Leila Schneps

Leila Schneps est une mathématicienne travaillant sur divers aspects de la théorie analytique des nombres et de la théorie de Galois. La théorie de Galois est une théorie qui nous permet d'affirmer que l'équation polynomiale suivante

$$x^5 - 6x + 3 = 0,$$

ne peut pas être résolue par des radicaux, une affirmation qui n'est pas immédiatement évidente. Étant donné un polynôme f à coefficients dans $\mathbb{Q}$, la théorie de Galois fournit un corps de décomposition de f, qui est le plus petit corps possible contenant toutes les racines du polynôme. Le corps de décomposition possède un groupe de Galois fini associé G. La théorie de Galois relie la théorie des corps et la théorie des groupes d'une manière profonde, et traduit le problème de la résolubilité de f en le problème de la résolubilité du groupe de Galois associé et, comme la plupart d'entre nous le savent, il existe de nombreuses techniques en théorie des groupes qui nous permettraient de répondre à cette question avec une relative aisance.

Ceci soulève la question de savoir si tous les groupes finis sont en fait des groupes de Galois d'une extension de radicaux : c'est ce qu'on appelle le problème inverse de Galois. Noether a proposé que les mathématiciens puissent progresser sur le problème inverse en plongeant G dans le groupe symétrique S_n, on obtient une G-action sur le corps $\mathbb{Q}(X_1, ..., X_n)$. Si E est le corps fixe sous cette action, il s'ensuit que $\mathbb{Q}(X_1, ..., X_n)$ est une extension de Galois de E de groupe de Galois G. Géométriquement, l'extension de Galois de E correspond à une projection de variétés

$$\pi : \mathbb{A}^n \to \mathbb{A}^n/G,$$

pour un n-espace affine sur $\mathbb{Q}$. Si P est un point $\mathbb{Q}$-rationnel de $\mathbb{A}^n/G$ qui se relève en $Q \in \mathbb{A}^n(\overline{\mathbb{Q}})$, alors les conjugués de Q sous l'action du groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sont les sQ tels que $s \in H_{\mathbb{Q}} \subset G$, et $H_{\mathbb{Q}}$ est le groupe de décomposition en Q. Si $H_{\mathbb{Q}}$ est égal au groupe G, alors Q engendre une extension de corps de $\mathbb{Q}$ dont le groupe de Galois est G. Une variété est rationnelle sur $\mathbb{Q}$ si elle est birationnellement isomorphe sur $\mathbb{Q}$ à $\mathbb{A}^n$, ou si le corps des fonctions est isomorphe à $\mathbb{Q}(T_1, ..., T_n)$. C'est un théorème de Hilbert que si $\mathbb{A}^n/G$ est rationnel sur $\mathbb{Q}$, alors il existe un nombre infini de points P tels que $H_{\mathbb{Q}} = G$. C'est un corollaire du théorème d'irréductibilité de Hilbert.

Nous devons mentionner que $\overline{\mathbb{Q}}$ est une extension algébrique infinie de $\mathbb{Q}$ et qu'elle est, en un sens qui peut être directement quantifié, très grande. Elle est définie comme

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \text{ tel que } \alpha \text{ est algébrique sur } \mathbb{Q}\}.$$

Ceci est un objet très grand, car nous avons

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, ...) \subseteq \overline{\mathbb{Q}},$$

mais nous devons aussi avoir

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \sqrt[5]{2}, ...) \subseteq \overline{\mathbb{Q}},$$

Traduction des pages 159 à 168 de l'article arXiv https://arxiv.org/pdf/1910.01730.
Transcription en LaTeX : Denise Vella-Chemla.

et ainsi de suite. Il est possible de prouver que $\overline{\mathbb{Q}}$ est dénombrablement large. Vous savez probablement déjà que $\mathbb{Q}$ est dénombrable. On sait que

$$\overline{\mathbb{Q}} = \bigcup_{f \in \mathbb{Q}[x]} \{\text{racines de } f\},$$

car tout nombre algébrique est zéro d'un certain polynôme. Maintenant, nous savons que $\mathbb{Q}[x]$ est dénombrable.

