Théories de Galois géométriques

Pierre Cartier*
(IMJ et IHÉS)

17 décembre 2008

Table des matières

1 Virtualité et ambiguïté selon Galois

Galois décrit sa théorie comme une théorie de l'ambiguïté. Ce n'est là qu'une partie de ses ambitions. Je vais tâcher de faire une lecture de Galois aussi proche que possible de l'original. Un texte aussi riche admet certes beaucoup d'interprétations.

*Notes rédigées avec l'aide de Marie Anglade, à partir des exposés donnés à Brasilia du 28/02 au 1/03 de l'an 2008.

1.1 Un exemple élémentaire

Que signifie le nombre $\sqrt{5}$? On peut considérer ce nombre de plusieurs manières. Si l'on se place dans le cadre des nombres réels, où apparaît un côté analytique et une référence au moins implicite à l'infini, on connaît la loi des décimales de ce nombre ou une loi explicite d'approximation par des fractions. Mais on veut faire ici une théorie *algébrique*. Si l'on veut traiter ce nombre de manière algébrique, on peut tout d'abord entreprendre des calculs très simples, par exemple :

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2}$$

$$\frac{1+\sqrt{5}}{2+\sqrt{5}} = \frac{(1+\sqrt{5})(2-\sqrt{5})}{(2+\sqrt{5})(2-\sqrt{5})} = \frac{-3+\sqrt{5}}{-1} = 3-\sqrt{5}\,.$$

Ces calculs ne présupposent pas de théorie préliminaire des nombres réels et ne sont que des manipulations algébriques. Quelles en sont les caractéristiques ?

Une règle de calcul simple exprime la définition même du nombre : $\sqrt{5}\times\sqrt{5} = 5$. Mais, quand on développe ces calculs, on se rend compte assez rapidement qu'il y a une ambiguïté fondamentale et qu'il est impossible de distinguer algébriquement $\sqrt{5}$ et $-\sqrt{5}$. Remplacez $\sqrt{5}$ par $-\sqrt{5}$ et inversement : dans tous les cas, le calcul reste exact. La vraie raison de cela est que, dans tous ces calculs, on a utilisé la règle disant que $\sqrt{5}\times\sqrt{5} = 5$; or on a aussi $(-\sqrt{5})\times(-\sqrt{5}) = 5$. D'où une ambiguïté et une symétrie. La loi de symétrie s'exprime par un groupe et c'est la première apparition d'un groupe de Galois.

Peut-on lever l'ambiguïté ? Qu'est-ce qui va nous permettre de distinguer $\sqrt{5}$ de $-\sqrt{5}$? Tout le monde dira : le signe. Cela veut dire que dans les raisonnements que nous ferons, à côté des opérations telles que addition, multiplication, division, ... il nous faut introduire une relation de comparaison du type $a > b$ avec les règles de calcul usuelles et la convention $\sqrt{5} > 0$ d'où $-\sqrt{5} < 0$ et $-\sqrt{5} < 0 < \sqrt{5}$. On raisonne donc dans un corps ordonné.

Remarque sur les nombres complexes :

On peut traiter $\sqrt{-1}$ de manière analogue, mais on ne peut pas lever l'ambiguïté de la même manière, car si l'on posait $\sqrt{-1} > 0$ ou $\sqrt{-1} < 0$ on aurait dans les deux cas $-1 = \sqrt{-1}\times\sqrt{-1} > 0$ ce qui est absurde.

(Dans le plan complexe, une symétrie donne la passage à l'imaginaire conjugué. Le passage de $\sqrt{5}$ à $-\sqrt{5}$ sur la droite réelle n'est pas aussi évident.)

1.2 Solutions virtuelles

Donnons un exemple élémentaire avant de dégager une stratégie générale. Résoudre "virtuellement" l'équation $x^2-5=0$, ou $x^2+1=0$, ou plus généralement $x^2+ax+b=0$, c'est introduire des racines virtuelles r et s telles que l'on ait l'identité

$$x^2+ax+b = (x-r)(x-s)\,.$$

On a donc

$$r + s = -a\,, \tag{1}$$

$$rs = b\,. \tag{2}$$

On peut éliminer s par (1), d'où $s = -r - a$, puis calculer avec les puissances successives de r

1
r
$r^2 = -ar - b$
$r^3 = r^2 r = (-ar - b)r = -ar^2 - br = -a(-ar - b) - br = (a^2 - b)r + ab$
$\dots$

Tout se ramène en définitive à des expressions linéaires du type $\alpha r + \beta$ avec les règles de calculs

$$(\alpha r + \beta) + (\alpha' r + \beta') = (\alpha + \alpha')r + (\beta + \beta')$$

$$(\alpha r + \beta) \times (\alpha' r + \beta') = \alpha'' r + \beta''$$

avec $\alpha'' = \alpha\beta' + \beta\alpha' - a\alpha\alpha'$, $\beta'' = \beta\beta' - b\alpha\alpha'$. Dans le cas de l'équation $x^2 + 1 = 0$, avec les racines i et $-i$, on retrouve les règles de calcul usuelles sur les nombres complexes. En un sens, les nombres complexes sont virtuels, car on calcule avec un nouveau symbole i, qui n'a pas de sens au niveau des nombres "réels" usuels.

Reprenons tout cela de façon plus générale. Soit $x^n - c_1\, x^{n-1} + c_2\, x^{n-2} - \dots + (-1)^n\, c_n = 0$ une équation polynomiale arbitraire de degré n. Soient $r_1, \dots, r_n$ les racines virtuelles de cette équation, définies par l'identité

$$x^n - c_1\, x^{n-1} + \dots + (-1)^n\, c_n = \prod_{i=1}^{n} (x - r_i)\,.$$

Les relations entre coefficients et racines sont obtenues en comparant les coefficients des diverses puissances de x

$$(S)\ \begin{cases} \sum r_i = c_1 \\ \sum_{i<j} r_i\, r_j = c_2 \\ \sum_{i<j<k} r_i\, r_j\, r_k = c_3 \\ \dots \\ r_1 \dots r_n = c_n\,. \end{cases}$$

On a introduit n symboles $r_1, \dots, r_n$ et n relations formant le système (S). Plus abstraitement, on a construit un anneau A contenant le corps k (domaine de rationalité selon Galois, contenant les coefficients $c_1, \dots, c_n$) et engendré

par $r_1, \ldots, r_n$ satisfaisant aux relations (S). On prouve que A est un espace vectoriel de dimension $n!$ sur le corps k, avec une base formée des monômes $r_1^{\alpha_1} r_2^{\alpha_2} \ldots r_{n-1}^{\alpha_{n-1}}$ tels que $0 \leq \alpha_i \leq i$ pour $1 \leq i \leq n-1$. L'ambiguïté est ici totale et rien ne permet de distinguer une racine d'une autre. Il y a en fait un groupe particulier, le groupe d'ambiguïté ou groupe de symétrie de la situation, qui est le groupe S_n (d'ordre $n!$) formé des permutations σ de $\{1, 2, \ldots, n\}$. Il agit par automorphismes sur l'algèbre A en envoyant r_i sur $r_{\sigma(i)}$.

Le but de la théorie de Galois est de lever partiellement l'ambiguïté ou, pour le dire en termes de physique plus récente, de briser la symétrie. Selon une stratégie bien connue dans beaucoup de problèmes géométriques, qui consiste à remplacer un groupe naturel de symétrie par un groupe plus petit, le but de la théorie de Galois est donc de lever partiellement l'ambiguïté en remplaçant S_n par un groupe plus petit. On n'arrive pas en général à la lever totalement puisque, dans l'exemple donné au départ, $\sqrt{5}$ et $-\sqrt{5}$, quelle que soit la manière de procéder, sont toujours indiscernables algébriquement.

1.3 Première méthode pour lever l'ambiguïté

Supposons $c_1, \ldots, c_n$ rationnels et $k = \mathbb{Q}$ (pour simplifier) et supposons également que l'on sache qu'il existe n racines réelles. On identifie les racines "virtuelles" $r_1, \ldots, r_n$ et les racines "réelles" $\rho_1, \ldots, \rho_n$ par la substitution $r_1 \to \rho_1, \ldots, r_n \to \rho_n$ qui définit un homomorphisme $\omega : A \to \mathbb{R}$. Au lieu de faire les calculs dans $\mathbb{R}$, ce qui suppose toujours une petite erreur d'arrondi et une référence implicite à l'infinité de décimales, on peut les faire dans l'anneau A, enrichi par une relation d'ordre $a > b$ satisfaisant aux règles usuelles, plus la prescription $r_1 > r_2 > \ldots > r_n$ si l'on a choisi $\rho_1 > \rho_2 > \ldots > \rho_n$ (dans $\mathbb{R}$).

On peut raisonner ainsi de manière individualisée sur les racines (c'est-à-dire que chaque racine est maintenant bien identifiée, ρ_1 est définie comme étant la plus grande racine, ...) avec des algorithmes qui ne présupposent pas la construction des nombres réels par des approximations au moyen de nombres décimaux. L'enjeu est d'avoir des *méthodes finies, donc exactes*. Quand on fait de l'analyse numérique, il y a toujours des erreurs, quelle que soit la précision utilisée. Ces méthodes ont été développées par les spécialistes de la géométrie algébrique réelle (Bochniak, Coste, Roy), comme sous-produit de recherches géométriques.

Pendant longtemps, la théorie de Galois a été conçue comme quelque chose d'extrêmement abstrait, et pendant environ un siècle et demi, on n'avait pas les moyens de mettre en œuvre les calculs. On peut aujourd'hui trouver assez facilement le groupe de Galois d'un polynôme de degré 18 ou 20, mais pas beaucoup plus.

Les racines complexes peuvent être traitées de façon analogue. La représentation géométrique des nombres complexes par les points d'un plan permet d'individualiser les racines, en disant par exemple que telle racine est la seule qui soit à l'intérieur de tel cercle.

1.4 Deuxième méthode pour lever l'ambiguïté

Le spectre Σ de l'anneau A se compose des idéaux premiers de A. Ils sont en nombre fini. Faisons *l'hypothèse de séparabilité*. Autrement dit, supposons qu'il n'y a pas de racines multiples. Cette hypothèse se traduit en disant que le discriminant[1] du polynôme donné $P(X) = X^n - c_1 X^{n-1} + \ldots + (-1)^n c_n$ est non nul. On peut alors décomposer A en somme directe de corps $A = K_1 \oplus \ldots \oplus K_m$, chacun de ces corps étant stable par multiplication. Les idéaux premiers sont :

$$\begin{cases} \mathfrak{p}_1 = \cdot \oplus K_2 \oplus \ldots \oplus K_m \\ \mathfrak{p}_2 = K_1 \oplus \cdot \oplus \ldots \oplus K_m \\ \ldots \\ \mathfrak{p}_m = K_1 \oplus \ldots \oplus K_{m-1} \oplus \ . \end{cases}$$

On a $A/\mathfrak{p}_i \approx K_i$ et $\Sigma = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ est le spectre.

On se rend compte qu'il y a de la géométrie algébrique sous-jacente. On peut dire que la théorie de Galois est de la géométrie algébrique où tout est de dimension zéro. La grande nouveauté de la géométrie algébrique selon Grothendieck, c'est que tout varie. ("Les constantes ne sont que des variables qui se reposent".) On ne considère donc pas en général un seul espace, mais toute une famille. C'est ici déjà bien visible : dans la construction donnée ci-dessus, on fixe les constantes $c_1, c_2, \ldots, c_n$ mais si on les fait varier, on a un espace de paramètres à n dimensions et pour chaque valeur des paramètres on a, au-dessus, une fibre, qui est un espace d'un nombre fini de points.

