

Groupes stables et interprétabilité dans les groupes algébriques

Rapport de stage

Arthur Molina-Mounier

Sous la direction de Katrin Tent, Université de Münster (Allemagne)

16 août 2024

Table des matières

1	Introduction	2
2	Introduction mathématique	3
2.1	Bases de théorie des modèles	3
2.2	Rang de Morley et conjecture de Cherlin-Zilber	4
3	Définissabilité dans les groupes réductifs	7
3.1	Cas des corps	7
3.2	Généralisation aux anneaux	9
4	Bi-interprétabilité dans les groupes de Chevalley	13
4.1	Systèmes de racines et groupes de Chevalley	13
4.2	Schéma de groupe de Chevalley-Demazure	14
4.3	Interprétation de R dans $G(R)$	15
4.4	Conséquences de la bi-interprétation	16

1 Introduction

Remerciements : Je tiens à remercier Katrin Tent, mon encadrante pendant ce stage, pour le temps qu'elle m'a accordé, ainsi que pour l'opportunité de découvrir la recherche en théorie des modèles. Je souhaite également remercier toutes les chercheuse·s, étudiant·e·s et doctorant·e·s qui m'ont chaleureusement accueilli et intégré lors de mon court séjour à Münster ; tout particulièrement Davide Carolillo, avec lequel j'ai partagé un bureau. Tous les deux en stage sur le même sujet, nous avons beaucoup travaillé ensemble.

La théorie des modèles est une branche de la logique mathématique qui s'intéresse aux propriétés logiques (i.e caractérisables par des formules mathématiques) des structures étudiées couramment (groupes, anneaux, etc). On y traite par exemple des questions de définissabilité, c'est-à-dire qu'on s'intéresse aux genres de sous-ensembles qu'il est possible de définir dans une structure donnée, via des formules logiques. Ces questions sont fréquemment très complexes, même (et parfois *particulièrement*) pour des structures usuelles. Par exemple, le célèbre 10^e problème de Hilbert est fondamentalement une question portant sur la classe des sous-ensembles de \mathbb{Z} qu'il est possible de définir, en imposant certaines conditions sur les formules utilisées (diophantianité).

En théorie des groupes, c'est la théorie de la stabilité, et du rang de Morley fini, notamment développée par Cherlin et Zilber, qui a émergé, et nombre des problèmes importants du domaine sont encore non résolus. L'approche consiste à étudier les groupes qui respectent des propriétés de rigidité combinatoire fortes, restreignant la complexité de leurs théories, c'est-à-dire limitant ce que les formules logiques sont capables d'exprimer. Malgré le degré d'abstraction de ces restrictions, leurs conséquences sont fortes, et facilement interprétables dans la théorie des groupes, ce qui en fait des objets d'étude très intéressants.

Néanmoins, plusieurs difficultés émergent. D'une part, la théorie (ensemble des formules vraies) de beaucoup de structures usuelles est en fait très mal comprise. Les outils introduits par la théorie de la stabilité, comme le rang de Morley, sont donc difficiles à utiliser en général, sauf sur des structures avec des théories relativement simples. D'autre part, la compréhension des structures stables reste encore extrêmement partielle, avec beaucoup de zones d'ombres concernant la forme de ces objets. Une des plus remarquables est la conjecture de Cherlin-Zilber, qui s'interroge sur la forme des groupes dits de *rang de Morley fini*.

Le stage s'est déroulé du 18 mars au 21 juillet 2024 à l'institut de mathématiques de l'université de Münster. Avant le début du semestre de cours, j'ai assisté à la conférence de recherche de mi-année de l'université. Ne connaissant rien sur la stabilité et seulement les bases de la théorie des modèles au début du stage, la majeure partie a consisté en l'apprentissage du domaine de la stabilité, via le cours *Stable Groups* donné par Katrin Tent elle-même, et en parallèle l'étude des articles [ST21] (dans un premier temps) et [KRT99], qui avaient pour but de me familiariser avec certaines questions de recherches du domaine. Il me fut également nécessaire de consulter des ouvrages et articles (comme [Bor91], [Abe69], [Ste16] ou [Hal15]) pour m'instruire sur la théorie des groupes de Lie, des

groupes algébriques et des groupes de Chevalley, outils centraux que je ne connaissait pas non plus avant ce stage. Dans un second temps, il m'a été confié d'essayer de généraliser les résultats présentés dans [KRT99] : mes résultats sont présentés en seconde partie.

Tout au long du semestre, j'ai également assisté à plusieurs séminaires et présentations autour de la théorie des modèles : le séminaire *Model Theory and Combinatorics* organisé par Martin Hils et Rob Sullivan, le séminaire de recherche du département (*Oberseminar*) et le séminaire informel entre étudiants pré-doctorants (*Unterseminar*).

La première partie est une introduction générale aux questions de stabilité de groupes, avec des rappels de théorie des modèles, où sont présentés les notions importantes du domaine. La seconde partie concerne les résultats établis dans [KRT99], plus précisément un résultat de définissabilité, que je suis parvenu à légèrement généraliser au cours du stage. Enfin, la dernière partie porte sur l'article [ST21], qui prouve, dans un cadre légèrement plus restreint, une propriété beaucoup plus forte de *bi-interprétabilité* dont j'explorerai les conséquences.

2 Introduction mathématique

2.1 Bases de théorie des modèles

On énonce ici quelques notions fondamentales en théorie des modèles. On ne travaillera qu'en logique du premier ordre : toute quantification porte sur des éléments des structures, et non des ensembles d'éléments ou des prédicats.

Définition 2.1.1. Un langage \mathcal{L} est un ensemble de symboles : soit des prédicats, soit des symboles fonctionnels, chacun prenant un nombre fixe et fini d'arguments, son arité (les constantes sont vu comme des symboles fonctionnels d'arité 0).

Exemple 2.1.2. Le langage de la théorie des ensembles est simplement $\mathcal{L}_{\text{ens}} = (\in)$ où \in est un prédicat binaire. Celui des anneaux est $\mathcal{L}_{\text{ann}} = (0, 1, +, \cdot, -)$ où $0, 1$ sont des constantes, $-$ un symbole fonctionnel unaire et $+, \cdot$ des symboles fonctionnels binaires.

Définition 2.1.3. Étant donné un langage \mathcal{L} , une \mathcal{L} -structure \mathcal{M} est la donnée :

- Un ensemble M , parfois appelé "univers".
- Pour chaque prédicat n -aire P , un ensemble $P^{\mathcal{M}} \subseteq M^n$ de tuples d'éléments satisfaisant le prédicat, son interprétation.
- Pour chaque symbole fonctionnel n -aire f , une fonction ensembliste $f^{\mathcal{M}} : M^n \rightarrow M$, également qualifiée d'interprétation. Quand $n = 0$, ceci définit un élément donné de M .

