdot diag\left(h_1(g), \ldots, h_m(g)\right)$$

définit un homomorphisme de G dans $GL_m(\mathbb{Z}[H])$. En effet, on a

$$\begin{aligned}
x_{\pi_{g_1g_2}(i)}h_i(g_1g_2) &= g_1g_2x_i \\
&= g_1x_{\pi_{g_2}(i)}h_i(g_2) \\
&= x_{\pi_{g_1}\circ\pi_{g_2}(i)}h_{\pi_{g_2}(i)}(g_1)h_i(g_2)
\end{aligned}$$

pour tout i entre 1 et m. Ceci implique que $\pi_{g_1} \circ \pi_{g_2} = \pi_{g_1g_2}$ et que pour tout i, $h_i(g_1g_2) = h_{\pi_{g_2}(i)}(g_1)h_i(g_2)$. Alors

$$\begin{aligned}
\varphi(g_1g_2) &= Mat(\pi_{g_1g_2}) \cdot diag(h_1(g_1g_2), \ldots, h_m(g_1g_2)) \\
&= Mat(\pi_{g_1} \circ \pi_{g_2}) \cdot diag(h_{\pi_{g_2}}(1)(g_1)h_1(g_2), \ldots, h_{\pi_{g_2}(m)}(g_1)h_m(g_2)) \\
&= Mat(\pi_{g_1}) \cdot Mat(\pi_{g_2}) \cdot diag(h_{\pi_{g_2}(i)}(g_1)) \cdot diag(h_i(g_2)) \\
&= Mat(\pi_{g_1}) \cdot diag(h_i(g_1)) \cdot Mat(\pi_{g_2}) \cdot diag(h_i(g_2)) \\
&= \varphi(g_1)\varphi(g_2),
\end{aligned}$$

car

$$Mat(\pi_{g_2}) \cdot diag(h_{\pi_{g_2}(1)}(g_1), \ldots, h_{\pi_{g_2}(m)}(g_1)) \cdot Mat(\pi_{g_2})^{-1} = diag(h_i(g_1)).$$

Cet homomorphisme est de plus injectif, puisque $\varphi(g) = 1$ implique immédiatement que la permutation π_g est triviale et que tous les facteurs supplémentaires $h_i(g)$ sont égaux à 1. On a alors nécessairement $g = 1$, ce qui indique que le noyau de φ est restreint à l'unité. Ceci conclut la démonstration. ⊠

Le plongement φ de G dans $GL_m(\mathbb{Z}[H])$ construit dans la démonstration qui précède est aussi appelé *représentation monomiale du groupe G sur le groupe H*.

Précisons à présent le résultat en ajoutant une hypothèse au lemme précédent, ce qui nous donne le deuxième lemme :

Lemme 4.3.5
Si G est un groupe qui possède un sous-groupe H d'indice fini m et si H se plonge dans un groupe linéaire d'ordre n à coefficients entiers, alors G se plonge dans $GL_{mn}(\mathbb{Z})$.

Démonstration — Notons ι le plongement $H \hookrightarrow GL_n(\mathbb{Z})$. Le plongement convoité découle de celui de G dans $GL_m(\mathbb{Z}[H])$ précédemment obtenu et noté φ. En fait, $\varphi(G)$ est composé uniquement de matrices dont les éléments appartiennent au groupe H. Notons $a = (a_{ij})$ une telle matrice dans $\varphi(G)$, et $\psi(a)$ la matrice d'ordre mn composée de m^2 blocs d'ordre n, chacun d'entre eux constituant l'image par ι de l'élément correspondant dans la matrice a. $\psi(a)$ reste inversible par construction. L'application ψ ainsi définie par $a \mapsto \psi(a)$ permet de définir une nouvelle application

$$\begin{array}{rccc} \mathfrak{p}: & G & \longrightarrow & GL_{mn}(\mathbb{Z}) \\ & g & \longmapsto & \psi \circ \varphi(g). \end{array}$$

On peut vérifier que, puisque φ et ι sont des homomorphismes injectifs, $\mathfrak{p}$ lui-même constitue un plongement, ce qui achève la démonstration de notre second lemme. ⊠

Utilisons à présent le résultat ainsi obtenu pour démontrer le résultat que nous cherchons, à savoir :

Théorème 4.3.6
Tout groupe nilpotent de type fini se plonge dans un groupe linéaire à coefficients entiers.