$$\mathbb{Q}[x] = \bigcup_{n=0}^{\infty} \mathbb{Q}[x]_{\leq n},$$

où $\mathbb{Q}[x]_{\leq n}$ est l'ensemble des polynômes en x de degré $\leq n$. Nous avons également

$$\mathbb{Q}[x]_{\leq n} \simeq \mathbb{Q}^{n+1},$$

sous l'isomorphisme donné explicitement par

$$a_0 + a_1 x + \cdots + a_n x^n \mapsto [a_0, a_1, ..., a_n].$$

On sait que $\mathbb{Q}^N$ est dénombrable pour tout N, ce qui implique que $\mathbb{Q}[x]$ est fini. Par le théorème fondamental de l'arithmétique, l'ensemble des zéros de f est fini avec une taille égale au degré de f sauf si $f = 0$, donc $\overline{\mathbb{Q}}$ est une union dénombrable d'ensembles finis, par conséquent il est dénombrable. On peut également montrer que $[\overline{\mathbb{Q}} : \mathbb{Q}]$ est dénombrablement infini. Pour commencer, ce doit être la taille d'une base pour $\overline{\mathbb{Q}}/\mathbb{Q}$ et toute base est dénombrable dans $\overline{\mathbb{Q}}$, ce qui implique que $[\overline{\mathbb{Q}} : \mathbb{Q}]$ est dénombrable. Tout ce qui reste à montrer est que $[\overline{\mathbb{Q}} : \mathbb{Q}]$ n'est pas fini. Pour un autre exercice, on pourrait prouver que la combinaison linéaire $\sqrt{2} + \sqrt{3}$ est algébrique.

Comme exercice similaire, prenons le polynôme dans $\mathbb{Q}[x]$ donné par

$$f_n(x) = x^3 + x + n,$$

pour tout entier n. Nous aimerions prouver que $f_n(x)$ a un seul zéro sur $\mathbb{R}$. On sait déjà que $f_n(x)$ a au moins 3 zéros dans $\mathbb{C}$. Par le théorème fondamental de l'arithmétique, si $\alpha \in \mathbb{C}$, alors $f_n(\alpha) = 0$ implique que $f_n(\overline{\alpha}) = 0$. Puisque f_n est de degré 3, cela implique qu'au moins une solution est réelle. Cela découle de l'analyse élémentaire. Si l'on considère f_n comme une fonction sur $\mathbb{R}$, alors

$$f_n'(x) = 3x^2 + 1$$

implique que $f_n(x)$ est monotone croissante. Cela implique à son tour qu'il existe une intersection avec l'axe $y = 0$ et le résultat s'ensuit.

Nous aimerions également montrer que le polynôme est irréductible sur $\mathbb{Q}$. Par le lemme de Gauss, cela équivaut à prouver que le polynôme est irréductible sur $\mathbb{Z}$. Commençons par écrire le polynôme.

$$f_n(x) = (x - c)(x^2 + ax + b).$$

Le polynôme se scinde de cette façon, car il n'y a qu'un seul zéro réel. Si c est un entier, alors le polynôme est irréductible.

$$f_n(x) = x^3 + (a - c)x^2 + (b - ac)x - bc = x^3 + x + m.$$

Comparons maintenant les coefficients.

$$\begin{aligned} a - c = 0 &\implies a = c, \\ b - ac = 1 &\implies b = 1 + c^2, \\ bc = m &\implies m = -(c^3 + c). \end{aligned}$$

Nous concluons que si $m = -(c^3 + c)$ pour un certain $c \in \mathbb{Z}$, alors

$$f_n(x) = (x - c)(x^2 + cx + (1 + c^2)).$$

Il s'ensuit que le polynôme est irréductible sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$.

Le théorème d'irréductibilité énonce que si K est un corps de nombres, alors pour tout n, l'espace affine $\mathbb{A}^n$ (ou l'espace projectif $\mathbb{P}^n$) possède la propriété de Hilbert sur K. Une variété (quasi-projective) X sur un corps K est dite satisfaire la propriété de Hilbert si X n'est pas mince, où un sous-ensemble A de $X(K)$ est "mince" s'il est contenu dans une union finie d'ensembles de type (C_1) ou (C_2). On peut aussi dire que l'ensemble est mince s'il existe un morphisme

$$\pi : V \to W,$$

où la dimension de W est inférieure ou égale à la dimension de V et le morphisme n'a pas de sections transversales rationnelles. De plus, on doit avoir [1]