On confond fréquemment \mathcal{M} et M pour alléger les notations. Si M est une \mathcal{L} -structure et $C \subseteq M$ quelconque, on note $\mathcal{L}(C)$ le langage \mathcal{L} auquel on a adjoint des constantes pour chaque élément de C , qu'on interprète par les éléments correspondant.

Exemple 2.1.4. Un ensemble (resp. un anneau) est muni d'une \mathcal{L}_{ens} -structure (resp. une \mathcal{L}_{ann} -structure) naturelle.

Définition 2.1.5. L'ensemble des *termes* du langage \mathcal{L} est construit récursivement :

- Une variable libre est un terme.
- Un symbole fonctionnel appliqué au bon nombre de termes est lui-même un terme (en particulier, les constantes sont toujours des termes).

Alors l'ensemble des \mathcal{L} -formules est défini récursivement ainsi :

- \perp est une formule (désignant le faux).
- Un symbole de prédicat appliqué à des termes de \mathcal{L} est une formule, dite *atomique*.
- Une combinaison booléenne (par \neg , \wedge , \vee) de formules est une formule.
- Si ψ est une formule dans laquelle une variable libre (non quantifiée) x apparaît, alors $\forall x\psi$ et $\exists x\psi$ sont des formules.

Définition 2.1.6. Si φ est une \mathcal{L} -formule et M une \mathcal{L} -structure, on dit que M satisfait φ , noté $M \models \varphi$ si la formule est vraie dans M (dans un sens précis qu'on ne définira pas par souci de concision). Si la formule a des variables libres, elle est satisfaite quand il existe des éléments de M la rendant vraie quand on les remplace.

Une \mathcal{L} -théorie T est un ensemble de \mathcal{L} -formules consistentes (i.e. ne prouvant pas de contradiction). Alors un *modèle* de T est une \mathcal{L} -structure M dans laquelle toutes les formules de T sont satisfaites, noté $M \models T$. Si une formule φ est vraie dans tout modèle de T , on dit que T prouve φ , ou que φ est une conséquence de T , noté $T \models \varphi$. On confond fréquemment T avec l'ensemble de ses conséquences.

Une théorie T est dite *complète* si pour toute \mathcal{L} -formule φ , soit $\varphi \in T$, soit $\neg\varphi \in T$.

Exemple 2.1.7. Un anneau est une \mathcal{L}_{ann} -structure, modèle de la théorie des anneaux T_{ann} , composée des axiomes des anneaux.

Définition 2.1.8 (Définissabilité). Soit M une \mathcal{L} -structure, $n \geq 1$, $A \subseteq M^n$. On dit que A est *définissable* (sur M) s'il existe $\varphi(\bar{x})$ une $\mathcal{L}(M)$ -formule telle que $A = \varphi(M) = \{\bar{b} \in M^n, \varphi(\bar{b})\}$.

De plus, une fonction $f : M^n \rightarrow M^k$ est dite définissable s'il existe une formule $\varphi(\bar{x}, \bar{y})$ telle que $f(\bar{x}) = \bar{y} \iff M \models \varphi(\bar{x}, \bar{y})$.

2.2 Rang de Morley et conjecture de Cherlin-Zilber

Définition 2.2.1 (Types). Soit M une \mathcal{L} -structure, $B \subseteq M$ et $q(x_1, \dots, x_n) = q(\bar{x})$ un ensemble de $\mathcal{L}(B)$ -formules à n variables libres. On dit qu'il est *réalisé dans M* par $\bar{a} \in M^n$ si pour tout $\varphi(\bar{x}) \in q(\bar{x})$, $M \models \varphi(\bar{a})$.

Alors un *type* sur B est un ensemble $p(\bar{x})$ de $\mathcal{L}(B)$ -formules à n variables libres tel que tout sous-ensemble fini soit réalisé dans M (i.e est consistant), et maximal pour l'inclusion, i.e pour tout $\varphi(\bar{x})$, soit $\varphi(\bar{x}) \in p(\bar{x})$, soit $\neg\varphi(\bar{x}) \in p(\bar{x})$. Si il n'est pas maximal pour l'inclusion, on parle de type *partiel*.

Remarque 2.2.2. Informellement, les types caractérisent entièrement les propriétés logiques des tuples. Cependant, il arrive souvent qu'il existe des types sans aucun élément

les réalisant, ce qui est assez malvenu pour la théorie développée par la suite, où on souhaiterait avoir un modèle “aussi grand que possible” en un sens.

Par exemple, la formule $\exists y((y^2 < 2 \implies y < x) \wedge ((y > 0 \wedge y^2 > 2) \implies y > x)$ est consistante avec les axiomes des anneaux ordonnés, donc fait partie d’un type par l’axiome du choix, mais comme cette formule définit $\sqrt{2}$, il n’est pas réalisé dans $(\mathbb{Q}, +, \cdot, <)$.

Définition 2.2.3 (Saturation). Soit M un modèle d’une théorie T . Alors M est *saturé* si pour tout $B \subseteq M$ avec $|B| < |M|$, tout type sur B est réalisé dans M .

Remarque 2.2.4. L’existence de modèles saturés est non triviale. En outre, la condition de cardinalité est nécessaire, car sinon on pourrait définir un type contenant toutes les formules $x \neq m$ pour $m \in M$, qui serait trivialement impossible à satisfaire.

Un modèle ainsi saturé est parfois appelé “modèle monstre”, car la saturation assure que tous les éléments dont l’existence est consistante avec la théorie, existent bel et bien.

On peut maintenant définir la notion centrale de *rang de Morley*.

Définition 2.2.5 (Rang de Morley). Soit T une \mathcal{L} -théorie complète avec des modèles infinis, M un modèle saturé, et $S \subseteq M$. On définit alors $MR(\varphi)$, le *rang de Morley* de φ ainsi :

- (i) $MR(\varphi) \geq 0$ ssi $\varphi(M) \neq \emptyset$.
- (ii) Si α est un ordinal, $MR(\varphi) \geq \alpha + 1$ ssi il existe une famille infinie $(\varphi_i)_{i \in \mathbb{N}}$ de $\mathcal{L}(M)$ -formules telle que $\varphi_i(M) \subseteq \varphi(M)$ pour tout i , et $\varphi_i(M) \cap \varphi_j(M) = \emptyset$ pour tous $i \neq j$.
- (iii) Si α est un ordinal limite, alors $MR(\varphi) \geq \alpha$ ssi $MR(\varphi) \geq \beta$ pour tout $\beta < \alpha$.
- (iv) On écrit $MR(\varphi) = -1$ si $\varphi(M) = \emptyset$ et $MR(\varphi) = \infty$ si $MR(\varphi) \geq \alpha$ pour tout ordinal α .

