SÉMINAIRE N. BOURBAKI

ANDRÉ BLANCHARD

Groupes algébriques et équations différentielles linéaires

Séminaire N. Bourbaki, 1952, exp. n° 17, p. 103-109

<http://www.numdam.org/item?id=SB_1948-1951__1__103_0>

Séminaire BOURBAKI
(Décembre 1949)

GROUPES ALGÉBRIQUES ET ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES

par André BLANCHARD

(d'après E.R. KOLCHIN [1]).

Le but de cette étude est d'établir une théorie de Galois pour les corps à dérivation, et les équations différentielles linéaires. La théorie est nettement plus compliquée que la théorie de Galois classique, à cause de problèmes non résolus, en particulier à propos des quotients des groupes algébriques ; cependant, on obtient la condition nécessaire et suffisante pour qu'une équation linéaire homogène soit résoluble par "intégrales" ou par "exponentielles d'intégrales", etc.

1. Groupes algébriques de matrices.

Soit K un corps commutatif algébriquement clos, de caractéristique provisoirement quelconque que l'on désignera par p et de degré de transcendance infini sur le corps premier. Dans ce paragraphe, K nous servira de "domaine universel".

L'ensemble des matrices carrées à n lignes et n colonnes est un espace vectoriel sur K où l'on peut parler de variétés algébriques. Nous dirons qu'un groupe de matrices est algébrique si l'ensemble des matrices de ce groupe est une variété algébrique, privée des points tels que $\det(a_{ij}) = 0$.

EXEMPLES. - Le groupe de toutes les matrices inversibles, le groupe unimodulaire, le groupe des matrices "triangulaires" inversibles, tout groupe fini de matrices.

Lorsque la variété d'un groupe G n'est pas irréductible, on voit facilement que la composante irréductible de l'unité est un sous-groupe distingué G_o de G et que G/G_o est un groupe fini. Les composantes irréductibles de G sont disjointes, on a une notion de connexion analogue à la notion topologique.

De façon plus générale, on peut définir la notion de groupe algébrique : c'est la donnée d'un certain nombre (fini) de variétés abstraites isomorphes avec une loi de groupe sur l'ensemble somme des variétés considérées comme ensemble de points, telle que toute translation soit une correspondance birationnelle birégulière partout définie. Tout groupe algébrique n'est pas un groupe algébrique de matrices (Variétés abéliennes ...).

Si G est un groupe algébrique et H un sous-groupe algébrique distingue, on ne sait pas si G/H peut être muni d'une structure de groupe algébrique. Cependant il existe un théorème de Jordan-Hölder sous la forme suivante : Si l'on a deux suites de composition formées de groupes algébriques, il existe des "raffinements" isomorphes formés de groupes algébriques (on utilise la démonstration de Zassenhaus en montrant que les sous-groupes que l'on construit sont algébriques).

On a encore le théorème suivant : Si G est un groupe algébrique, le groupe des commutateurs de G est un groupe algébrique. De plus, si G est connexe, son groupe des commutateurs l'est aussi.

Notion de groupe résoluble : On dira que G est résoluble s'il possède une suite de composition formée de sous-groupes algébriques telle que les quotients successifs (dont on ne sait pas s'il sont algébriques) soient abéliens.

En utilisant les groupes de commutateurs, on montre que si G est résoluble et connexe, G possède une suite de composition formée de sous-groupes connexes.

THÉORÈME. - La condition nécessaire et suffisante pour qu'un groupe de matrice puisse être mis sous forme triangulaire est qu'il soit sous-groupe d'un groupe algébrique de matrices résoluble et connexe.

La suffisance se montre exactement comme dans le cas des groupes de Lie.

Pour voir la nécessité, considérons les groupes :

T : groupes des matrices triangulaires : tous les éléments au-dessous de la diagonale principale sont nuls.

T_1 : sous-groupe de T formé des matrices telles que $a_{ii} = 1$.

T_2 : sous-groupe de T_1 formé des matrices telles que la première diagonale au-dessus de la principale soit nulle.

...

T_i : sous-groupe de T_{i-1} formé des matrices telles que la i-ième diagonale au-dessus de la principale soit nulle.

Désignons encore par D (resp. D^0) le groupe additif (resp. multiplicatif) de la droite, c'est-à-dire de K .

