Géométrie algébrique et nombre p-adique

Marc Abboud

Ecole d'été mathéphysique

Le but de mon exposé est de vous montrer la preuve du fait suivant que je démontre dans un papier.

Theorem 0.1. *Soit d un entier et H un groupe nilpotent qui agit de manière fidèle sur $\mathbf{C}^d$ par automorphismes polynomiaux, alors*

$$d \geq \mathrm{vdl}(H)$$

où $\mathrm{vdl}(H)$ *est la longueur de résolubilité virtuelle de H.*

Il y a beaucoup de mots différents dans ce théorème et on va les voir un à un. La preuve utilise des groupes de Lie et de l'analyse p-adique. Je fais donc des rappels de géométrie différentielle, de groupe de Lie et j'introduis l'analyse p-adique avant de vous montrer comment prouver ce théorème. Les résultats que je présente dans ce texte sur la géométrie différentielle ou les groupes de Lie sont énoncés sans preuve mais ils peuvent tous être retrouvés dans les polys de Frédéric Paulin. Surtout la géométrie différentielle se comprend avec des dessins et il n'y en a pas dans ce texte, je ne peux que conseiller vivement d'aller voir un poly ou un livre pour des illustrations plus complètes des objets que j'utilise ici.

La première partie est consacrée à des rappels d'analyse et de géométrie différentielle, la deuxième aux groupes de Lie, la troisième à la construction des nombres p-adiques et à l'analyse p-adique, la quatrième définit la notion de groupes nilpotents et la dernière partie est consacrée à la preuve du théorème. Les deux parties qui contiennent des maths moins communes et intéressantes sont surtout les parties 3 et 5.

1 Géométrie Différentielle

On va d'abord parler d'analyse sur $\mathbf{R}^n$ avant de parler de variétés. Pour une très bonne ressource sur la géométrie différentielle, regarder le poly de Frédéric Paulin ou celui d'Olivier Biquard.

1.1 sur $\mathbf{R}^n$

Definition 1.1. Soit U un ouvert de $\mathbf{R}^n$ et $f : U \to \mathbf{R}^m$ une fonction continue. Soit $x \in U$, on dit que f est *différentiable* au point x s'il existe une application linéaire $L_x : \mathbf{R}^n \to \mathbf{R}^m$ telle que

$$f(x+h) =_{h\to 0} f(x) + L_x(h) + o(||h||)$$

L_x est la différentielle de f au point x, on la note $D_x f$.

On dit que f est différentiable sur U si elle est différentiable en tout point de U. Être différentiable est donc une propriété locale. Par définition de la différentielle, si $c : \mathbf{R} \to U$ est une courbe C^1 sur U, alors $\frac{d}{dt}_{|t=0} f(c(t)) = D_{c(0)} f(\dot{c}(0))$.

L'application f est alors C^1 si la fonction $x \in U \mapsto D_x f \in M_{n\times m}(\mathbf{R}) \simeq \mathbf{R}^{nm}$ est continue. Si on peut itérer le procédé de prendre la différentielle sur chaque point de U, on dit que f est C^∞. Une fonction C^∞ est appelée lisse. Dans la suite, toutes les fonctions qu'on considère seront lisses sauf mention contraire.

Example 1.2. Soit $f : \mathbf{R} \to \mathbf{R}$ une fonction dérivable en un point a, alors on sait que

$$f(a+h) =_{h\to 0} f(a) + f'(a)h + o(|h|)$$

Donc la différentielle de f au point a est l'application linéaire $h \mapsto f'(a)h$.

Example 1.3. Tout application linéaire est différentiable en tout point et sa différentielle est elle-même.

Si $B : \mathbf{R}^n \times \mathbf{R}^n \to \mathbf{R}^m$ est une application bilinéaire, alors B est différentiable en tout point x, y et on a $D_{(x,y)}B(u, v) = B(u, y) + B(x, v)$.

Definition 1.4. Une fonction lisse $\varphi : U \to \mathbf{R}^n$ est un *difféomorphisme* si elle admet un inverse qui est aussi lisse. C'est un *difféomorphisme local* si localement autour de chaque point de U la restriction de φ est un difféomorphisme, c'est équivalent à ce que la différentielle soit injective en chaque point.

Definition 1.5. Un *champ de vecteurs* sur un ouvert $U \subset \mathbf{R}^n$ est une fonction $X : U \to \mathbf{R}^n$.

Les champs de vecteurs doivent être vus comme une fonction qui en chaque point de l'ouvert nous dit dans quelle direction aller et avec quelle vitesse. Plus précisément, une équation différentielle est une équation de la forme

$$\dot{c}(t) = X(c(t))$$

avec une condition initiale $c(0) = x \in U$, cette équation est l'équation différentielle associée à X. Une solution c de l'équation est appelée une courbe intégrale de x.

Example 1.6. Soient $e_1, \cdots, e_n$ la base canonique de $\mathbf{R}^n$, alors le champ de vecteurs X_{e_i} est défini par $X_{e_i}(x) = e_i$. Les courbes intégrales de X_{e_i} sont les droites verticales qui varient selon la i-ème coordonnée.

On a une image claire sur $\mathbf{R}^n$ des vecteurs tangents en un point. On dit qu'un vecteur tangent en un point x est la donnée d'une courbe $c :]-\varepsilon, \varepsilon[\to \mathbf{R}^n$ telle que $c(0) = x$ et d'un vecteur $v = \dot{c}(0)$. Physiquement, un vecteur tangent est un vecteur vitesse et on note $T_x\mathbf{R}^n$ l'ensemble des vecteurs tangents en x. En particulier, si $f : U \subset \mathbf{R}^n \to \mathbf{R}^m$ est une fonction lisse, alors la différentielle de f au point x induit une application linéaire sur les espaces tangents $D_x f : T_x U \to T_{f(x)}\mathbf{R}^m$. En effet, si $c :]-\varepsilon, \varepsilon[\to \mathbf{R}^n$ est une courbe telle que $c(0) = x$, alors $f \circ c$ est une courbe $]-\varepsilon, \varepsilon[\to \mathbf{R}^m$ telle que $f \circ c(0) = f(x)$ et on a $\frac{d}{dt}_{|t=0} f \circ c(t) = D_{c(0)} f(\dot{c}(0)) = D_x f(\dot{c}(0))$.