Comme on travaille dans un modèle saturé, on peut confondre le rang de Morley d’une formule et celui de l’ensemble qu’elle définit.

Exemple 2.2.6. Les rationnels vus en tant qu’ensemble ordonné $(\mathbb{Q}, <)$ n’ont pas de rang de Morley, c’est à dire $MR(\mathbb{Q}) = \infty$. En effet, \mathbb{Q} est l’union disjointe d’une infinité de copies de $]0, 1[$, qui lui sont isomorphes.

Proposition 2.2.7. *Quelques propriétés du rang de Morley :*

- Si $S \subseteq M$ définissable, $MR(S) > 0$ si et seulement si S est infini.
- Pour φ, ψ des $\mathcal{L}(M)$ -formules, si $M \models \varphi \rightarrow \psi$, ou de manière équivalente $\varphi(M) \subseteq \psi(M)$, alors $MR(\psi) \leq MR(\varphi)$.
- Pour φ, ψ des $\mathcal{L}(M)$ -formules, $MR(\varphi \vee \psi) = \max(MR(\varphi), MR(\psi))$.

Définition 2.2.8 (Degré de Morley). Soit φ une formule telle que $MR(\varphi) = \alpha$ soit défini. Alors il y a un nombre au plus fini (et même borné) d de formules φ_i ($1 \leq i \leq d$) de rang de Morley α telles que $\varphi_i(M) \subseteq \varphi(M)$ pour tout $1 \leq i \leq d$. Le plus grand d possible est fini, et appelé *degré de Morley* de φ , noté $Mdeg(\varphi)$.

Il y a en fait une caractérisation plus simple des structures où le rang de Morley est toujours défini.

Définition 2.2.9. Soit M un modèle saturé d'une théorie T , et $\{0, 1\}^*$ l'ensemble des suites finies de 0 et de 1. Un *arbre binaire* dans T est la donnée d'une famille d'ensembles $(B_s)_{s \in \{0, 1\}^*}$ tels que :

- Pour tout $s \in \{0, 1\}^*$, B_s est définissable.
- Pour tout $s \in \{0, 1\}^*$, B_{s0} et B_{s1} sont des sous-ensembles disjoints de B_s ($s0$ et $s1$ représentent la concaténation).

Une théorie qui ne contient aucun arbre binaire est dite *totalelement transcendante*.

Proposition 2.2.10. Si T est une théorie complète avec des modèles infinis et M un modèle saturé, alors le rang de Morley est toujours défini si, et seulement si, T est totalelement transcendante.

Démonstration. \Rightarrow par contraposée, il existe φ telle que $MR(\varphi) = \infty$. Alors, on peut montrer qu'il existe φ_0, φ_1 deux formules de rang de Morley ∞ telles que $\varphi_0(M), \varphi_1(M) \subseteq \varphi(M)$ sont disjoints (voir [Tao09], Théorème 4.4, (iv)). En itérant, on obtient un arbre binaire.

\Leftarrow par contraposée, supposons qu'il existe un arbre binaire (φ_s) dans T . L'ordre lexicographique sur $\text{Ord} \times \omega$ est un bon ordre. Si, par l'absurde, on suppose que le rang de Morley est toujours défini, en minimisant d'abord MR puis $Mdeg$, on obtient $\varphi = \varphi_s$ dans l'arbre, de rang et de degré de Morley minimaux. Or chacun des deux enfants auraient ou un degré, ou un rang de Morley strictement plus petit, une contradiction. \square

La finitude du rang de Morley (i.e $MR(M) < \omega$) est une condition combinatoire très forte, qui restreint fortement ce qui est possible dans une structure algébrique.

Proposition 2.2.11. G désigne un groupe de rang de Morley fini. On a :

- Il n'existe pas de suite strictement décroissante infinie de sous-groupes définissables. En particulier, une intersection quelconque de sous-groupes définissables est en réalité finie, donc définissable. Remarquablement, l'intersection des sous-groupes définissables d'indice fini est elle-même d'indice fini, et on l'appelle composante connexe G° .
- Tout endomorphisme injectif et définissable de G est un automorphisme.
- Un ensemble définissable $A \subseteq G$ est dit indécomposable si pour tout $H \leq G$ définissable, $|\{aH, a \in A\}| \in \{1, \infty\}$. Alors le groupe engendré par une famille quelconque d'ensemble indécomposables contenant tous 1 est définissable.
- Si K est un corps de rang de Morley fini, il est algébriquement clos (théorème de Macintyre) et ne possède pas de sous-anneaux stricts infinis définissables.

On peut voir le rang de Morley comme une sorte de "dimension" de la structure, où le rang 0 correspond aux points, le rang 1 aux lignes, le rang 2 aux plans, etc. Il donne alors une quantification de la complexité d'une théorie et de la quantité d'ensembles

définissables associés. Malheureusement, il est en général très difficile à calculer, car cela requiert une compréhension globale des ensembles définissables dans la théorie donnée. Rien que dans l'anneau \mathbb{Z} , la question de quels sous-ensembles sont définissables d'une certaine manière est au centre du célèbre dixième problème de Hilbert.

Néanmoins, il existe un cas remarquable où le calcul est plus simple.

Théorème 2.2.12. *Un groupe algébrique sur un corps algébriquement clos est de rang de Morley fini, égal à sa dimension (de Zariski).*

Cette propriété est remarquable, et a laissé entrevoir la possibilité d'une nouvelle approche de la géométrie algébrique, fondée sur la notion de rang de Morley fini. Malheureusement, le statut de conjecture de la proposition suivante met pour le moment à mal cet espoir.

Conjecture 2.2.13 (Cherlin-Zilber). *Tout groupe infini, simple de rang de Morley fini est un groupe algébrique sur un corps algébriquement clos.*

Remarque 2.2.14. Actuellement, la conjecture n'a été prouvée que pour les rangs inférieurs à 3 :

- Tout groupe de rang de Morley 1 est commutatif.
- Tout groupe de rang de Morley 2 est résoluble.
- Un groupe simple de rang de Morley 3 est isomorphe à $\mathrm{PSL}_2(K)$ pour K un corps algébriquement clos.

Dans l'optique de résoudre cette question, les chercheur·euse·s souhaitent comprendre les propriétés des groupes algébriques du point de vue de la théorie des modèles. Il est en particulier intéressant de savoir s'il est possible de retrouver le corps de base d'un groupe algébrique à partir d'uniquement ses propriétés logiques.