Point crucial :

Le groupe d'ambiguïté S_n agit sur A, donc sur Σ. Si l'on choisit[2] un élément $\mathfrak{p}_i$ du spectre Σ correspondant à un "foncteur fibre" (ce qui revient à lever partiellement l'ambiguïté), on dispose d'un sous-groupe G_i de S_n, à savoir le stabilisateur de $\mathfrak{p}_i$. Par définition, $\sigma \in G_i \Leftrightarrow \sigma(\mathfrak{p}_i) = \mathfrak{p}_i$.

Remarque importante :

Si l'on choisit un des $\mathfrak{p}_i$, on descend du groupe symétrique à un groupe plus petit. On a brisé la symétrie et levé partiellement l'ambiguïté, mais il y a m choix possibles. On ne dispose donc pas d'un sous-groupe du groupe symétrique, mais de m sous-groupes et il est facile de voir que ces différents sous-groupes de S_n sont conjugués les uns des autres.

Conclusion :

La donnée d'un corps k, domaine de rationalité pour Galois, et d'un polynôme séparable P de $k[X]$, de degré n, (que Galois ne suppose jamais irréductible contrairement à ce que feront ses successeurs (Artin, Emmy Noether)) définit une classe de conjugaison de sous-groupes du groupe des permutations S_n. En ce sens, il n'y a pas de groupe de Galois d'une équation.

[1] Ce discriminant est calculable par une formule universelle en $c_1, \ldots, c_n$, par exemple $c_1^2 - 4c_2$ dans le cas $n = 2$.

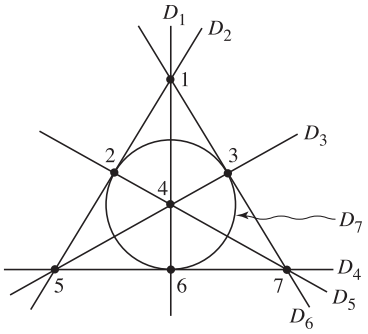
[2] Ce qui revient à choisir un corps K contenant k et une factorisation $P(X) = (X - \rho_1) \ldots (X - \rho_n)$ dans $K[X]$.

1.5 Recherches algorithmiques

Il n'est pas très facile de calculer explicitement le groupe de Galois d'une équation. J'ai détenu à un certain moment un bref record du monde. J'avais traité l'exemple de l'équation :

$$x^7 - 7x + 3 = 0\,.$$

Un des sous-groupes du groupe des permutations de 7 lettres particulièrement intéressant provient du plan de Fano :



"Droites" $D_1, \ldots, D_7$, la dernière correspond au cercle passant par $2, 3, 6$

$$\begin{array}{lll} D_1 = 146 & D_2 = 125 & D_3 = 345 \\ D_4 = 567 & D_5 = 247 & D_6 = 137 \\ & D_7 = 236 & \end{array}$$

C'est un plan projectif sur le corps à deux éléments[3]. Il y a donc 7 points dans ce plan projectif et puisqu'un plan projectif contient autant de droites que de points, il y a aussi 7 droites (l'une de ces "droites" est un cercle sur la figure). Chaque droite contient 3 des 7 points. Si une équation a 7 racines, il faut trouver 7 groupements de 3 racines qui ont un rôle particulier. Si l'on trouve ces 7 groupements, chaque groupement fournira une somme ou un produit. Donc, si l'on peut associer les 7 racines de l'équation aux points d'un tel plan projectif, il y aura 7 blocs (droites) de 3, donc 7 nouveaux nombres. Certains blocs de 3 racines sont privilégiés, la symétrie est donc brisée. Les permutations qui vont persister sont celles qui ont la propriété de permuter les 7 points de telle manière que 3 points alignés donnent 3 points alignés. On vérifie facilement que le groupe obtenu est d'ordre 168. C'est le groupe $PGL(3, \mathbb{F}_2)$. Cette stratégie fonctionne dans le cas de l'équation $x^7 - 7x + 3 = 0$, dont le groupe de Galois est donc isomorphe à $PGL(3, \mathbb{F}_2)$.

[3]Si un corps a q éléments, le plan projectif correspondant a $q^2 + q + 1$ points ; ici $q = 2$, le plan projectif correspondant a donc 7 points.

Le problème qui s'était posé quand je me suis occupé de cette question (en 1978) était de trouver un exemple explicite d'équation dont le groupe de Galois soit ce groupe-là. En effet, on a fait la

Conjecture : *Tout groupe fini simple peut se réaliser comme groupe de Galois d'une équation à coefficients rationnels.*

Cette conjecture est très loin d'être démontrée aujourd'hui, et mon travail était un des tout premiers pas vers cette conjecture. En effet, parmi les groupes simples, le premier est d'ordre 60, le suivant est le groupe précédent d'ordre 168. On a depuis fait beaucoup mieux.

Galois lui-même était conscient de la difficulté de déterminer le groupe de Galois d'une équation choisie au hasard, sans une motivation provenant d'un autre problème. Il y eut quelques progrès de 1850 à 1970, mais seul l'avènement des ordinateurs a permis une avancée substantielle. La difficulté est d'énumérer, à conjugaison près, les sous-groupes du groupe de permutations S_n, et de donner des critères calculables pour les distinguer. Par développement d'idées remontant à Lagrange, et quelques idées nouvelles en théorie des groupes, J.-M. Arnaudiès et A. Valibouze ont mis au point des méthodes complètement programmées pour les équations de degré $n \leq 16$ (ou peut-être un peu mieux aujourd'hui). Les travaux en géométrie algébrique réelle de l'École de Rennes ont un potentiel d'application qui n'a pas été exploité.

1.6 Explication du texte de Galois

On a 2 corps commutatifs :
k corps où sont les coefficients
$K \supset k$ corps où sont les n racines de l'équation $P(X) = 0$ de degré n.
Le polynôme $P(X)$ appartient à $k[X]$.

On considère l'ensemble de toutes les factorisations

$$P(X) = (X - s_1) \dots (X - s_n)$$

de P dans $K[X]$. Il y en a $n!$, toutes déduites de l'une d'entre elles par permutation des facteurs. (Les s_i sont des éléments de K.)

Dans le cas particulier $n = 3$, on a 6 permutations correspondant aux 6 factorisations :

$$P(X) = (X - a)(X - b)(X - c)$$
$$P(X) = (X - a)(X - c)(X - b)$$
$$P(X) = (X - b)(X - a)(X - c)$$
$$P(X) = (X - b)(X - c)(X - a)$$
$$P(X) = (X - c)(X - a)(X - b)$$
$$P(X) = (X - c)(X - b)(X - a)\,.$$

Galois donne alors la définition : deux factorisations

$$P(X) = \prod_{i=1}^{n} (X - a_i)\,, \quad P(X) = \prod_{i=1}^{n} (X - b_i)$$

sont équivalentes si, pour tout polynôme F à n variables à coefficients dans k, on a

$$F(a_1, \ldots, a_n) = 0 \Leftrightarrow F(b_1, \ldots, b_n) = 0\,.$$

Les classes d'équivalence de cette relation sont les "groupes" au sens de Galois. Dans le cas particulier $n = 3$, on peut avoir 3 groupes formés chacun de 2 permutations

$$\begin{cases} abc \\ acb \end{cases} \quad \begin{cases} bac \\ cab \end{cases} \quad \text{et} \quad \begin{cases} bca \\ cba \end{cases}.$$

Il est facile de montrer que ces paquets correspondent exactement aux éléments du spectre de l'algèbre A introduite au n° 1.4. Il y a ici deux sens au mot permutation : on permute des boîtes sans savoir ce qu'il y a dedans ou bien on permute ce qui est dans les boîtes et non pas les boîtes. Il faut distinguer les racines et les noms des racines.

Je termine par deux interprétations. Un *torseur* est défini par un groupe G à p éléments, un ensemble X à p éléments et une action de G sur X

$$G \times X \to X\,, \quad (g, x) \mapsto gx\,.$$

L'hypothèse "torseur" (on dit aussi "simplement transitif") est que dans l'équation $gx = y$, x et y étant donnés, il y a toujours un g et un seul dans G qui convient. Le point délicat est que, quand on a un tel torseur, il y a un autre groupe caché H qui est l'ensemble des permutations des éléments de X qui commutent à toutes les actions de G[4]. On montre que ce groupe H a le même nombre d'éléments que G, il lui est même isomorphe. La distinction entre permutation des boîtes et permutation des boules dans les boîtes est là. *Les groupes au sens de Galois sont en fait des torseurs*; cela tient à ce que dans un de ces "groupes", il n'y a pas d'élément privilégié. En géométrie, un espace affine est un torseur pour le groupe des translations, et il n'a pas d'origine fixée.

On peut aussi introduire la *topologie de Zariski*. On dispose de l'ensemble F formé des $n!$ factorisations de la forme

$$P(X) = (X - a_1) \ldots (X - a_n)$$

dans l'ensemble $K[X]$ des polynômes à coefficients dans K. Les systèmes $(a_1, \ldots, a_n)$ correspondants forment une partie finie $\tilde{F}$ de l'espace K^n de dimension n sur K. Mais le fait que l'on a deux corps k et K permet d'introduire la topologie de Zariski sur K^n (relative à k) : une partie fermée Φ est l'ensemble des solutions d'un système d'équations

$$H_j(a_1, \ldots, a_n) = 0 \quad \text{pour } 1 \leq j \leq m\,,$$

[4] H est l'ensemble de toutes les transformations f de X dans X qui ont la propriété que $f(gx) = g(fx)$ quel que soient x dans X et g dans G.

où les m polynômes H_j sont à coefficients dans k. Alors $\tilde{F}$ est une partie fermée de K^n, et *les groupes au sens de Galois sont les composantes irréductibles* (ou connexes) *de* $\tilde{F}$.

2 Riemann et la monodromie

2.1 Le rôle des singularités et des exceptions

La théorie des revêtements est née des problèmes de monodromie. Poincaré l'a développée et Grothendieck a réalisé une synthèse formelle entre cette théorie des revêtements et la théorie de Galois en les faisant découler d'une théorie plus générale et plus abstraite : *la théorie des catégories galoisiennes*. Cette présentation des catégories galoisiennes de Grothendieck est un des buts de son premier séminaire SGA1. Elle s'applique très bien aux fonctions algébriques. Le but de Grothendieck était d'ailleurs de présenter la théorie des revêtements d'une manière qui puisse ensuite s'appliquer aux variétés algébriques ou aux schémas, qui en sont la généralisation, et qui, par conséquent, en fournisse le cadre naturel et les concepts. C'était le point de départ de ce qui sera une de ses grandes créations : la cohomologie étale. Mais, dans les applications que donne Grothendieck, les revêtements ont essentiellement un nombre fini de feuillets. Riemann va plus loin, et traîte les équations différentielles par ces méthodes, en commençant par la fonction hypergéométrique, où il faut, en général, une infinité de feuillets. Au lieu de travailler comme Grothendieck le fait avec un *groupe pro-fini* (c'est-à-dire une tour de groupes finis les uns au-dessus des autres, et un passage à la limite intéressant, mais relativement formel), Riemann utilise des groupes discrets infinis. Quand, quelques années plus tard, Grothendieck est revenu sur ces problèmes et a inventé les *catégories tannakiennes*, il a étendu cette construction en remplaçant des groupes finis, ou des tours de groupes finis, par des groupes algébriques ou des tours de groupes algébriques. (Selon la terminologie de Serre, une tour de groupes finis est un groupe pro-fini, une tour de groupes algébriques, un groupe pro-algébrique.) Essayons de présenter les idées géométriques de Riemann.