Definition 1.7 (Tiré en arrière d'un champ de vecteurs)**.** Soient U, V deux ouverts de $\mathbf{R}^n$, $\varphi : U \to V$ un difféomorphisme local et Y un champ de vecteurs sur V, le tiré en arrière de Y est le champ de vecteurs X sur U tel que

$$\forall x \in U, \quad X(x) = (D_x\varphi)^{-1}(Y(\varphi(x)))$$

On peut remarquer que c'est la seule formule qui a un sens d'un point de vue homogénéité.

Theorem 1.8 (Cauchy-Lipschitz)**.** *Pour tout champ de vecteurs X et tout point x de U, il existe un temps $\varepsilon > 0$ et une unique courbe $c_{x,\varepsilon} :]-\varepsilon, +\varepsilon[\to U$ telle que $c_{x,\varepsilon}(0) = x$ et $c_{x,\varepsilon}$ est une courbe intégrale de X.*

Ainsi tout champ de vecteurs peut s'intégrer de manière locale et admet des courbes intégrales locales. Par unicité, lorsqu'on veut étendre une courbe intégrale, il y a une unique manière de le faire. Si x est un point de U, on note $\varepsilon_{X,x}$ le plus grand temps ε telle qu'il existe une courbe intégrale $c :]-\varepsilon, \varepsilon[\to U$ de X telle que $c(0) = x$, la courbe intégrale maximale passant par x est alors la courbe intégrale $c_x :]\varepsilon_{X,x}, \varepsilon_{X,x}[\to U$ de X telle que $c(0) = x$.

Definition 1.9 (Les flots)**.** Soit X un champ de vecteurs, on a vu que X admettait des courbes intégrales locales. Un flot est un objet global qui les encode toutes. Soit

$$V_X = \bigsqcup_{x \in U}]-\varepsilon_{X,x}, \varepsilon_{X,x}[\times \{x\},$$

on peut montrer que V_X est un ouvert de $\mathbf{R} \times \mathbf{R}^n$. Le flot maximal Φ_X associé à X est l'unique fonction $\Phi_X : V_X \to U$ telle que $\Phi_X(t, x) = c_x(t)$ où c_x est l'unique courbe intégrale maximale de X passant par x. On écrira Φ au lieu de Φ_X si le contexte est clair. On note $\Phi_t := \Phi(t, \bullet)$.

Proposition 1.10 (Propriétés du flot)**.** *Voici les différentes propriétés du flot*

1. *Soient $s, t \in \mathbf{R}$, alors $\Phi(s, \Phi(t, x)) = \Phi(t, \Phi(s, x)) = \Phi(s + t, x)$.*
2. *$\Phi_0 = \mathrm{id}$ et pour tout temps t, Φ_t est un difféomorphisme d'inverse Φ_{-t}.*
3. *$\frac{\partial}{\partial t}\Phi_t(x) = X(\Phi_t(x))$.*

1.2 Les variétés

On sait maintenant faire de l'analyse sur $\mathbf{R}^n$, les variétés sont des espaces géométriques qui localement ressembe à $\mathbf{R}^n$ et c'est donc le bon objet sur lequel faire de l'analyse.

Definition 1.11. Soit V un espace métrique, V est une variété différentielle si pour tout point x de V, il existe un ouvert U contenant x et un homéomorphisme $\varphi : U \to W$ où W est un ouvert de $\mathbf{R}^n$. On dit que φ, U est une carte en x de V. On demande de plus que si $\psi : U' \to W'$ est une autre carte locale de V en x, alors l'application $\psi \circ \varphi^{-1} : \varphi(U \cap U') \to W'$ est C^∞.

Soit $f : V \to V'$ une application continue entre deux variétés, f est lisse en un point $x \in V$ si pour toute carte locale φ de V en x et toute carte locale ψ de V en $f(x)$, la fonction $\psi \circ f \circ \varphi^{-1}$ est lisse.

On sait donc définir des fonctions lisses mais il faut comprendre ce que la différentielle d'une fonction veut dire sur une variété. Concrètement, on a envie de passer dans les cartes et prendre la différentielle dans les cartes mais cette opération dépend de la carte que l'on choisit. Pour remédier à ce problème, on définit l'espace tangent de la variété en un point.

Definition 1.12. Si $\varphi : U \to \mathbf{R}^n$ est une carte locale de V, on note $x_i : U \to \mathbf{R}$ les fonctions telles que $\varphi = (x_1 \cdots, x_n)$, on dit que les x_i sont des *coordonnées locales* sur V.

Definition 1.13. Soit V une variété et x un point de V, un *jet de courbe* en x est une fonction C^1 $c :]-\varepsilon, \varepsilon[\to V$ telle que $c(0) = x$. Fixons une carte locale φ de V en x. Le *vecteur tangent* d'une courbe c en x est le vecteur $v = \frac{d}{dt}_{|t=0} \varphi \circ c(t) \in \mathbf{R}^n$. Un vecteur tangent est donc un couple de la forme (x, v) où x est un point de la variété V et v est le vecteur dérivé d'une courbe c telle que $c(0) = x$ au temps 0. On identifie deux couples $(x, v), (x, w)$ si les courbes dont proviennent v et w ont même vecteur dérivé en 0. L'espace des vecteurs tangents en x est un espace vectoriel.

Cette définition ne dépend pas de la carte φ choisie car si on prenait une autre carte ψ, le difféomorphisme $\psi \circ \varphi^{-1}$ induit un isomorphisme sur l'espace des vecteurs tangents vu par rapport à la carte φ et la carte ψ par la différentielle $D_{\varphi(x)}(\psi \circ \varphi^{-1})$ donc on peut les identifier.

