

Groupes de matrices de Chevalley

Adrien Deloro

Thé du DMA

10 juin 2020

Dans cette partie :

① Introduction

- Groupes de géométries linéaires
- Groupes de Chevalley

② Trois versions de Chevalley

- Groupes de Lie
- Groupes algébriques
- Groupes finis

③ En logique mathématique

- Parties définissables
- Contexte rangé

L'algèbre linéaire, c'est vulgaire

- ① Un *2-sous-groupe de Sylow* est un sous-groupe dont chaque élément est d'ordre une puissance de 2, et maximal en tant que tel.

(Vérifiez que cette définition généralise bien la vôtre.)

→ Les 2-sous-groupes de Sylow de $GL_n(\mathbb{C})$ sont-ils conjugués ?

- ② La *décomposition de Chevalley* dans $GL_n(\mathbb{C})$ affirme :

tout $g \in GL_n(\mathbb{C})$ s'écrit de façon unique $g = s \cdot u$ avec s « semi-simple » (= diagonalisable), u « unipotent » (= $I_n + \text{nilpotent}$), et $us = su$.

→ Cet énoncé a-t-il un sens groupe-théorique ? I.e., sauriez-vous le traduire *sans référence à l'algèbre matricielle* $M_n(\mathbb{C})$?

Les *méthodes* de l'algèbre linéaire ont quelque chose de trivial, mais ses *objets* sont fondamentaux et dignes d'estime.

« Créer un poncif, c'est le génie. »

L'idée centrale de l'algèbre, c'est l'équivalence :

structure sur un ensemble $\leftrightarrow$ groupe agissant sur cet ensemble

$\rightarrow$: prendre le groupe d'automorphismes de la structure pertinente.

$\leftarrow$: prendre toutes les relations n -aires préservées par l'action du groupe.

Une instance de cette équation :

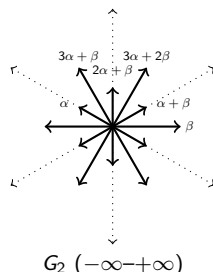
géométries linéaires = groupes de matrices [d'un certain type]

Cette idée n'a cristallisé qu'en 1872 (soit longtemps après Euclide).

Repères historiques

- Klein (« Programme d'Erlangen ») a unifié « les » géométries linéaires en langage groupe-théorique.
- Lie (« Transformationsgruppen ») a dégagé des concepts centraux, mais *pour le seul modèle réel/complexe* : c'est la « théorie de Lie ».
- Killing, Cartan classifièrent les grps de Lie simples.
- Chevalley a compris que l'analyse/la géo. diff. n'ont pas grand rôle, mais qu'on peut *varier le corps*.
Les « groupes de type Lie » étaient nés.
- Galois avait montré la simplicité de $\mathrm{PSL}_2(\mathbb{F}_p)$.

Essayons de préciser ça.



L'unification d'Erlangen

Naïvement, il y a *plusieurs* géométries linéaires (= espaces avec des lignes).

- Origine fixée ?
- Passage au projectif ?
- Préservation du volume ?
- Préservation des angles, des distances ?
(Très mauvais concepts. Il faut parler de *formes quadratiques*.)

En termes modernes :

- géométrie vectorielle générale : GL_n ;
- projective : PGL_n ;
- géométrie du déterminant : SL_n ;
- géométries « des orthogonalités » : $O(q)$;
- la *géométrie linéaire symplectique* : Sp_n .

Fin XIXe siècle, malgré Jordan (et Galois !), ces groupes étaient pris pour des variétés différentielles — on étudiait « leur valeur dans $\mathbb{R}$ ».

Les familles de Chevalley

Chevalley a compris que les objets de la géométrie avaient un sens absolu, universel, indépendant de $\mathbb{R}$ et du cas particulier de la physique.

En travaillant sur $\mathbb{Z}$, il a créé le modèle sur tout corps des groupes de transformations. Ceci permet de raisonner en famille.

La *notation de Chevalley* classe ainsi les « groupes classiques » (connus en 1900 et correspondant à des géométries linéaires naturelles) :

- A_n (ne surtout pas confondre avec Alt_n !) : groupe spécial linéaire ;
- B_n : groupe orthogonal, dimension impaire
- C_n : groupe symplectique (néologisme de H. Weyl, mais pas méchant) ;
- D_n : groupe orthogonal, dimension paire ;

ainsi que les « groupes exceptionnels » : E_6, E_7, E_8, F_4, G_2 .