Nous avons montré dans le théorème **2.6.9** que tout groupe nilpotent de type fini G est presque sans torsion, c'est-à-dire qu'il admet un sous-groupe $H \trianglelefteq G$ d'indice fini m qui est sans torsion.

H est alors un sous-groupe de G nilpotent de type fini. D'après le corollaire **2.6.13** de la page 51, H est donc lui-même de type fini. On a alors un

plongement $H \hookrightarrow GL_n(\mathbb{Z})$ et le résultat en découle : d'après le lemme **4.3.5**, G se plonge alors dans $GL_{mn}(\mathbb{Z})$.

On a finalement montré qu'il est possible de plonger n'importe quel groupe nilpotent de type fini dans un groupe linéaire, et plus précisément dans un groupe de matrices triangulaires supérieures à diagonale unitaire si le groupe en question est sans torsion. Cela permet une étude plus simple de ces groupes qui peuvent être assez complexes à première vue.

Bibliographie

[1] Kargapolov Mikhaïl et Merzliakov Iouri (1985).
Éléments de la théorie des groupes.
Editions Mir, Moscou.

[2] Hall Philip, (1979).
The Edmonton Notes on Nilpotent Groups.
Queen Mary College mathematics notes. Mathematics Department,
Queen Mary College, London.

[3] Baumslag Gilbert, (1971).
Lecture notes on nilpotent groups.
American Mathematical Society, Providence, Rhode Island.

Annexe
Biographie de Mal'cev

Anatoly Ivanovitch Mal'cev
(ou Malcev ou Maltsev)

Né le **27 novembre 1909** à Misheronsky, près de Moscou en Russie ;
Mort le **7 juillet 1967** à Novosibirsk, en URSS.

Le père d'Anatoly Ivanovitch Mal'cev est un souffleur de verre, ce qui laisse penser que son arrière-plan social est celui d'une famille relativement pauvre. Cependant, ses facultés en matière de mathématiques ne tardent pas à se révéler, et ses professeurs à l'école secondaire déjà sont rapidement convaincus de son destin de mathématicien remarquable.

Il étudie à l'université d'État de Moscou, où il est diplômé en 1931, alors qu'il enseigne déjà en parallèle dans une école secondaire. Il continue alors à enseigner dans la ville d'Ivanovo, au Nord-Est de Moscou, tout en retournant régulièrement à la capitale pour y discuter de ses recherches avec Kolmogorov.

Après avoir publié, de son propre chef, différents travaux sur la logique et la théorie des modèles, puis un article sur les plongements d'anneaux dans des corps en réponse à une question de Kolmogorov, Mal'cev écrit en 1937 une dissertation sur les groupes abéliens sans torsion de rang fini. Il étudie ensuite pour sa thèse à l'institut Steklov de l'Académie des Sciences d'URSS, tout en continuant d'enseigner à Ivanovo. C'est en 1941 qu'il obtient le grade de Docteur ès Sciences.

Il devient ensuite, en 1944, Professeur à l'Institut Pédagogique d'Ivanovo, où il continue son travail sur la théorie des groupes, donnant les

preuves d'importants résultats sur les groupes linéaires et en particulier sur les groupes linéaires résolubles. Mal'cev étudie également les groupes de Lie et les algèbres topologiques. C'est pour son travail sur le premier de ces sujets qu'il est récompensé en 1946 par le prix d'État. Il crée en outre une synthèse de la théorie des algèbres et des algorithmes, qu'il nomme "algèbre constructive".

En 1960, Mal'cev est reçu à l'Institut Mathématique de Novosibirsk, et reçoit le titre de président du Département d'Algèbre et de Logique à l'Université d'État de Novosibirsk.

C'est à l'âge de 57 ans que Mal'cev décède, lors de la Conférence de Topologie de Novosibirsk, après y avoir donné sa dernière conférence sur des algèbres que l'on nomme aujourd'hui "algèbres de Mal'cev", et qui constituent une généralisation naturelle des algèbres de Lie.

Index