Les articles que j'ai étudié s'intéressent chacun à un genre précis de groupes algébriques, et énoncent des résultats forts concernant la définissabilité du corps ou de l'anneau de base du groupe. J'ai par la suite cherché des généralisations dans un cas spécifique non traité par l'article original.

3 Définissabilité dans les groupes réductifs

3.1 Cas des corps

Dans le but de prouver la conjecture de Cherlin-Zilber, une des stratégies envisagées est d'identifier dans un premier temps le corps de base d'un groupe de rang de Morley fini. En effet, cet élément de construction des groupes algébriques est totalement invisible quand on n'a à disposition que le groupe abstrait. C'est pourquoi il est intéressant d'essayer de déterminer quand il est possible de définir le corps de base à l'intérieur d'un groupe algébrique. C'est le sujet de l'article [KRT99], où le résultat suivant est démontré :

Théorème 3.1.1. *Si G est un k -groupe isotrope absolument presque simple, alors k est définissable dans $G(k)$.*

Tout d'abord, il faut un certain nombre de définitions pour comprendre l'énoncé. On se fondera sur la théorie des groupes algébriques linéaires (établie par exemple dans [Bor91]), sans l'expliquer plus en détail.

Définition 3.1.2. k désigne un corps, K sa clôture algébrique, et G un k -groupe réductif, i.e de radical unipotent trivial. On supposera k infini, car il est trivial de définir un sous-groupe d'un groupe fini : il suffit d'expliciter tous ses éléments. On note G_a et G_m les schémas de groupes additif et multiplicatif, respectivement. G est appelé *k -presque simple* s'il ne possède aucun sous-groupe normal connexe défini sur k . Si on enlève l'hypothèse de définition sur k , on dit que G est *absolument presque simple*.

Un *tore* de G est un sous-groupe commutatif T défini sur k qui, quand on étend le corps de base à K , est isomorphe à $(K^*)^n$, $n > 0$. Un *sous-groupe de Borel* de G est un sous-groupe maximal, connexe et résoluble de G : il contient nécessairement un tore de G , maximal pour l'inclusion. Un sous-groupe fermé de G contenant un sous-groupe de Borel est dit *parabolique*.

Le groupe G est dit *k -isotrope* si il existe un sous-groupe parabolique propre et non-trivial défini sur k ; sinon on dit qu'il est *anisotrope*.

Soit $P \leq G$ un sous-groupe parabolique de radical unipotent U . Un complément L de U dans P est appelé *sous-groupe de Levi* de P . De tels sous-groupes existent toujours et sont à leur tour réductifs.

Définition 3.1.3. Soit $S \subseteq G$ un tore. Il existe un couplage entre $\text{Mor}(S, G_m)$ le groupe des caractères et $\text{Mor}(G_m, S)$ le groupe des sous-groupes à un paramètres de S . Si $\alpha \in \text{Mor}(S, G_m)$ et $\beta \in \text{Mor}(G_m, S)$, alors il existe un unique $\langle \alpha, \beta \rangle \in \mathbb{Z}$ tel que $\alpha \circ \beta \in \text{Mor}(G_m, G_m)$ est égal à $x \mapsto x^{\langle \alpha, \beta \rangle}$.

Définition 3.1.4. Soit T un k -tore maximal. T agit par conjugaison sur $\mathfrak{g} = \text{Lie}(G)$, et pour tout $\alpha \in \text{Mor}(T, G_m)$, il existe un espace de poids $\mathfrak{g}_\alpha = \{X \in \mathfrak{h}, \forall t \in T, t \cdot X = \alpha(t)X\}$. Si $\alpha \neq 0$ et $\mathfrak{g}_\alpha \neq \{0\}$, on dit que α est une *racine* (on remarquera l'analogie presque parfaite avec la définition dans le cas des algèbres de Lie).

De manière duale, à toute racine α on peut associer une *coracine* α^\vee , définie par

$$\forall \beta \in \text{Mor}(S, G_m), \langle \beta, \alpha^\vee \rangle(\alpha, \alpha) = 2(\beta, \alpha)$$

où (\cdot, \cdot) est un produit scalaire adapté.

Ces prérequis posés, on a le résultat suivant :

Proposition 3.1.5 ([KRT99], 2.2). *Soit G un k -groupe k -isotrope et absolument presque simple. Alors pour tout k -sous-groupe parabolique P de G , il existe un k -sous-groupe $V \subseteq Z(U)$ avec une structure de L -module irréductible donnée par l'action par conjugaison.*

Lemme 3.1.6 ([KRT99], 3.1). *Soit $L \leq P$ un k -sous-groupe de Levi d'un k -sous-groupe parabolique P de G , et Z le centre de L . Alors $Z(k)$ et $L(k)$ sont des sous-groupes définissables de G .*

Proposition 3.1.7. *Soit P un sous-groupe parabolique minimal de G , et V le L -module irréductible obtenu via 3.1.5. Soit $v \in V(k)$ non trivial. Alors $Z(k) \cdot v$ contient tous les éléments de la forme t^2v , $t \in k^*$.*

Exemple 3.1.8. En règle générale, on ne peut pas faire mieux que les carrés. Prenons l'exemple de $G = \mathrm{SL}_2$. Alors on peut prendre

$$\begin{aligned} P &= \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \\ U = Z(U) &= \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \\ L = Z(L) &= \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \end{aligned}$$

les groupes des matrices triangulaires supérieures, unitriangulaires supérieures et diagonales, respectivement.

Alors $V = U$ a une structure de L -module où l'addition est le produit et la multiplication par un scalaire la conjugaison. On remarque alors que pour tout α inversible et tout λ ,

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} 1 & \alpha^2\lambda \\ 0 & 1 \end{pmatrix}$$

Preuve du théorème 3.1.1. Avec les mêmes notations que la proposition précédente, on définit $k' \subseteq V(k)$ comme l'ensemble des éléments de la forme $x \cdot v - y \cdot v$, où $x, y \in Z(k)$. Il est clairement définissable.

- Si $\mathrm{car}(k) \neq 2$, alors tout élément distinct de ± 1 s'écrit comme une différence de carrés d'éléments non nuls via $z = \frac{1}{4}((z+1)^2 - (z-1)^2)$. Si $\mathrm{car}(k) > 3$, on a de plus $\pm 1 = \frac{1}{16}((\pm 1+4)^2 - (\pm 1-4)^2)$ puisque $1 \neq 4$.
- Si $\mathrm{car}(k) = 2$, alors $t \mapsto t^2$ est un morphisme de corps et $k' = \{t^2v, t \in k^*\}$.