Ces derniers ont été dégagés à partir de 1890. Ils correspondent eux aussi à des géométries linéaires, mais pas intuitives.

Dans cette partie :

① Introduction

Groupes de géométries linéaires
Groupes de Chevalley

② Trois versions de Chevalley

Groupes de Lie
Groupes algébriques
Groupes finis

③ En logique mathématique

Parties définissables
Contexte rangé

Groupes de Lie linéaires

Un *groupe de Lie*, c'est un groupe qui est aussi une variété (sur $\mathbb{R}$).
Un *groupe de Lie linéaire*, c'est un sous-groupe $G \leq \mathrm{GL}_n(\mathbb{R})$ fermé.

Observation

Un groupe de Lie simple est linéaire.

Démonstration.

G agit sur $T_e G := \{\text{vecteurs vitesses en } e\} \simeq \mathbb{R}^n$.

D'où un morphisme $G \rightarrow \mathrm{Aut}(\mathbb{R}^n) = \mathrm{GL}_n(\mathbb{R})$. L'action est non triviale et G simple, donc $G \hookrightarrow \mathrm{GL}_n(\mathbb{R})$. (Réfléchir un peu pour l'image fermée.) $\square$

La géo. diff. sert à obtenir sur G des contraintes d'alg. linéaire :
il y a *beaucoup plus* de structure en jeu que la seule loi de groupe.

Les 2-sous-groupes de Sylow d'un groupe de Lie sont-ils conjugués ? Je pense bien que oui mais je ne sais pas si c'est écrit quelque part.

Classification des groupes de Lie simples

Théorème (Lie-Killing-Cartan ; formulation très anachronique)

Soit G un groupe de Lie simple. Alors G est de Chevalley.

Démonstration.

- En fait $T_e G$ porte *une structure d'un genre nouveau* (en 1880) : une *algèbre de Lie* = e.v.+loi interne *non associative*.
(La géométrie différentielle réduit de la théorie des groupes à de l'algèbre générale.)
- L'algèbre de Lie $\mathfrak{g} = \text{Lie}(G)$, dans son action sur elle-même, voit émerger des symétries fabuleuses : les *systèmes de racines*.
(La théorie des représentations réduit de l'algèbre générale à de l'algèbre linéaire.)
- Ces systèmes de racines s'abstraient en entités combinatoires.
(La géométrie élémentaire réduit de l'algèbre linéaire à de la combinatoire.)
- On classe les « systèmes de racines », et les algèbres de Lie simples.
- Enfin $\mathfrak{g}$ contraint G par l'exponentielle matricielle. □

Groupes algébriques linéaires

Un *groupe algébrique* (sur un corps $\mathbb{K}$), c'est un groupe qui est aussi une variété algébrique (disons, définie par des équations).

Un *groupe algébrique linéaire*, c'est un groupe de matrices $G \leq \mathrm{GL}_n(\mathbb{K})$ donné par des équations polynomiales.

Observation

Un groupe algébrique simple est linéaire.

Important : « simple » est toujours au sens groupe-théorique. Les courbes elliptiques ne sont pas simples en tant que groupes abstraits (ni linéaires).

Démonstration.

Au « co- » près, comme précédemment. □

Comme précédemment, les méthodes ne sont *pas* groupe-théoriques.

Classification des groupes algébriques simples

Théorème (Chevalley)

Soit G un groupe algébrique simple. Alors G est de Chevalley.

Démonstration.

En variant le corps, reconstruire les infinitésimaux et l'algèbre de Lie. □

Author's message : le calcul différentiel a progressivement évincé le calcul infinitésimal. Le coût d'élimination des infiniment petits, c'est l'introduction de limites (avec leur lourdeur formelle) ; l'intérêt est aussi pédagogique.

En fait on passe juste de $\mathbb{R}$ à $\mathbb{R}[\varepsilon]$ avec $\varepsilon \ll 1$ (ce qui paraît requérir un ordre). Posant plutôt $\varepsilon^2 = 0$, on voit qu'on peut partir de $\mathbb{K}$ quelconque.