$$A \subset \pi(W(K)).$$

Nous avons mentionné plus tôt la définition d'une extension de corps en utilisant la notion d'homomorphisme (de monomorphisme, pour être plus précis). Par exemple, $\mathbb{R}/\mathbb{Q}$ est une extension de corps où l'homomorphisme est simplement l'inclusion triviale. $\mathbb{C}/\mathbb{R}$ et $\mathbb{C}/\mathbb{Q}$ sont également des extensions de corps avec l'application d'inclusion comme homomorphisme définissant. Maintenant, si nous prenons un corps K et un sous-ensemble non vide de ce corps noté S. Le sous-corps de K engendré par S est défini comme l'intersection de tous les sous-corps de K qui contiennent S. Par exemple, le sous-corps de $\mathbb{R}$ engendré par l'élément unique $\{1\}$ est $\mathbb{Q}$ et le sous-corps de $\mathbb{C}$ engendré par $\{i\}$ est $\mathbb{Q}(i)$. $\mathbb{Q}(i)$ représente l'adjonction d'une racine. Si L/K est une extension de corps et A est contenu dans L, alors nous écrivons généralement $K(A)$ pour le sous-corps de L engendré par l'union $K \cup A$. C'est ce qu'on appelle le corps obtenu en adjoignant A à K. L'adjonction d'une racine est la brique de base pour les extensions de corps. On peut montrer que

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\},$$

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\},$$

où tous les coefficients sont rationnels. Une extension de corps L/K est dite simple si l'on peut écrire

$$L = K(\alpha),$$

pour $\alpha \in L$.

1. Jean-Pierre Serre, *Topics in Galois Theory* (Boston : Jones and Bartlett Publishers, 1992).

On peut prouver que si K est un corps et f est un polynôme irréductible dans $K[x]$, où $L := K[x]/(f(x))$, alors on a l'équivalence : L est un corps, l'application de K à L donnée par $a \mapsto a+(f)$ est une extension de corps, l'élément $x+(f)$ dans L est une racine de f, et $L = K(\alpha)$ où $\alpha = x+(f)$. Si K est un corps et $f \in K[x]$ est un polynôme de degré n où $\alpha_1, ..., \alpha_n$ sont les racines de f dans une certaine extension de K, alors $K(\alpha_1, ..., \alpha_n)$ est le corps de décomposition de f sur K. Le corps de décomposition peut être vu comme le plus petit corps sur lequel f peut se scinder en un produit de facteurs linéaires. À titre d'exemple, prenons le polynôme

$$f = x^4 - 3x^3 + 2x^2.$$

On peut le factoriser en

$$f = x^2(x-1)(x-2).$$

Cela implique que le corps de décomposition de f sur $\mathbb{Q}$ est $\mathbb{Q}$ auquel on a adjoint 0, 1 et 2, ce qui est simplement $\mathbb{Q}$. On peut également prouver que les corps de décomposition existent toujours et qu'ils sont uniques. Si K est un corps et $f \in K[x]$ est un polynôme, alors il existe un corps de décomposition L/K pour f. De plus, si L_1/K et L_2/K sont tous deux des corps de décomposition pour f, alors il existe un isomorphisme de corps $\iota : L_1 \to L_2$ tel que

$$\iota(a) = a,$$

pour tout $a \in K$.

Nous devrions également définir la notion de degré d'une extension de corps. Commençons par noter que pour L/K une extension de corps, L est un espace vectoriel sur le corps K (rappelons qu'en algèbre linéaire, les espaces vectoriels sont toujours définis sur des corps). Vous aimeriez peut-être montrer par vous-même que tous les axiomes usuels d'un espace vectoriel sont satisfaits. Cette sorte de fusion étrange entre l'algèbre linéaire et la théorie des corps est typique de la théorie de Galois. Si L/K est une extension, alors le degré de L/K (noté $[L : K]$) est défini comme la dimension de L en tant qu'espace vectoriel sur K. L'extension est dite finie si le degré est fini, ce qui implique évidemment que L est un espace vectoriel sur K de dimension finie. Si non, alors l'extension doit être infinie. Par exemple, si L/K est une extension telle que $[L : K] = p$ pour un certain premier p, alors l'extension est simple si et seulement si $L = K(\alpha)$ pour un certain $\alpha \in L$. Pour prouver cela, commençons par considérer le degré. On sait déjà que