Definition 1.14. Pour une variété V, on définit le fibré tangent TV qui est la donnée pour chaque point x de V de l'espace tangent au-dessus de X. C'est un espace qui a une structure de variété différentielle mais je ne vais pas l'expliciter plus que ça ici. Un champ de vecteurs sur V est alors une fonction lisse $X : V \to TV$ telle que pour tout x de V, $X(x)$ est un vecteur tangent en x.

Avec cette définition on voit comment un champ de vecteurs sur un ouvert de $\mathbf{R}^n$ induit un champ de vecteurs local sur V. En effet soit $\varphi : U \to \mathbf{R}^n$ une carte locale de V et $X : \varphi(U) \to \mathbf{R}^n$ un champ de vecteurs sur $\varphi(U)$, alors $\widetilde{X} := X \circ \varphi$ est un champ de vecteurs sur U. En effet, on note Φ_t le flot de X sur $\varphi(U)$, soit $x \in U$, alors $\widetilde{X}(x) = X(\varphi(x)) = \frac{d}{dt}_{|t=0} \Phi_t(\varphi(x))$ et la fonction $t \mapsto \varphi^{-1} \circ \Phi_t(\varphi(x))$ est un jet de courbe C^1 en x. En particulier, si $x_1, \cdots, x_n$ sont les coordonnées locales sur V associée à φ, alors on note $\frac{\partial}{\partial x_i}$ le champ de vecteurs sur U qui correspond au champ de vecteurs X_{e_i} sur $\varphi(U)$. C'est le champ de vecteurs sur V dont les courbes intégrales consistent à augmenter la coordonnée x_i avec une vitesse 1 dans la carte $\varphi(U)$.

On peut maintenant définir l'application tangente pour une application entre variétés qui généralise la notion de différentielle.

Definition 1.15. Soit $f : N \to M$ une application lisse entre variété, pour tout $x \in N$, f induit une application linéaire sur les espaces tangents en x et $f(x)$ que l'on note $T_x f : T_x N \to T_{f(x)} M$ et qui est définie ainsi. Soit $\varphi : U \subset N \to \mathbf{R}^n$ et $\psi : V \subset M \to \mathbf{R}^m$ des cartes locales de N et M en x et $f(x)$, alors $T_x f$ est défini comme la différentielle en $\varphi^{-1}(x)$ de l'application $\psi \circ f \circ \varphi^{-1}$ et cette définition ne dépend pas du choix des cartes.

L'application $Tf : (x, v) \in TV \mapsto T_x f(v)$ est appelée *application tangente* de f.

1.2.1 Le crochet de Lie de champs de vecteurs

On veut construire une opération de crochet de Lie sur les champs de vecteurs. L'exemple le plus classique est celui des opérateurs linéaires sur un espace vectoriel E. Pour $a, b \in \mathcal{L}(E)$ le crochet défini par $[a, b] := a \circ b - b \circ a$ est un crochet de Lie. On va adopter un autre point de vue sur les champs de vecteurs pour les interpréter comme des opérations linéaires et pouvoir définir le crochet de Lie de champs de vecteurs.

Definition 1.16. On considère l'espace $\mathcal{F} := C^\infty(V, \mathbf{R})$ des fonctions lisses de la variété V vers $\mathbf{R}$. On appelle *dérivation* une application linéaire $\delta : \mathcal{F} \to \mathcal{F}$ telle que pour tout $f, g \in F, \delta(fg) = \delta(f)g + f\delta(g)$ (la règle de Leibnitz). On note $\mathrm{Der}(\mathcal{F})$ l'espace des dérivations sur $\mathcal{F}$.

On a le crochet de Lie sur $\mathrm{Der}(\mathcal{F})$ défini par $[\delta, \delta'] = \delta \circ \delta' - \delta' \circ \delta$.

Pour tout champs de vecteurs X, on peut définir une dérivation canoniquement associée $\mathcal{L}_X : \mathcal{F} \to \mathcal{F}$ ainsi

$$\mathcal{L}_X(f)(x) = T_x f(X(x)) = \frac{d}{dt}_{|t=0} f(\Phi_t^X(x))$$

C'est à dire que le champs de vecteurs X dérive la fonction f au point x selon la direction du vecteur tangent $X(x)$ en x. En fait, c'est la seule manière de construire des dérivations.

Theorem 1.17. *Pour toute dérivation $\delta : \mathcal{F} \to \mathcal{F}$ il existe un unique champ de vecteurs X tel que $\delta = \mathcal{L}_X$*

Definition 1.18. Soient X, Y deux champs de vecteurs sur V, on définit le crochet de Lie $[X, Y]$ comme l'unique champs de vecteurs associé à la dérivation $[\mathcal{L}_X, \mathcal{L}_Y]$ c'est à dire que l'on a $\mathcal{L}_{[X,Y]} = \mathcal{L}_X \circ \mathcal{L}_Y - \mathcal{L}_Y \circ \mathcal{L}_X$.

C'est à dire que le crochet de Lie entre deux champs de vecteurs est le champ de vecteur qui mesure à quel point dériver selon la direction induite par X puis dériver selon la direction induite par Y est une opération différente de celle où on dérive par rapport à Y puis par rapport à X.

Proposition 1.19. *Soient X, Y deux champs de vecteurs sur une variété V et $x \in V$, alors*

1. *$[X, Y](x) = 0$ si et seulement si les flots locaux de X et Y en x commutent pour tout temps suffisament peits.*
2. *Soit Φ_t^X le flot local associé à X en x, alors $[X, Y](x) = \frac{d}{dt}_{|t=0}(\Phi_t^X)^* Y(x)$.*
3. *Soit U un ouvert de V, alors $[X, Y]_{|U} = [X_{|U}, Y_{|U}]$.*
4. *Si $\varphi : V' \to V$ est un difféomorphisme, alors $[\varphi^* X, \varphi^* Y] = \varphi^*[X, Y]$.*
5. *Soit $\varphi : U \subset V \to \mathbf{R}^n$ une carte locale de V et $x_1, \cdots, x_n$ les coordonnées locales associées, alors si X s'écrit $X(x) = \sum_i u_i(x)\partial_i$ et $Y(x) = \sum_i v_i(x)\partial_i$, on a*

$$[X, Y](x) = \sum_{i=1}^{n} \left(\sum_{j=0}^{n} u_j(x) \frac{\partial v_j}{\partial x_j}(x) - v_j(x) \frac{\partial u_i}{\partial x_j}(x) \right) \partial_i.$$

6. *Si on reste dans des cartes locales et que l'on considère X et Y comme des fonctions $X, Y : U \to \mathbf{R}^n$, alors $[X, Y](x) = \mathcal{L}_X(Y)(x) - \mathcal{L}_Y(X)(x)$.*

1.3 Sous-variétés

Une variété est considérée sans espace euclidien ambiant. Les sous-variétés permettent d'exhiber des exemples de variétés à partir d'un espace ambiant euclidien.

