AUTOUR DU PROBLEME INVERSE DE GALOIS

Pierre Dèbes

- Le but de l'exposé est de présenter un panorama du problème inverse de la théorie de Galois.

- La question a le mérite d'être simple à poser: un groupe fini G étant donné, peut-on trouver une équation polynômiale à coefficients dans le corps **Q** des rationnels dont le groupe de Galois soit le groupe G, ou, de façon équivalente, une extension galoisienne de **Q** de groupe G ?

Gal. Inv. : *pour tout groupe fini* G*, a-t-on* G = Gal(E/**Q**) ?

- C'est une question naturelle. Quand on apprend la théorie de Galois et que l'on regarde les permutations des racines qui sont autorisées, on en vient forcément à se demander si le groupe qu'elles constituent peut être n'importe quel groupe *a priori*. Ce serait satisfaisant: la théorie des groupes, née de la théorie des équations, serait juste la théorie qu'il faut.

- Mais la théorie des groupes est aujourd'hui omniprésente et on peut penser inversement que c'est elle qui est le domaine universel et que la théorie des équations en est un de ses champs d'application.

- En tout cas la réponse est incertaine, même conjecturalement: la théorie inverse de Galois est un domaine où les énoncés principaux s'appellent ``problèmes'', que l'on ne se hasarde pas à transformer en ``conjectures''. Comme nous allons voir, cette incertitude demeure: les problèmes principaux restent non résolus.

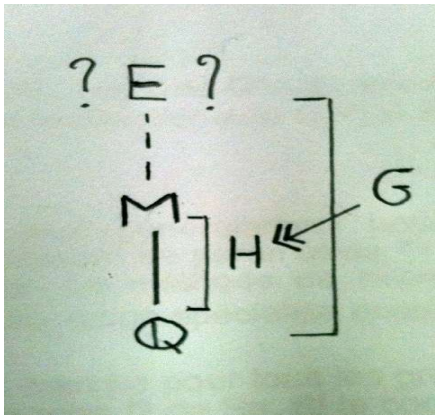
- Pour faire un premier point rapide, on peut dire qu'il y a un certain nombre de groupes pour lesquels la réponse est positive. D'abord les groupes abéliens, qu'il est facile de réaliser à partir d'extensions cyclotomiques. Le cas des groupes résolubles est beaucoup plus difficile; c'est un des résultats les plus profonds du domaine:

Théorème (Shafarevitch 1954): **Gal. Inv.** *vrai pour* G *résoluble*.

- Il s'agit d'empiler des extensions abéliennes de façon que l'ensemble soit galoisien et corresponde à un dévissage abélien du groupe résoluble donné. Plus précisément, il faut résoudre une succession de problèmes de plongement à noyau abélien.

- Problème de plongement:

  Etant donnés une extension galoisienne M/**Q** de groupe H et un épimorphisme de G dans H, existe-t-il une extension galoisienne E/**Q** de groupe G telle que la surjection de Gal(E/**Q**) sur H=Gal(M/**Q**) fournie par la théorie de Galois corresponde à l'épimorphisme donné? Le problème est dit scindé si l'épimorphisme G —> H a une section et on appelle noyau du problème celui de ce morphisme.



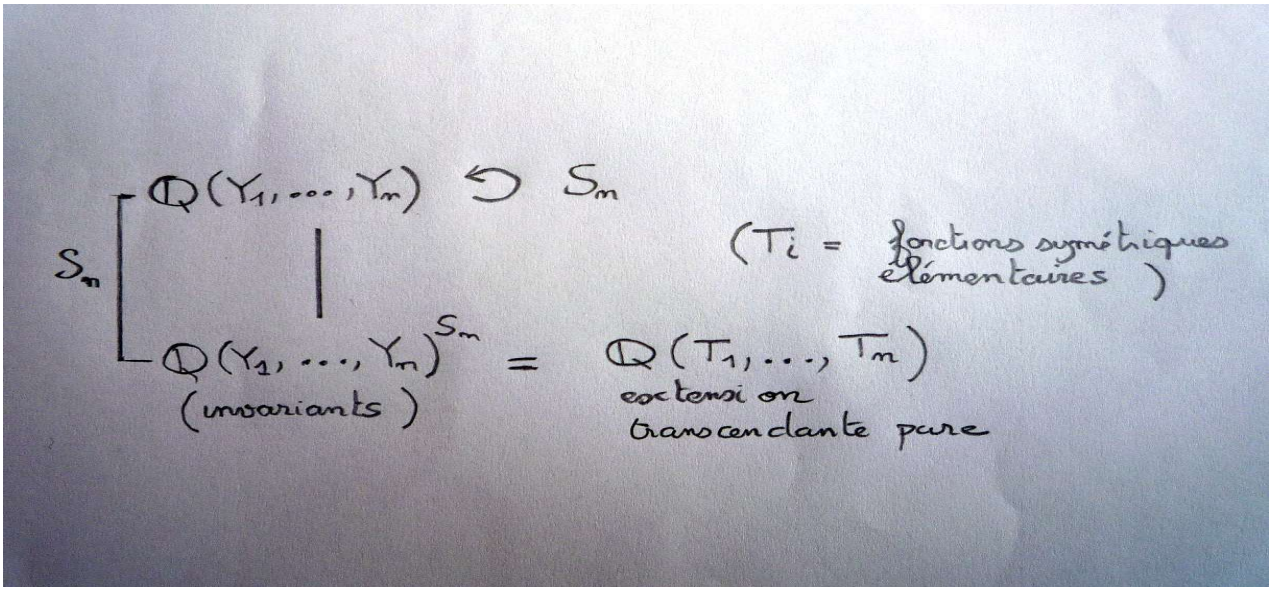
- La difficulté du théorème de Shafarevitch est inextricable. A tel point que la preuve, incomplète dans sa première version, a été réparée plusieurs fois, notamment par Ishanov, mais contestée plusieurs fois aussi. Il faudra attendre 45 ans et le livre de Neukirch-Schmidt-Wingberg pour avoir une preuve admise par la communauté.