Dans tous les cas, $(k', +)$ muni de l'addition de $V(k)$ est isomorphe à $(k, +)$. On peut alors définir la multiplication en posant $(x \cdot v)(y \cdot v) = (xy) \cdot v$ et en prolongeant linéairement. \square

Remarque 3.1.9. La preuve de l'article original oublie la subtilité du cas $\mathrm{car}(k) = 3$, et par conséquent la preuve est incomplète. Cependant, le résultat reste vrai malgré tout, ce que j'établis ci-dessous.

3.2 Généralisation aux anneaux

La définissabilité des corps paraît plus utile dans le cadre de la conjecture de Cherlin-Zilber, mais on étudie aussi le cas plus général où le corps de base est remplacé par un anneau intègre. Cela permet de décrire bien plus de groupes, et de caractériser leurs propriétés de théorie des modèles, tout en gardant les mêmes outils. La question sur laquelle je me suis penchée est la suivante : à quels anneaux R peut-on généraliser le résultat du théorème 3.1.1 ?

Cela a déjà été fait pour les anneaux intègres profinis dans [NST21], mais les méthodes employées étaient spécifiques à ces objets. Par conséquent, j'ai simplement repris les conclusions de l'article, plus précisément 3.1.7. Attendu que R soit intègre, il suffit de poser $k = \text{Frac}(R)$ et les mêmes arguments marchent, *mutatis mutandis*, en remplaçant $Z(k)$, $L(k)$ et $V(k)$ par $Z(R)$, $L(R)$ et $V(R)$ quand cela est nécessaire. La question est alors de déterminer pour quels anneaux R on peut recouvrer l'anneau entier à partir des carrés des unités, et ce de manière définissable.

Définition 3.2.1. Soit R un anneau intègre. On dit qu'il a la propriété $(*)$ s'il existe $\alpha_1, \dots, \alpha_m \in R$ et $A \subseteq R$ fini tel que

$$R \simeq \sum_{i=1}^m \alpha_i X$$

où $X = \{u^2, u \in R^\times\} \cup A$.

Remarque 3.2.2. Quand $0 \in A$, cela permet au nombre de carrés d'unités requis d'être borné, plutôt qu'un nombre fixe, comme 2 dans l'article original.

Théorème 3.2.3. Soit R intègre, $k = \text{Frac}(R)$, G un k -groupe k -isotrope et absolument presque simple. Supposons que R a la propriété $(*)$. Alors R est définissable dans $G(R)$.

Démonstration. En réutilisant les notations de l'article, soit $v \in V(R)$ non trivial. On sait que $Z(R)$ est définissable et $Z(R) \cdot v$ contient tous les éléments de la forme $u^2 v$, $u \in R^\times$. Soient $(\alpha_i)_{1 \leq i \leq m}$ et A comme dans la définition, en supposant sans perte de généralité que $1 \notin A$. On ajoute l'ensemble fini $P = \{\alpha_i v, a \alpha_i v \mid 1 \leq i \leq m, a \in A\} \subseteq V(R)$ à nos paramètres. Pour $1 \leq i \leq m$, $a \in A$, posons $S_{i,1} = Z(R) \cdot \alpha_i v$ et $S_{i,a} = \{a \alpha_i v\}$, tous deux définissables. On peut maintenant définir

$$R' = \bigcup_{(a_i) \in (A \cup \{1\})^m} \sum_{i=1}^m S_{i,a_i}$$

définissable car A est fini. Par $(*)$, il est isomorphe à $(R, +)$, en utilisant l'addition héritée de $V(R)$.

Pour conclure, il nous faut définir la multiplication sur R' . Soient $\alpha, \alpha' \in R$, et $x, x' \in Z(R)$ qui agissent par c^2, c'^2 . Écrivons

$$\alpha \alpha' = \sum_{k=1}^m \alpha_k c_{\alpha, \alpha', k}, \quad c_{\alpha, \alpha', k} \in X$$

Alors les $c_{\alpha, \alpha', k} \alpha_k v$ sont de la forme $z_{\alpha, \alpha', k} \cdot v'_{\alpha, \alpha', k}$ avec $z_{\alpha, \alpha', k} \in Z(R)$ et $v'_{\alpha, \alpha', k} \in P$, par une distinction de cas facile. On définit alors

$$(x \cdot \alpha v)(x' \cdot \alpha' v) = \sum_{i=1}^m (x x' z_{\alpha, \alpha', k}) \cdot v'_{\alpha, \alpha', k}$$

Quand α, α' parcourent les α_i et $a\alpha_i$ (en nombre fini), on peut prendre le nombre fini de $z_{\alpha, \alpha', k}$ en paramètres, en plus de P , et la définition ci-dessus définit la multiplication sur chaque $S_{i, a}$, qui peut être prolongée par linéarité en une multiplication sur R' qui coïncide avec celle de R . Par conséquent, R est définissable dans $G(R)$. \square

Proposition 3.2.4. *On a les exemples suivants :*

- (i) *Tout corps a la propriété (*).*
- (ii) *Pour p premier impair, \mathbb{Z}_p , l'anneau des entiers p -adiques, a la propriété (*).*
- (iii) *Pour p premier impair, $\mathbb{Z}_p \cap \mathbb{Q}$ a la propriété (*).*
- (iv) *\mathbb{Z}_2 a la propriété (*).*
- (v) *$\mathbb{Z}_2 \cap \mathbb{Q}$ a la propriété (*).*

Démonstration. (i) Quand R est un corps, il a été mentionné précédemment que le cas de la caractéristique 3 n'avait pas été complètement considéré par l'article. On peut simplement résoudre le problème en permettant à chacun des carrés d'être égal à zéro, i.e en prenant $A = \{0\}$.

- (ii) Tout élément de \mathbb{Z}_p est de la forme $\pm x^2$ ou bien $x^2 - y^2$, x, y unités (démontré dans l'article [NST21], avant le théorème 4.9). Encore une fois on prend $A = \{0\}$.
- (iii) Soit $x = \frac{a}{b} \in \mathbb{Z}_p \cap \mathbb{Q}$, $p \nmid b$. Quand $p \mid a$, $a \pm b$ n'est jamais divisible par p , et la preuve dans le cas des corps fonctionne encore. Quand $p \nmid a$, ce n'est pas forcément le cas. Si par exemple $p \mid a + b$, on utilise le cas précédent pour écrire $x + 1 = \frac{a+b}{b} = u^2 - v^2$ avec u, v des unités. Alors $x = u^2 - v^2 - 1$. Par conséquent, on peut choisir $m = 3$, $\alpha_3 = 1$ et $A = \{-1, 0, 1\}$, ou bien $m = 4$, $\alpha_3 = 1$, $\alpha_4 = -1$ et $A = \{0\}$.
- (iv) En prenant $A = \{0\}$, on remarque qu'un élément de \mathbb{Z}_2 est le carré d'une unité ssi il est congruent à 1 modulo 8. En effet,

$$(2x + 1)^2 = 8b + 1 \iff x^2 + x - 2b = 0$$

qui a toujours une racine par le lemme de Hensel. Alors tout élément de \mathbb{Z}_2 peut être écrit comme somme d'au plus 8 carrés d'unités, prouvant qu'il a la propriété (*) avec $m = 8$, $\alpha_1 = \dots = \alpha_8 = 1$.