La théorie de Galois nous donne un certain groupe de transformations sur les racines, et l'on cherche à en donner une interprétation géométrique. L'idée de Riemann est que *la source de ces transformations est à chercher dans les singularités*. C'est dans son travail sur la fonction hypergéométrique que cette idée prend toute sa force. Pour Riemann, la propriété essentielle de la fonction hypergéométrique de Gauss est qu'elle satisfait à une équation différentielle du second ordre qui admet des singularités, en deux ou trois points selon le point de vue adopté : 0 et 1 sont certainement des points singuliers, mais une des idées fortes de Riemann est que, quand on étudie des fonctions d'une variable complexe, il faut aussi regarder ce qui se passe à l'infini. Il est commode, dans ce cas, d'ajouter un point à l'infini au plan complexe, pour construire ce qu'on appelle la *sphère de Riemann*. Ce point à l'infini est la troisième singularité. Nous reviendrons plus loin sur la fonction hypergéométrique.

Il y aurait à ce propos tout un débat épistémologique à faire sur ce qu'est un objet idéal tel qu'un point à l'infini. Il y eut pendant très longtemps une croyance implicite en une ontologie réaliste des mathématiques, qui voulait que, s'il y a des points à l'infini, il ne puisse y en avoir que d'une seule manière. Un des grands chocs épistémologiques du dix-neuvième siècle fut de s'apercevoir que, si l'on fait de la géométrie projective, il faut ajouter au plan *toute une ligne droite de points à l'infini*, mais que, si l'on fait de la géométrie conforme (c'est-à-dire qu'on considère les transformations qui ne respectent pas les distances, mais seulement les angles), il faut ajouter un unique point à l'infini, pour obtenir la sphère de Riemann. Les choses sont analogues en dimension supérieure. Donc, aujourd'hui, nous rencontrons un problème épistémologique récurrent dans beaucoup de questions géométriques : on dispose d'un espace ouvert, c'est-à-dire non compact, avec des bords indéfinis, et le problème est de construire des compactifications[5]. Pour cela, on doit ajouter à des espaces qui ont une certaine vertu naturelle des objets idéaux qui les rendront compacts et qui permettront de faire disparaître des exceptions et d'appliquer des techniques générales beaucoup plus puissantes.

Un exemple contemporain est fourni par les *espaces de configurations* : on se demande par exemple comment classer les systèmes de quatre points sur une droite. Dans un premier temps, on les prend distincts, et il s'agit de savoir ensuite quelles sont les configurations limites. Si j'ai quatre points distincts, comment peuvent-ils dégénérer ? L'étude soignée de la dégénérescence est importante. En géométrie algébrique, on a des situations analogues. En *géométrie énumérative*, on veut compter par exemple combien il y a de surfaces quadriques qui s'appuient sur quatre droites données et qui coupent un plan selon une conique donnée... En général, pour avoir des formules de comptage nettes, on est obligé d'admettre des configurations dégénérées. Par exemple, une conique peut dégénérer en deux droites qui se coupent, ou même en une droite double, et c'est toujours un problème délicat de choisir les configurations dégénérées admissibles. Là aussi, l'ontologie réaliste implicite des mathématiques n'est pas toujours un bon guide, parce qu'il faut justement admettre la diversité.

Ces problèmes de compactification n'ont en général pas une seule solution, mais plusieurs. Une analyse des singularités, dans l'esprit de Riemann, permet de le voir. Il faut décrire ces diverses compactifications, peut-être les établir sous forme d'une hiérarchie avec des transformations de l'une dans l'autre, peut-être s'apercevoir que l'une d'entre elles est plus universelle que les autres et les coiffe toutes... L'étude de ces compactifications dans les problèmes de classification que Grothendieck appelle *problèmes des modules* a été très important pour lui, et c'est toujours un problème d'actualité. Revenons à Riemann.

Selon Riemann, il faut donc chercher la source de bien des phénomènes non pas dans la régularité, mais dans la singularité. C'est la singularité qui déteint sur le régulier et qui explique les phénomènes du régulier. J'ai donné précédemment la définition du groupe de Galois d'une équation, mais comme

[5]Sans entrer dans les définitions techniques, disons qu'un plan illimité est un espace ouvert, mais qu'une sphère est un espace compact, refermé sur lui-même sans échappatoire possible.

je l'ai mentionné, le calcul effectif de ce groupe de Galois est difficile et les méthodes géométriques sont justement celles qui nous fournissent, non pas le groupe entier, mais des éléments privilégiés de ce groupe. Chaque singularité engendrant par monodromie un élément du groupe ou un sous-groupe cyclique du groupe, il faut ensuite regrouper tous ces éléments pour en déduire la structure du groupe de Galois. Nous construisons donc le groupe de Galois en fabriquant explicitement certains éléments, d'origine géométrique. Compte tenu de l'analogie entre courbes algébriques et nombres algébriques, on a, après Frobenius, fait fonctionner ces méthodes dans le cadre arithmétique. Ce fut là un grand succès. En arithmétique, le moyen le plus puissant pour construire le groupe de Galois, par engendrement, c'est de déterminer les transformations de Frobenius correspondant à chacun des nombres premiers ou tout au moins, aux quelques privilégiés qui, justement, sont les endroits où les choses se passent mal. *C'est aux endroits où les choses se passent mal qu'il est intéressant de regarder selon cette philosophie générale.*

Je vais essayer maintenant de traduire cela plus explicitement dans deux domaines. Tout d'abord, celui des équations algébriques, ensuite celui des équations différentielles, en suivant d'assez près, sinon les détails mathématiques, tout au moins la stratégie de Riemann.

2.2 Cas des fonctions algébriques

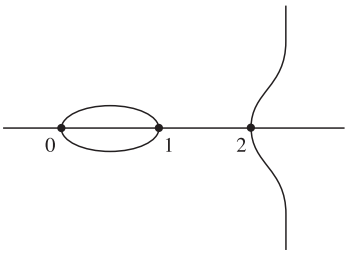
Je traiterai deux exemples particuliers.

Exemple 1 : $y^2 = x(x-1)(x-2)$.

C'est celui d'une extension quadratique. Dans cet exemple, il faut considérer *y comme étant l'inconnue et x comme un paramètre.* Il y a un double point de vue, le point de vue *arithmétique* consistant à dire : "je n'ai pas une équation quadratique... mais toute une famille dépendant d'un paramètre x qu'on prendra rationnel". Quand x est différent de 0, 1 ou 2, l'équation équivaut à quelque chose du type $y^2 = c$ avec $c \neq 0$, équation qui a deux racines, et dont le groupe de Galois peut être d'ordre 1 ou 2, selon les *propriétés arithmétiques* du nombre c (dépendant elles-mêmes des propriétés arithmétiques de x). Dans les cas singuliers, si x vaut 0, 1 ou 2, cette équation devient $y^2 = 0$. Elle n'est plus séparable. La racine double $y = 0$ n'est pas un nombre virtuel, c'est un vrai nombre. Pas de groupe de Galois, ou plutôt, ce groupe est d'ordre 1 ! Si l'on voit cela comme une variation de paramètres, pour x différent de 0, 1 ou 2, on a un groupe de Galois d'ordre 1 ou 2, et pour les valeurs exceptionnelles, ce groupe est d'ordre 1. A partir de ce qui se passe autour de 0, 1 et 2, peut-on fabriquer une monodromie qui va nous donner le groupe de Galois ?

Autre façon de procéder que je qualifierai de *géométrique* : considérer que x est une variable. Nous avons au départ le corps de rationalité, *le corps des fonctions rationnelles en x* (nous prendrons les coefficients dans l'ensemble des nombres complexes pour simplifier). On veut fabriquer une extension de ce corps en ajoutant des fonctions de x sous forme d'une racine de l'équation $y^2 = x(x-1)(x-2)$. Il y a de nouveau un double point de vue : nous pouvons, soit

considérer que les fonctions de x sont données, ce sont les fonctions rationnelles, et que l'on veut étendre les fonctions dont on dispose en ajoutant aux fonctions rationnelles certaines fonctions irrationnelles ; c'est comme cela que l'on raisonnait au dix-huitième siècle, par exemple chez Legendre. On parle alors de fonctions algébriques du type $F(x, y)$, étant entendu que $y = \sqrt{x(x-1)(x-2)}$. L'ambiguïté est qu'il y a pour chaque valeur de x deux possibilités pour y. Mais que se passe-t-il quand on fait varier x : le signe change-t-il ou non ? Cette ambiguïté doit être contrôlée pour tenir compte des variations. Ce point de vue fait jouer un rôle différent à x et à y. Par contre, si l'on raisonne vraiment de manière géométrique, on considérera l'équation donnée comme une équation définissant une courbe dans le plan de coordonnées x, y. Voici l'allure de la courbe :



Si l'on considère, comme on le faisait au dix-huitième siècle, x comme la variable indépendante et y comme la variable dépendante, cela signifie que l'on va considérer la projection qui envoie un point de la courbe de coordonnées x, y sur le point x de l'axe des abscisses. Géométriquement, on choisit dans le plan une direction privilégiée qui rabat tout par projection verticale sur une droite horizontale (horizontal et vertical étant à prendre dans un sens purement métaphorique). La vision est celle d'une courbe dans le plan avec une projection sur une droite[6]. *Les points singuliers, non pas de la courbe, mais de la projection sont ceux où la tangente est verticale.* Décrivons l'analogue à 3 dimensions : on a une surface décrite par une équation du type $F(x, y, z) = 0$, on projette sur le plan xy et les points singuliers sont ceux où le plan tangent à la surface contient une direction verticale, c'est-à-dire ce que l'on appelle le *contour apparent* de la surface. *Les singularités correspondent géométriquement au contour apparent.*

L'idée de Riemann est de voir comment l'on peut interpréter géométriquement le groupe de Galois. Cela se fait de la manière suivante : l'équation $y^2 = x(x-1)(x-2)$ est invariante si l'on change y en $-y$. La symétrie de Galois est à x fixé (par convention, dans la théorie de Galois, les données ne bougent provisoirement pas) ; x est donc considéré provisoirement *comme donné, mais indéterminé.* On change par contre y en $-y$. On fait géométriquement une symétrie par rapport à l'axe des abscisses. Le groupe de Galois apparaît donc comme une propriété de cette courbe par rapport à la projection : *il y a une*

[6] Si l'on ne fait pas la distinction entre variables indépendantes et dépendantes, il ne reste qu'une courbe dans le plan.

symétrie de la courbe compatible avec la projection[7]. Le groupe de Galois correspond à cette symétrie ; c'est un groupe d'ordre 2, contenant, comme dans tout groupe, la transformation identique $(x, y) \mapsto (x, y)$ et aussi $(x, y) \mapsto (x, -y)$.

Si l'on voulait revenir à un *groupe de Galois arithmétique*, il faudrait fixer x, lui donner par exemple la valeur 5, d'où une équation particulière : $y^2 = 60$ (équivalente du point de vue de la théorie de Galois à l'équation $y^2 = 15$). A quel groupe de Galois cette équation correspond-elle ? Cela dépend de la nature arithmétique de x. On a ici $x = 5$ et 15 n'est pas un carré parfait, donc on a un groupe d'ordre 2. Mais on pourrait trouver des valeurs de x particulières pour lesquelles y^2 serait un carré parfait, le groupe de Galois dégénérerait donc de nouveau. Il y a donc deux problèmes différents dans ce genre d'équation : une *stratégie géométrique* où l'on traite x comme un paramètre indéterminé, et où l'on raisonne sur des fonctions ou géométriquement sur des courbes, des surfaces ou des variétés algébriques, et *une stratégie arithmétique* où l'on spécialise la valeur de x et où l'on s'intéresse aux propriétés arithmétiques des nombres obtenus. La question est du type : un point particulier de la courbe correspondant à une valeur de x particulière est-il un point rationnel, c'est-à-dire un point dont les deux coordonnées sont des nombres rationnels ?