- On sait aussi réaliser le groupe symétrique Sn, le groupe alterné An, ainsi qu'un certain nombre de groupes simples. Pour les familles classiques telles que PSLn(q), PSUn(q), on sait le faire en gros quand q=p^f est petit par rapport à n. Mais par exemple, la question reste ouverte pour PSL2(5^f) si f>2, PSL2(3^f) si f>3, PSL3(3^f) si f>2, PSL4 (2^f) si f>1. On sait en revanche réaliser tous les 26 groupes simples sporadiques sauf un: ne manque que le groupe de Mathieu M23. Pour des résultats plus complets, je renvoie au livre de Malle et Matzat ainsi qu'aux tables de Klueners et Malle.

- Après ce premier coup d'oeil, revenons à l'histoire. Je la ferai commencer à **Hilbert** qui traite le cas du groupe symétrique Sn dans un article de 1892. La méthode est classique et reste instructive. On commence par montrer que

Le polynôme générique P = Y^n + T1 Y^{n-1} + ... + Tn dont les coefficients T1,...,Tn sont des indéterminées a pour groupe de Galois Sn sur le corps **Q**(T1,...,Tn).

E. Noether présenterait les choses différemment. Elle dirait, et dira, 25 ans plus tard (dans un article de 1918, et un autre de 1913 dans lequel ses idées apparaissent déjà): on fait agir Sn sur un corps **Q**(Y1,...,Yn) engendré par n indéterminées. Le corps des invariants est le corps **Q**(Y1,...,Yn) engendré par les fonctions symétriques élémentaires des éléments Y1,...,Yn. C'est une extension transcendante pure et l'extension associée est galoisienne de groupe Sn.

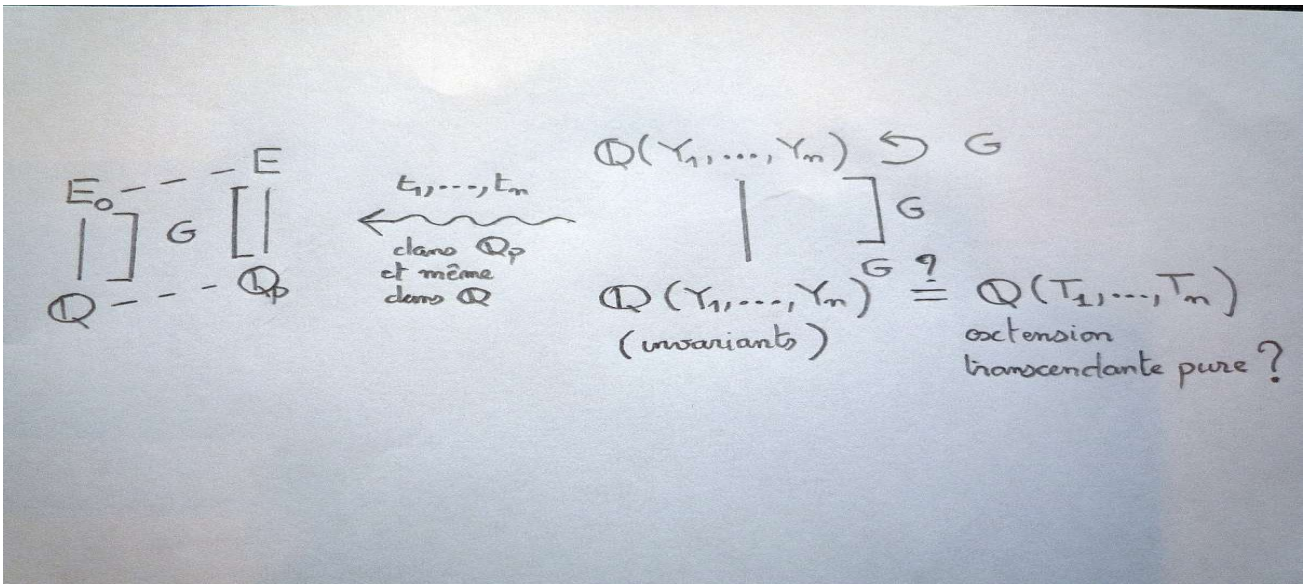


Le résultat suivant est la contribution majeure de Hilbert:

Théorème d'irréductibilité de Hilbert: *pour ``beaucoup'' de (t1,...,tn) dans* **Q**^n *(précisément, dans un sous-ensemble Zariski dense), le polynôme* P(t1,...,tn) *est irréductible dans* **Q**[Y] *et a* Sn *pour groupe de Galois*.

- Le théorème d'irréductibilité de Hilbert, qui est vrai plus généralement pour tout polynôme en Y dont les coefficients dépendent rationnellement de paramètres T1,...,Tn algébriquement indépendants, est un résultat fondateur. La méthode de Hilbert est toujours utilisée: on construit des familles de polynômes, qu'on spécialise ensuite.