$$[L : K] = p > 1,$$

ce qui implique que $L \neq K$, donc il doit exister un α dans $L \setminus K$. Considérons la chaîne d'inclusions :

$$K \subseteq K(\alpha) \subseteq L.$$

D'après la loi de la tour (que nous aborderons sous peu), nous devons avoir

$$p = [L : K] = [L : K(\alpha)][K(\alpha) : K].$$

C'est une multiplication de deux facteurs, donc l'un des degrés doit être l'unité et l'autre doit être p. Si $[L : K(\alpha)] = p$, alors

$$[K(\alpha) : K] = 1.$$

C'est une contradiction, car cela impliquerait que $K = K(\alpha)$, ce qui implique que $\alpha \in K$, mais nous avons déjà dit que $\alpha \in L$. Si, d'un autre côté, $[L : K(\alpha)] = 1$, alors nous avons

$$L = K(\alpha),$$

ce qui est ce que nous voulions prouver. En guise de remarque, notons que toute extension finie d'extensions de corps de $\mathbb{Q}$ est simple.

Fournissons quelques définitions supplémentaires : commençons une fois de plus avec une extension de corps L/K avec $\alpha \in L$. α est dit algébrique sur K s'il existe un polynôme non nul f dans $K[x]$ tel que

$$f(\alpha) = 0.$$

α est transcendant sur K s'il n'est pas algébrique. Spécifiquement, un nombre complexe est dit être un nombre algébrique s'il est algébrique sur $\mathbb{Q}$. En d'autres termes, c'est le zéro d'un certain polynôme à coefficients rationnels. Un nombre complexe est appelé un nombre transcendant s'il n'est pas un nombre algébrique. Bien qu'il puisse être très difficile de prouver qu'un nombre est transcendant (pensez à π, par exemple), le plan complexe est presque entièrement composé de nombres transcendants, et il est relativement rare qu'un nombre soit algébrique. Si vous ne croyez pas cela, vous pourriez chercher des images qui fournissent une visualisation des nombres algébriques dans le plan complexe comparés aux nombres transcendants. Notez que ceci est distinct du fait de dire que π est irrationnel. La preuve dans les deux cas est très longue, mais Cartwright a remarqué que la preuve par Hermite de l'irrationalité de π peut être grandement simplifiée. Le premier exemple d'un nombre algébrique qui vous viendra probablement à l'esprit est $\sqrt{2}$. Encore une fois, nous soulignons que ceci est distinct de la rationalité ou de l'irrationalité, car $\sqrt{2}$ n'est certainement pas un nombre rationnel. Cela devrait également rendre immédiatement clair que la droite réelle contient des nombres algébriques.

On peut prouver assez facilement que les extensions de corps finis sont également algébriques, mais la réciproque n'est pas vraie. À titre d'exemple, considérons l'extension donnée par

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, ...)/\mathbb{Q}.$$

C'est une extension algébrique de degré infini. Maintenant, si nous commençons par une extension de corps L/K telle que $\alpha \in L$ est algébrique sur K, alors le polynôme minimal de α sur K est le polynôme unitaire $m \in K[x]$ de plus petit degré tel que

$$m(\alpha) = 0.$$

Nous aimerions réellement faire quelque chose avec ces définitions, alors formulons quelques énoncés pour une extension de corps L/K. Si $\alpha \in L$ est algébrique sur K, alors le polynôme minimal existe et est unique. Le polynôme minimal sur α est l'unique polynôme unitaire irréductible $m \in K[x]$ qui satisfait $m(\alpha) = 0$. Si $f \in K[x]$ satisfait $f(\alpha) = 0$, alors m divise f. Ce lemme signifie que nous pouvons déterminer si un polynôme est minimal ou non, mais pour ce faire, nous devons vérifier qu'il est irréductible. Il y a de bons tests pour l'irréductibilité des polynômes. Nous avons mentionné le lemme de Gauss : en fait, ce lemme est vrai chaque fois que vous avez un polynôme sur un domaine factoriel, pas seulement les entiers.