Il est clair que T/T_1 est isomorphe à $(D^0)^n$ et T_i/T_{i+1} à D^{n-1} . Ces groupes étant abéliens, le théorème est démontré.

La démonstration précédente donne un résultat un peu plus fort : Soit G un sous-groupe algébrique connexe de T , en considérant les $G \cap T_i$, on peut

montrer que G possède une suite de composition dont les quotients sont isomorphes soit à D soit à D^0. Lorsque tous les quotients sont isomorphes à D (resp. D^0) on dira que G est de type additif (resp. multiplicatif). (KOLCHIN emploie l'expression anticompact (resp. quasicompact), notion qu'il définit pour tout groupe algébrique, mais sans intérêt ici).

2. Corps à dérivations (ou corps différentiels).

On se restreindra au cas d'une seule dérivation (corps différentiel ordinaire).

Une dérivation sur un corps F est un endomorphisme d de sa structure d'espace vectoriel sur le corps premier tel que $d(x.y) = y.dx + x.dy$.

L'ensemble $d^{-1}(0)$ est un sous-corps de F appelé corps des constantes et que l'on désignera dans toute la suite par K .

Si $F \subset L$, F et L étant deux corps différentiels, Φ une partie de L , on note $F\{\Phi\}$ (resp. $F\langle\Phi\rangle$) le plus petit anneau (resp. corps) stable pour d et contenant F et Φ .

On notera également $F\{x\}$ l'anneau des polynômes à une infinité d'indéterminées : x , dx , $d^2 x$, ... , $d^n x$, ... muni de la dérivation $d(d^n x) = d^{n+1} x$. Il est facile de définir aussi $F\{x , y\}$ ... etc. Dans de tels anneaux, le mot idéal signifiera idéal stable pour la dérivation.

Supposons maintenant (et jusqu'à la fin de l'exposé) que la caractéristique est nulle. RITT a établi des théorèmes analogues à ceux des anneaux noethériens :

Tout idéal parfait (c'est-à-dire tel que $x^n \in \mathfrak{a}$ entraîne $x \in \mathfrak{a}$) est de façon unique l'intersection d'un nombre fini d'idéaux premiers.

Notion de solution : Soit $\mathfrak{a}$ un idéal de $F\{y_1 , ... , y_n\}$. On appelle solution de $\mathfrak{a}$ un système fini d'éléments $\eta_1 ... \eta_n$ d'une certaine extension de F , tels qu'en "substituant" ces éléments dans les différents polynômes de $\mathfrak{a}$, on trouve 0 . On dit qu'une solution est générique si elle n'est solution d'aucun polynôme non contenu dans $\mathfrak{a}$. Seuls les idéaux premiers ont des solutions génériques. Elles ont toutes la même dimension (au sens habituel de la géométrie algébrique), dimension qui ne varie pas par extension du corps F . Pour qu'une solution soit générique, il faut et il suffit qu'elle ait la même dimension qu'une solution générique.

THÉORÈME des zéros de Hilbert. - Si α est un idéal premier de $F\{y_1, \ldots, y_n\}$ et si f appartient à $F\{y_1, \ldots, y_n\}$, et jouit de la propriété que toute solution de f est solution de α alors $f \in \alpha$.

THÉORÈME. - F est linéairement disjoint de toute extension K' de K sur laquelle d opére trivialement (extension du corps des constantes par des constantes).

En effet, soit $\sum_{i=1}^{n} \ell_i y_i = 0$ une relation linéaire entre $y_i \in F$ à coefficients $\ell_i \in K''$. En différentiant n fois, on voit que le Wronskien $\det(y_i^{(j)})$ est nul, donc qu'il existe une relation linéaire entre les y_i à coefficients dans K.

C.Q.F.D.

On en déduit : si un système de constantes vérifie des équations algébriques à coefficients dans F, il vérifie un système équivalent d'équations à coefficients dans K.

3. Extensions normales.

Soit L une extension de F ; on dit qu'un ensemble S de F-isomorphismes de L est abondant si, étant donné un corps intermédiaire F_1, le corps des invariants de l'ensemble des F_1-isomorphismes appartenant à S est F_1. RADBENBUSH a montré que l'ensemble de tous les F-isomorphismes de L est abondant.