Definition 1.20. Soit $f : \mathbf{R}^n \to \mathbf{R}^m$ une application lisse. Soit $x \in \mathbf{R}^n$, on dit que f est une immersion en x si la différentielle de f en x est injective (ce qui implique $n \leq m$). On dit que f est une submersion en x si la différentielle de f en x est surjective (ce qui implique $n \geq m$).

Il y a 5 manières équivalentes de définir les sous-variétés de $\mathbf{R}^n$, on en expose ici que 2.

Definition 1.21. Soit V un sous-espace de $\mathbf{R}^n$ et x un point de V, on dit que V est une sous-variété en x si

1. (Paramétrisation) Il existe une application $\varphi : U \subset \mathbf{R}^d \to \mathbf{R}^n$ telle que $\varphi(0) = x$ et $\varphi(U) \subset V$ et φ est une immersion en 0, l'espace tangent en x de V est alors l'image de $D_0\varphi$.
2. (Équation) Il existe un ouvert $W \subset \mathbf{R}^n$ contenant x et une application $f : W \to \mathbf{R}^a$ qui est une submersion en x telle que $W \cap V = f^{-1}(\{0\})$. L'espace tangent en x de V est alors le noyau de $D_x f$.

On peut montrer que ces deux définitions sont équivalentes. En pratique, on travaille quasiment toujours avec des sous-variétés car le fait de posséder un espace ambiant rend plusieurs définitions plus concrètes comme celle de vecteur tangent par exemple (il suffit de prendre les vecteurs vitesses dans $\mathbf{R}^n$ des courbes qui restent dans la sous-variété V). Un autre point intéressant est que la représentation par équation des sous-variétés permet de trouver facilement l'espace tangent en chaque point comme on le verra dans le cas des groupes de Lie.

Example 1.22. Soit $\mathbb{S}^n$ la sphère unité en dimension n, alors $\mathbb{S}^n$ est donnée par l'équation $||x||^2 = 1$. Soit f la fonction définie par $f(x) = ||x||^2$, alors pour tout $x \in \mathbb{S}^n, D_x f(h) = 2\langle x, h\rangle$. Donc l'espace tangent de $\mathbb{S}^n$ en x est bien l'orthogonal de x.

2 Les groupes de Lie

Un groupe de Lie est un groupe qui a une structure de variété différentielle compatible avec les lois de groupe. Plus précisément,

Definition 2.1. Un groupe G est un ensemble muni d'une opération $\cdot : G \times G \to G$ telle que

1. il existe un élement neutre e tel que $\forall g \in G, eg = ge = g$.
2. Pour tout $g \in G$, il existe $h \in G$ tel que $gh = hg = e$.
3. Pour tout $g, h, f \in G, (fg)h = f(gh)$.

Definition 2.2. Un groupe de Lie sur $\mathbf{R}$ est un groupe muni d'une structure de variété différentielle lisse telle que

1. Si on note $\iota : G \to G$ la fonction de passage à l'inverse, alors ι est lisse.
2. pour tout $g \in G$, on écrit $L_g : h \in G \mapsto gh$, alors L_g est lisse.

Un morphisme de groupes de Lie est alors un morphisme de groupe qui est aussi lisse au sens des variétés différentielles.

Example 2.3. Soit n un entier, $GL_n(\mathbf{R})$ est un ouvert de $M_n(\mathbf{R}) \simeq \mathbf{R}^{n^2}$, c'est donc une variété différentielle. Comme le produit matriciel et le passage à l'inverse sont donnés par des formules polynomiales en les coefficients, c'est un groupe de Lie réel.

Le groupe $(\mathbf{R}^d, +)$ est un groupe de Lie commutatif de dimension $\mathbf{R}$, $\mathbf{S}^1$ est un groupe de Lie commutatif de dimension 1.

$O_n(\mathbf{R}) = \{A \in GL_n(\mathbf{R}) : {}^tAA = \mathrm{id}\}$ et $SO_n(\mathbf{R})$ sont aussi des groupes de Lie réel. Le groupe $U_n = \left\{U \in GL_n(\mathbf{C}) : U^\dagger U = \mathrm{id}\right\}$ et SU_n sont des groupes de Lie réels (mais pas complexe, mea culpa Benji !!).

2.1 L'algèbre de Lie d'un groupe de Lie

Definition 2.4. Une algèbre de Lie $\mathfrak{g}$ sur $\mathbf{R}$ est un espace vectoriel réel muni d'une opération bilinéaire $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ telle que

1. Pour tout $X \in \mathfrak{g}, [X, X] = 0$.
2. Pour tout $X, Y, Z \in \mathfrak{g}, [X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0$.

On dit que $[\cdot,\cdot]$ est le crochet de Lie de $\mathfrak{g}$.

Étant donné que G est aussi une variété différentielle, on peut parler de l'espace tangent en l'identité qui traduit la géométrie de G autour de l'élément neutre. Mais comme la multiplication est lisse, la géométrie autour de l'élément neutre se transporte par multiplication donc la structure de l'espace tangent en l'identité a des impacts sur la géométrie globale du groupe. On note $\mathfrak{g}$ l'espace tangent de G en son élément neutre. C'est l'algèbre de Lie de G, on définit le crochet de Lie dans la suite.