La partie arithmétique elle-même fait semblant de se géométriser si l'on tient compte du fait qu'un nombre premier p joue le rôle d'un point. Dans mon exposé sur le spectre, j'ai dit que le spectre de l'anneau des entiers est l'ensemble des nombres premiers, auquel on adjoint un objet exceptionnel que l'on peut appeler 0 ou l'infini. Si l'on voit l'ensemble $\mathbb{Z}$ des entiers relatifs à son tour comme une courbe dont les points sont les nombres premiers, on rajoute une dimension. On a rajouté une dimension arithmétique et la courbe n'est plus de dimension 1, mais de dimension arithmétique 2, parce que les nombres eux-mêmes ont une mobilité. Toute cette stratégie a été grandement développée pendant les quarante dernières années, et l'on peut dire que la thèse d'André Weil, sur le problème de Mordell, a inauguré ce point de vue.

Revenons à Riemann. Il fait tout d'abord une étude de la *ramification*, c'est-à-dire de ce qui se passe autour des points singuliers.

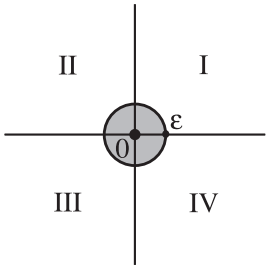
Exemple 2 : $y^4 = x$.

Montrons que dans ce cas, il y a une monodromie liée à la racine quatrième de l'unité $i = e^{2\pi i/4}$ (si y avait été élevé à la puissance n, cette monodromie aurait été liée à la racine n-ième de l'unité $e^{2\pi i/n}$). Or $i^4 = 1$; donc si, dans l'équation on remplace y par iy, rien ne change : $(iy)^4 = y^4$. On a donc découvert une symétrie dans l'équation : on peut, sans changer x, multiplier y par i et, plus généralement, par n'importe quel élément du groupe cyclique engendré par i ($\mu_4 = \{1, i, i^2, i^3\}$). Il est facile de voir que pour l'équation $y^4 = x$, si ω

[7] Quand on veut formaliser tout cela de manière purement algébrique, sans recours à la géométrie, comme les mathématiques modernes ont tendance à vouloir le faire, on écrit *une formule algébrique qui est une figure* : paradoxe...

satisfait l'équation $\omega^4 = 1$, on aura $(\omega y)^4 = x$. La multiplication par ω définit une symétrie de l'équation.

Reprenons l'équation $y^4 = x$. Quel est le point de vue de Riemann ?

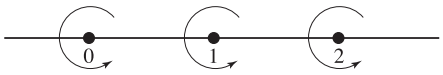


Le plan complexe est découpé en quatre secteurs déterminés par les deux axes (axe réel et axe imaginaire). Pour simplifier les choses, plaçons-nous autour de 0 et considérons les nombres complexes x tels que $|x| \leq \varepsilon$. La stratégie consiste à oublier l'origine. On a fait un trou dans le disque et tourner autour de ce trou, de cet obstacle géométrique, a un sens. Chaque secteur est un morceau simplement connexe[8] du plan et un théorème classique nous dit que, tant que x reste dans l'un de ces quatre secteurs, on peut choisir une solution particulière de l'équation $y^4 = x$ qui dépende continuement de x. Autrement dit, on peut trouver une fonction $f(x)$ définie et continue pour tout x de ce secteur, holomorphe (à l'intérieur en tous cas) et qui vérifie l'équation $(f(x))^4 = x$. Dans le cas du secteur I, on peut la spécialiser en imposant par exemple $f(1) = 1$. Une fois décrite cette fonction, on a réussi à faire tourner la fonction initiale : $\sqrt[4]{x}$ pour $x > 0$, définie comme l'unique racine quatrième réelle et positive. Le secteur I permet de tourner d'un quart de tour et fait passer d'une détermination de la racine quatrième sur l'axe réel à une détermination sur l'axe imaginaire positif. C'est le début de la monodromie : on part d'une solution de l'équation dans une direction, on remplit un secteur et on obtient une solution sur une autre direction. On peut continuer (un quart de tour, puis 2, puis 3, puis 4). Mais, quand on a fait le tour complet, on ne revient pas au point de départ. On ne retombe pas sur $\sqrt[4]{x}$, mais sur $i \times \sqrt[4]{x}$. (D'une manière générale, si l'on résout l'équation $y^n = x$, et si l'on part de la solution réelle positive, on revient à cette solution multipliée par $e^{2\pi i/n}$.) Si l'origine n'était pas singulière, il y aurait une seule détermination pour tout le disque. C'est cette singularité qui fait apparaître la multiplication par i. On peut continuer : un deuxième tour nous enverra sur $i^2 \times \sqrt[4]{x}$, un troisième tour sur $i^3 \times \sqrt[4]{x}$ et l'on retombera sur la solution initiale au quatrième tour. Il faut donc tourner quatre fois autour de l'origine pour retrouver la détermination initiale de la racine quatrième de x. Voilà décrite la ramification dans un exemple simple.

Compliquons maintenant l'exemple et revenons à l'équation $y^2 = x(x-1)(x-2)$. On part de la solution réelle positive dans l'intervalle $]0, \varepsilon[$ et on la

[8] Ceci signifie que tout chemin fermé, partant d'un point a et y revenant, se contracte continuement sur le point a. Ceci est possible car il n'y a pas de trou dans un quart de plan.

fait tourner d'un tour dans le sens direct autour de 0. On trouve la solution opposée[9].



Pourquoi avoir choisi le point singulier 0 ? On aurait pu choisir le point singulier 1 ou le point singulier 2, et tourner autour de 1 ou tourner autour de 2. Il se trouve que si l'on fait la même construction autour des points 1 et 2, le résultat est identique. (Dans le cas des équations différentielles, par contre, la monodromie des divers points joue différemment.) On peut dire que, si l'on part d'une détermination de la fonction y en fonction de x et que l'on fait des monodromies autour des divers points, on a deux possibilités : retrouver la première détermination ou la retrouver au signe près. C'est tout simplement parce qu'il n'y a que deux valeurs de y pour chaque valeur de x. Voilà très rapidement expliquée la méthode de monodromie de Riemann pour les fonctions algébriques.

On pourrait décrire autrement la situation. Si l'on veut raisonner globalement, on introduit deux demi-plans $\mathbb{C}_+$: partie imaginaire positive et $\mathbb{C}_-$: partie imaginaire négative. Ces domaines $\mathbb{C}_+$ et $\mathbb{C}_-$ sont simplement connexes. Donc, d'après les théorèmes généraux, il existe dans $\mathbb{C}_+$ une fonction f_+ holomorphe satisfaisant à $(f_+(x))^2 = x(x-1)(x-2)$ que l'on peut normaliser en disant qu'au delà de 2, $f_+ > 0$. De la même façon f_- est définie pour x dans $\mathbb{C}_-$ par $(f_-(x))^2 = x(x-1)(x-2)$. On peut aussi prendre $-f_+$ et $-f_-$. Chacune de ces fonctions a des conditions limites : que se passe-t-il quand x devient réel ? Il faut éliminer 0, 1, 2 et avec les quatre morceaux dont on dispose (les fonctions f_+ et $-f_+$ sur $\mathbb{C}_+$, et les fonctions f_- et $-f_-$ sur $\mathbb{C}_-$) en faire un seul, c'est-à-dire rapiécer ces quatre morceaux : c'est la définition d'une surface de Riemann par recollement.

Donnons un point de vue *géométrique*. On considère la courbe d'équation $y^2 = x(x-1)(x-2)$ en prenant cette fois x et y complexes (on se retrouve avec *quatre* paramètres réels[10]). Si, dans l'équation $y^2 = x(x-1)(x-2)$, on sépare partie imaginaire et partie réelle, on a deux équations. Vu du point de vue de la géométrie réelle, on a une surface plongée dans un espace à quatre dimensions. C'est la surface de Riemann décrite ci-dessus, et Riemann nous a appris à en faire un découpage en quatre morceaux que l'on recolle. C'est le début de la topologie combinatoire : pour étudier une surface, on la découpe en morceaux, chacun des morceaux étant relativement facile à contrôler puisque c'est un domaine simplement connexe. Et tout se passe dans la manière dont se fait le recollement au bord de ces domaines.

[9] On a vu précédemment qu'une racine n-ième a une monodromie décrite par les racines n-ièmes de l'unité. Pour $n = 2$, on a les racines 2-ièmes 1 et -1 de 1.

[10] Un nombre complexe $z = u + iv$ correspond à deux nombres réels u et v !

2.3 Exemple de la fonction hypergéométrique

Considérons la fonction hypergéométrique de Gauss définie par :

$$F(z) = 1 + \frac{\alpha\beta}{\gamma}\, z + \frac{\alpha\beta}{\gamma}\frac{(\alpha+1)(\beta+1)}{(\gamma+1)}\frac{z^2}{2!} + \dots \tag{1}$$

Elle contient comme cas particuliers presque toutes les fonctions dites spéciales. Elle est la solution d'une certaine équation différentielle du second ordre, régulière sauf en 0, 1 et l'infini. Les singularités apparaissent dans les coefficients de l'équation différentielle : ce sont des fonctions rationnelles de z qui ont des pôles en 0, 1 et l'infini. La série de puissances (1) converge quand $|z| < 1$ (le rayon de convergence est 1, sauf dans les cas dégénérés). Peut-on aller au delà de $|z| < 1$? Euler a découvert une représentation intégrale : au moyen des intégrales eulériennes, on transforme

$$F(z) = 1 + \frac{\alpha\beta}{\gamma}\, z + \frac{\alpha\beta}{\gamma}\frac{(\alpha+1)(\beta+1)}{(\gamma+1)}\frac{z^2}{2!} + \dots$$

en une intégrale d'un type particulier :

$$F(z) = \int_0^1 f(t \mid \beta, \gamma)(1 - tz)^{-\alpha}\, dt\,. \tag{2}$$

Quel est l'avantage de cette représentation intégrale ? S'il existe un nombre réel t entre 0 et 1 tel que $1 - tz = 0$, il peut y avoir une difficulté. Or, il est très facile de voir que cela signifie que z est réel et $z > 1$; on va donc faire une *coupure* sur $[1, +\infty[$. Partout ailleurs, l'intégrale a un sens. On a obtenu une fonction définie pour toute valeur complexe de z sauf sur la coupure $[1, +\infty[$.

Il faut maintenant regarder ce qui se passe lorsque l'on tourne autour de la singularité $z = 1$. Si l'on s'approche par le dessous ou par le dessus de la coupure, on ne trouve pas la même limite. On a le phénomène de monodromie et on a deux déterminations, mais *on reste dans l'ensemble des solutions de l'équation différentielle.* A partir d'une solution déterminée de l'équation différentielle, on procède comme suit : prolongement analytique par une représentation intégrale, étude le long de la coupure, monodromie, nouvelle solution. Grâce à quoi, on a associé au point 1 une transformation, qui à partir d'une solution de l'équation différentielle au voisinage de 0, en fabrique deux autres sur la coupure $[1, +\infty[$. On peut voir que 0 aussi joue un rôle particulier dans d'autres solutions de la même équation. Il faut donc prendre les monodromies autour de 0 et de 1. Riemann nous enseigne à examiner le rôle de l'infini. Il y a là aussi une monodromie, mais elle se déduit de celles déjà considérées autour de 0 et 1.