On dit que L est une extension normale de F si le groupe des F-automorphismes de L est abondant. Dans ce cas, si $G(F_1)$ désigne le groupe des F_1-automorphismes de L, la correspondance $F_1 \longrightarrow G(F_1)$ est biunivoque. Pour que $G(F_1)$ soit distingué dans $G(F)$, il faut et il suffit que F_1 soit invariant pour tout élément de $G(F)$; alors $G(F)/G(F_1)$ est isomorphe à un groupe abondant de F-automorphismes de F_1.

En général, on ne sait pas si F_1 normal entraîne $G(F_1)$ distingué dans $G(F)$. On ne sait pas non plus caractériser de façon simple les sous-groupes de $G(F)$ qui sont de la forme $G(F_1)$.

4. Extensions de Picard-Vessiot.

Soit F un corps différentiel de corps des constantes K, et soit $P(y)$ un "polynôme différentiel" sur F, c'est-à-dire un élément de $F\{y\}$: $P(y) = d^n y + \ldots + p_i d^i y + \ldots$ où $p_i \in F$. Alors il existe une extension L

de F qui contient n solutions $\eta_1 , \dots , \eta_n$ de P , linéairement indépendantes sur le corps des constantes de L .

On dira que L est une extension de Picard-Vessiot de F , si on a $L = F\langle \eta_1 , \dots , \eta_n \rangle$ et si le corps des constantes de L est K . Nous nous bornerons à de telles extensions.

1er THÉORÈME FONDAMENTAL. - Le groupe des F-automorphismes de L est isomorphe à un groupe algébrique de matrices de degré n .

Soit G(F) le groupe des F-automorphismes de L . Toute solution de $P(y) = 0$ étant combinaison linéaire à coefficients dans K des η_i , G(F) se réalise comme groupe de matrices de degré n sur K : si $\sigma \in G(F)$, $\sigma \eta_j = \sum_{i=1}^{n} k_{ij} \eta_i$.

Reste à prouver que G(F) est un groupe algébrique.

Soit $\mathfrak{A}$ l'idéal de $F\{y_1 , \dots , y_n\}$ formé des polynômes différentiels s'annulant pour $y_i = \eta_i$. Nous introduisons alors n^2 constantes indéterminées ℓ_{ij} . L'application $y_j \to \sum_{i=1}^{n} \ell_{ij} \eta_i$ définit une application de $L\{y_1 , \dots , y_n\}$ dans $L[\ell_{ij}]$. Si $\mathfrak{A}''$ est l'image de $\mathfrak{A}$, il y a d'après le théorème de disjonction linéaire du n° 2 , un idéal $\mathfrak{A}'$ de $K[\ell_{ij}]$ tel que ℓ_{ij} est un zéro de $\mathfrak{A}''$ si et seulement si ℓ_{ij} est un zéro de $\mathfrak{A}'$. Si τ est un isomorphisme de L , on a $\tau \eta_j = \sum_{i=1}^{n} k_{ij} \eta_i$ (où les k_{ij} sont des constantes d'une certaine extension de L). On montre que pour que k_{ij} définisse un isomorphisme de L , il faut et il suffit qu'il soit une solution de $\mathfrak{A}'$ et que $\det(k_{ij}) \neq 0$. Or, pour qu'un F-isomorphisme soit un automorphisme il faut et il suffit que les k_{ij} soient dans K , ce qui achève la démonstration.

2e THÉORÈME FONDAMENTAL. - Toute extension de Picard-Vessiot est normale.

Soient L une extension de Picard-Vessiot de F , et F_1 un corps intermédiaire. On montre que F est le corps des invariants des F-automorphismes de L . Si l'on remarque que, pour tout corps intermédiaire F_1 , L est extension de Picard-Vessiot de F_1 , il suffit d'appliquer le résultat précédent à F_1 pour démontrer le théorème.

Si $G(F_1)$ est le groupe des F_1-automorphismes de L . $G(F_1)$ est un sous-groupe algébrique de G(F) ; si $G(F_1)$ est distingué on montre que $G(F)/G(F_1)$ est le groupe de tous les automorphismes de F_1 , mais on ne sait pas si F_1 est normal. On ne sait pas non plus si tout corps intermédiaire normal sur F

est une extension de Picard-Vessiot de F .