Example 2.5. L'espace tangent en l'identité de $GL_n(\mathbf{R})$ est $M_n(\mathbf{R})$. Plus généralement, pour un espace vectoriel réel V, on note $GL(V)$ le groupe de Lie des applications linéaires inversibles sur V et $\mathfrak{gl}(V)$ l'espace tangent en l'identité de $GL(V)$ qui est l'ensemble des applications linéaires sur V.

Soit $g \in G$, on note $\iota_g : h \in G \mapsto h^{-1}gh$ l'application de conjugaison par g. On peut différentier ι_g en l'identité:

$$\mathrm{Ad} : g \in G \mapsto T_e\iota_g \in GL(T_eG)$$

l'application Ad est la représentation adjointe de G, c'est une application lisse entre variété différentielle et on peut encore la différentier en l'identité.

$$\mathrm{ad} = T_e \,\mathrm{Ad} : T_eG \to \mathfrak{gl}(T_eG)$$

Ainsi, pour tout $X \in \mathfrak{g}, \mathrm{ad}(X)$ est une application linéaire sur $\mathfrak{g}$. On définit le crochet de Lie sur $\mathfrak{g}$ ainsi

$$\forall X, Y \in \mathfrak{g}, \quad [X, Y] := \mathrm{ad}(X)(Y)$$

On peut montrer que $\mathfrak{g}$ munit de cette opération est bien une algèbre de Lie, c'est fait dans n'importe quel poly sur les groupes de Lie.

Example 2.6. On considère le groupe de Lie réel $GL_n(\mathbf{R})$. Soit $A \in GL_n(\mathbf{R})$, l'application ι_A est linéaire donc sa différentielle est elle-même. Donc $\mathrm{Ad}(A) = \iota_A$ vu comme application linéaire sur $M_n(\mathbf{R})$. Soit $Y \in M_n(\mathbf{R})$ on veut maintenant différentier l'application $A \in GL_n(\mathbf{R}) \mapsto (\iota_A : Y \mapsto AYA^{-1}) \in \mathfrak{gl}(M_n(\mathbf{R})$ en l'identité par rapport à A. Cette application est la composée de la fonction $A \in GL_n(\mathbf{R}) \mapsto (A, A^{-1}) \in GL_n(\mathbf{R})^2$ dont la différentielle en l'identité est

$$X \in M_n(\mathbf{R}) \mapsto (X, -X) \in M_n(\mathbf{R})^2$$

et de la fonction $B, C \in GL_n(\mathbf{R}) \times GL_n(\mathbf{R}) \to (Y \mapsto BYC) \in \mathfrak{gl}(M_n(\mathbf{R}))$ dont la différentielle en $(\mathrm{id}, \mathrm{id})$ est

$$U, V \in M_n(\mathbf{R})^2 \mapsto (Y \mapsto UY + YV) \in \mathfrak{gl}(M_n(\mathbf{R}))$$

par la règle de la chaîne on obtient que pour tout $X, Y \in M_n(\mathbf{R})$, $\mathrm{ad}(X)(Y) = XY - YX$ et on retrouve bien le crochet de commutation de matrices que l'on connait.

Example 2.7. Un autre exemple utile en mécanique quantique est le groupe $SO_n(\mathbf{R})$. On sait que la sous-variété $O_n(\mathbf{R})$ est définie par l'équation ${}^tAA = \mathrm{id}$, lorsque l'on différentie cette équation en l'identité on obtient ${}^tX + X = 0$. Ainsi, l'algèbre de Lie $\mathfrak{o}_n(\mathbf{R}) = \mathfrak{so}_n(\mathbf{R})$ est celle des matrices antisymétriques muni du crochet de Lie des matrices.

2.2 L'algèbre des champs de vecteurs invariants

On sait que pour n'importe quelle variété différentielle, on peut considérer l'algèbre de Lie des champs de vecteurs sur la variété. Ici, on a une loi de groupe en plus donc on va considérer les champs de vecteurs qui sont invariants par cette loi.

Definition 2.8. On dit qu'un champ de vecteurs $\overline{X}$ sur G est invariant par translation si pour tout $g \in G$, on a

$$(L_g)^* \overline{X} = \overline{X}.$$

On note ${}^G\Gamma(T(G))$ l'algèbre de Lie des champs de vecteurs invariants par translation.

En particulier, on voit que la valeur de $\overline{X}$ en e détermine complètement X, en effet

$$\overline{X}(g) = (L_{g^{-1}})^* \overline{X}(g) = T_e L_g(\overline{X}(e))$$

Réciproquement, si X est un élément de $\mathfrak{g}$ alors X détermine un unique champ de vecteurs invariant par translation $\overline{X}$ qui est défini par $\overline{X}(g) := T_e L_g(X)$.

Proposition 2.9. *L'application $X \in \mathfrak{g} \mapsto \overline{X} \in {}^G\Gamma(T(G))$ est un isomorphisme d'algbèbre de Lie.*

On a donc une interprétation de l'algèbre de Lie de G comme une algèbre de champs de vecteurs.

Proposition 2.10. *Tout morphisme de groupes de Lie $f : G \to H$ induit un morphisme d'algèbre de Lie par l'application tangente $T_e g : T_e(G) \to T_e(H)$.*

On peut définir maintenant l'application exponentielle d'un groupe de Lie.

Definition 2.11. Soit $X \in \mathfrak{g}$, alors X définit un unique champ de vecteurs $\overline{X}$ invariant sur G, soit Φ_t le flot associé à $\overline{X}$, on définit

$$\exp(X) := \Phi_1(e)$$

Proposition 2.12. *On a les propriétés suivantes*

1. $\exp : \mathfrak{g} \to G$ *est une application lisse.*
2. *l'application $t \in \mathbf{R} \mapsto \exp(tX)$ est la courbe intégrale de $\overline{X}$ passant par e et c'est un morphisme de groupes de Lie.*
3. *La différentielle de* exp *en 0 est l'identité.*
4. *L'image de* exp *est un ouvert de G qui engendre la composante connexe de l'élément neutre de G.*

L'application exponentielle permet de relever des applications sur les espaces tangents, plus précisément

Definition 2.13. Soit U un ouvert de G contenant id et tel que $U^{-1} = U$ et H un groupe de Lie. Un *morphisme local* de groupe de Lie est une application lisse $\varphi : U \to H$ tel que $\varphi(e_g) = e_H$ et pour tout $x, y \in U$ tel que $xy \in U$, on a $\varphi(xy) = \varphi(x)\varphi(y)$. Un morphisme local induit un morphisme d'algèbre de Lie par son application tangente en l'élément neutre.