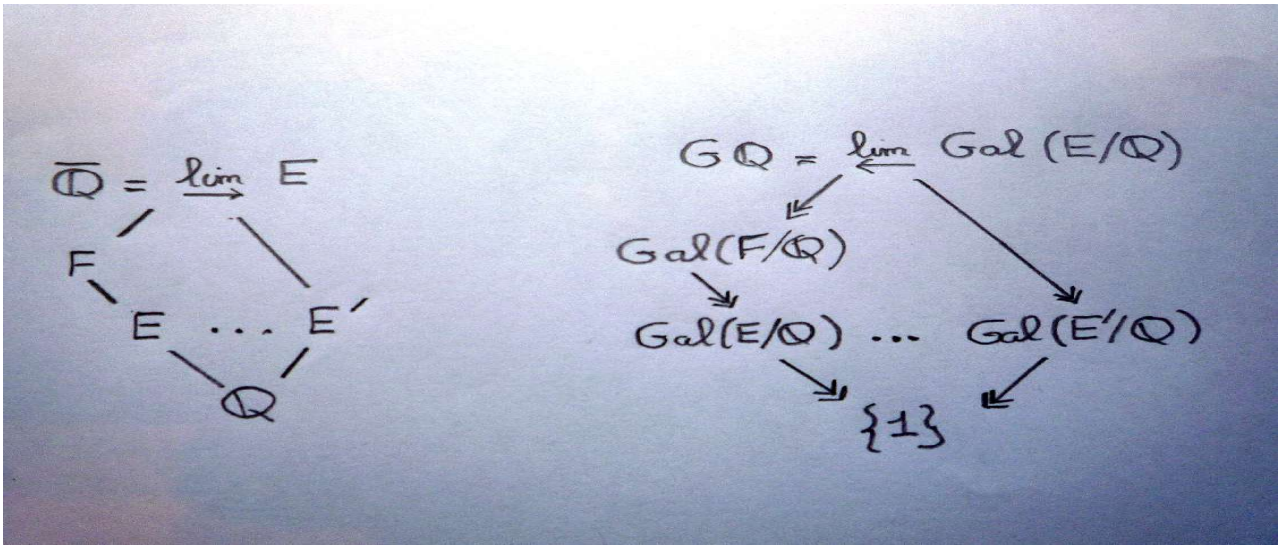
- Noether introduit la possibilité que la méthode de Hilbert marche pour tous les groupes: le groupe Sn peut en effet être remplacé par tout sous-groupe G de Sn. **Si** le corps des invariants **Q**(Y1,...,Yn)^G est une extension transcendante pure **Q**(T1,...,Tn), on peut comme ci-dessus spécialiser l'extension (galoisienne de groupe G) **Q**(Y1,...,Yn)/ **Q**(Y1,...,Yn)^G (ci-dessous à droite) grâce au théorème de Hilbert, et obtenir ainsi une extension de **Q** de groupe G.



- Mais il est faux en général que **Q**(Y1,...,Yn)^G soit une extension transcendante pure. Cela sera montré par Swan en 1969 et Voskressenski en 1970; le problème sera également étudié en détail par Lenstra en 1974. Comme l'a remarqué Saltmann en 1984, il y a une raison somme toute assez simple pour laquelle le programme de Noether ne peut pas marcher en général. Comme indiqué ci-dessus à gauche, dans le cas favorable où le corps des invariants est une extension transcendante pure, toute extension galoisienne de **Q**p de groupe G serait spécialisation de l'extension de Noether en un n-uplet (t1,,...,tn) à composantes dans **Q**p (un fait appelé ``propriété verselle'' qui correspond ici au théorème de la base normale de Noether). Mais grâce à l'hypothèse, le n-uplet (t1,,...,tn) pourrait en fait être choisi à composantes dans **Q**. L'extension de **Q** correspondante serait une extension galoisienne de groupe G induisant l'extension initiale de **Q**p. Or il est faux en général qu'une extension galoisienne de **Q**p provienne d'une extension galoisienne de **Q** de même groupe. Il y a un contre-exemple dû à Wang pour p=2 et G=**Z**/8**Z**. Cet exemple est fameux car il avait été initialement donné en 1948 pour infirmer un théorème ``démontré'' 15 ans plus tôt par Grunwald (l'énoncé de Grunwald reste cependant correct en dehors des cas mis en évidence par Wang).

- En tout cas, le programme de Noether, qui fournissait une théorie inverse de Galois rêvée, tombe à l'eau. Il reste cependant un problème intéressant. On continue d'étudier dans quels cas le corps des invariants **Q**(Y1,...,Yn)^G est une extension transcendante pure. Cela a ouvert de nombreuses voies de recherche, conduisant par exemple à la notion d'extension générique (une extension galoisienne d'une extension transcendante pure qui ait la propriété verselle ci-dessus). L'extension de Noether est aussi le prototype de ce qu'on appelle aujourd'hui G-torseur, une notion qui occupe une place centrale en théorie de Galois (géométrique).

- L'utilisation du **groupe de Galois absolu** G**Q** = Gal(**Q**alg/**Q**) est une autre étape importante pour le problème, pour sa présentation et son évolution historique. La clôture séparable de **Q** (ou plus généralement d'un corps k) s'obtenant comme réunion (ou limite inductive) d'extensions galoisiennes finies, le groupe Gal(**Q**alg/**Q**) s'écrit comme limite projective de groupes finis.



- Le groupe de Galois absolu Gk d'un corps k est l'archétype de groupe profini. L*es* deux théories se sont développées à partir des années 50, s'enrichissant mutuellement, sous l'influence de mathématiciens comme Krull, Melnikov, Nielsen, Schreier, Serre, Ershov, Fried, Jarden, Herfort, Ribes, Zalesski, Lubotzky, van den Dries, etc.

- Pourquoi le groupe G**Q** est-il important? D'abord, il permet de reformuler la question de départ comme celle de la recherche des quotients finis de G**Q**. Cela lui donne plus de substance. La question s'étend d'elle-même, pour devenir:

Qu'est ce que ce groupe G**Q** ?