3e THÉORÈME FONDAMENTAL. - L'ensemble des groupes de la forme $G(F_1)$ est l'ensemble de tous les sous-groupes algébriques de $G(F)$.

On sait déjà que tout $G(F_1)$ est algébrique.

Soient G^0 un sous-groupe algébrique de $G(F)$ et F^0 le corps des invariants de G^0 . Supposons $G^0 \neq G(F^0)$, il y a alors un polynôme $f(k_{ij})$ qui est nul pour tout $\sigma = (k_{ij})$ $(\sigma \in G^0)$, et non nul pour tout $\sigma \in G(F^0)$. Si H_{ij} est la matrice inverse du Wronskien des η_j , $f(\sum_k H_{k_i} y_j^{(k)})$ est un polynôme différentiel de $L\{y_1, \ldots, y_n\}$ qui admet pour solution $\sigma\eta_1, \ldots, \sigma\eta_n$ pour tout $\sigma \in G^0$ et non pour tout $\sigma \in G(F^0)$. Parmi les polynômes qui ont cette propriété, soit g un de ceux qui ont le moins de termes. Si on transforme g par un automorphisme $\tau \in G^0$, g_τ a la même propriété, et si $g_\tau \neq g$, parmi les $g - \lambda(g - g_\tau)$ on trouverait un polynôme plus court, donc $g = g_\tau$. Les coefficients de g étant invariants par G^0 sont dans F^0 , donc sont invariants par $G(F^0)$, donc $g(\sigma\eta_j) = 0$ pour tout $\sigma \in G(F^0)$, contrairement à l'hypothèse.

On démontre encore le théorème suivant :

THÉORÈME. - La dimension du groupe algébrique $G(F)$ est égale au degré de transcendance de L sur F .

5. Applications de la théorie à la résolution de équations.

On commence par montrer les résultats suivants :

1° Si F' est une extension de F et $L' = F'\langle \eta_1 \ldots \eta_n \rangle$, le groupe des F'-automorphismes de L' est isomorphe au groupe des $L \cap F'$-automorphismes de L (Démonstration classique).

2° Pour qu'un polynôme différentiel $P(y)$ puisse s'écrire sous la forme $Q(R(y))$, il faut et il suffit que le groupe G puisse s'écrire sous la forme : $\sigma = \begin{pmatrix} \sigma_1 & * \\ 0 & \sigma_2 \end{pmatrix}$.

DÉFINITIONS. - Nous dirons qu'une extension L de F est une extension par intégrale (resp. exponentielle d'intégrale) si L est de la forme

$F\langle\alpha\rangle$ où α satisfait à l'équation $dy = a$ (resp. $dy = ay$) où a est dans F.

Il est évident que le groupe des F-automorphismes de L est alors le groupe additif D (resp. le groupe multiplicatif D^0) de la droite.

De ce qui précède on déduit facilement les conditions nécessaires et suffisantes pour qu'une équation différentielle linéaire $P(y) = 0$ soit résoluble par intégrales (resp. etc.) en fonction de la structure du groupe G : désignons par G_o la composante connexe de l'unité dans G. On a alors la classification suivante :

P(y) résoluble par :

Intégrales, exponentielles d'intégrales et fonctions algébriques.	G_o résoluble
Intégrales et exponentielles d'intégrales	$G = G_o$ résoluble
Exponentielles d'intégrales et fonctions algébriques	G_o résoluble de type multiplicatif
Intégrales et fonctions algébriques.	G_o résoluble de type additif.
Intégrales et radicaux	G résoluble et G_o de type additif.
etc.	etc.
Fonctions rationnelles	$G = \{1\}$.

BIBLIOGRAPHIE

[1] KOLCHIN (E.R.). - Algebraic groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations, Annals of Math., t. 49, 1948, p. 1-42.

Les mémoires suivants ont été publiés postérieurement à la date de l'exposé précédent ; ils apportent des extensions importantes de la théorie :

[2] KOLCHIN (E.R.). - Galois theory of differential fields, Amer. J. Math., t. 75, 1953, p. 753-824.

[3] KOLCHIN (E.R.). - On the theory of differentiable fields, Amer. J. Math., t. 77, 1955, p. 868-894.

[Février 1958]