Proposition 2.14. *Soit G, H deux groupes de Lie et $Tf : \mathfrak{g} \to \mathfrak{h}$ un homomorphisme entre les algèbres de Lie, alors il existe un morphisme local $f : U \to H$ dont l'application tangente est Tf. Deux tels morphismes locaux coîcident sur un ouvert contenant l'identité.*

Si G est simplement connexe, alors Tf se relève de manière unique en un morphisme de groupes de Lie $f : G \to H$.

Proposition 2.15. *Soit $f : G \to H$ un morphisme de groupe continu entre deux groupes de Lie, alors f est lisse.*

3 Suites de Cauchy, norme ultramétrique

3.1 Suites de Cauchy et espace complet

Soit X un espace métrique muni d'une distance $d : X \times X \to X$. Une suite (x_n) est de Cauchy si pour tout $\varepsilon > 0$, il existe un entier $N \geq 0$, tel que pour tout n, m, on a $d(x_n, x_m) < \varepsilon$.

Un espace est complet si les suites de Cauchy convergent.

Proposition 3.1. $\mathbf{R}$ *est complet.*

Si un espace n'est pas complet, on peut le compléter. C'est à dire prendre un espace un peu plus gros dans lequel toutes les suites de Cauchy convergent. Plus précisément,

Theorem 3.2. *Soit X un espace métrique, il existe un unique espace métrique Y tel que X est dense dans Y et tel que Y est complet, Y s'appelle le complété de X.*

Par exemple, le complété de $\mathbf{Q}$ pour la valeur absolue est $\mathbf{R}$.

3.1.1 L'exemple des séries formelles

Soit $\mathbf{K}$ un corps et $\mathbf{K}[X]$ l'espace vectoriel des polynômes à une variable à coefficients dans $\mathbf{K}$. On définit une valuation v sur $\mathbf{K}[X]$ ainsi: si $P = \sum_i a_i X^i$ où les coefficients a_i sont presque tous nuls, alors

$$v(P) := \min \{k \in \mathbf{N} : a_k \neq 0\}$$

$v(P)$ est alors l'ordre d'annulation de P en 0 ou bien la plus grande puissance du polynôme X qui divise P. On définit une norme associée à v par $||P|| := e^{-v(P)}$. C'est à dire que plus un polynôme est divisible par X, plus il est petit. En particulier, la suite (X^n) tend vers 0. Cet espace n'est pas complet, en effet soit (P_n) la suite définie par $P_n = \sum_{k=0}^{n} X^k$, alors $v(P_n - P_m) \leq \min(m, n)$ car tous les termes en X^l pour $l \leq n$ sont tués. Le complété de $\mathbf{K}[X]$ pour cette norme est $\mathbf{K}[[X]]$ l'espace des séries formelles à coefficients sur $\mathbf{K}$.

3.1.2 Les nombres p-adiques et les espaces ultramétriques

Soit $\mathbf{K}$ un corps, on appelle valeur absolue sur $\mathbf{K}$ une application $|\cdot| : \mathbf{K} \to \mathbf{R}_+$ telle que $|\cdot|$ est une distance avec les propriétés suivantes

$$|1| = 1, \quad |xy| = |x|\,|y|$$

On dit qu'une norme est ultramétrique si on peut remplacer l'inégalité triangulaire peut être remplacée par

$$|x + y| \leq \max(|x|, |y|)$$

Si $|\cdot|$ est une valeur absolue ultramétrique, alors l'ensemble $\{x \in \mathbf{K} : |x| \leq 1\}$ est un anneau dont les éléments inversibles sont les éléments de norme 1. La manière la plus simple de créer des valeurs absolues ultramétrique est d'utiliser les valuations.

Une application $v : \mathbf{K} \to \mathbf{R} \cup \{\infty\}$ est une valuation si

1. $v(0) = \infty$.
2. $v(xy) = v(x) + v(y)$.
3. $v(x + y) \geq \min(v(x), v(y))$.

L'exemple à avoir en tête est celui des valuations p-adiques sur les entiers, que l'on peut étendre aux rationnels. Un autre exemple est l'ordre d'annulation en 0 des polynômes. À toute valuation v, on peut associer une valeur absolue ultramétrique $|\cdot|_v := e^{-v(\cdot)}$ (on aurait pu prendre n'importe quel autre nombre que e).

Dans la suite on suppose que $\mathbf{K}$ est un corps muni d'une valeur absolue ultramétrique pour laquelle il est complet. Les espaces ultramétriques ont une géométrie très différente de celle que l'on connaît.

Proposition 3.3. *Dans* $\mathbf{K}$ *une série* $\sum a_n$ *converge si et seulement si* $a_n \to 0$.

Proof. Si $a_n \to 0$, alors on note $S_N = \sum_{k=0}^{N} a_k$, on montre que c'est une suite de Cauchy. Comme $a_n \to 0$, on a que la suite $u_k = \max_{n \geq k} |a_n|$ tend vers 0, et alors $S_n - S_m = \sum_{k=n+1}^{m} a_k$, donc $|S_n - S_m| \leq u_n$ et c'est donc une suite de Cauchy donc elle est convergente. □

Proposition 3.4. *1. Si* $a, b \in \mathbf{K}$ *et* $|a| > |b|$, *alors* $|a + b| = |a|$.

2. Tout point d'une boule peut être vu comme le centre de la boule.

3. Pour deux boules distinctes, on a la dichotomie suivante: soit elles sont disjointes, soit l'une est inclue dans l'autre.