Un autre test est le critère d'Eisenstein. Celui-ci énonce que si p est un nombre premier et

$$f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

un polynôme qui satisfait

$$\begin{gathered} p \nmid a_n, \\ p \text{ divise } a_i \text{ pour } i = 0, 1, ..., n-1, \\ p^2 \nmid a_0. \end{gathered}$$

Si ces critères sont remplis, alors le polynôme est irréductible sur $\mathbb{Q}$. Nous nous acheminons maintenant vers un résultat fondamental connu sous le nom de loi de la tour. Avant cela, nous allons énoncer quelques autres résultats. Si α est algébrique sur K avec pour polynôme minimal $m \in K[x]$ et (m) l'idéal engendré par m, alors l'application donnée par

$$\begin{gathered} \tilde{\phi} : K[x]/(m) \to K(\alpha), \\ \tilde{\phi}(f + (m)) = f(\alpha), \end{gathered}$$

est un isomorphisme. De plus, si L/K est une extension de corps et $\alpha \in L$ est algébrique sur K. Supposons que le polynôme minimal m de α sur K soit de degré d, alors

$$K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \text{ pour } a_0, ..., a_{d-1} \in K\}.$$

De plus, une base pour $K(\alpha)$ sur K est donnée par $1, \alpha, ..., \alpha^{d-1}$. Aussi,

$$[K(\alpha) : K] = d.$$

Pour en finir avec la loi de la tour, disons que nous commençons par une chaîne d'extensions de corps de degré fini $K \subseteq L \subseteq M$. Soient $l_1, l_2, ..., l_r$ une base pour L/K et $m_1, m_2, ..., m_r$ une base pour M/L. Il s'ensuit que $\{l_i m_j\}$ est une base pour M/K, où i varie de 1 à r et j varie de 1 à s. De plus, le degré des extensions peut être décomposé en un produit :

$$[M : K] = [M : L][L : K].$$

La preuve est essentiellement de l'algèbre linéaire. Il y aurait beaucoup à dire sur la théorie de Galois, mais j'espère que cette introduction aura été une bonne motivation à l'étudier. Je devrais dire que l'approche moderne (par opposition à la classique) de la théorie de Galois est due à Grothendieck et est basée sur des propriétés théoriques de catégories abstraites, plutôt que sur l'algèbre linéaire [2]. Vous pouvez également aller beaucoup plus loin avec le problème inverse de Galois et le relier à certains autres domaines (les espaces de modules et les groupes de classes d'applications, par exemple) [3].

Leila Schneps a également trouvé des résultats concernant les algèbres de Lie, en particulier une version elliptique d'une algèbre de Lie appelée l'algèbre de Lie de Kashiwara-Vergne [4]. Nous avons

2. Ian Stewart, *Galois Theory* (USA : Chapman & Hall, 2004).

3. Leila Schneps and P. Lochak, *The Inverse Galois Problem, Moduli Spaces and Mapping Class Groups* (Cambridge : Cambridge University Press, 1997).

4. Leila Schneps, *Double shuffle and Kashiwara-Vergne Lie algebras*, *J. Algebra* 367, 54–74 (2012).

donné plus tôt la définition de base d'une algèbre de Lie en termes d'espaces vectoriels. On peut définir naturellement la notion de sous-algèbre de Lie. Une application linéaire entre deux algèbres de Lie $\phi : \mathfrak{g} \to \mathfrak{h}$ est appelée un homomorphisme d'algèbres de Lie si

$$\phi([X, Y]) = [\phi(X), \phi(Y)].$$

Si l'application est une bijection, alors ϕ est un isomorphisme d'algèbres de Lie, et si c'est une application d'une algèbre de Lie dans elle-même, alors c'est un automorphisme d'algèbre de Lie. Si $\mathfrak{g}$ est une algèbre de Lie et X est un élément de $\mathfrak{g}$, alors l'application linéaire d'algèbres de Lie définie par

$$\mathrm{ad}_X(Y) = [X, Y]$$

est connue sous le nom d'application adjointe ou représentation adjointe. C'est évidemment juste le crochet de Lie à nouveau, donc si l'on compose n crochets de Lie, on peut écrire $(\mathrm{ad}_X)^n(Y)$. L'application adjointe peut également être vue comme l'application linéaire de $\mathfrak{g}$ vers l'espace des opérateurs linéaires sur $\mathfrak{g}$. Un calcul montre que

$$\mathrm{ad}_{[X,Y]} = \mathrm{ad}_X \mathrm{ad}_Y - \mathrm{ad}_Y \mathrm{ad}_X = [\mathrm{ad}_X, \mathrm{ad}_X].$$

Cela signifie que l'application adjointe est un homomorphisme d'algèbres de Lie.