Une équation différentielle du second ordre a un espace de solutions de dimension 2. La monodromie associée à 0, 1 ou l'infini permet de construire des transformations linéaires dans cet espace qui, à une solution donnée, font correspondre d'autres solutions. Il est important de regarder le groupe engendré par ces trois monodromies : *le groupe de monodromie de cette équation.*

Dans la section suivante, ce groupe de monodromie nous servira à construire le groupe de Galois d'une équation différentielle. Pour le moment, nous donnons une description de la surface de Riemann de la fonction hypergéométrique. Tout d'abord, nous coupons[11] le plan $\mathbb{C}$ des nombres complexes selon les demi-droites allant de $-\infty$ à 0 et de 1 à $+\infty$. Il faut imaginer que chacune des coupures crée deux bords et qu'un point x de $]1,+\infty[$ par exemple se dédouble en $x+i0$ (au-dessus) et $x-i0$ (au-dessous).

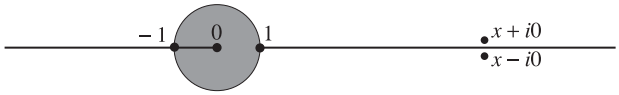
Grâce au prolongement analytique de la fonction hypergéométrique, nous disposons d'une solution $F_1(z)$ de l'équation différentielle hypergéométrique

$$\frac{d^2F}{dz^2} + \frac{\gamma-(\alpha+\beta+1)\,z}{z(1-z)}\,\frac{dF}{dz} - \frac{\alpha\beta}{z(1-z)}\,F = 0 \tag{3}$$

définie sur le plan coupé P. On montre qu'il existe une unique autre solution de la forme

$$F_2(z) = z^{1-\gamma}(1 + c_1\,z + c_2\,z^2 + \ldots) \tag{4}$$

dans le domaine hachuré ci-dessous, obtenu en ôtant le rayon $]-1,0]$ du cercle



défini par $|z|<1$. Cette solution se prolonge à tout P, et la solution générale de l'équation différentielle (3) sur P est de la forme $F_{c_1,c_2} = c_1\,F_1 + c_2\,F_2$ avec c_1, c_2 dans $\mathbb{C}$.

A chacune de ces solutions, on attache un "feuillet" P_{c_1,c_2}, qui est une copie de P. La monodromie dans le sens positif autour de 1 va attacher la lèvre inférieure de $]1,+\infty[$ dans le feuillet P_{c_1,c_2} à la lèvre supérieure de $]1,+\infty[$ dans un autre feuillet $P_{c_1',c_2'}$ de manière à faire se raccorder les valeurs limites $F_{c_1,c_2}(x-i0)$ et $F_{c_1',c_2'}(x+i0)$ pour $x>1$. On fait la même chose pour la monodromie en sens inverse autour de 1, et les monodromies directes et inverses autour de 0.

De proche en proche, on accroche au feuillet principal $P_{1,0}$ (correspondant à la fonction $F = 1\cdot F_1 + 0\cdot F_2$) une famille de feuillets qui forment une espèce d'accordéon : c'est la surface de Riemann S de la fonction hypergéométrique. *Le groupe de monodromie apparaît alors comme un groupe de transformations géométriques de cette surface S.*

[11] Le lecteur pourra imaginer une feuille de papier échancrée au moyen de deux coups de ciseaux. Il pourra aussi s'aider d'une réalisation matérielle.

3 Théorie de Galois des équations différentielles

3.1 Les équations différentielles et leurs solutions

Les équations différentielles ordinaires que nous étudierons sont des *équations linéaires* ; on peut sans difficulté ramener une équation linéaire d'ordre n à n équations d'ordre 1, et les propriétés générales des solutions des équations différentielles sont plus faciles à présenter dans le cadre des systèmes d'équations d'ordre 1, parce que l'on a à sa disposition la technologie des matrices. Le calcul matriciel est d'ailleurs une invention mathématique majeure du vingtième siècle[12] ; en tous cas, dans l'immense histoire de l'évolution de la notion de nombre, elle restera comme une étape très importante.

Le point essentiel de la philosophie de Riemann est de ramener les propriétés des équations différentielles à l'étude des singularités. Dans la théorie de Galois des équations différentielles, nous verrons plus loin, que dans le cas du type de Fuchs, les choses sont relativement simples. Nous verrons aussi qu'il y a des équations très simples, qui ne sont pas du type de Fuchs, et où il faut modifier les idées de monodromie. Dans ce cas, si l'on voulait être très formel, il faudrait introduire des groupoïdes de chemins, mais je me contenterai de signaler où sont les difficultés et de donner une solution pratique.

Notations :

• $S \subset \mathbb{C}$ est un ensemble fini de singularités : $S = \{s_1, \ldots, s_n\}$;

• $X = \mathbb{C}\backslash S$ est le plan des nombres complexes privé de S. C'est un ouvert du plan complexe et nous aurons à considérer des fonctions holomorphes sur des ouverts de X.

La théorie s'applique à un type particulier d'équations différentielles, ou de systèmes d'équations différentielles, dans lesquels les coefficients des équations sont des fonctions rationnelles avec tous leurs pôles dans S. Il faut donc introduire l'anneau $\mathcal{O} = \mathcal{O}_X$ des fonctions rationnelles sur $\mathbb{C}$ avec les pôles dans S. Il est assez facile d'en décrire la structure. Soit g le polynôme unitaire ayant comme racines les éléments de S :

$$g(z) = \prod_{s \in S} (z - s) = \prod_{i=1}^{n} (z - s_i)\,. \tag{1}$$

L'anneau des fonctions en question est l'anneau des fractions $P(z)/g(z)^r$ ayant un polynôme au numérateur et une puissance de g au dénominateur :

$$\mathcal{O} = \mathbb{C}\left[z, \frac{1}{g}\right]\,. \tag{2}$$

Utilisons ces notations pour poser le problème.

[12] Inventées par Cayley vers 1860, les matrices n'ont pris leur essor qu'après leur utilisation intensive en Mécanique Quantique vers 1930. Elles n'étaient pas enseignées en France vers 1950, et sont devenues le Pont-aux-Ânes aujourd'hui.

L'équation différentielle écrite sous forme matricielle et différentielle est :

$$dF(z) = A(z)\,dz\,F(z)\,. \tag{3}$$

Cette écriture est préférable, parce qu'une grande partie de la théorie se généralise immédiatement au cas où l'on aurait des fonctions rationnelles, holomorphes ou méromorphes, de plusieurs variables complexes ; l'expression $A(z)\,dz$, s'il y avait plusieurs variables, s'écrirait alors comme une somme de termes de la forme $A_j(z_1,\ldots,z_n)\,dz_j$. Dans l'équation (3), $A(z) = (a_{ij}(z))_{\substack{1\leq i\leq N\\ 1\leq j\leq N}}$, est une matrice à N lignes et N colonnes, ce qu'on note $A(z)\in\mathbb{C}^{N\times N}$, où les fonctions a_{ij} sont dans $\mathcal{O}$. De plus[13] $F(z) = {}^t(F_1(z),\ldots,F_N(z))$ est la fonction inconnue, et l'on a $F(z)\in\mathbb{C}^N$.

Prenons un exemple. L'équation hypergéométrique s'écrit sous la forme

$$z(1-z)\,F''(z) + (\lambda+\mu z)\,F'(z) + \nu F(z) = 0\,.$$

Pour avoir un système, on prendra F et F' comme inconnues. Si l'on divise par $z(1-z)$, on obtiendra comme coefficients deux fonctions rationnelles dont les pôles seront en 0 et 1.

Il n'y a, la plupart du temps, que des solutions locales à l'équation (3), mais pas de solutions définies dans tout X. Soit U un ouvert de $\mathbb{C}$ qui ne rencontre pas S, ou, ce qui revient au même, un ouvert de X. On note $\mathcal{S}(U)$ l'ensemble des fonctions $F : U\to\mathbb{C}^N$ qui vérifient l'équation différentielle donnée, autrement dit, l'ensemble des solutions dans U.

La famille des ensembles de solutions $\mathcal{S}(U)$ forme un *faisceau* : a) une solution dans un certain ouvert reste une solution dans un ouvert plus petit ; b) si l'ouvert U est obtenu en réunissant deux ouverts U' et U'', une solution dans U' et une solution dans U'' qui coïncident sur l'intersection de ces deux ouverts, se recollent pour former une solution sur l'ouvert U tout entier. (On peut toujours recoller deux fonctions holomorphes pour en faire une sur un domaine plus grand.)

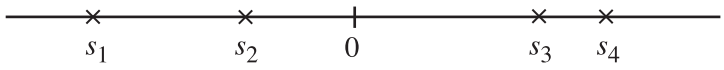
Ce faisceau est *localement constant* : si l'on se place en un point z_0 donné de X, et que l'on prenne un voisinage connexe U assez petit de z_0, on peut trouver, sur ce voisinage, N solutions linéairement indépendantes de telle sorte que la solution la plus générale sur U (ou sur un ouvert plus petit $V\subset U$) soit une combinaison linéaire de celles-ci à coefficients constants. (Localement, les fonctions qui appartiennent au faisceau sont décrites par N constantes.)

3.2 Monodromie des solutions

Pour simplifier l'exposé, et parce que cela se rencontre dans les exemples les plus courants, supposons l'ensemble S des singularités formé de nombres réels. On peut, dans ce cas, découper le plan complexe en trois morceaux :

[13] Les vecteurs dans $\mathbb{C}^N$ sont représentés par des matrices à N lignes et 1 colonne, transposées de la forme ${}^t u$, où u est une matrice à 1 ligne et N colonnes, explicitée en $(u_1,\ldots,u_N)$.

$\mathbb{C} = \mathbb{C}_+ \cup \mathbb{R} \cup \mathbb{C}_-$ ($\mathbb{C}_+$ ensemble des nombres complexes de partie imaginaire strictement positive, $\mathbb{R}$ ensemble des nombres réels, c'est-à-dire des nombres complexes de partie imaginaire nulle, et $\mathbb{C}_-$ ensemble des nombres complexes de partie imaginaire strictement négative).

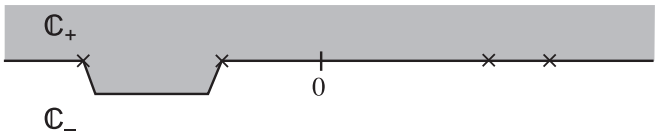


Les singularités supposées réelles sont représentées sur la figure par s_1, s_2, s_3, s_4.

Théorème 1. (Théorème général) *Si U est simplement connexe et si $z_0 \in U$, alors, pour tout $F_0 \in \mathbb{C}^N$, il existe une unique solution $F \in \mathcal{S}(U)$ avec $F(z_0) = F_0$.*

Du point de vue intuitif, "simplement connexe" veut dire "sans trou", le trou pouvant être réduit à un point. Plus formellement, cela signifie qu'étant donnés deux points de cet ouvert, on peut toujours aller par un chemin continu de l'un à l'autre de ces deux points (l'ouvert est connexe) et qu'une fois choisi un chemin allant de l'un à l'autre de ces deux points, n'importe quel autre chemin continu reliant ces deux points, aussi compliqué soit-il, peut se déformer continuement pour redonner le chemin choisi au départ. Si la frontière de l'ouvert se compose d'un nombre infini de courbes, seule la définition formelle convient.

Ce théorème s'applique à $U = \mathbb{C}_+$ ou $\mathbb{C}_-$. Mais comment relie-t-on ce qui se passe dans le demi-plan supérieur à ce qui se passe dans le demi-plan inférieur ? On montre que les solutions des équations traversent un peu la frontière : on peut légèrement déformer l'ouvert $\mathbb{C}_+$, de manière à rester toujours en dehors des singularités, mais à déborder vers le bas. Une telle déformation laisse l'ouvert simplement connexe.