3.1.3 Les nombres p-adiques

Soit p un nombre premier. Sur l'ensemble des entiers relatifs $\mathbf{Z}$ on a la valuation p-adique v_p définie par

$$v_p(x) := \max \left\{ k \geq 0 : p^k \text{ divise } x. \right\}$$

Cette valuation vérifie bien toutes les propriétés nécessaires et on peut l'étendre à l'ensemble des fractions d'entiers $\mathbf{Q}$ par $v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b)$, cette définition ne dépend pas du choix de représentant pour la fraction $\frac{a}{b}$. On définit la valeur absolue $|\cdot|_p$ sur $\mathbf{Q}$ par $|x|_p := p^{-v_p(x)}$.

On définit $\mathbf{Z}_p$ comme le complété de $\mathbf{Z}$ pour la distance induite par $|\cdot|_p$ et $\mathbf{Q}_p$ comme le complété de $\mathbf{Q}$ pour cette même distance. $\mathbf{Z}_p$ est alors la boule unité de $\mathbf{Q}_p$ et la valuation p-adique s'y étend de façon naturelle.

$\mathbf{Z}_p$ est un espace totalement discontinu, équipotent à l'ensemble de Cantor. On peut voir $\mathbf{Z}_p$ comme une limite projective ainsi

$$\mathbf{Z}_p = \left\{ (a_n) \in \prod \mathbf{Z}/p^n\mathbf{Z} : a_{n+1} \equiv a_n \mod p^n \right\}$$

On peut aussi voir $\mathbf{Z}_p$ autrement (ce qui explique le terme de "bre-nom"), Tout entier x s'écrit en base p de manière unique $x = x_n x_{n-1} \cdots x_1 x_0$.

$$x = \sum_{i \geq 0} x_i p^i$$

où les x_i sont presque tous nuls, la valuation p-adique est alors égale à $v_p(x) = \min \{ i \in \mathbf{N} : x_i \neq 0 \}$, et on voit qu'en fait construire $\mathbf{Z}_p$ revient à faire la même construction entre les polynômes et les séries formelles. Ainsi, un nombre p-adique est un nombre entier qui a une écriture infini vers la gauche en base p (les bre-noms !!), un "vrai" entier est alors un nombre p-adique dont l'écriture en base p est finie.

4 Groupes nilpotents

Soit G un groupe, pour deux éléments $a, b \in G$, on définit le crochet $[a, b] := aba^{-1}b^{-1}$. Deux éléments de G commutent si et seulement si leur crochet est nul. On peut prendre des crochets successifs d'éléments et on notera $[x_1, \cdots, x_d] = [x_1, \cdots, [x_{d-1}, x_d] \cdots]$. Si H, K sont deux sous-groupes de G, on note $[H, K]$ le groupe engendré par $\{[h, k] : h \in H, k \in K\}$.

Sur un groupe commutatif, tous les crochets sont nuls par définition. Les groupes nilpotents sont une généralisation des groupes commutatifs.

Être nilpotent signifie que prendre des crochets successifs ne donne que l'élément neutre au bout d'un temps fixé qui ne dépend pas des éléments choisis pour le crochet. Plus précisément,

Definition 4.1. Soit G un groupe, on définit une suite de sous-groupes $D^n(G)$ et $D_n(G)$ ainsi.

$$D^0(G) = D_0(G) = G, \quad D^{n+1}(G) = [G; D^n(G)], \quad D_{n+1}(G) = [D_n(G), D_n(G)]$$

On dit que G est nilpotent s'il existe un entier e tel que $D^e(G) = \{0\}$ et on dit que G est résoluble s'il existe un indice f tel que $D_f(G) = \{0\}$ et on appelle le plus petit entier f qui vérifie cette propriété la *longueur dérivée* de G que l'on note $\mathrm{dl}(G)$.

En particulier, un groupe nilpotent est résoluble.

La grande différence est que dans la suite $D^n(G)$ on fait des crochets avec n'importe quel élément alors que dans le cas de la suite $D_n(G)$ on ne s'autorise à faire des crochets qu'avec les éléments qui sont déjà des crochets.

Example 4.2. Un groupe commutatif est nilpotent et résoluble de longueur dérivée 1.

On peut montrer que toute matrice de $SL_n(\mathbf{R})$ est un crochet de matrices de déterminant 1, donc $SL_n(\mathbf{R}), [SL_n(\mathbf{R})] = SL_n(\mathbf{R})$ n'est pas nilpotent.

Enfin, le groupe des transformations affines $\{x \mapsto ax + b : a, b \in \mathbf{R}, a \neq 0\}$ est résoluble mais pas nilpotent. En effet, le crochet de deux transformations est une application linéaire de la forme $x \mapsto cx$ et le groupes des applications linéaires est commutatif sur $\mathbf{R}$ mais aucune application linéaire commute avec les translations, sauf l'identité.

On définit exactement les mêmes définitions pour les algèbres de Lie où le crochet de commutation est remplacé par le crochet de Lie avec les suites de sous-algèbre de Lie $D^i(\mathfrak{g})$ et $D_i(\mathfrak{g})$.

Si on revient aux groupes de Lie, on peut se demander le lien entre la nilpotence d'un groupe de Lie et celle de son algèbre de Lie. On a le thèorème suivant

Theorem 4.3. *Soit G un groupe de Lie connexe, de dimension finie sur $\mathbf{R}$, alors $D^i(G)$ est un sous-groupe de Lie d'algèbre de Lie $D^i(\mathfrak{g})$ et de même $D_i(G)$ est un sous-groupe de Lie d'algèbre de Lie $D_i(\mathfrak{g})$.*

On a un théorème équivalent sur $\mathbf{Q}_p$ la différence est qu'il peut existe des petits sous-groupes compacts ouverts autour de l'identité sur $\mathbf{Q}_p$, on ne peut donc pas espérer avoir un résultat global avec des informations sur l'algèbre de Lie.