Si $\mathfrak{g}_1$ et $\mathfrak{g}_2$ sont des algèbres de Lie, alors la somme directe de $\mathfrak{g}_1$ et $\mathfrak{g}_2$ est la somme directe en termes d'espaces vectoriels, où le crochet est donné comme on pourrait s'y attendre :

$$[(X_1, X_2), (Y_1, Y_2)] = ([X_1, Y_1], [X_2, Y_2]).$$

On peut facilement vérifier que cette somme directe est une autre algèbre de Lie par rapport à ce crochet de Lie. Si $\mathfrak{g}$ est une algèbre de Lie réelle ou complexe de dimension finie et $X_1, ..., X_N$ est une base pour $\mathfrak{g}$ vue comme un espace vectoriel, alors on a des constantes de structure uniques telles que

$$[X_j, X_i] = \sum_{k=1}^{N} c_{jik} X_k.$$

Celles-ci sont connus sous le nom de constantes de structure et sont utilisées en physique théorique. Les constantes de structure satisfont à deux conditions qui sont dérivées de l'antisymétrie du crochet de Lie et de l'identité de Jacobi.

Comme avec tout objet mathématique, on s'intéresse habituellement à certains types spéciaux qui ont de belles propriétés. Par exemple, une algèbre de Lie est irréductible si les seuls idéaux dans $\mathfrak{g}$ sont $\{0\}$ et $\mathfrak{g}$. En théorie des algèbres de Lie, une sous-algèbre de Lie $\mathfrak{h}$ d'une algèbre de Lie $\mathfrak{g}$ est un idéal dans $\mathfrak{g}$ si $[X, H] \in \mathfrak{h}$ pour tout $X \in \mathfrak{g}$ et $H \in \mathfrak{h}$. Une algèbre de Lie est simple si elle est irréductible et $\dim \mathfrak{g} \geq 2$. À titre d'exemple, une algèbre de Lie unidimensionnelle ne peut pas avoir d'idéaux autres que elle-même ou l'idéal trivial. Elle est irréductible en tant qu'algèbre de Lie, mais elle ne peut pas être une algèbre de Lie simple en raison de la dimensionalité. Moins trivialement, nous pouvons montrer que $\mathfrak{sl}(2, \mathbb{C})$ est une algèbre de Lie simple. Si l'on prend l'algèbre de Lie comme étant l'espace des matrices triangulaires supérieures 3×3 avec des zéros sur la diagonale principale, alors cette algèbre de Lie est nilpotente. Si $\mathfrak{g}$ est l'espace des matrices 2×2 de la forme

$$\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}$$

avec a, b et c complexes, alors l'algèbre de Lie est résoluble mais non nilpotente.

Comme nous l'avons déjà dit, une algèbre de Lie peut toujours être associée à un groupe de Lie, et vice versa. Un bon point de départ pour cela serait de considérer l'algèbre de Lie associée à un groupe de Lie matriciel. Il est assez typique de se concentrer sur les groupes de Lie matriciels lors du début de l'étude de la théorie de Lie, car ces groupes sont beaucoup plus simples à appréhender. Un problème de la théorie des groupes de Lie peut être transféré à l'algèbre de Lie correspondante, et comme nous l'avons souligné, les algèbres de Lie peuvent être étudiées avec des techniques d'algèbre linéaire élémentaires que nous connaissons tous. Par exemple, l'algèbre de Lie de l'espace euclidien est juste l'espace euclidien à nouveau, car il s'avère abélien et isomorphe à $\mathbb{R}^n$ avec le crochet de Lie trivial. L'algèbre de Lie du groupe du cercle est isomorphe à la droite réelle, et l'algèbre de Lie du tore $\mathbb{T}^n$ est également isomorphe à $\mathbb{R}^n$, essentiellement parce que le tore est égal à un produit de cercles.