Pareil : est-ce qu'on pourrait faire plus de groupes ?

Groupes simples finis

Un *groupe fini*, c'est un groupe abstrait G dont l'ordre est fini.

Noter l'absence — apparente — de structure supplémentaire : on n'a *aucun* moyen de raisonner en famille/varier un système de coordonnées/adjoindre des infinitésimaux.

Théorème (classification des groupes simples finis)

Les groupes simples finis sont :

- $\mathbb{Z}/p\mathbb{Z}$ pour p premier ;
- $\text{Alt}(n)$ pour $n \geq 5$;
- les groupes simples finis « de type Lie » (Chevalley ou « Chevalley-Steinberg », variantes finitaires vicieuses) ;
- 26 exceptions inattendues, « sporadiques ».

Attention ! ne pas confondre « sporadique » avec « exceptionnel » (E_6, E_7, E_8, F_4, G_2).

Pour les sporadiques, on n'a même pas de géométrie linéaire associée.

Groupes simples finis

Théorème (CGSF sommaire)

Soit G un groupe simple fini. Aux exceptions près, G est de Chevalley.

Esquisse de démonstration (tient dans la marge).

Considérer les involutions de G .



Lemme (Lemme-clef; Feit-Thompson)

Un groupe simple fini non-abélien possède une involution.

Esquisse de démonstration.

Avec la théorie des caractères. (NB : certifié COQ.)



Est-ce qu'on pourrait faire *moins* de groupes ?

Dans cette partie :

① Introduction

Groupes de géométries linéaires
Groupes de Chevalley

② Trois versions de Chevalley

Groupes de Lie
Groupes algébriques
Groupes finis

③ En logique mathématique

Parties définissables
Contexte rangé

Raisons de l'ubiquité ?

Pourquoi cette ubiquité des groupes de Chevalley ?

Réponse naïve : les groupes sont surtout des groupes de matrices. Réponse naïve : ~~les groupes sont surtout des groupes de matrices.~~

C'est faux ! La « théorie des groupes » n'existe pas. Il y a des théories pour diverses sous-familles de groupes (de Chevalley, hyperboliques, finis, . . .), mais pas d'énoncé

- *général*
- *correct*
- *intéressant*

vrai pour tous les groupes simultanément.

C'est un miracle que dans le cas fini de tels énoncés existent.

Ce qu'ont de commun les groupes de Lie, les groupes algébriques, les groupes finis, c'est leur « modération » logique.

La théorie des modèles propose *des* contextes pour formaliser la « modération ». Je dois parler de *parties définissables*.

Parties définissables

Soit $\mathbb{S}$ une structure algébrique. On considère les parties données par :

- les équations à paramètres (ex. : $\{(a, b, c, d) : ad - bc = 0\}$) ;
- les combinaisons « et/ou/non » (ex. : $\{(a, b, c, d) : ad - bc \neq 0\}$) ;
- les projections $\mathbb{S}^{n+1} \rightarrow \mathbb{S}^n$ (ex. : $\{(a, b, c, d) : \exists x : x \cdot (ad - bc) = 1\}$) ;
- les quotients par relations d'équivalence de cette nature (ex. avec $\mathbb{S} = \mathbb{C} : \text{GL}_n(\mathbb{C})/\{(g, h) : \exists \lambda : g = \lambda h\}$).

Nb. On rate de nombreuses constructions naturelles. De toute façon, $|\mathcal{P}_{\text{déf}}(\mathbb{S})| \ll |\mathcal{P}(\mathbb{S})|$.

Faits

- $\mathbb{S} = (\mathbb{C}; 0, +, 1, \cdot)$: *pas besoin des quantificateurs ni des relations d'équivalence (Chevalley-Tarski ; Poizat).*
- $\mathbb{S} = (\mathbb{R}; 0, +, 1, \cdot, <)$: *pas besoin des quantificateurs (Seidenberg-Tarski).*
- $\mathbb{S} = (\text{GL}_n(\mathbb{C}); 1, \cdot)$: *$\text{SL}_n(\mathbb{C})$ est définissable (Gauß).*

Rang de Morley

Définition (Morley, ou Zilber, ou Borovik, ou Poizat)