Theorem 4.4. *Soit G un groupe de Lie de dimension finie sur $\mathbf{Q}_p$, il existe un sous-groupe ouvert $G_0 \subset G$ tel que les sous-groupes $D^i(G_0)$ sont des sous-groupes de Lie d'algèbre de Lie $D^i(\mathfrak{g})$ et de même les sous-groupes $D_i(G_0)$ sont des sous-groupes de Lie d'algèbre de Lie $D_i(G_0)$.*

Enfin, on a besoin d'une dernière définition. Soit G un groupe et H un sous-groupe de G. On regarde les sous-ensembles de G de la forme $gH := \{gh : h \in H\}$. Attention, ce n'est en général pas un groupe si $g \notin H$, c'est seulement un ensemble. On peut montrer qu'il existe un sous-ensemble $\mathcal{R}$ de G tel que G est l'union disjoite

$$G = \bigsqcup_{g \in \mathcal{R}} gH$$

Le choix de $\mathcal{R}$ n'est pas unique mais sa taille l'est. Si on peut choisir $\mathcal{R}$ fini, alors on dit que H est d'indice fini dans G.

La *longueur dérivée virtuelle* de G est définie comme le minimum $\min\{\mathrm{dl}(H) : H \subset G \text{ d'indice fini}\}$ on la note $\mathrm{vdl}(G)$.

5 Le théorème

En géométrie algébrique, on regarde des objets polynomiaux sur des variétés. Ici on va regarder l'exemple concret de $\mathbf{C}^d$.

Definition 5.1. Une *transformation polynomiale* $f : \mathbf{C}^d \to \mathbf{C}^d$ est une fonction telle que f s'écrive $f = (f_1, \cdots, f_d)$ et telle que chaque f_i soit un polynôme à d variables à coefficients complexes.

Un *automorphisme polynomial* est une transformation polynomiale inversible dont l'inverse est aussi polynomial. On note $\mathrm{Aut}(\mathbf{C}^d)$ le groupe des automorphismes polynomiaux sur $\mathbf{C}^d$.

Example 5.2. En dimension 2, $f(x,y) = (x^2, y)$ est une transformation polynomiale mais pas un automorphisme. Toutes les applications linéaires sont des transformations polynomiales. Un exemple non trivial de transformations polynomiales est par exemple $f(x,y) = (x + y^4, y)$ d'inverse $g(x,y) = (x - y^4, y)$.

<++>
On a maintenant tous les outils pour énoncer et donner une idée de la preuve du théorème suivant.

Theorem 5.3. *Soit H un sous-groupe nilpotent de type fini de $\mathrm{Aut}(\mathbf{C}^d)$, alors*

$$d \geq \mathrm{vdl}(H)$$

On dit qu'un groupe H est de type fini pour un groupe signfie qu'il existe un nombre fini d'éléments $h_1, \cdots, h_s$ tels que tout élément de H s'écrit comme produit des h_i (au sens de la composition).

Idée de Preuve Le fait que le groupe soit de type fini signifie que si l'on note $\mathcal{C}$ l'ensemble des coefficients qui apparaissent dans les formules de h_i, alors pour tout élément g obtenu par composition des h_i, les coefficients de g sont obtenues à partir de formules polynomiales en les éléments de $\mathcal{C}$. Cela siginifie que si l'on prend $\mathbf{K}$ le plus petit corps contenant tous les éléments de $\mathcal{C}$, le groupe H est en fait un sous-groupe de $\mathrm{Aut}(\mathbf{K}^d)$.

Proposition 5.4. *Il existe un nombre premier p tel que l'on peut trouver un plongement $\iota : \mathbf{K} \to \mathbf{Q}_p$ et tel que tous les éléments de $\mathcal{C}$ soient envoyés par ι dans $\mathbf{Z}_p$. C'est à dire que $\mathbf{K}$ peut être vu comme un corps inclus dans $\mathbf{Q}_p$ et tous les éléments de H ont leur coefficients dans $\mathbf{Z}_p$.*

Maintenant comme tout automorphisme polynomial est automatiquement analytique on a en fait que H est un sous-groupe nilpotent de type fini de $\mathrm{Diff}^{an}(\mathbf{Z}_p^d)$. On montre ensuite qu'il existe un sous-groupe de type fini $H' \subset H$ tel que $H' \subset \mathrm{Diff}_1^{an}(\mathbf{Z}_p^d)$ (on fait en sorte que tous les éléments de H' soient congrus à l'identié modulo p).

Maintenant, tout élément f de H' est dans un flot Φ_t, on peut alors regarder le champ de vecteurs associés $\mathbf{X}_f = \frac{\partial \Phi_t}{\partial t}_{|t=0}$. Ainsi, en regardant l'algèbre de champs de vecteurs engendrée par tous les X_f pour $f \in H'$, on obtient une algèbre de Lie $\mathfrak{h}$.

Theorem 5.5. *$\mathfrak{h}$ est l'algèbre de Lie d'un groupe de Lie de dimension finie nilpotent $G \subset \mathrm{Diff}^{an}(\mathbf{Z}_p^d)$ dans lequel H' est dense, on a donc que $\mathfrak{h}$ est nilpotente, de dimension finie et de plus,* $\mathrm{dl}(\mathfrak{h}) \geq \mathrm{vdl}(H') \geq \mathrm{vdl}(H)$.

Le fait que $\mathfrak{h}$ est nilpotente et de dimension finie est directe car le groupe de Lie associé l'est. La borne sur la longueur dérivée vient du fait que sur $\mathbf{Q}_p$ l'algèbre de Lie donne des informations sur des petits sous-groupes ouverts autour de id et pas sur le groupe total, on doit donc faire intervenir la longueur dérivée virtuelle au lieu de la longueur dérivée.

Et on conclut avec le résultat suivant qui est un résultat qui est connu sur $\mathbf{R}$ ou $\mathbf{C}$ et dont la preuve fonctionne de la même manière sur $\mathbf{Z}_p$.

Theorem 5.6. *Soit M une variété différentielle et $\mathfrak{h}$ une algèbre de Lie de champs de vecteurs nilpotente sur M, alors*

$$\dim X \geq \mathrm{dl}(\mathfrak{h}).$$

En regroupant les deux derniers théorèmes, on a bien $d \geq \mathrm{dl}(\mathfrak{h}) \geq \mathrm{vdl}(H') \geq \mathrm{vdl}(H)$ et le thèorème est démontré.