Soit G un groupe de Lie matriciel. L'algèbre de Lie $\mathfrak{g}$ de G est l'ensemble de toutes les matrices X telles que $e^{tX} \in G$ pour tout réel t. Si nous prenons le groupe linéaire général, il y a une certaine ambiguïté car il y a une différence entre $\mathrm{Lie}(\mathrm{GL}(n, \mathbb{R}))$ et $\mathfrak{gl}(n, \mathbb{R})$, puisqu'ils ont des algèbres de Lie différentes provenant d'un crochet de Lie de champs de vecteurs dans le premier cas et d'un crochet de commutateur de matrices dans le second cas (c'est-à-dire que c'est une algèbre de Lie matricielle). Cependant, on peut prouver qu'il existe un isomorphisme explicite entre les algèbres de Lie données par une composition d'applications naturelles

$$\mathrm{Lie}(\mathrm{GL}(n, \mathbb{R})) \to T_{\mathbb{I}_n}\mathrm{GL}(n, \mathbb{R}) \to \mathfrak{gl}(n, \mathbb{R}).$$

Le premier isomorphisme est un espace vectoriel entre l'algèbre de Lie et l'espace tangent au groupe de Lie à la matrice identité. Cependant, le groupe linéaire général est un sous-ensemble ouvert de $\mathfrak{gl}(n, \mathbb{R})$, il y a donc un isomorphisme de l'espace tangent à l'algèbre de Lie matricielle. Si G est un groupe de Lie matriciel avec une algèbre de Lie correspondante $\mathfrak{g}$ et que X et Y sont des éléments de $\mathfrak{g}$, alors les éléments suivants sont vrais :

$$\begin{aligned} AXA^{-1} &\in \mathfrak{g} \text{ pour tout } A \in G, \\ sX &\in \mathfrak{g} \text{ pour tout } s \in \mathbb{R}, \\ X + Y &\in \mathfrak{g}, \\ XY - YX &\in \mathfrak{g}. \end{aligned}$$

Il s'ensuit que l'algèbre de Lie d'un groupe de Lie matriciel est une algèbre de Lie réelle où le crochet est donné par ce que l'on pourrait appeler le commutateur :

$$[X, Y] = XY - YX.$$

Un groupe de Lie matriciel est complexe si son algèbre de Lie associée est un sous-espace complexe de $M_n(\mathbb{C})$. Les groupes linéaires généraux et spéciaux sur les nombres complexes sont des exemples évidents de groupes de Lie de matrices complexes.

Pour donner quelques exemples, l'algèbre de Lie de $\mathrm{GL}(n, \mathbb{C})$ est l'espace de toutes les matrices $n \times n$ à entrées complexes, l'algèbre de Lie de $\mathrm{SL}(n, \mathbb{C})$ est la même avec des entrées réelles, l'algèbre de

Lie de $\mathrm{SL}(n,\mathbb{C})$ est l'espace de toutes les matrices complexes $n \times n$ à trace nulle, et on peut deviner ce qu'est l'algèbre de Lie de $\mathrm{SL}(n,\mathbb{R})$. Les algèbres de Lie de ces groupes sont dénotées par les lettres gothiques habituelles. En continuant de cette façon, l'algèbre de Lie du groupe unitaire $\mathrm{U}(n)$ consiste en l'espace des matrices complexes telles que l'on a pour l'adjoint

$$X^* = -X$$

et l'algèbre de Lie de $\mathrm{SU}(n)$ est le sous-espace de l'espace précédent où l'on prend les matrices à trace nulle. L'algèbre de Lie du groupe orthogonal $\mathrm{O}(n)$ est l'espace des matrices réelles telles que

$$X^{\mathrm{Tr}} = -X$$

et l'algèbre de Lie du groupe orthogonal spécial est le même à nouveau. Un groupe intéressant engendré de manière finie est le groupe de Heisenberg discret H. Il peut être défini comme le tableau suivant pour les entiers x, y et z :

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}.$$

L'algèbre de Lie de ce groupe est l'espace de toutes les matrices de la forme

$$\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$$

où a, b et c sont des nombres réels [5].