Le problème inverse devient un problème direct. Ce problème s'inscrit dans un contexte encore plus large: l'étude du foncteur

k corps |——> groupe profini Gk

et de façon plus générale encore, celle du foncteur

S schéma |——> groupe fondamental π1(S)

puisque

Gk = π1(Spec k)

- Ce point du vue se développera dans les années 70, sous l'impulsion notamment de Grothendieck, et sera poursuivi par la suite par beaucoup d'autres. Notre problème est maintenant inscrit dans une problématique d'envergure.

- Le groupe de Galois absolu Gk peut être déterminé dans plusieurs situations classiques: c'est le groupe trivial pour k=**C**, le groupe **Z**/2**Z** pour k=**R**, le groupe profini **Z**^ (complétion profinie de **Z**) pour k=**F**q, etc.

- Pour k=**Q**, la question reste mystérieuse. Il y a une conjecture de Shafarevitch pour k égal à la clôture abélienne **Q**ab de **Q**:

Conjecture de Shafarevitch: *le groupe de Galois absolu* G**Q**ab *est isomorphe au groupe profini libre à un nombre dénombrable de générateurs*.

Ce qui, via un théorème d'Iwazawa, revient à dire que tout problème de plongement sur **Q**ab est résoluble. Comme **Q**ab est de dimension cohomologique ≤ 1, il suffirait de montrer que tout problème de plongement scindé (cf. p.2) sur **Q**ab est résoluble. Il existe une ``super-conjecture'' qui affirme que ce dernier énoncé serait vrai sur **Q** lui-même:

Super-conjecture: *tout problème de plongement scindé sur* **Q** *est résoluble*.

L'intérêt de cette super-conjecture est qu'elle contient la conjecture de Shafarevitch et le problème inverse de Galois. D'après un résultat classique d'Ikeda de 1960, cette super-conjecture est vraie pour des problèmes de plongement à noyau abélien.

- Sans surprise déterminer G**Q** est un problème difficile. On est reconduit vers le problème **Gal Inv** qui constitue une première étape.

- J'en arrive à l'idée centrale de l'approche d'aujourd'hui dont je daterai l'apparition autour des années 60-70 et qui continue de se développer aujourd'hui:

Revêtements de la droite projective P1

- L'idée est de construire
  > des extensions E/k(T), ce qu'on peut voir comme
  > des polynômes P(T,Y) dans k(T)[Y], ce qu'on peut voir encore comme
  > des revêtements algébrique (ramifiés) f: X –> **P**1.

L'avantage du dernier point de vue est que pour un corps k de caractéristique 0, plongé dans **C**, on dispose de la théorie topologique des revêtements, et en particulier des outils de topologie algébrique que sont le groupe fondamental et la monodromie.

- Partant d'une extension E/k(T) ou d'un polynôme P(T,Y), on peut lui associer un revêtement f: X –> **P**1: celui dont un modèle affine est la première projection (t,y) –> t de la courbe d'équation P(t,y)=0 vers la droite affine; c'est aussi celui dont l'extension de corps de fonctions est isomorphe à E/k(T). Dans ce contexte, il y a un résultat fondateur, dû à Riemann et Hurwitz, qui concerne la correspondance inverse: le théorème d'existence de Riemann.

- **Théorème d'existence de Riemann**

(a) *Les revêtements topologiques finis (non ramifiés) de* **P**1(**C**) \ **t** *(sphère de Riemann privée d'un ensemble fini* **t** *de points) sont algébriques, c'est-à-dire, proviennent d'une extension* E/**C**(T) *ou d'un polynôme* P(T,Y) *dans* **C**(T)[Y], *comme rappelé ci-dessus*.
(b) *En conséquence, le problème inverse de Galois est vrai sur le corps* **C**(T).

- Le (b) se déduit du (a) grâce aux deux faits suivants:
  - construire un revêtement topologique galoisien de groupe d'automorphismes un groupe donné G ne pose pas de difficultés: les groupes d'automorphismes de revêtements de **P**1(**C**) \ **t** sont les quotients du groupe fondamental topologique de **P**1(**C**) \ **t**, lequel est isomorphe au groupe libre à r-1 générateurs où r= card(**t**) ; il suffit donc de prendre r assez grand,
  - le groupe d'automorphismes d'un revêtement galoisien correspond au groupe de Galois de l'extension associée E/**C**(T) des corps de fonctions.

- La preuve du (a) utilise essentiellement des outils d'analyse complexe: surfaces de Riemann, monodromie. Un point crucial est que le corps des fonctions méromorphes sur **P**1(**C**) est le corps **C**(T) des fractions rationnelles à coefficients dans **C**.

- Du résultat sur k=**C**, on déduit celui sur k= **Q**alg, et à partir de là, le problème devient un problème de descente, sur **Q**. La majorité des travaux se concentrent désormais sur la forme régulière du problème inverse de Galois:

Gal. Inv. Rég. : *pour G groupe fini, a-t-on*
- G = Gal(E/**Q**(T)) *avec* E/**Q** *régulière, ou de façon équivalente*
- G = Aut(f:X –>**P**^1) *avec* f : X –>**P**^1 *Galois défini sur* **Q** ?

- La condition de régularité, qui est que **Q** soit algébriquement fermé dans E (c'est-à-dire, l'intersection de E et **Q**alg vaut **Q**) assure que le groupe de Galois est le même au-dessus de **Q**(T), qu'au-dessus de **C**(T), et donc est le même à la fin de la descente (quand elle est possible) qu'au début de la descente.

- L'énoncé **Gal. Inv. Rég.** a l'autre avantage par rapport à **Gal. Inv.** qu'il est plausible pour tout corps k: c'est un énoncé géométrique.