D'après le théorème ci-dessus, si l'on a une solution dans un ouvert simplement connexe et que l'on peut agrandir cet ouvert simplement connexe en un ouvert un peu plus grand qui évite les singularités et reste simplement connexe, la solution se prolonge. Chaque solution F_+ du demi-plan supérieur se prolonge donc par continuité à l'axe réel à l'exception bien entendu des singularités. Les solutions F_- du demi-plan inférieur se prolongent avec les mêmes propriétés. On peut donc procéder au recollement[14], c'est-à-dire choisir un des intervalles I limités

[14] Rappelons un théorème classique de Schwarz qui affirme : si une fonction définie et continue sur un ouvert U de $\mathbb{C}$ est holomorphe dans $U \cap \mathbb{C}_+$ et $U \cap \mathbb{C}_-$, alors elle est holomorphe dans U.

par deux singularités et s'arranger pour faire se correspondre une solution F_+ du demi-plan supérieur et une solution F_- du demi-plan inférieur. On dira qu'elles se correspondent sur I si la valeur limite de F_+ sur la coupure supérieure de I coïncide avec la valeur limite de F_- sur la coupure inférieure de I. (Il suffirait en fait de le vérifier en un seul point.) On a ainsi établi une relation entre les solutions supérieures et les solutions inférieures.

Théorème 2. *Pour chaque intervalle I de $\mathbb{R}$ limité par deux singularités, il existe un isomorphisme $\alpha_I : \mathcal{S}(\mathbb{C}_+) \to \mathcal{S}(\mathbb{C}_-)$ unique tel que $F_+ \in \mathcal{S}(\mathbb{C}_+)$ et $F_- \in \mathcal{S}(\mathbb{C}_-)$ se correspondent par α_I si et seulement si F_+ et F_- ont même limite en tout point z_0 de I.*

Comment fabrique-t-on, à partir de là, le groupe de monodromie ? Choisissons un point base. La seule manière de raisonner correctement serait de prendre tous les points base à la fois et de raisonner directement, non pas en termes de groupes, mais de *groupoïdes*. Je ne le ferai pas ici et je prendrai un point base ; on me pardonnera ce péché originel.

Choisissons un point base $\zeta \in \mathbb{C}_+$. On sait (théorème 1) que, dans ce cas, on a un isomorphisme :

$$\mathcal{S}(\mathbb{C}_+) \approx \mathbb{C}^N .$$

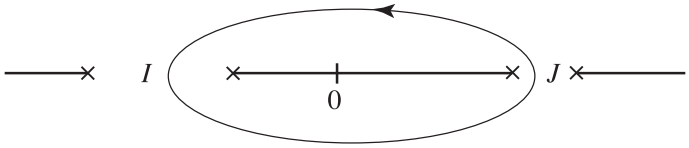
Pour le définir, à chaque solution F du demi-plan supérieur, on associe sa valeur $F(\zeta)$ au point particulier ζ. On va définir des automorphismes de cet espace de solutions $\mathcal{S}(\mathbb{C}_+)$ et puisque l'on en a choisi une base, cela se traduira par des matrices. On va, par ce biais, décrire de manière combinatoire le groupe fondamental $\pi_1(X;\zeta)$ de l'espace $X = \mathbb{C}\backslash S$ et fabriquer une représentation linéaire de ce groupe agissant dans $\mathbb{C}^N$.

Si I et J sont deux intervalles réels distincts dont les extrémités appartiennent à S, on va définir un automorphisme $\beta_{I,J}$ de l'espace $\mathcal{S}(\mathbb{C}_+)$, ou ce qui revient au même, d'après l'identification de $\mathcal{S}(\mathbb{C})$ à $\mathbb{C}^N$ au moyen du point base, une matrice. Le sous-groupe de $GL_N(\mathbb{C})$ engendré par ces matrices $\beta_{I,J}$ est *le groupe de monodromie de l'équation différentielle.*

Nous donnons deux constructions de $\beta_{I,J}$:

• Posons $\beta_{I,J} = \alpha_I^{-1}\,\alpha_J$; autrement dit, on part du demi-plan supérieur, on passe au demi-plan inférieur par la porte J, puis on revient au demi-plan supérieur par la porte I.

• Si l'on retire du plan complexe $\mathbb{C}$ privé de S la réunion des intervalles I (les composantes connexes de $\mathbb{R}\backslash S$), on a coupé le plan en deux demi-plans $\mathbb{C}_+$ et $\mathbb{C}_-$ sans point commun, chacun d'eux étant simplement connexe. Posons $\mathbb{C}(I) = \mathbb{C}_+ \cup I \cup \mathbb{C}_-$; c'est un ouvert simplement connexe de $\mathbb{C}$; si l'on rajoutait deux intervalles distincts I et J, l'ouvert obtenu serait encore connexe, mais non plus simplement connexe, car on aurait créé une possibilité de tourner autour des singularités dans cet ouvert.

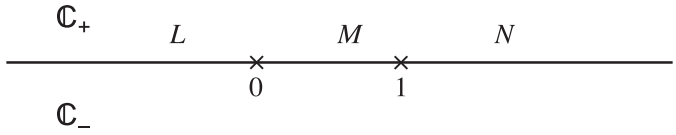


Toute solution $F \in \mathcal{S}(\mathbb{C}_+)$ se prolonge donc en une solution F_I de $\mathcal{S}(\mathbb{C}(I))$. Alors $\beta_{I,J}(F)$ est la solution G définie dans $\mathbb{C}_+$ telle que

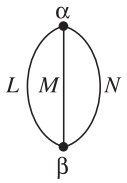
$$G_I = F_J \quad \text{sur} \quad \mathbb{C}_- \, .$$

Remarque 1. Cela s'adapte au cas où S n'est pas contenu dans $\mathbb{R}$, la géométrie est simplement un peu plus compliquée.

Explicitons le cas où S se compose de 0 et de 1 : on a trois intervalles, $]-\infty, 0[$, $]0, 1[$ et $]1, +\infty[$. Il y a donc trois portes et en fait trois points singuliers, le point à l'infini étant le troisième. Pour être bien comprises, ces choses doivent être vues sur la sphère de Riemann : en plus des points que l'on voit, il y a un point à l'infini. L'inversion $z \mapsto \frac{1}{z}$ change le point 0 en le point à l'infini et envoie 1 sur lui-même ; on peut donc traiter le point à l'infini à l'aide de cette transformation. (Ceci est possible parce que, quand on change z en $\frac{1}{z}$ dans une fonction rationnelle, on obtient encore une fonction rationnelle.) La situation est décrite par la figure :



Le squelette de cette situation est décrit par un graphe à deux sommets et trois arêtes. Quand on ne veut ouvrir qu'une porte, on ne considère qu'une seule arête. Mais, dans un tel graphe, il y a trois arbres maximaux, chacun d'eux contenant une arête et une seule. Ouvrir une porte revient à rendre la situation connexe, mais en la gardant simplement connexe. On peut prendre deux points α et β, α étant le ζ de tout à l'heure



et décrire un groupe de la façon suivante : on prend tous les chemins allant de α à α, mais comme tourner autour de α ne donne rien d'intéressant, on réalise un

tel chemin en passant un certain nombre de fois intermédiaires par β. A chaque passage intermédiaire de α vers β ou de β vers α, on a trois possibilités, trois branches possibles qui correspondent exactement aux intervalles I et J donnés précédemment. Le choix des points α et β permet de remplacer le groupoïde fondamental de l'espace X par un sous-groupoïde fini. Cette stratégie, qui consiste à prendre, non pas un point base, mais plusieurs, a été recommandée par Grothendieck et amplement utilisée par Deligne. L'avantage est que si l'on choisit les deux points, il y a une symétrie évidente dans la situation géométrique (passer à l'imaginaire conjugué) ; dans cette symétrie, on échange les deux points bases et donc on ne la perd pas.

Remarque 2. On a le choix d'un groupe fondamental associé à un point base, ou le choix de la situation égalitaire où l'on considère tous les chemins avec toutes les origines et toutes les extrémités finies. Dans ce deuxième cas, on a quelque chose de parfaitement démocratique, mais d'assez lourd ; par contre, dans le premier cas, on perd une grosse partie de l'information. On peut se placer dans des situations intermédiaires, c'est d'ailleurs comme cela que l'on a les renseignements les plus intéressants.

Remarque 3. J'ai choisi, non pas un point base, mais l'ouvert $\mathbb{C}_+$ ou l'ouvert $\mathbb{C}_-$; le choix de ζ à l'intérieur de $\mathbb{C}_+$ ou de $\mathbb{C}_-$ était totalement insignifiant, par contre, ce qui fait sens c'est le choix du demi-plan $\mathbb{C}_+$ ou du demi-plan $\mathbb{C}_-$. Sur la dernière figure, le sommet α ne représente pas un point particulier, mais tout le demi-plan supérieur et le point β tout le demi-plan inférieur. Cela marche parce que les deux demi-plans $\mathbb{C}_+$ et $\mathbb{C}_-$ sont simplement connexes et que l'on peut par conséquent utiliser le théorème 1 sur les équations différentielles. Voilà les secrets d'une stratégie dont Deligne a fait un très grand usage et dont nous avons appris à nous servir.

3.3 Groupe de Galois : cas de Fuchs

Ce cas est particulièrement facile à décrire. C'est celui où $A(z) = \sum_{i=1}^{n} \frac{A_i}{z-s_i}$, $A_1, \ldots, A_n$ étant des matrices dans $\mathbb{C}^{N\times N}$. Tous les points singuliers y compris l'infini correspondent à des pôles d'ordre 1. Nous verrons tout à l'heure une situation dans laquelle le point à l'infini compte et change les choses.

Définition. *Le groupe de Galois de l'équation différentielle est le plus petit sous-groupe algébrique*[15] *de $GL_N(\mathbb{C})$ contenant l'image de la représentation de monodromie de $\pi_1(X;\zeta)$.*

Le groupe $\pi_1(X;\zeta)$ est en général infini. C'est un groupe discret et dénombrable, mais ce n'est pas un groupe continu. Il peut être fini. Ce groupe a une représentation linéaire, car nous avons construit un homomorphisme de $\pi_1(X;\zeta)$ dans

[15] Un sous-groupe G du groupe $GL_N(\mathbb{C})$ de matrices est *algébrique* s'il existe des polynômes $P_1, \ldots, P_r$ à N^2 variables et coefficients complexes tels que l'élément $g = (g_{ij})$ de $GL_N(\mathbb{C})$ appartienne à G si et seulement si l'on a $P_1(\ldots g_{ij} \ldots) = \ldots = P_r(\ldots g_{ij} \ldots) = 0$.

$GL_N(\mathbb{C})$. Il y a donc une image : $\pi_1(X;\zeta)$ s'envoie sur un certain sous-groupe de $GL_N(\mathbb{C})$.

Il se peut que ce groupe image soit fini. Cela signifie que dans ce cas, les solutions de l'équation différentielle que nous considérons sont des fonctions algébriques. On peut alors faire le pont entre les deux théories de la monodromie selon Riemann. C'est d'ailleurs un problème que l'on a beaucoup étudié : *dans quels cas une fonction hypergéométrique peut-elle être une fonction algébrique.* Pour le savoir, on emploie des méthodes qui ont été recommandées par Riemann et développées en détail à la fin du dix-neuvième siècle par Halphen et Schwarz. Donc, si cette image est finie, cela signifie que les solutions de l'équation différentielle sont des fonctions algébriques et le groupe fini que l'on obtient permet de construire une surface de Riemann qui correspond à des fonctions algébriques.