Un *groupe de rang de Morley fini* est un groupe dont les définissables portent une dimension entière, « à la Zariski » :

- $\dim\{g\} = 0$;
- $\dim A \geq n + 1$ ss'il existe des B_i déf. de $\dim \geq n$ avec $\bigsqcup_{i \in \mathbb{N}} B_i \subseteq A$;
- constructions naturelles sur les fibres des fonctions
(typiquement si $f : A \rightarrow B$, alors $\dim A = \dim \operatorname{im} f + \dim \text{fibre générique}$) ;
- un truc technique sur l'infini ($\leftarrow$ pour que ça reste de la théorie des modèles).

Exemple

Soient $\mathbb{K}$ alg. clos et G un groupe de Chevalley simple à valeurs dans $\mathbb{K}$. Alors G est « de rang de Morley fini ».

(Le rang/dimension est alors la dimension de la géo. alg., et conforme à l'intuition.)

La conjecture de Cherlin-Zilber

Un groupe de rang de Morley fini, c'est un groupe dont les définissables portent une dimension entière.

Conjecture (Cherlin, Zilber ; fin années 1970)

Soit G simple de rang fini. Alors G est un groupe de Chevalley à valeurs dans un corps alg. clos.

Nb., pour qui connaît l' o -minimalité :

Théorème (Peterzil-Pillay-Starchenko, 2000)

Si $(G, \cdot)$ est un groupe simple définissable dans une structure o -minimale, alors c'est (à peu près) un groupe de Chevalley sur un corps « comme $\mathbb{R}$ ».

Démonstration — cas o -minimal.

Reconstruire le calcul infinitésimal, et donc la notion d'algèbre de Lie. Puis faire comme au XIXe siècle. □

Conjecture de Cherlin-Zilber et CGSF

Conjecture (Cherlin, Zilber ; fin années 1970)

Soit G simple de rang fini. Alors G est de Chevalley sur un corps alg. clos.

Il n'y a *aucun* moyen de conquérir de l'information infinitésimale.

Le bon cadre méthodologique pour penser Cherlin-Zilber, ce n'est pas les groupes algébriques ; c'est la théorie des groupes finis.

Borovik a suggéré de transposer CGSF — involutions, centralisateurs, fortement réels — vers le paysage rangé. Pierre angulaire :

Théorème (Borovik-Poizat, 1990)

Soit G de rang de Morley fini. Alors ses 2-sous-groupes de Sylow sont conjugués ; leur structure est classifiée.

- Ouvert pour $p > 2$.
- Pas d'information sur la non-trivialité (pas de « Feit-Thompson »).

Nombreuses involutions : succès

Théorème (Altinel-Borovik-Cherlin, 2008)

Soit G simple de rang de Morley fini. Si G contient (non définissable) $\bigoplus_{\mathbb{N}} \mathbb{Z}/2\mathbb{Z}$, alors $G \simeq \mathbb{G}(\mathbb{K})$.

- Même en supposant que G a des involutions,
- même en supposant que tous les sous-quotients simples de G ont des involutions. . .
- la conjecture de Cherlin-Zilber est ouverte.
- Sans involutions c'est pire encore.
- Aveu : sans involutions, il n'y a *pas* de stratégie d'ensemble.

Je m'arrête ici ; merci !

Diapo suivante et dernière : bibliographie.

Pour aller voir ailleurs. . .

- Algèbre géométrique : *Classical groups and geometric algebra* (L. Grove), ou *The Geometry of the classical groups* (D. Taylor).
(Le lumineux traité d'E. Artin a fini par vieillir un peu.)
- Groupes de Chevalley : *Simple groups of Lie type* (R. Carter).
(Ne pas confondre avec *Finite groups* etc., du même, autrement plus corsé.)
- *Intro. to Lie algebras and rep. theory* (J. Humphreys).
(Ce livre a la sévère pureté du cristal ; à vous d'en saisir les motivations.)
- *Groups of finite Morley rank* (A. Borovik et A. Nesin).
(Un chef-d'œuvre de pédagogie.)
- Groupes en théorie des modèles : *Groupes stables* (B. Poizat).
(Plus dur car prérequis logiques et géométriques ; l'esthète sera récompensé.)