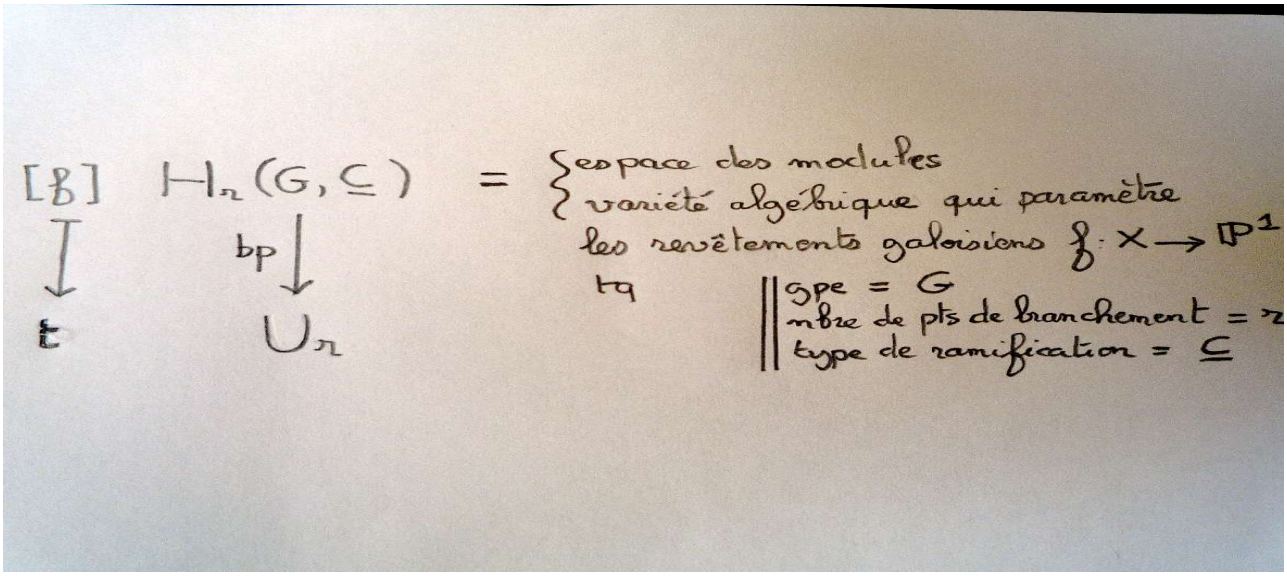
- Le théorème d'irréductibilité de Hilbert fournit l'implication

Gal. Inv. Rég. pour G sur **Q** ==> **Gal. Inv.** pour G (sur **Q**)

- le problème se scinde ensuite en plusieurs directions qui correspondent à 3 grandes idées de ces 40 dernières années.

1/3 *Rigidité et espaces de Hurwitz*

- les espaces de Hurwitz sont les espaces de modules Hr(G,C) de revêtements (galoisiens) de groupe G, dont on fixe le nombre r ≥ 3 de points de branchement et un certain invariant C lié au type de ramification.
  (Plus précisément, C est l'ensemble {C1,...,Cr} des classes de conjugaison dans G de certains générateurs distingués des groupes d'inertie associés aux point de branchement t1,...,tr; ces groupes sont cycliques et conjugués et leurs ordres sont les indices de ramification correspondants).



Les espaces de Hurwitz sont des variétés algébriques (non irréductibles en général) dont les points paramètrent les revêtements indiqués ci-dessus. L'application bp: Hr (G,C) —> Ur ci-dessus est celle qui envoie le point [f] représentant la classe d'isomorphisme du revêtement f:X—>**P**^1 sur l'ensemble de ses points de branchement. L'ensemble Ur est la variété qui paramètre les ensembles de r points distincts dans **P**^1.

- Les espaces de Hurwitz sont définis sur des corps cyclotomiques bien compris, qui sont le corps **Q** dans les bons cas. De plus, le corps de rationalité d'un point [f] sur Hr (G,C) correspond au ``corps des modules'' du revêtement f, lequel, dans de nombreuses circonstances, est le plus petit corps de définition de f. Via les espaces de Hurwitz, le problème **Gal.Inv.Rég.** — trouver des revêtements définis sur **Q** — est ramené à celui de la recherche de points **Q**-rationnels sur la variété Hr(G,C).

Problème: *pour* G *donné, trouver* (r,C) *tel que* Hr(G,C)(**Q**) *soit non vide*.

- Notre connaissance des espaces de Hurwitz est parfois suffisante pour résoudre positivement ce problème. Là encore, le théorème d'existence de Riemann est la clé: l'idée est que la géométrie des espaces de Hurwitz, et dans une certaine mesure leur arithmétique, sont contraints, et même déterminés dans certains cas, par leur structure topologique. L'outil central est l'application bp: Hr(G,C) —> Ur qui est un revêtement algébrique fini non ramifié.

  o exemple 1: pour certaines données (r,G,C) dites **rigides**, Hr(G,C) est irréductible et le revêtement Hr(G,C) —> Ur est de degré n(r,G,C)=1 et défini sur **Q**. Les revêtements sont alors déterminés par leurs points de branchement; l'espace de Hurwitz Hr(G,C) est birationnel sur **Q** à l'espace projectif **P**^r. La question a alors une réponse positive, et donc aussi celle de la réalisation du groupe G. Cette méthode est apparue dans les années 70, dans des travaux indépendants de Thompson, Fried, Matzat, et popularisée par Thompson qui a réalisé de cette façon le plus gros groupe simple sporadique, le Monstre, avec r=3 points de branchement seulement.