Nous pourrions aussi nous demander si le lien entre les groupes de Lie et les algèbres de Lie se transmet aux applications entre elles, et cela s'avère être le cas : les homomorphismes de groupes de Lie entre deux groupes de Lie induisent une application entre les algèbres de Lie correspondantes. On peut démontrer comme conséquence que les groupes de Lie isomorphes doivent avoir des algèbres de Lie isomorphes. Spécifiquement, si G et H sont des groupes de Lie matriciels avec des algèbres de Lie respectives $\mathfrak{g}$ et $\mathfrak{h}$ et si Φ est un homomorphisme de groupes de Lie, alors il existe une application unique linéaire réelle d'algèbres de Lie telle que

$$\Phi(e^X) = e^{\phi(X)}.$$

Cette application a plusieurs propriétés :

$$\begin{aligned} \phi(AXA^{-1}) &= \Phi(A)\phi(X)\Phi(A)^{-1}, \\ \phi([X,Y]) &= [\phi(X), \phi(Y)], \\ \phi(X) &= \frac{d}{dt}\Phi(e^{tX}). \end{aligned}$$

5. Brian C. Hall, *Lie Groups, Lie Algebras, and Representations : An Elementary Introduction* (Switzerland : Springer, 2015).

En lien avec ses études des algèbres de Lie de Kashiwara-Vergne, Leila Schneps a étudié le groupe de Grothendieck-Teichmüller [6]. L'algèbre de Lie elliptique de Kashiwara-Vergne a certaines propriétés qui sont similaires à l'algèbre de Lie de Grothendieck-Teichmüller $\mathfrak{grt}$, où $\mathfrak{grt}$ est l'espace des polynômes $b \in \mathfrak{ie}_2$ qui satisfont la relation du pentagone, munie du crochet de Poisson (ou d'Ihara)

$$\{b, b'\} = [b, b'] + d_b(b') - d_{b'}(b).$$

Le groupe de Grothendieck-Teichmüller $GT(\mathbb{Q})$ peut être défini comme le groupe formé par les automorphismes de l'opérade unitaire dans les groupoïdes complets de Malcev $PaB^{\wedge}_{+}$, qui se réduisent à l'identité sur les ensembles d'objets de l'opérade. La théorie de Grothendieck-Teichmüller a été créée dans le but d'étudier les groupes d'automorphismes des groupes de classes de correspondance profinis, où ces groupes sont les fondamentaux des espaces de modules des surfaces de Riemann de tous les genres et tout nombre de points marqués. Le but est de trouver de nouvelles propriétés de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, ou même finalement de montrer que $GT(\mathbb{Q})$ est égal à $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ [7].

L'ensemble des associateurs de Drinfel'd, noté $Ass(\mathbb{Q})$, est en bijection avec l'ensemble des équivalences catégoriques d'opérades unitaires dans les groupoïdes complets de Malcev

$$\nu : PaB^{\wedge}_{+} \to CD^{\wedge}_{+}$$

de l'opérade de tresses parenthésées complétées vers l'opérade de diagrammes de cordes. Un associateur de Drinfel'd peut être interprété comme un morphisme d'opérades dans les groupoïdes. Il y a une action naturelle de $GT(\mathbb{Q})$ sur l'ensemble des associateurs de Drinfel'd $Ass(\mathbb{Q})$ par translation à droite. Explicitement, il y a un morphisme

$$\nu : PaB \to CD^{\wedge}$$

qui représente un élément de $Ass(\mathbb{Q})$. Le morphisme

$$\nu \circ \gamma : PaB \to CD^{\wedge}$$

représente l'action d'un élément de $GT(\mathbb{Q})$ sur ν et peut être défini comme un composé où le morphisme ν est étendu à la complétion de l'opérade de tresses parenthésées [8].

6. Pierre Lochak and Leila Schneps, *Open problems in Grothendieck-Teichmüller theory*, *Proceedings of Symposia in Pure Mathematics*, 75, 165–186 (2006).

7. Leila Schneps, *The Grothendieck-Teichmüller group : a survey*, in Pierre Lochak et Leila Schneps (éds.), *Geometric Galois Actions, 1* (Cambridge : Cambridge University Press, 1997).

8. Benoit Fresse, *Homotopy of Operads and Grothendieck-Teichmüller Groups : The Applications of Rational Homotopy Theory Methods* (Providence. Rhode Island : American Mathematical Society, 2017).