- (v) $A = \{0\}$. Soit $x = \frac{a}{b} = \frac{ab}{b^2} \in \mathbb{Z}_2 \cap \mathbb{Q}$, b impair. Soit $k \in \mathbb{Z}$ impair tel que $k^2 + ba \geq 3$ (ba pourrait être négatif). Ensuite, soustrayons des carrés (au plus 7) comme $\frac{1}{b^2}$ jusqu'à ce que le numérateur soit congruent à 3 modulo 8. On a alors $x + \frac{k^2}{b^2} - \frac{1}{b^2} - \dots - \frac{1}{b^2} = \frac{y}{b^2}$ avec $y \equiv 3[8]$.

Le théorème des trois carrés de Legendre affirme que y peut s'écrire comme somme de trois carrés $r^2 + s^2 + t^2$, et comme les seuls résidus quadratiques modulo 8 sont $\{0, 1, 4\}$, chacun d'entre eux est nécessairement congruent à 1 modulo 8, donc impair. Alors

$$x = \left(\frac{r}{b}\right)^2 + \left(\frac{s}{b}\right)^2 + \left(\frac{t}{b}\right)^2 + \left(\frac{1}{b}\right)^2 + \dots + \left(\frac{1}{b}\right)^2 - \left(\frac{k}{b}\right)^2$$

Tous les numérateurs sont impairs, donc tous ces carrés sont des unités, montrant que la propriété (*) est vraie avec $m = 11$. □

Proposition 3.2.5. *On a les résultats de stabilité suivants :*

- (i) Si R a la propriété (*) et $R \subseteq R'$ avec R' finiment engendré en tant que R -module, alors R' a la propriété (*).
- (ii) Si R a la propriété (*) et $I \subseteq R$ est un idéal premier, alors R/I a la propriété (*).
- (iii) Si R a la propriété (*) avec $A \subseteq \{0\}$ et $S \subseteq R$ multiplicatif, alors $S^{-1}R$ a la propriété (*).
- (iv) Si R a la propriété (*) avec $A = \emptyset$ et soit $2 = 0$ ou $2 \in R^\times$, alors $R[[X]]$, l'anneau des séries entières à coefficients dans R , a la propriété (*).

Démonstration. Sans perte de généralité, on supposera que l'isomorphisme dans la définition de la propriété (*) est une égalité.

- (i) Soit X, α_i comme dans la définition de la propriété (*) pour R . Soient $\beta_1, \dots, \beta_k \in S$ tels que $R' = \sum_{j=1}^k \beta_j R$. Alors

$$R' = \sum_{j=1}^k \sum_{i=1}^m \alpha_i \beta_j X$$

- (ii) Clair en appliquant l'application quotient à la définition. Le fait que I soit premier est seulement nécessaire pour que R/I reste intègre.
- (iii) Soit $\frac{r}{s} \in S^{-1}R$, $r \in R$, $s \in S$. On peut écrire $rs = \sum_{i=1}^m \alpha_i x_i^2$ avec $x_i \in R^\times \cup \{0\}$. Alors

$$\frac{r}{s} = \sum_{i=1}^m \alpha_i \left(\frac{x_i}{s}\right)^2$$

permet de conclure. La condition sur A est seulement suffisante, il suffirait que A ne soit seulement stable (d'une manière appropriée) par l'action multiplicative de S par multiplication.

- (iv) Quand $2 = 0$, l'application carré est un morphisme d'anneaux injectif comme dans le cas des corps de caractéristique 2. Supposons $2 \in R^\times$. Soit $\bar{b} = \sum_{n \in \mathbb{N}} b_n X^n \in R[[X]]$. Remarquons que les unités dans $R[[X]]$ sont précisément les éléments avec un coefficient constant dans R^\times . On souhaite trouver des $(a_{i,n})_{1 \leq i \leq m, n \in \mathbb{N}} \subseteq \mathbb{R}$ tels que $\bar{b} = \sum_{i=1}^m \alpha_i (\sum_{n \in \mathbb{N}} a_{i,n} X^n)^2$. On procède par récurrence sur n :

- $n = 0$: on obtient $\sum_{i=1}^m \alpha_i a_{i,0}^2 = b_0$ par la définition de la propriété (*), avec $a_{i,0} \in R^\times$ pour tout $1 \leq i \leq m$. Comme les coefficients constants sont des unités, il en ira de même pour les éléments de $R[[X]]$ qui seront construits.

- On suppose qu'on a déjà défini les éléments $a_{i,j}$ pour $j < n$ et $1 \leq i \leq m$. L'égalité ci-dessus prise au coefficient n donne

$$\sum_{i=1}^m \alpha_i \left(2a_{i,0}a_{i,n} + \sum_{k=1}^{n-1} a_{i,k}a_{i,n-k} \right) = b_n$$

Prenons alors x_i tel que

$$\sum_{i=1}^m \alpha_i x_i^2 = \frac{1}{2} \left(b_n - \sum_{i=1}^m \sum_{k=1}^{n-1} a_{i,k}a_{i,n-k} \right)$$

et posons $a_{i,n} = a_{i,0}^{-1} x_i^2$.

□

4 Bi-interprétabilité dans les groupes de Chevalley

Dans la partie précédente, on s'intéressait à un résultat de définissabilité ; celle du corps de base dans le groupe. Cependant, pour d'autres types de groupes, on peut montrer une propriété beaucoup plus forte, la *bi-interprétabilité*. Informellement, la bi-interprétabilité de deux structures donne un moyen de traduire une proposition valant pour l'une en une proposition valant pour l'autre, ce qui est particulièrement intéressant quand les langages sont différents, et permet de déduire des propriétés de théorie des modèles de l'un à partir de l'autre, et vice-versa. L'article [ST21] montre la bi-interprétabilité entre R et $G(R)$ où R est un anneau et G un *groupe de Chevalley*.

4.1 Systèmes de racines et groupes de Chevalley

Soit \mathfrak{g} une algèbre de Lie complexe, et $\mathfrak{h} \subseteq \mathfrak{g}$ une *sous-algèbre de Cartan*, ce qui est ici une sous-algèbre commutative maximale pour l'inclusion et auto-normalisante, i.e $\forall X \in \mathfrak{g}, (\forall H \in \mathfrak{h}, [H, X] \in \mathfrak{h}) \implies X \in \mathfrak{h}$.