- Le degré n(r,G,C) du revêtement bp: Hr(G,C) —> Ur peut être calculé en général: c'est le degré du revêtement topologique associé et son calcul est une question de pure théorie des groupes. La méthode peut être tentée de façon systématique pour tout groupe donné. Obtenir n(r,G,C) = 1 tient cependant du miracle.

  o exemple 2: On peut assouplir la condition de rigidité ``n(r,G,C) = 1''. Pour cela on peut essayer de construire, grâce à des sections hyperplanes de l'espace Hr(G,C), des courbes de genre 0, possédant de plus un point **Q**-rationnel (qu'on trouve en général ``à l'infini'' en examinant la ramification du revêtement bp: Hr(G,C) —> Ur). Une telle courbe est alors birationnelle à **P**1 sur **Q**, et on peut à nouveau conclure que Hr(G,C)(**Q**) est non vide. Ici aussi la nature topologique de la notion de genre et des espaces de Hurwitz permet de se ramener à des calculs de pure théorie des groupes. Ces calculs peuvent être compliqués, au point parfois de recourir à un ordinateur. Cette méthode est due à Fried et a été développée par Matzat qui l'a utilisée pour réaliser de nombreux groupes simples.

- Le problème de cette approche est qu'en dehors des cas ``chanceux'', on ne sait pas trop comment trouver des points **Q**-rationnels sur les espaces de Hurwitz. On en connait d'ailleurs qui n'en possèdent pas: c'est ainsi le cas si

(*) G=D_{2p^m} *le groupe diédral d'ordre* 2p^m, p>11 *premier*, m ≥ 1, r ≤ 4 *et* C *arbitraire*.

On conjecture que c'est aussi le cas plus généralement avec r ≤ r0 à la place de r ≤ 4 où r0>0 est un entier quelconque, quitte à remplacer ``p premier > 11'' par ``p premier assez grand'' (en fonction de r0). Avec un nombre limité de points de branchement, on ne pourrait ainsi réaliser qu'un nombre fini de groupes diédraux (alors que 3 suffisent

pour le Monstre). Cela contredit l'intuition naive qu'il existerait une réalisation ``universelle'' pour tous les groupes diédraux D_{2p^m} (avec p fixé). L'exemple (*) est lié au fait que sur la tour des courbes modulaires Y^1(p^m), les points **Q**-rationnels disparaissent au delà d'un certain niveau m. Sa généralisation conjecturale découlerait de la ``conjecture de torsion forte'' sur les points de torsion d'une variété abélienne — sur un corps de nombres et pour une dimension donnée, une variété abélienne n'a qu'un nombre fini de points de torsion rationnels —. Le problème diophantien de trouver des points **Q**-rationnels sur des espaces de Hurwitz est donc assez subtil.

2/3 *Recollement et déformation*

- Ces techniques ont permis des avancées importantes pour le problème **Gal.Inv.Rég.** dans le cas où le corps de base k est un corps valué complet (au lieu d'être le corps **Q** dans sa forme initiale). Par exemple, on peut prendre pour k le corps **Q**_p des nombres p-adiques ou le corps **Q**((x)) des séries de Laurent formelles à coefficients dans **Q**. Le pionnier dans cette direction est Harbater, à qui on doit le résultat:

Théorème: *Le problème* **Gal.Inv.Rég.** *a une réponse positive si* k *est un corps valué complet. C'est-à-dire, pour* G *groupe fini, on a* G = Gal(E/k(T)) *avec* E/k *régulière, ou de façon équivalente*, G = Aut(f:X –>**P**^1) *avec* f : X –>**P**^1 *Galois défini sur* k**.**

- La méthode en fait véritablement, au même titre que le théorème d'existence de Riemann, un résultat de théorie inverse de Galois: un énoncé plus précis permet, à partir de revêtements galoisiens élémentaires définis sur k (par exemple des revêtements cycliques), de construire un revêtement galoisien défini sur le même corps k et de groupe engendré par les groupes des revêtements élémentaires (supposés plongés au départ dans un groupe commun). C'est une démarche constructive.

- Il y a maintenant plusieurs variantes de la preuve:

  - à base de recollements d'espaces analytiques rigides (au sens de Tate) ou formels (au sens de Grothendieck),

  - à base de déformations: on construit à la main un revêtement d'une courbe singulière (une chaine connexe de plusieurs **P**^1): en gros on réalise un assemblage de revêtements élémentaires. On déforme ensuite ce revêtement singulier en un revêtement lisse d'un seul **P**^1.