Un sous-groupe fini est automatiquement un groupe algébrique, donc il n'y a rien à faire dans ce cas. Par contre, si le groupe est infini, puisque que n'importe quel groupe de matrices a une enveloppe algébrique, cela signifie que, parmi tous les groupes algébriques qui contiennent cette image, il y en a un plus petit que les autres. Comment le calcule-t-on ? On cherche toutes les relations polynomiales satisfaites par tous les éléments de l'image de $\pi_1(X;\zeta)$; cela donne un certain nombre d'équations, celles qui sont identiquement satisfaites par l'image de $\pi_1(X;\zeta)$. Puis on redescend, on cherche les solutions de ce système d'équations ; elles sont plus nombreuses que celles dont on était parti évidemment, et l'on construit comme cela l'enveloppe algébrique de l'image de $\pi_1(X;\zeta)$. C'est par définition le groupe de Galois de l'équation considérée, dans le cas de Fuchs.

Pourquoi l'appelle-t-on le groupe de Galois ? Parce que la définition que je viens de donner est un cas particulier de la définition de Picard et Vessiot. Picard et Vessiot ont démontré vers 1910 l'analogue du théorème de Galois. Le théorème de Galois dit qu'une équation algébrique est résoluble par radicaux si et seulement si son groupe de Galois est résoluble, d'où la terminologie. On dira qu'une équation différentielle est *résoluble par quadrature* si, partant des fonctions rationnelles (ou algébriques), prenant les fonctions dont la dérivée est une fonction rationnelle (par exemple la fonction logarithme), puis des combinaisons linéaires de telles fonctions, rajoutant à cela les primitives de toutes celles dont on dispose déjà, etc., la hiérarchie ainsi obtenue contient assez de fonctions pour trouver les solutions de l'équation. Dans le cas de Fuchs, le théorème de Picard et Vessiot dit, en particulier, que l'équation est résoluble par fonctions algébriques si et seulement si l'image de $\pi_1(X;\zeta)$ est finie, qu'elle est résoluble par fonctions algébriques et quadratures si et seulement si le groupe de Galois défini plus haut est résoluble. C'est pour cela qu'on s'est beaucoup intéressé à la théorie des groupes de Lie résolubles et des groupes de matrices résolubles.

3.4 Groupe de Galois : cas général

On voudrait aller plus loin que le cas de Fuchs, et définir en général le groupe de Galois.

Mise en garde : considérons l'équation différentielle $F' = F$ qui peut s'écrire $dF = F dz$. Il n'y a pas de singularités (la fonction constante égale à 1 n'a pas de pôle) donc, compte tenu des notations précédentes, on a $X = \mathbb{C}$. Comme $\mathbb{C}$ est simplement connexe, d'après le théorème général, on sait que cette équation a une solution holomorphe dans tout le plan. Cette solution est $F(z) = ce^z$. On peut maintenant se demander *si l'on est dans le cas de Fuchs. Non* : parce que si l'on change z en $\zeta = \frac{1}{z}$ pour ramener l'infini à 0, l'équation s'écrit $dF = -\frac{1}{\zeta^2} F d\zeta$, *il n'y a pas de singularité à distance finie et, à l'infini, il y a une singularité qui n'est pas du type de Fuchs,* car c'es un pôle d'ordre 2.

Une conséquence : l'équation différentielle $dF = -\frac{1}{\zeta^2} F d\zeta$ a comme solution $ce^{1/\zeta}$ et $e^{1/\zeta}$ est holomorphe en dehors de l'origine, mais elle a une singularité essentielle à l'origine. Si on la développe naïvement en série de puissances de $\frac{1}{\zeta}$, on a une infinité de termes, les termes en puissance de $\frac{1}{\zeta}$ correspondent à des pôles ; on a donc formellement un pôle d'ordre infini en $\zeta = 0$. Cette singularité ne se présente pas dans le cas de Fuchs.

Examinons rapidement la monodromie. L'équation différentielle $dF = F\,dz$ n'a pas de singularité pour z fini. Le cas où z est infini correspond, par le changement de variable $\zeta = \frac{1}{z}$, à l'équation

$$dF = F \cdot \left(-\frac{d\zeta}{\zeta^2} \right) . \tag{4}$$

La monodromie, dans le cas de Fuchs, associée à une singularité $z = a$ provient de la singularité du premier ordre

$$dF = \frac{F\,dz}{z - a}\, F + \dots \tag{5}$$

et au fait que l'intégrale de Cauchy $\int_\gamma \frac{A(z)\,dz}{z-a}$ pour un circuit γ autour de a donne une contribution, alors qu'une intégrale analogue avec $(z-a)^2$ au dénominateur est nulle. En conclusion, *l'équation $dF = F\,dz$ ne présente aucune monodromie.* Avec la définition précédente, le groupe de Galois est réduit à l'identité.

Comment peut-on corriger cela[16] ? En regardant de près, on s'aperçoit que *le groupe de Galois différentiel est un groupe de transformations sur les constantes d'intégration de l'équation.* Dans le cas de l'équation $dF = F\,dz$ d'ordre $N = 1$, la solution générale est $F(z) = ce^z$ avec une seule constante d'intégration c. Les transformations linéaires pour $N = 1$ sont de la forme $c \mapsto \lambda c$ avec λ complexe, $\lambda \neq 0$ (ce qu'on écrit $\lambda \in \mathbb{C}^\times$). Mais le groupe $\mathbb{C}^\times$ étant de dimension 1 comme

[16] Jean-Pierre Ramis et ses collaborateurs introduisent un groupe de ramification "sauvage" dans le cas "non Fuchs", et retrouvent le groupe de Galois comme enveloppe algébrique de la monodromie ordinaire et sauvage.

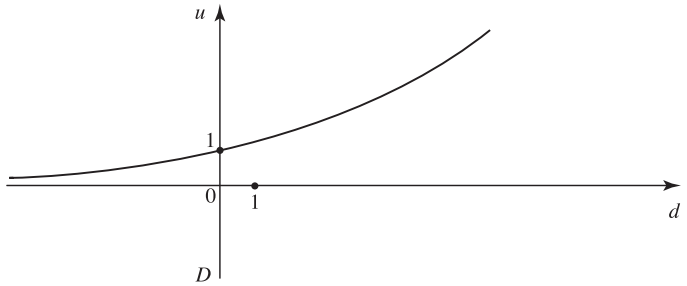
groupe de Lie complexe, tout sous-groupe algébrique de $\mathbb{C}^\times$ est fini ou égal à $\mathbb{C}^\times$ tout entier. Si le groupe de Galois associé à l'équation $dF = F\,dz$ était fini, cela signifierait que l'exponentielle est une fonction algébrique, et ceci est *faux*. La seule possibilité restante est donc $\mathbb{C}^\times$. Je ne vais pas prouver que le groupe de Galois est effectivement $\mathbb{C}^\times$, mais indiquer la philosophie sous-jacente.

Il y a une notion importante dans les équations différentielles, c'est celle de *résolvante*. Si l'on connaît la valeur F_0 de la solution de l'équation différentielle en un point z_0, et que l'on souhaite connaître cette solution en un autre point z, on sait que $F(z) = U(z, z_0)\,F_0$, la résolvante $U(z, z_0)$ étant un élément de $GL_N(\mathbb{C})$. C'est une matrice dépendant de deux variables complexes, toutes deux en dehors de S, et qui permet de résoudre les équations, d'où son nom de résolvante. De manière concrète, cette résolvante s'obtient en prenant une matrice à N lignes et N colonnes dont les colonnes forment un système linéairement indépendant de solutions de l'équation différentielle, ce que l'on appelle un *système fondamental de solutions*. Ce point de vue de la résolvante est commode ; la formule fondamentale est

$$U(z, z') \times U(z', z'') = U(z, z'')\,, \tag{6}$$

et l'on dit parfois que c'est la *loi des états intermédiaires* dans l'évolution : pour aller de z à z'', il faut être passé par z'. C'est là que le groupoïde montre son nez parce qu'un groupoïde c'est quelque chose qui dépend non pas d'un point, mais de deux points, et la formule (6) traduit une propriété du groupoïde. Donc le point essentiel est de calculer cette résolvante.

Dans le cas particulier de l'équation $dF = Fdz$, on montre facilement que la résolvante est : $U(z', z) = e^{z'-z}$. Posons $e^{z'-z} = u$ et regardons, dans l'espace à trois coordonnées, z, z' et u la surface R définie par cette équation. (Dans le cas d'un système d'équations, u serait une matrice dans $GL_N(\mathbb{C})$, z et z' seraient dans $\mathbb{C}$.) Il faut maintenant jouer le jeu des adhérences algébriques, non pas au niveau du groupe (ce qui voudrait dire l'on fixe z et z' et l'on regarde l'adhérence), mais en tenant compte du point de départ et du point d'arrivée. On doit regarder la surface d'équation $e^{z'-z} = u$ dans $G = \mathbb{C} \times \mathbb{C} \times \mathbb{C}^\times$ et prendre l'enveloppe algébrique de cela. Quelles sont les variétés algébriques en dimension 3 : l'espace tout entier, des surfaces, des courbes, des points. On a déjà une surface, donc les variétés contenant cette surface ne peuvent être que des surfaces ou l'espace tout entier. Regardons les surfaces. Autrement dit, cherchons s'il existe des polynômes P vérifiant $P(z, z', e^{z'-z}) = 0$. Prenons comme variables z, $z' - z$ et u, de manière à réduire les choses à deux variables, plaçons-nous dans le plan, supposons $u \neq 0$, autrement dit enlevons une droite du plan, et regardons la courbe d'équation $u = e^d$ (les deux variables sont u et d, j'ai posé $z' - z = d$) :



Cherchons l'adhérence algébrique de cette courbe. Qu'y a-t-il, dans le plan, comme variétés algébriques qui la contiennent ? Les seules variétés algébriques du plan sont : un ensemble fini de points, le plan tout entier ou une courbe algébrique. Cela ne peut pas être une courbe algébrique parce que la courbe exponentielle d'équation $u = e^d$ n'est pas algébrique. L'adhérence ne peut donc être que le plan tout entier, à l'exception bien entendu de la droite d'équation $u = 0$. Il est facile de voir, quand on repasse aux variables z, z', u précédentes, que l'on retrouve tout l'espace $\mathbb{C}\times\mathbb{C}\times\mathbb{C}^\times$ et que *le groupe de Galois est le groupe* $\mathbb{C}^\times$ *tout entier* (je simplifie un peu). C'est-à-dire que la liberté, l'ambiguïté porte sur la constante c. Les seules symétries possibles dans les solutions de l'équation différentielle sont de multiplier c par une constante. On a toute liberté et donc on trouve le groupe multiplicatif $\mathbb{C}^\times$ comme groupe de Galois.

Si l'on veut comparer ma présentation à celle de Fuchs, il faut tenir compte d'un point assez subtil. Revenons à la situation précédente, et à la courbe exponentielle $E : u = e^d$ dans le plan $\mathbb{C}^2$ à deux coordonnées complexes d, u. La résolvante ne doit pas s'annuler, il faut donc se restreindre au plan privé de la droite $u = 0$, c'est-à-dire le produit $\mathbb{C} \times \mathbb{C}^\times$. La courbe E est contenue dans $\mathbb{C} \times \mathbb{C}^\times$, elle n'est pas algébrique et la seule variété algébrique la contenant est $\bar{E} = \mathbb{C} \times \mathbb{C}^\times$; on dit que $\bar{E}$ est l'adhérence de Zariski de E. Pour obtenir un groupe, il faut se limiter au cas où $z = z' = z_0$ pour z_0 fixé ; cela correspond à la droite verticale $D : d = 0$. Notre stratégie est la suivante :

passer de E à son adhérence de Zariski $\bar{E}$ *puis* faire l'intersection avec D.