Définition 4.1.1. Soit $\alpha \in \mathfrak{h}^*$ une forme linéaire. On définit

$$\mathfrak{g}_\alpha = \{X \in \mathfrak{g}, \forall H \in \mathfrak{h}, [H, X] = \alpha(H)X\}$$

C'est un sous-espace de \mathfrak{g} . Quand il est non trivial, on dit que α est une *racine* de \mathfrak{g} et on appelle \mathfrak{g}_α *l'espace racine* associé.

Définition 4.1.2. On note Σ l'ensemble de toutes les racines. Le *rang* de \mathfrak{g} (et du groupe G associé, quand il y en a) est la dimension du sous-espace vectoriel de \mathfrak{h}^* engendré par les éléments de Σ .

Remarque 4.1.3. Les racines sont un outil essentiel dans la classification des algèbres de Lie. L'ensemble Σ possède une structure géométrique qu'on appelle *système de racines*. Les systèmes de racines caractérisent entièrement l'algèbre de Lie \mathfrak{g} , et tous les systèmes de racines possibles sont connus et classifiés :

- Quatres familles infinies : $A_n, B_m, C_m, D_m, n \geq 1, m \geq 2$. Elles correspondent à des groupes de Lie classiques comme par exemple PSL, SO, SU, etc.
- Cinq systèmes dit *exceptionnels* : G_2, F_4, E_6, E_7, E_8 . L'approche de Chevalley a permis de leur associer des groupes algébriques.

Proposition 4.1.4. *Il existe une décomposition*

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Sigma} \mathfrak{g}_\alpha$$

où chaque \mathfrak{g}_α est de dimension 1 et engendré par un vecteur X_α .

L'application exponentielle

$$x_\alpha : \begin{cases} \mathbb{C} & \rightarrow G \\ t & \rightarrow \exp(tX_\alpha) \end{cases}$$

est un morphisme de groupe, définissant un sous-groupe $U_\alpha \leq G$, appelé sous-groupe racine correspondant à α .

Prop. + Définition 4.1.5 (Groupe de Chevalley). Soit G un groupe de Lie complexe, $\mathfrak{g} = \text{Lie}(G)$, $\mathfrak{h} \subseteq \mathfrak{g}$ une sous-algèbre de Cartan et Σ un système de racines.

Le sous-groupe de G engendré par tous les sous-groupes racines U_α pour $\alpha \in \Sigma$ est qualifié de *groupe de Chevalley* (cf. [Ste16], §3).

4.2 Schéma de groupe de Chevalley-Demazure

Prop. + Définition 4.2.1. On se donne un groupe de Chevalley G . Étant un groupe de matrices, il admet des représentations fidèles dans $\text{GL}_d(\mathbb{C})$. Il est possible d'en choisir une (en changeant de base) telle que les coordonnées de $x_\alpha(t)$ soient des polynômes à coefficients entiers en t (cf. [Abe69], 1.2).

Alors, la représentation tire en arrière les formes coordonnées X_{ij} ($1 \leq i, j \leq d$) sur G , et on pose $\mathbb{Z}[G] = \mathbb{Z}[X_{ij}, 1 \leq i, j \leq d]$ l'anneau engendré, muni de la multiplication matricielle. On définit alors le *schéma de groupe de Chevalley-Demazure* associé à G , qui à un anneau R associe

$$G(R) = \text{Hom}(\mathbb{Z}[G], R)$$

Remarque 4.2.2. On peut voir $G(R)$ comme l'ensemble des points R -rationnels de G , i.e l'ensemble des matrices de G dont toutes les coordonnées sont dans R ; de la même manière qu'on définit les groupes comme $\text{GL}_n(\mathbb{Z})$. De façon semblable, on peut identifier un élément $g \in G(R)$ avec la matrice $(X_{ij}(g))$.

On note $\mathcal{L}_{\text{gp}} = (1, \cdot^{-1}, \cdot)$ le langage des groupes et $\mathcal{L}_{\text{ann}} = (0, 1, +, \cdot)$ le langage des anneaux.

Définition 4.2.3 (Interprétation). Soient M et N deux structures, potentiellement sur des langages différents. Une *interprétation* de M dans N est une surjection $f : A \rightarrow M$ avec $A \subseteq N^n$ telle que, pour tout $k \geq 1$, la préimage par f de tout sous-ensemble définissable de M^k est à son tour définissable.

Exemple 4.2.4. La définition des rationnels à partir de couples d'entiers, courante en théorie des ensembles, représente une interprétation. En prenant $M = \mathbb{Q}$ en tant que $\mathcal{L}_{\text{corps}}$ -structure et $N = \mathbb{Z}$ en tant que \mathcal{L}_{ann} -structure, l'application

$$f : \begin{cases} \{(x, y), y \neq 0\} \subseteq \mathbb{Z}^2 & \rightarrow \mathbb{Q} \\ (x, y) & \mapsto \frac{x}{y} \end{cases}$$

est une interprétation.

Remarque 4.2.5. Étant donné une interprétation de M dans N et une interprétation de N dans L , on peut obtenir une interprétation de M dans L en composant les applications.

Définition 4.2.6 (Bi-interprétation). Soit M une \mathcal{L} -structure et N une \mathcal{L}' -structure. Il y a une *bi-interprétation* entre M et N si :

- (i) Il y a une interprétation de M dans N , et de N dans M .
- (ii) Les interprétations composées, vues comme opérations sur M et N , sont définissables dans chacune des structures respectives.

Exemple 4.2.7. Dans le cas $M = R$ dans le langage des anneaux et $N = G(R)$ dans le langage des groupes, la bi-interprétation est la donnée de quatre choses :

- (i) Une interprétation de R dans $G(R)$: ici, une identification entre R et un sous-groupe commutatif définissable $R' \leq G(R)$ tel que l'addition dans R corresponde à la multiplication de R' et que la multiplication de R soit \mathcal{L}_{gp} -définissable dans R' .
- (ii) Une interprétation de $G(R)$ dans R : ici, une identification entre $G(R)$ et un sous-groupe $G(R)^\dagger \leq \text{GL}_d(R)$, avec $G(R)^\dagger$ définissable dans \mathcal{L}_{ann} (la structure de groupe est simplement la multiplication matricielle).
- (iii) Un isomorphisme \mathcal{L}_{gp} -définissable de $G(R)$ vers $G(R)^\dagger$, l'image de $G(R)^\dagger$ dans $\text{GL}_d(R')$.
- (iv) Un isomorphisme \mathcal{L}_{ann} -définissable de R vers R'^\dagger , l'image de R' dans $\text{GL}_d(R)$.