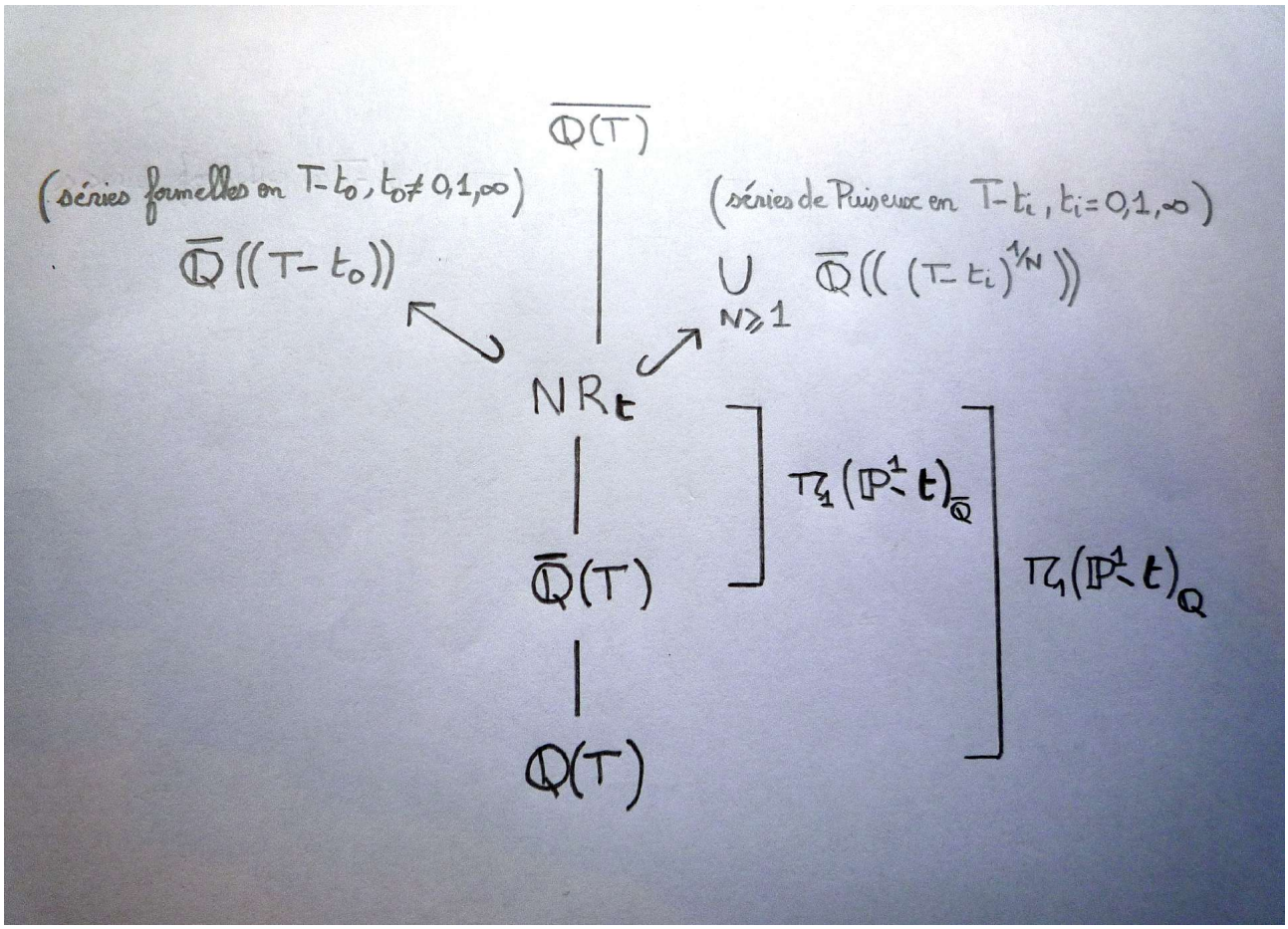
    Il faut dans les deux cas des résultats qui garantissent que le revêtement obtenu, par recollement ou par déformation, soit algébrique (et pas seulement analytique). La clé réside dans des résultats de type GAGA (donnant une correspondance Géométrie Analytique - Géométrie Algébrique).

  - il existe une preuve algébrique élémentaire qui a l'avantage (ou l'inconvénient) de démonter tout le mécanisme géométrique. Cette preuve est presque totalement formelle: l'utilisation de la complétude est concentrée dans un lemme, le lemme de Cartan, qui est un résultat de décomposition de matrices sur des anneaux de séries convergentes à coefficients dans k; sa preuve requiert un passage à la limitedans k.

- Ces techniques de recollement et de déformation ont suscité de nombreux travaux et ont été développées et utilisées avec succès pour d'autres problèmes, au delà du problème inverse. L'inconvénient est que pour notre problème **Gal.Inv.Rég.** les corps k auquels ces techniques s'appliquent sont gros; en particulier, cette approche ne donne rien pour k=**Q**.

3/3 *Grothendieck-Teichmuller-Ihara*

- L'idée est d'attaquer de front l'étude de l'action de G**Q** sur les revêtements, pris tous ensemble, munis de leurs liens, c'est-à-dire, l'action sur la clôture algébrique **Q**(T)alg de **Q**(T). On limite un peu le cadre en se restreignant à la partie NR**t** de **Q**(T)alg non ramifiée au-dessus d'un ensemble fini **t** de points de **P**^1, que, pour simplifier, on prend ici égal à **t** = {0,1,infini}. La situation est la suivante:



- La théorie de Galois fournit la suite exacte

$$1 \longrightarrow \pi 1(\mathbf{P}^1 \setminus \mathbf{t})\mathbf{Q}\text{alg} \longrightarrow \pi 1(\mathbf{P}^1 \setminus \mathbf{t})\mathbf{Q}\text{alg} \longrightarrow G\mathbf{Q} \longrightarrow 1$$

dont le noyau π1(**P**^1**t**)**Q**alg est bien connu puisqu'il s'agit du complété profini du groupe fondamental topologique de **P**^1(**C**)**t**, lequel est isomorphe au groupe libre F(2) à 2 générateurs.

- Cette suite exacte est scindée: on obtient des sections st: G**Q** —> π1(**P**^1**t**)**Q** associées aux points t = 0, 1, infini en plongeant le corps NR**t** dans les corps de séries de Puiseux en T, T-1, 1/T (respectivement) et à coefficients dans **Q**alg, sur lesquels le groupe G**Q** a une action naturelle; pour t_0 différent de 0, 1, infini, on peut aussi plonger NR**t** dans les corps de séries formelles en T-T0 à coefficients dans **Q**alg. On obtient de cette façon des actions

  G**Q** —> Aut(F(2)^)

  qui coincident comme actions extérieures, c'est-à-dire modulo les automorphismes intérieurs de π1(**P**^1**t**)**Q**alg.