On a $D \subset \bar{E}$, donc le résultat final est la droite D formée des points $(0, u)$ avec $u \neq 0$: *le groupe de Galois est* $\mathbb{C}^\times$. Une stratégie à la Fuchs serait la suivante :

faire l'intersection de D avec E, d'où un seul point $(0, 1)$ dans $D \cap E$, *puis* prendre l'adhérence de Zariski.

Comme un point est un cas particulier de variété algébrique, le résultat final est le point $(0, 1)$ et *le groupe de Galois est réduit à* 1.

La différence provient de ce que les deux opérations effectuées ne sont pas permutables.

J'ai seulement pris cet exemple simple pour montrer la nécessité du groupoïde ; je dois dire qu'il est polémique. Quand j'ai présenté mes idées dans des séminaires de spécialistes : "définition du groupoïde de Galois d'une équation

différentielle : l'adhérence de Zariski du groupoïde fondamental", on m'a dit : "dans le cas de Fuchs, oui, mais cela ne marche pas dans les autres cas". Si, et d'une manière étonnamment simple. J'insiste parce qu'il est important de savoir prendre le bon degré de généralité. On dit souvent : les groupoïdes sont un luxe, ils ne sont pas beaucoup plus que des groupes, ne contiennent pas plus d'information, et sont juste commodes dans certains cas. Mais ce n'est pas vrai, et en voilà un exemple particulier. Avec la notion de groupoïde, on fabrique une théorie de Galois des équations différentielles, qui a toutes les propriétés que l'on peut en attendre. Une fois que l'on a le groupoïde, on peut retrouver le groupe, mais pour attraper le groupe, il faut passer par l'intermédiaire du groupoïde comme cet exemple le montre. J'ai démontré que cette théorie est équivalente à celle de Picard et Vessiot ; ce n'est pas très difficile de le prouver une fois que l'on est dans le bon cadre, et c'est même tautologique quand on s'y prend bien[17].

3.5 Indications sur la méthode tannakienne[18]

Pour calculer le groupe de Galois différentiel, j'ai donné l'impression que j'avais résolu l'équation. Naturellement, ce n'est pas ce que l'on veut faire, on veut d'abord obtenir le groupe de Galois différentiel, et ensuite s'en servir pour faire l'étude des solutions. La méthode tannakienne est une stratégie (introduite par Grothendieck) qui permet de calculer en principe le groupe de Galois connaissant l'équation, sans la résoudre. De même, j'ai parlé, pour la théorie de Galois ordinaire, de stratégies qui ont été transformées en logiciels et même en progiciels, et qui permettent, ayant l'équation, de détecter son groupe de Galois sans la résoudre numériquement. J'avais dit précédemment que le groupe de Galois comme groupe de permutations n'était défini qu'à conjugaison près. C'est la même chose ici, l'image de $\pi_1(X;\zeta)$ dans $GL_N(\mathbb{C})$ n'est définie qu'à conjugaison près.

La construction du groupe de Galois d'une équation différentielle s'appuie sur un théorème démontré par Maurer vers 1890, et ressuscité par Chevalley dans son premier livre sur les groupes algébriques (publié vers 1950). Ce théorème affirme qu'un groupe algébrique de matrices de type $N \times N$ est défini par la donnée d'un certain nombre de tenseurs T_α construits sur l'espace $V = \mathbb{C}^N$, le groupe se composant des transformations g de V qui laissent invariants les tenseurs T_α (ou, éventuellement, multiplient certains de ceux-ci par une constante). Par exemple, le groupe orthogonal laisse fixe une certaine forme quadratique de la forme $\sum_{\lambda,\mu} g_{\lambda\mu}\, v^\lambda\, v^\mu$, le groupe $GL_N(\mathbb{C})$ laisse fixe l'élément de volume $dz^1 \wedge \ldots \wedge dz^N$ à un scalaire près,...

[17] Signalons que B. Malgrange et H. Umemura ont développé des idées très analogues dans le cadre des *équations différentielles non linéaires*. Comme Picard et Vessiot, et leurs successeurs, je me suis limité aux équations différentielles linéaires.

[18] Tannaka est un mathématicien japonais qui a montré, vers 1935, comment reconstruire un groupe compact à partir de ses représentations linéaires.

Puisque le groupe de Galois d'une équation différentielle du type $dF = AF\,dz$ est par définition un groupe algébrique G, il convient de décrire les tenseurs sur l'espace $V = \mathbb{C}^N$ invariants par G. De l'équation différentielle agissant par construction sur les vecteurs de V, on définit naturellement une équation différentielle pour chaque type T de tenseurs. Les tenseurs invariants de type T par le groupe de Galois G sont par définition ceux qui sont constants en vertu de l'équation différentielle de type T. Par exemple, le groupe G sera contenu dans le groupe orthogonal associé à une forme quadratique $\sum_{\lambda,\mu} g_{\lambda\mu}\, v^\lambda\, v^\mu = q(v)$ si et seulement si, pour toute solution $F(z)$ de l'équation $dF = AF\,dz$, on a

$$d\left(\sum_{\lambda,\mu} g_{\lambda\mu}\, F^\lambda(z)\, F^\mu(z)\right) = 0\,.$$

C'est un critère effectif qui ne nécessite pas de résoudre l'équation, car il équivaut à $gA + {}^tAg = 0$, où g est la matrice symétrique $(g_{\lambda\mu})$ et ${}^tA$ la transposée de A.

Une *symétrie de l'équation différentielle* $dF = AF\,dz$ est une transformation linéaire $g : V \to V$ telle que $gA = Ag$. On peut l'interpréter comme un tenseur invariant dans $V \otimes V^*$, et par suite *toute symétrie de l'équation différentielle commute aux opérations du groupe de Galois* sur V. On a donc deux groupes commutant l'un à l'autre. Sophus Lie cherchait le groupe de Galois d'une équation différentielle ; il s'est trompé et a étudié le groupe des symétries de l'équation. D'ailleurs, plus le groupe de symétrie de l'équation est gros, plus l'équation est facile à résoudre, comme nous l'a appris Sophus Lie, alors que résoudre une équation, c'est forcer son groupe de Galois à être le plus petit possible (pour réduire l'ambiguïté). La relation de commutation mentionnée plus haut implique d'ailleurs que, plus le groupe de symétries est gros, plus le groupe de Galois est petit.

L'erreur de Sophus Lie a été féconde, puisqu'elle lui a permis de construire le magnifique édifice des groupes qui portent son nom.

3.6 Le groupe de Galois "cosmique"

Les méthodes de la théorie de Galois des équations différentielles s'appliquent aux fonctions élémentaires, telles que le logarithme et l'exponentielle. Depuis une vingtaine d'années, une nouvelle classe de fonctions est sortie du ghetto où elle végétait : les *polylogarithmes*. Pour tout entier $k = 0, 1, 2, \ldots$ posons

$$Li_k(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^k}\,,$$

la série étant convergente pour $|z| < 1$. Les premières valeurs sont

$$Li_0(z) = \sum_{n=1}^{\infty} z^n = \frac{z}{1-z}\,,$$

$$Li_1(z) = \sum_{n=1}^{\infty} \frac{z^n}{n} = \log\left(\frac{1}{1-z}\right) .$$

La fonction $Li_2(z) = \sum_{n=1}^{\infty} z^n/n^2$ est connue sous le nom de *dilogarithme* et a été introduite par Euler vers 1735. Euler s'en est servi pour calculer la somme de la série $\sum_{n=1}^{\infty} \frac{1}{n^2}$, égale par définition à $Li_2(1)$, et a trouvé la valeur $\pi^2/6$ (résolvant ainsi ce qui était connu sous le nom de *problème de Bâle*). Plus généralement, on a

$$Li_k(1) = \sum_{n=1}^{\infty} \frac{1}{n^k} = \zeta(k) ,$$

où ζ est la fonction célèbre de Riemann. Ceci explique l'intérêt (assez récent) porté par les arithméticiens à ces fonctions.

L'équation différentielle s'établit immédiatement

$$dLi_k(z) = Li_{k-1}(z)\,\frac{dz}{z} \qquad \text{pour } k \geq 1 .$$

Les fonctions $Li_k(z)$ s'obtiennent donc par itération de primitives, et on en déduit facilement un prolongement analytique au plan coupé le long de la demi-droite $[1, +\infty[$. Le groupe de Galois différentiel se calcule très facilement, ainsi que la monodromie, et l'on peut facilement construire la surface de Riemann sur laquelle toutes les fonctions $Li_k(z)$ deviennent uniformes (généralisant le cas du logarithme).

Sans être plus précis, disons qu'*un nombre spécial est une valeur spéciale d'une fonction spéciale.* Par exemple, $Li_2(z)$ est une fonction spéciale dont $\zeta(2)$, obtenu en faisant $z = 1$, est une valeur spéciale. Sous le vocable de "périodes", Kontsevich et Zagier ont défini une classe de nombres, qui répondent certainement au nom de nombres spéciaux. Les périodes possèdent des groupes de symétrie, dont l'origine est liée aux groupes de Galois différentiels. Il y a là l'ébauche d'une théorie de Galois des nombres transcendants, alors que la théorie de Galois usuelle ne considère que les nombres algébriques. On attend d'une telle théorie de nouveaux théorèmes de transcendance : par exemple, on sait depuis 1979 (Apéry) que $\zeta(3)$ est irrationnel ; on espère prouver que $\zeta(3)$, $\zeta(5)$, $\zeta(7)$, ... sont des nombres transcendants.

Changeons complètement de registre. La théorie des particules élémentaires est dominée par les diagrammes que Feynman a introduits vers 1950, et dont chacun code une intégrale multiple compliquée. Toute une technologie s'est développée, permettant par exemple d'intégrer numériquement une fonction de 24 variables, à la précision du millième. Un des champions est Broadhurst, qui a beaucoup étudié les constantes nouvelles que l'on trouve dans ces calculs, et qu'on désigne sous le nom de "multizetas", car elles généralisent les nombres zeta $\zeta(k) = \sum_{n=1}^{\infty} 1/n^k$. Tout ceci est du travail numérique expérimental, peu de choses sont démontrées, et c'est là le défi. Mais Broadhurst sait calculer avec

20000 décimales, et détecter des relations linéaires grâce à des algorithmes très performants. Même si une relation n'est pas démontrée, qui en doutera si elle est satisfaite avec 20000 décimales ?

Du point de vue mathématique, la théorie des *motifs*, entrevue par Grothendieck vers 1960, et maintenant établie (depuis 2000) sur des bases solides, définit des *groupes de Galois motiviques*, qui fournissent des symétries sur ces constantes mathématiques multizeta. Du point de vue physique, le "modèle standard" des particules élémentaires laisse inexpliquées les masses des quarks par exemple, et les constantes de couplage. Il y a là 20 à 30 constantes, que l'on mesure expérimentalement, mais dont on n'a aucune explication. Sur le modèle du groupe de Galois motivique, j'ai donc imaginé un *groupe de Galois cosmique*, qui agirait sur les constantes fondamentales[19]. Il s'agirait de symétries d'un type très différent des symétries géométriques de l'espace-temps, ou des symétries de jauge (elles-mêmes géométrisées grâce aux notions d'espaces fibrés). Pour l'instant, il ne s'agit que d'un nom, mais les résultats récents d'Alain Connes et Mathilde Marcolli donnent une première assise solide à des spéculations bien hardies.

[19] Ou plutôt, sur les expressions nommées *lagrangiens*, où entrent ces constantes, et dont la donnée décrit sans ambiguïté le modèle physique.