Proposition 4.2.8. $G(R)$ est interprétable dans R .

Démonstration. Il y a une surjection évidente de $\mathbb{Z}[\mathbf{T}] = \mathbb{Z}[T_{ij}, 1 \leq i, j \leq d]$ (où les T_{ij} sont des indéterminées) vers $\mathbb{Z}[G]$. Comme $\mathbb{Z}[\mathbf{T}]$ est noethérien, le noyau est engendré par un nombre fini de polynômes $P_1(\mathbf{T}), \dots, P_s(\mathbf{T})$. Alors

$$g \in G(R) \iff \forall 1 \leq l \leq s, P_l(g_{ij}) = 0 \tag{1}$$

où l'on voit $G(R)$ comme sous-ensemble de $M_d(R)$. □

4.3 Interprétation de R dans $G(R)$

Proposition 4.3.1 ([ST21], Corollaire 1.7). *Si G est de rang au moins 2, pour toute racine α le groupe $U_\alpha(R)$ est définissable, sauf peut-être si $G = \text{Sp}_4(R)$, $\text{car}(R) = 0$ et $R/2R$ est infini. Dans tous les cas, $U_\alpha(R)Z(R)$ est définissable.*

Remarque 4.3.2. La preuve de ce résultat constitue la majeure partie de l'article, et procède par une étude détaillée de chaque système de racines possible, en montrant l'existence de certains éléments distingués du groupe, appelés "témoins toriques".

L'application $x_\alpha : R \mapsto U_\alpha(R)$ est un morphisme de groupes, mais pour montrer l'interprétation, on veut montrer que la multiplication dans R correspond à une opération définissable dans $U(R)$, i.e que l'application

$$\begin{cases} U_\alpha(R) \times U_\alpha(R) & \rightarrow U_\alpha(R) \\ (x_\alpha(r), x_\alpha(s)) & \mapsto x_\alpha(rs) \end{cases}$$

est définissable. En réalité, on a résultat plus général :

Proposition 4.3.3. *Soient α, β, γ des racines. Sous l'hypothèse que G est de rang au moins 2, les applications*

$$\begin{cases} U_\alpha(R) & \rightarrow U_\beta(R) \\ x_\alpha(r) & \mapsto x_\beta(r) \end{cases}$$

et

$$m_{\alpha\beta\gamma} : \begin{cases} U_\alpha(R) \times U_\beta(R) & \rightarrow U_\gamma(R) \\ (x_\alpha(r), x_\beta(s)) & \mapsto x_\gamma(rs) \end{cases}$$

sont définissables dans le langage des groupes. En particulier, il y a une correspondance entre la multiplication dans R et l'opération $m = m_{\alpha\alpha\alpha}$ dans $R' = U_\alpha(R)$, pour un α fixé.

Remarque 4.3.4. Les résultats précédents reposent sur l'hypothèse que le groupe de Chevalley est de rang au moins 2, à chaque fois de manière cruciale. Par conséquent, cette méthode n'est pas du tout adaptée à l'étude des groupes de Chevalley de rang 1, et c'est pourquoi j'ai étudié l'article [KRT99] dans un second temps : le résultat est plus faible, mais l'approche est plus générale et englobe les groupes de rang 1.

4.4 Conséquences de la bi-interprétation

La bi-interprétation donne une manière d'exprimer les opérations d'une structure dans le langage de l'autre. Ici, le sens crucial est le résultat de 4.3.3, qui permet d'exprimer la multiplication de R (dans le langage des anneaux) à l'intérieur de R' (dans le langage des groupes).

Proposition 4.4.1. *L'affirmation que (R', \cdot, m) définit un anneau commutative intègre peut donc être exprimée par une certaine formule $P_1(\bar{g})$, où \bar{g} représente un ensemble de paramètres de $G(R)$. Comme cette formule définit à elle seule la structure d'anneau, pour tout groupe H tel que $H \models \exists \bar{h} P_1(\bar{h})$, on peut associer un certain anneau A_H . Pour toute \mathcal{L}_{ann} -formule φ , il existe une \mathcal{L}_{gp} -formule φ' telle que $A_H \models \varphi$ si et seulement si $H \models \varphi'$.*

De manière analogue, pour tout anneau S , les équations de (1) définissent la loi de groupe de $G(S)$ dans le langage des anneaux, et par conséquent, pour toute \mathcal{L}_{gp} -formule ψ , il existe une \mathcal{L}_{ann} -formule ψ' telle que $G(S) \models \psi$ si et seulement si $S \models \psi'$.

Références

- [Abe69] Eiichi ABE. “Chevalley groups over local rings”. In : *Tohoku Mathematical Journal* 21.3 (1969), p. 474-494. DOI : [10.2748/tmj/1178242958](https://doi.org/10.2748/tmj/1178242958). URL : <https://doi.org/10.2748/tmj/1178242958>.
- [Bor91] Armand BOREL. *Linear Algebraic Groups*. eng. Second Enlarged Edition.. Graduate Texts in Mathematics 126. New York, NY : Springer New York, 1991. ISBN : 9781461209416.
- [Hal15] Brian HALL. *Lie Groups, Lie Algebras, and Representations : An Elementary Introduction*. eng. Second edition. T. 222. Graduate Texts in Mathematics. Cham : Springer Nature, 2015. ISBN : 9783319134673.
- [KRT99] L. KRAMER, G. RÖHRLE et K. TENT. “Defining k in $G(k)$ ”. In : *Journal of Algebra* 216.1 (1999), p. 77-85. ISSN : 0021-8693. DOI : <https://doi.org/10.1006/jabr.1998.7771>. URL : <https://www.sciencedirect.com/science/article/pii/S0021869398977717>.
- [NST21] Andre NIES, Dan SEGAL et Katrin TENT. “Finite axiomatizability for profinite groups”. In : *Proceedings of the London Mathematical Society* 123.6 (2021), p. 597-635. DOI : <https://doi.org/10.1112/plms.12420>. eprint : <https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/plms.12420>. URL : <https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/plms.12420>.
- [ST21] Dan SEGAL et Katrin TENT. *Defining R and $G(R)$* . 2021. arXiv : [2004.13407](https://arxiv.org/abs/2004.13407) [math.GR]. URL : <https://arxiv.org/abs/2004.13407>.
- [Ste16] Robert STEINBERG. *Lectures on Chevalley Groups*. T. 66. A.M.S. University Lecture Series. 2016.
- [Tao09] Terence TAO. *ω -Stable Theories : Introduction*. <https://terrytao.wordpress.com/wp-content/uploads/2009/11/w-stable-theories1.pdf>. Consulté : 2024-08-16. 2009.