- Un résultat important du domaine, le théorème de Belyi, montre que le morphisme G**Q** —> Aut(F(2)^) est injectif (dans sa forme initiale, le théorème de Belyi affirme que toute courbe définie sur **Q**alg peut être présentée comme revêtement de **P**^1 ramifié seulement au-dessus de 0, 1 et infini; un élément de G**Q** qui agit trivialement sur tout revêtement de **P**^1 ramifié seulement au-dessus de 0, 1 et infini agit alors trivialement sur toute courbe définie sur **Q**alg; cela le force à être trivial).

- L'action G**Q** —> Aut(F(2)^) est calculable. En effet, les éléments de π1(**P**^1**t**)**Q**alg correspondent à des chemins sur la sphère de Riemann qui agissent sur des racines de polynômes (définissant les revêtements), lesquelles sont vues ici comme séries formelles ou séries de Puiseux; l'action se fait via la monodromie et peut se calculer par les techniques de prolongement analytique.

- Ihara a montré que l'image du morphisme G**Q** —> Aut(F(2)^) était contenu dans un groupe profini, qui était déjà apparu dans un autre contexte (celui des algèbres quasi-Hopf quasi-triangulaires). Ce groupe, découvert par Drinfel'd, qu'on appelle le groupe de Grothendieck-Teichmuller et qu'on note GT^ est relativement explicite puisqu'il est défini par générateurs et relations (dans un environnement profini).

- Une question se pose naturellement:

Question: *Le groupe* G**Q** *est-il isomorphe au groupe* GT^ ?

- Y répondre positivement serait une avancée majeure (même si cela pourrait ne pas impliquer immédiatement une solution du problème inverse de Galois: on ne sait pas en effet montrer que tout groupe fini est quotient de GT^). D'autres variantes du groupe GT^, coincées entre les groupes G**Q** et GT^, mais dont on ne sait montrer si ce sont réellement de nouveaux groupes, c'est-à-dire, s'ils sont différents de GT^, ont depuis été définies. Cette approche a suscité de nombreux travaux, notamment de l'école française et de l'école japonaise. Il en existe une version pro-l (pour lesquelles les revêtements considérés sont de degré une puissance d'un nombre premier l) qui est plus avancée, car les groupes pro-l sont plus simples que les groupes profinis.

Conclusion et retour sur Hilbert

- Ces trois approches ont conduit a des progrès importants au cours des quatre dernières décennies. Elles ont ouvert de nouvelles voies qui continuent d'être explorées et d'irriguer le domaine. Mais au bout du compte, pour ce qui est du problème de départ, le mystère ne s'est pas dissipé. On peut même penser qu'il s'est

épaissi. Nous avions à l'origine le problème **Gal. Inv.** S'y est ajouté le problème **Gal. Inv. Rég.**, lequel a acquis son intérêt propre et son indépendance. Et le mystère est peut-être même triple: si on connaît l'implication

Gal. Inv. Rég. sur **Q** ==> **Gal. Inv.** sur **Q**

l'écart entre les deux conditions est encore assez flou: y a-t-il beaucoup plus de groupes qui sont groupes de Galois sur **Q** que sur **Q**(T) ? Le théorème d'irréductibilité de Hilbert, qui donne l'implication ci-dessus, est la véritable clef de voûte du domaine: à partir d'une extension galoisienne de **Q**(T) de groupe donné G, on peut construire non seulement une mais de multiples extensions de **Q** de groupe G pouvant avoir de surcroît des propriétés remarquables. Y en a-t-il trop, ou de trop belles?

BIBLIOGRAPHIE (Ouvrages généraux)

Field arithmetic, M. Fried and M. Jarden, Springer-Verlag, (1986) 1st edition, (2000) 2nd edition.

Topics in Galois theory, J.-P. Serre, *Jones and Bartlett Publ.*, Boston, (1992).

The Grothendieck theory of Dessins d'Enfants, L. Schneps editor, *London Math. Soc. Lecture Note Series*, **200**, Cambridge Univ. Press, (1994).

Recent developments in the Inverse Galois Problem, M. D. Fried et al. editors, *Contemp. Math.*, **186**, A.M.S., (1995).

Groups as Galois groups - an introduction, H. Voelklein, *Cambridge Studies in Advanced Math.*, **53**, Cambridge Univ. Press, (1996).

Geometric Galois Actions (I & II), L. Schneps & P. Lochak editors, *London Math. Soc. Lecture Note Series*, **242 & 243**, Cambridge Univ. Press, (1997).

Aspects of Galois Theory, H. Voelklein et al. editors, *London Math. Soc. Lecture Note Series*, **256**, Cambridge Univ Press, (1999).

Inverse Galois Theory, G. Malle and B. H. Matzat, Springer-Verlag, (1999).

Arithmétique des revêtements algébriques, B. Deschamps éd., *Sém. et Congrès*, ***5***, *S.M.F.*, (2001).

Arithmetic Fundamental Groups and Noncommutative Algebra, M. D. Fried and Y. Ihara editors, *Proc. of Symp. in Pure Math.*, **70**, A.M.S., (2002).

Groupes de Galois arithmétiques et différentiels, D. Bertrand et P. Dèbes éditeurs, *Séminaires et Congrès*, **13**, S.M.F., (2006).

Cohomology of Number Fields, J. Neukirch, A. Schmidt and K. Wingberg, *Grundlehren de mathematischen Wissenschaften*, **323**, Springer, (2008).

Arithmétique des revêtements de la droite, P. Dèbes, notes de cours, (2009), http://math.univ-lille1.fr/~pde/ens.html .

Groupes de Galois arithmétiques et différentiels, D. Bertrand, P. Boalch, J.-M. Couveignes et P. Dèbes éditeurs, *Séminaires et Congrès*, S.M.F., (à paraître).